

Item Bank ID	410251	Item Bank Name	Information and Cyber Security		Answer
Item Text	Option Text 1	Option Text 2	Option Text 3	Option Text 4	
IPSec is designed to provide security at the _____	Transport layer	Network layer	Application layer	Session layer	B
_____ operates in the transport mode or the tunnel mode.	IPSec	SSL	PGP	SET	A
In IPSec ESP protocols stands for	Encryption Special Protocol	Encapsulating Security Payload	Encoding Special Payload	Entry Segment Protocol	B
In IPSec role of Security Association(SA) is	Security for data	Security from virus	Security from Intrusion	Security for Integrity	C
VPN is abbreviated as _____	Visual Private Network	Virtual Protocol Network	Virtual Private Network	Virtual Protocol Networking	D
_____ uses the idea of certificate trust levels.	X509	PGP	KDC	SSL	A
PGP offers _____ block ciphers for message encryption.	RSA	ECC	AES	IDEA	B
PGP have not used which cryptographic algorithms? i)DES ii) AES iii)RSA iv)Rabin	i), ii), iv)	i), iii), iv)	ii), iii), iv)	i), ii), iii)	A
Which one of the following is not a higher -layer SSL protocol?	Alert Protocol	Handshake Protocol	Alarm Protocol	Change Cipher Spec Protocol	C
Which protocol is used to convey SSL related alerts to the peer entity?	Alert Protocol	Handshake Protocol	Upper-Layer Protocol	Change Cipher Spec Protocol	A
Number of phases in the handshaking protocol?	2	3	4	5	C
In the Handshake protocol action, which is the last step of the Phase 2 : Server Authentication and Key Exchange?	Server_done	Server_key_exchange	Certificate_request	Crtificate_verify	A
In SSL the client_key_exchange message uses a pre master key of size –	48 bytes	56 bytes	64bytes	32bytes	A
Key Management in IPSec is done by_____	Tunnel Mode	Transport Mode	IKE	ESP	C
Oakley Protocol is used for_____	Encryption of Payload	Encryption Key Exchange	Generete Message Digest	Authorization Services	D
Typically, _____ can receive application data from any application layer protocol, but the protocol is <u>normally HTTP</u>	SSL	TLS	Either A or B	Both A or B	D
_____ is designed to provide security and compression services to data generated from the application layer.	SSL	TLS	Either A or B	Both A or B	D
In SSL which one of the following is not a session state parameter?	Master Secret	Cipher Spec	Peer Certificate	Server Write Key	D
In SSL which protocol consists of only 1 bit?	Alert Protocol	Handshake Protocol	Upper-Layer Protocol	Change Cipher Spec Protocol	D
In the alert protocol the first byte takes the value 1 or 2 which corresponds to _____ and _____ respectively.	Select, Alarm	Alert, Alarm	Warning, Alarm	Warning, Fatal	D

## Question Bank for Information and Cyber Security (ICS)

### 1. Why would a hacker use a proxy server?

- A. To create a stronger connection with the target.
- B. To create a ghost server on the network.
- C. To obtain a remote access connection.
- D. To hide malicious activity on the network.

**Correct Answer – D**

**Explanation –** Proxy servers exist to act as an intermediary between the hacker and the target and services to keep the hacker anonymous to the network.

### 2. What type of symmetric key algorithm using a streaming cipher to encrypt information?

- A. RC4
- B. Blowfish
- C. SHA
- D. MD5

**Correct Answer – A**

**Explanation –** RC4 uses streaming ciphers.

### 3. Which of the following is not a factor in securing the environment against an attack on security?

- A. The education of the attacker
- B. The system configuration
- C. The network architecture
- D. The business strategy of the company
- E. The level of access provided to employees

**Correct Answer – D**

**Explanation –** All of the answers are factors supporting the exploitation or prevention of an attack. The business strategy may provide the motivation for a potential attack, but by itself will not influence the outcome.

### 4. What type of attack uses a fraudulent server with a relay address?

- A. NTLM
- B. MITM
- C. NetBIOS
- D. SMB

**Correct Answer – B**

**Explanation –** MITM (Man in the Middle) attacks create a server with a relay address. It is used in SMB relay attacks.

### 5. What port is used to connect to the Active Directory in Windows 2000?

- A. 80
- B. 445
- C. 139
- D. 389

**Correct Answer – D**

**Explanation –** The Active Directory Administration Tool used for a Windows 2000 LDAP client uses port 389 to connect to the Active Directory service.

### 6. To hide information inside a picture, what technology is used?

- A. Rootkits
- B. Bitmapping

- C. Steganography
- D. Image Rendering

**Correct Answer – C**

**Explanation** – Steganography is the right answer and can be used to hide information in pictures, music, or videos.

**7. Which phase of hacking performs actual attack on a network or system?**

- A. Reconnaissance
- B. Maintaining Access
- C. Scanning
- D. Gaining Access

**Correct Answer – D**

**Explanation** – In the process of hacking, actual attacks are performed when gaining access, or ownership, of the network or system. Reconnaissance and Scanning are information gathering steps to identify the best possible action for staging the attack. Maintaining access attempts to prolong the attack.

**8. Attempting to gain access to a network using an employee's credentials is called the mode of ethical hacking.**

- A. Local networking
- B. Social engineering
- C. Physical entry
- D. Remote networking

**Correct Answer – A**

**Explanation** – Local networking uses an employee's credentials, or access rights, to gain access to the network. Physical entry uses credentials to gain access to the physical IT infrastructure.

**9. Which Federal Code applies the consequences of hacking activities that disrupt subway transit systems?**

- A. Electronic Communications Interception of Oral Communications
- B. 18 U.S.C. § 1029
- C. Cyber Security Enhancement Act 2002
- D. 18 U.S.C. § 1030

**Correct Answer – C**

**Explanation** – The Cyber Security Enhancement Act 2002 deals with life sentences for hackers who recklessly endanger the lives of others, specifically transportation systems.

**10. Which of the following is not a typical characteristic of an ethical hacker?**

- A. Excellent knowledge of Windows.
- B. Understands the process of exploiting network vulnerabilities.
- C. Patience, persistence and perseverance.
- D. Has the highest level of security for the organization.

**Correct Answer – D**

**Explanation** – Each answer has validity as a characteristic of an ethical hacker. Though having the highest security clearance is ideal, it is not always the case in an organization.

**11. What is the proper command to perform an Nmap XMAS scan every 15seconds?**

- A. nmap -sX -sneaky
- B. nmap -sX -paranoid
- C. nmap -sX -aggressive
- D. nmap -sX -polite

**Correct Answer – A**

**Explanation** – SX is used to identify a xmas scan, while sneaky performs scans 15 seconds apart.

**12. What type of rootkit will patch, hook, or replace the version of system call in order to hide information?**

- A. Library level rootkits
- B. Kernel level rootkits
- C. System level rootkits
- D. Application level rootkits

**Correct Answer – A**

**Explanation** – Library leve rootkits is the correct answer. Kerel level focuses on replaceing specific code while application level will concentrate on modifying the behavior of the application or replacing application binaries. The type, system level, does not exist for rootkits.

**13. What is the purpose of a Denial of Service attack?**

- A. Exploit a weakness in the TCP/IP stack
- B. To execute a Trojan on a system
- C. To overload a system so it is no longer operational
- D. To shutdown services by turning them off

**Correct Answer – C**

**Explanation** – DoS attacks force systems to stop responding by overloading the processing of the system.

**14. What are some of the most common vulnerabilities that exist in a network or system?**

- A. Changing manufacturer, or recommended, settings of a newly installed application.
- B. Additional unused features on commercial software packages.
- C. Utilizing open source application code
- D. Balancing security concerns with functionality and ease of use of a system.

**Correct Answer – B**

**Explanation** – Linux is an open source code and considered to have greater security than the commercial Windows environment. Balancing security. Ease of use and functionality can open vulnerabilities that already exist. Manufacturer settings, or default settings, may provide basic protection against hacking threats, but need to change to provide advance support. The unused features of application code provide an excellent opportunity to attack and cover the attack.

**15. What is the sequence of a TCP connection?**

- A. SYN-ACK-FIN
- B. SYN-SYN ACK-ACK
- C. SYN-ACK
- D. SYN-SYN-ACK

**Correct Answer – B**

**Explanation** – A three-handed connection of TCP will start with a SYN packet followed by a SYN-ACK packet. A final ACK packet will complete the connection.

**16. What tool can be used to perform SNMP enumeration?**

- A. DNSlookup
- B. Whois
- C. Nslookup
- D. IP Network Browser

**Correct Answer – D**

**Explanation** – SNMPPUtil and IP Network Browser is SNMP enumeration tool

**17. Which ports should be blocked to prevent null session enumeration?**

- A. Ports 120 and 445
- B. Ports 135 and 136
- C. Ports 110 and 137
- D. Ports 135 and 139

**Correct Answer – D**

**Explanation** – Port 139 is the NetBIOS Session port typically can provide large amounts of information using APIs to connect to the system. Other ports that can be blocked in 135, 137,138, and 445.

**18. The first phase of hacking an IT system is compromise of which foundation of security?**

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Authentication

**Correct Answer – B**

**Explanation** – Reconnaissance is about gathering confidential information, such as usernames and passwords.

**19. How is IP address spoofing detected?**

- A. Installing and configuring a IDS that can read the IP header
- B. Comparing the TTL values of the actual and spoofed addresses
- C. Implementing a firewall to the network
- D. Identify all TCP sessions that are initiated but does not complete successfully

**Correct Answer – B**

**Explanation** – IP address spoofing is detectable by comparing TTL values of the actual and spoofed IP addresses

**20. Why would a ping sweep be used?**

- A. To identify live systems
- B. To locate live systems
- C. To identify open ports
- D. To locate firewalls

**Correct Answer – A**

**Explanation** – A ping sweep is intended to identify live systems. Once an active system is found on the network, other information may be distinguished, including location. Open ports and firewalls.

**21. What are the port states determined by Nmap?**

- A. Active, inactive, standby
- B. Open, half-open, closed
- C. Open, filtered, unfiltered
- D. Active, closed, unused

**Correct Answer – C**

**Explanation** – Nmap determines that ports are open, filtered, or unfiltered.

**22. What port does Telnet use?**

- A. 22
- B. 80
- C. 20
- D. 23

**Correct Answer – D**

**Explanation** – Telnet uses port 23.

**23. Which of the following will allow footprinting to be conducted without detection?**

- A. PingSweep
- B. Traceroute
- C. War Dialers
- D. ARIN

**Correct Answer – D**

**Explanation** – ARIN is a publicly accessible database, which has information that could be valuable. Because it is public, any attempt to obtain information in the database would go undetected.

**24. Performing hacking activities with the intent on gaining visibility for an unfair situation is called \_\_\_\_\_.**

- A. Cracking
- B. Analysis
- C. Hacktivism
- D. Exploitation

**Correct Answer – C**

**Explanation** – Hacktivism is the act of malicious hacking for a cause or purpose.

**25. What is the most important activity in system hacking?**

- A. Information gathering
- B. Cracking passwords
- C. Escalating privileges
- D. Covering tracks

**Correct Answer – B**

**Explanation** – Passwords are a key component to access a system, making cracking the password the most important part of system hacking.

**26. A packet with no flags set is which type of scan?**

- A. TCP
- B. XMAS
- C. IDLE
- D. NULL

**Correct Answer – D**

**Explanation** – A NULL scan has no flags set.

**27. Sniffing is used to perform \_\_\_\_\_ fingerprinting.**

- A. Passive stack
- B. Active stack
- C. Passive banner grabbing
- D. Scanned

**Correct Answer – A**

**Explanation** – Passive stack fingerprinting uses sniffing technologies instead of scanning.

**28. Phishing is a form of \_\_\_\_\_.**

- A. Spamming
- B. Identify Theft
- C. Impersonation
- D. Scanning

**Correct Answer – C**

**Explanation** – Phishing is typically a potential attacker posing, or impersonating, a financial institution

**29. Why would HTTP Tunneling be used?**

- A. To identify proxy servers
- B. Web activity is not scanned
- C. To bypass a firewall
- D. HTTP is a easy protocol to work with

**Correct Answer – C**

**Explanation** – HTTP Tunneling is used to bypass the IDS and firewalls present on a network.

**30. Which Nmap scan is does not completely open a TCP connection?**

- A. SYN stealth scan
- B. TCP connect
- C. XMAS tree scan
- D. ACK scan

**Correct Answer – A**

**Explanation** – Also known as a “half-open scanning,” SYN stealth scan will not complete a full TCP connection.

**31. What protocol is the Active Directory database based on?**

- A. LDAP
- B. TCP
- C. SQL
- D. HTTP

**Correct Answer – A**

**Explanation** – Active4 direction in Windows 200 is based on a Lightweight Directory Access Protocol (LDAP).

**32. Services running on a system are determined by \_\_\_\_\_.**

- A. The system’s IP address.
- B. The Active Directory
- C. The system’s network name
- D. The port assigned

**Correct Answer – D**

**Explanation** – Hackers can identify services running on a system by the open ports that are found.

**33. What are the types of scanning?**

- A. Port, network, and services
- B. Network, vulnerability, and port
- C. Passive, active, and interactive
- D. Server, client, and network

**Correct Answer – B**

**Explanation** – The three types of accepted scans are port, network, and vulnerability.

**34. Enumeration is part of what phase of ethical hacking?**

- A. Reconnaissance
- B. Maintaining Access
- C. Gaining Access
- D. Scanning

**Correct Answer – C**

**Explanation** – Enumeration is a process of gaining access to the network by obtaining information on a user or system to be used during an attack.

**35. Keyloggers are a form of \_\_\_\_\_.**

- A. Spyware
- B. Shoulder surfing
- C. Trojan
- D. Social engineering

**Correct Answer – A**

**Explanation** – Keyloggers are a form of hardware or software spyware installed between the keyboard and operating system.

**36. What are hybrid attacks?**

- A. An attempt to crack passwords using words that can be found in dictionary.
- B. An attempt to crack passwords by replacing characters of a dictionary word with numbers and symbols.
- C. An attempt to crack passwords using a combination of characters, numbers, and symbols.
- D. An attempt to crack passwords by replacing characters with numbers and symbols.

**Correct Answer – B**

**Explanation** – Hybrid attacks do crack passwords that are created with replaced characters of dictionary type words.

**37. Which form of encryption does WPA use?**

- A. Shared key
- B. LEAP
- C. TKIP
- D. AES

**Correct Answer – C**

**Explanation** – TKIP is used by WPA

**38. What is the best statement for taking advantage of a weakness in the security of an IT system?**

- A. Threat
- B. Attack
- C. Exploit
- D. Vulnerability

**Correct Answer – C**

**Explanation** – A weakness in security is exploited. An attack does the exploitation. A weakness is vulnerability. A threat is a potential vulnerability.

**39. Which database is queried by Whois?**

- A. ICANN
- B. ARIN
- C. APNIC
- D. DNS

**Correct Answer – A**

**Explanation** – Who utilizes the Internet Corporation for Assigned Names and Numbers.

**40. Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?**

- A. Web-based
- B. Human-based
- C. User-based
- D. Computer-based

**Correct Answer – D**

**Explanation** – Whether using email, a fake website, or popup to entice the user, obtaining information from an individual over the Internet is a computer-based type of social engineering

**1) You are supposed to use hill cipher for encryption technique. You are provided with the following matrix,**

$$A = \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix}$$

**Is the given matrix 'A', a valid key to be used for encryption?**

- a. Yes
- b. No
- c. Can't be determined
- d. Data insufficient

**Answer:** b) No

**Explanation:**

For choosing any square matrix as a key, it should be taken care that the matrix is invertible, i.e. its inverse must exist. Here, in this case,

$$|A| = 0$$

Therefore, it means that 'A' is not an invertible matrix. Hence matrix 'A' cannot be chosen as a key matrix for encryption in the [Hill cipher](#).

**2) The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?**

- a. The input text is divided into two parts: one being left half and another one being right half.
- b. Swapping of the left and right halves are performed after each round.
- c. The plain text is converted into a matrix form first
- d. None of the above

**Answer:** c) The plain text is converted into a matrix form first

**Explanation:**

The fiestal structure does not require the conversion of the plain text into matrix form at any of its steps.

**3) Among the following given options, chose the strongest encryption technique?**

- a. DES ( Data Encryption Standard)
- b. Double DES
- c. Triple DES
- d. AES (Advance Encryption Standard)

**Answer:** d) AES (Advance Encryption Standard)

**Explanation:**

It has been proved that the AES performs much better than the all the other DES, whether it be single DES or series of DES.

**4) What is the full-form of RSA in the RSA encryption technique?**

- a. Round Security Algorithm
- b. Rivest, Shamir, Adleman
- c. Robert, Shamir, Addie
- d. None of the above

**Answer:** b) Rivest, Shamir, Adleman

**Explanation:**

The RSA algorithm was named after the three scientists who developed this technique and the name RSA is itself the abbreviation of their names: Rivest, Shamir, and Adleman.

**5) Consider the following steps,**

- i. Substitution bytes
- ii. Shift Rows
- iii. Mix columns
- iv. Add round key

**The above steps are performed in each round of which of the following ciphers?**

- a. Rail fence cipher
- b. Data Encryption Standard (DES)
- c. Advance Encryption Standard (AES)
- d. None of the above

**Answer:** c) Advance Encryption Standard (AES)

**Explanation:**

Each round of AES includes the mentioned steps.

**1) What is the block size of plain text in SHA- 512 algorithm?**

- a. 512 bits
- b. 1024 bits
- c. 2048 bits

- d. None of the above

**Answer:** b. 1024 bits

**Explanation:**

The SHA- 512 algorithm uses blocks of plain text one at a time to encrypt them into ciphertext. The size of each block in the SHA- 512 algorithm is 1024 bits.

**2) All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES?**

- i. Substitution bytes
- ii. Shift rows
- iii. Mix columns
- iv. Add round key

**Options**

- a. i.
- b. iii.
- c. All of the mentioned
- d. None of the mentioned

**Answer:** b. iii.

**Explanation:**

In the AES algorithm, the MIX COLUMN operation is performed in all the rounds except the final round of the algorithm.

**3) What does IDEA stand for in the world of cryptography?**

**or**

**The IDEA word in the IDEA algorithm is the abbreviation for which of the following?**

- a. Independent Decryption Environment Analysis
- b. International Defense Encryption Area
- c. International Data Encryption Algorithm
- d. None of the above

**Answer:** c. International Data Encryption Algorithm

**Explanation:**

The IDEA Algorithm stands for "International Data Encryption Algorithm".

**4) How many sub-keys in the total are used by the IDEA for encrypting the plain text into ciphertext?**

- a. 64 sub- keys
- b. 48 sub- keys
- c. 52 sub- keys
- d. Only one key and no subkeys

**Answer:** c. 52 sub- keys

**Explanation:**

There are a total of 8 rounds in the IDEA technique for encryption and each of them uses 6 keys. Apart from that, 4 extra keys are used in the final round that is the output transformation round. This gives us a total of 52 subkeys.

$$(8 \times 6) + 4 = 52$$

**5) "The number of rounds in the AES algorithm depends upon the key size being used."**  
**Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?**

- a. 128 key size: 10 rounds
- b. 192 key size: 12 rounds
- c. 256 key size: 14 rounds
- d. All of the above

**Answer:** d. All of the above

**Explanation:**

All the mentioned options display the correct relation between the number of rounds and the key size used in the AES algorithm.

**6) Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher?**

- a. Avalanche effect
- b. Completeness
- c. Both a. and b.
- d. None of the above

**Answer:** c. Both a. and b.

**Explanation:**

Avalanche effect and Completeness are the two characteristic properties of Block ciphers which differ them from stream ciphers.

**81. Public key encryption/decryption is not preferred because**

- a. it is slow

- b.** it is hardware/software intensive
- c.** it has a high computational load
- d.** all of the mentioned

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (d).all of the mentioned

- 82.** Which one of the following is not a public key distribution means?
- a.** Public-Key Certificates
  - b.** Hashing Certificates
  - c.** Publicly available directories
  - d.** Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (b).Hashing Certificates

- 83.** What is the PGP stand for?
- a.** Permuted Gap Permission
  - b.** Permuted Great Privacy
  - c.** Pretty Good Permission
  - d.** None of the mentioned

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (d).None of the mentioned

- 84.** PGP makes use of which cryptographic algorithm?
- a.** DES
  - b.** AES

c. RSA

d. Rabin

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (c).RSA

**85.** USENET is related to which of the following Public Key distribution schemes?

a. Public-Key Certificates

b. Public announcements

c. Publicly available directories

d. Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (b).Public announcements

**86.** Which of the following public key distribution systems is most secure?

a. Public-Key Certificates

b. Public announcements

c. Publicly available directories

d. Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (a).Public-Key Certificates

**87.** Which systems use a timestamp?

i) Public-Key Certificates

ii) Public announcements

iii) Publicly available directories

iv) Public-Key authority

a. i) and ii)

- b.** iii) and iv)
- c.** i) and iv)
- d.** iv) only

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (c).i) and iv)

- 88.** Which of these systems use timestamps as an expiration date?
- a.** Public-Key Certificates
  - b.** Public announcements
  - c.** Publicly available directories
  - d.** Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (a).Public-Key Certificates

- 89.** Which system uses a trusted third party interface?
- a.** Public-Key Certificates
  - b.** Public announcements
  - c.** Publicly available directories
  - d.** Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (a).Public-Key Certificates

- 90.** Publicly Available directory is more secure than which other system?
- a.** Public-Key Certificates
  - b.** Public announcements

- c. Public-Key authority
- d. None of the mentioned

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (b).Public announcements

1. A method used by an IDS that involves checking for a pattern to identify unauthorized activity.(*No Answer*)
  - a. **CORRECT:** Pattern Matching
  - b. Session Splicing
  - c. Protocol Decoding
  - d. State Table
2. A list or table of stored by a router (or switch) that controls access to and from a network. (*No Answer*)
  - . State Table
    - a. **CORRECT:** Access Control List (ACL)
    - b. Session Splicing
    - c. Packet Filter
3. An analysis method used by some IDS that looks for instances that are not considered normal behavior. (*No Answer*)
  - . Stateful Inspection
    - a. **CORRECT:** Anomaly Detection
    - b. Evasion
    - c. Pattern Matching
4. Bypassing a device, or performing another action, to attack or place malware on a target network without being detected. (*No Answer*)
  - . Packet Filter
    - a. State Table
    - b. **CORRECT:** Evasion
    - c. Honeypot

5. A type of firewall closely related to a packet filter that can track the status of a connection through use of a state table that keeps track of connection activities.(*No Answer*)
  - . Anomaly Detection
    - a. Protocol Decoding
    - b. **CORRECT:** Stateful Inspection
    - c. State Table
6. A tool that uses the monitoring of network traffic, detection of unauthorized access attempts, and notification of unauthorized access attempts to network administrator.(*No Answer*)
  - . Anomaly Detection
    - a. Access Control List (ACL)
    - b. **CORRECT:** Intrusion Detection System (IDS)
    - c. Session Splicing
7. A type of stateless inspection used in some routers and firewalls to limit flow of traffic to what is on the ACL.(*No Answer*)
  - . **CORRECT:** Packet Filter
    - a. Proxy Server
    - b. Evasion
    - c. State Table
8. A way of looking at raw packet data.(*No Answer*)
  - . Proxy Server
    - a. Session Splicing
    - b. **CORRECT:** Protocol Decoding
    - c. Pattern Matching
9. A server (or application) that intercepts the requests clients make of another server, fills the requests that it can, and then forwards the requests it can't handle on to the other server thus helping to improve performance and security.(*No Answer*)
  - . Honeypot
    - a. **CORRECT:** Proxy Server
    - b. Packet Filter
    - c. State Table

10. A table in which data about connection activity is kept by a stateful firewall.(*No Answer*)
- . Evasion
    - a. **CORRECT:** State Table
    - b. Honeypot
    - c. Proxy Server
11. Something set up on a separate network (or in DMZ) to attract hackers and lure them away from the real network; it logs keystrokes, provides other information about an attacker, and also provides warning that someone is trying to attack your network.(*No Answer*)
- . Proxy Server
    - a. State Table
    - b. Evasion
    - c. **CORRECT:** Honeypot
12. A way to change network address information in IP packet headers with a router by connecting multiple computers using one IP address connected to the Internet (or IP network) to convert many private addresses into one public address.(*No Answer*)
- . Access Control List (ACL)
    - a. **CORRECT:** Network Address Translation (NAT)
    - b. Anomaly Detection
    - c. Intrusion Detection System (IDS)
13. A method of avoiding detection by an IDS by sending portions of a request in different packets.(*No Answer*)
- . **CORRECT:** Session Splicing
    - a. Protocol Decoding
    - b. Pattern Matching
    - c. Evasion

1.

What are drawbacks of the host based IDS ?

- A.) Unselective logging of messages may increase the audit burdens
- B.) Selective logging runs the risk of missed attacks
- C.) They are very fast to detect

- D.) They have to be programmed for new patterns

**Show Answer**

**Answer: Option 'A'**

**Unselective logging of messages may increase the audit burdens**

2.

What are the different ways to classify an IDS ?

- A.) Zone based
- B.) Host & Network based
- C.) Network & Zone based
- D.) Level based

**Show Answer**

**Answer: Option 'B'**

**Host & Network based**

3.

What is major drawback of anomaly detection IDS ?

- A.) These are very slow at detection
- B.) It generates many false alarms
- C.) It doesn't detect novel attacks
- D.) None of the mentioned

**Show Answer**

**Answer: Option 'B'**

**It generates many false alarms**

4.

What are strengths of the host based IDS?

- A.) Attack verification
- B.) System specific activity
- C.) No additional hardware required
- D.) All of the mentioned

**Show Answer**

**Answer: Option 'D'**

**All of the mentioned**

5.

What are major components of intrusion detection system?

- A.) Analysis Engine
- B.) Event provider

- C.) Alert Database
- D.) All of the mentioned

**Show Answer**

**Answer: Option 'D'**

**All of the mentioned**

6.

What are strengths of the host based IDS?

- A.) Attack verification
- B.) System specific activity
- C.) No additional hardware required
- D.) All of the mentioned

**Show Answer**

**Answer: Option 'D'**

**All of the mentioned**

7.

What are characteristics of stack based IDS ?

- A.) They are integrated closely with the TCP/IP stack and watch packets
- B.) The host operating system logs in the audit information
- C.) It is programmed to interpret a certain series of packets
- D.) It models the normal usage of network as a noise characterization

**Show Answer**

**Answer: Option 'A'**

**They are integrated closely with the TCP/IP stack and watch packets**

8.

What are major components of intrusion detection system?

- A.) Analysis Engine
- B.) Event provider
- C.) Alert Database
- D.) All of the mentioned

**Show Answer**

**Answer: Option 'D'**

**All of the mentioned**

9.

What are characteristics of Network based IDS ?

- A.) They look for attack signatures in network traffic
- B.) Filter decides which traffic will not be discarded or passed
- C.) It is programmed to interpret a certain series of packet
- D.) It models the normal usage of network as a noise characterization

**Show Answer**

**Answer: Option 'A'**

**They look for attack signatures in network traffic**

10.

What are the different ways to classify an IDS ?

- A.) Zone based
- B.) Host & Network based
- C.) Network & Zone based
- D.) Level based

**Show Answer**

**Answer: Option 'B'**

**Host & Network based**

11.

What is major drawback of anomaly detection IDS ?

- A.) These are very slow at detection
- B.) It generates many false alarms
- C.) It doesn't detect novel attacks
- D.) None of the mentioned

**Show Answer**

**Answer: Option 'B'**

**It generates many false alarms**

1. -systematic tracking of incoming and outgoing traffic: to ascertain how an attack was carried out or how an event occurred on a network.

-intruders and network users often leave trail behind

-identify locations where relevant digital evidence exists

-crucial when developing data map of digital evidence(*No Answer*)

- a. SIM Cards
  - b. Windows Registry
  - c. **CORRECT: Network Forensics**
  - d. Drive Slack
2. -personal digital assistant: can be separated devices from mobile phones
- PDA houses a microprocessor, ROM, RAM, disk drive and various components
- most common PDA, although not referred to as such:IPAD(*No Answer*)
- . Partition
    - a. SIM Cards
    - b. EEPROM
    - c. **CORRECT: PDA's**
3. -a logical drive(*No Answer*)
- . EEPROM
    - a. PDA's
    - b. SIM Cards
    - c. **CORRECT: Partition**
4. - .EVE -> .DFT -> IOLogErrors
- .DD -> .DFT -> IOLogErrors -> MD5(*No Answer*)
- . Additional SIM Card Purposes
    - a. Types of The Formats ProDiscover Creates
    - b. **CORRECT: Files Found When Acquisition is Done (ProDiscover)**
    - c. Mobile Forensics Equipment
5. -allows you to create a representation of another computer on an existing physical computer.
- a virtual machine is just a few files on your hard drive: must allocate space to it; dynamic or static
- a virtual machine recognizes components of the physical machine its on: virtual OS is limited by the physical machines O/S and RAM. (*No Answer*)

- . Partition
  - a. **CORRECT:** Virtual Machine
  - b. Drive Slack
  - c. SIM Cards
- 6. Considerations
  - determine the scope of the investigation.
  - determine what the case requires
  - whether you should collect all info
  - what to do in case of scope creep
- \*the key is to start with a plan but remain flexible in the face of new evidence(*No Answer*)
- . **CORRECT:** Examination Plan
  - a. Drive Slack
  - b. Partition
  - c. SIM Cards
- 7. Can be exported as:
  - RTF ~good for thumbnails and book marks
  - TEXT~plain text(*No Answer*)
- . Drive Slack
  - a. Write Blockers
  - b. Windows Registry
  - c. **CORRECT:** ProDiscover Report
- 8. -UNIX DD~most common raw image format
  - .EVE~has case metadata information(*No Answer*)
- . EnCase Output Formats
  - a. Five Major Categories
  - b. ProDiscover Report
  - c. **CORRECT:** Types of The Formats ProDiscover Creates
- 9. -electronically erasable programmable read-only memory
  - how phones store system data

-enables service providers to reprogram phones without having to physically access memory chips

-OS is stored in ROM: nonvolatile memory(*No Answer*)

- . Partition
  - a. file system
  - b. **CORRECT: EEPROM**
  - c. SIM Cards

10. -file manipulation: file names and extensions/ hidden property

-disk manipulation: hidden partitions/bad clusters

-encryption: bit shifting/stenography(*No Answer*)

- . Windows Registry
  - a. Examination Plan
  - b. Virtual Machine
  - c. **CORRECT: Data-hiding Techniques**

11. -gives us a road map to data on a disk

-type of file system an OS used determines how data is stored on the disk(*No Answer*)

- . **CORRECT: file system**
  - a. Drive Slack
  - b. EEPROM
  - c. SIM Cards

12. -the main concerns with mobile devices are loss of power and synchronization with PC's or the cloud (wired or wireless).

-all mobile devices have volatile memory that may contain valuable information: making sure they don't lose power before you can retrieve RAM data is critical.

-isolated the device from incoming signals with one of the following options: shielded container (paint can, enclosures), use the Faraday Bag, use eight layers of anti-static bags, aluminum foil.

-if device is not isolated, the data of the device will continue to change while in custody of the specialist.(*No Answer*)

- . Additional SIM Card Purposes
  - a. Network Forensics
  - b. **CORRECT:** Acquisition Procedures for Mobile Devices
  - c. Challenges With Mobile Devices

13. -acquisition~preservation~collection

-validation~discrimination~culling

~examination~extraction~review

~reconstruction~analysis

~reporting~presentation~production(*No Answer*)

- . Network Forensics
  - a. **CORRECT:** Five Major Categories
  - b. SIM Cards
  - c. Write Blockers

14. -a database that stores hardware and software configuration information, network connections, user preferences, and setup information.

-can contain valuable info about current/past applications and user created information(*No Answer*)

- . SIM Cards
  - a. **CORRECT:** Windows Registry
  - b. file system
  - c. Write Blockers

15. -unused space in a cluster between the end of an active file and the end of a cluster. (Includes RAM slack and file slack)(*No Answer*)

- . SIM Cards
  - a. file system

- b. Write Blockers
- c. **CORRECT: Drive Slack**

16. -subscribers identity module cards

-found most commonly in GSM devices

-microprocessor and from 16KB to 4MB EEPROM

-GSM refers to mobile phones as "mobile station" and divides a station into two parts: the sim card and the mobile equipment and common network in global networks

-portability of information makes SIM cards versatile(*No Answer*)

- . EEPROM
  - a. PDA's
  - b. **CORRECT: SIM Cards**
  - c. Drive Slack

17. -EnCase (E01)

-RAW (DD)

-SMART (S01)

-Sleuth Kit (AFF)(*No Answer*)

- . Five Major Categories
  - a. **CORRECT: Different FTK Output Formats**
  - b. EnCase Output Formats
  - c. Network Forensics

18. -How long a piece of information lasts on a system versus data that must be collected and preserved before its lost, corrupted, or backed up.

Order:

- 1-live network devices (switches/routers)
- 2-live computers/laptops (RAM and processes)
- 3-live other devices (smartphones, PDA's)

4-Devices/computers already OFF

5-Removable media/cables-adapters/documents(*No Answer*)

. **CORRECT:** Order of Volatility

- a. Partition
- b. Drive Slack
- c. Network Forensics

19. -devices are 'live' computers; traditional "stand-alone OFF computers" approach may be inadequate

-devices are connected to 'live' wireless networks; traditional "disconnect" or "segregate" approach network forensics may be inadequate

-devices lack hardware, software and operating system standardization; many variables affect forensic and eDiscovery techniques and analysis results.

-devices are dynamic in location; communications and operability; computers are mostly static.*(No Answer)*

. **CORRECT:** Challenges With Mobile Devices

- a. Write Blockers
- b. Network Forensics
- c. Acquisition Procedures for Mobile Devices

20. -analog

-digital personal communications service (PC's)

-third-generation (3G and 4G): increased bandwidth

\*continuing to evolve*(No Answer)*

. Data-hiding Techniques

- a. **CORRECT:** Three Generations of Mobile Phone Technology
- b. Order of Volatility
- c. Challenges With Mobile Devices

21. -identifies the subscriber to the network

-stores personal information

-stores address books and messages

-stores service-related information(*No Answer*)

- . Five Major Categories
  - a. ProDiscover Report
  - b. **CORRECT:** Additional SIM Card Purposes
  - c. SIM Cards

22. -hardware utilized for protecting source/hard drive from data alteration/tampering while collecting, preserving, and reviewing CSI.

-prevents operating systems and computer programs from making "writes" to the hard drive being acquired, examined, or analyzed.

-write blockers sits between the suspect/source drive and your analysis computer. (It is usually a hardware device, but software based write blockers may be utilized.*(No Answer)*

- . file system
  - a. Drive Slack
  - b. SIM Cards
  - c. **CORRECT:** Write Blockers

23. primary Windows based:

-EnCase

-Forensic Tool Kit (FTK)

-ProDiscover

-OSForensics

primarily Linux based:

-Sleuth Kit and Autopsy

-Helix

-Knoppix STD

-SMART(*No Answer*)

- . Computer Forensic and EDiscovery Tool Needs

- a. **CORRECT:** Computer Forensic Software Tools
  - b. Network Forensics
  - c. Mobile Forensics Equipment
24. -SIM card readers: a combination hardware/software device used to access the SIM card. You need to be in a forensic lab equip with appropriate anti-static devices.

-general forensic procedure for SIM cards:

- 1-remove the back panel of device
- 2-remove the battery
- 3-remove the SIM card
- 4-insert the SIM card into the card reader
- 5-extract relevant information

-a variety of SIM card readers are on the market: some are forensically sound and some are not

-documenting messages that haven't been read yet is critical: use a video camera to capture each screen, if data cannot be extracted with forensic hardware/software

-mobile forensic tools and utilities:

- Ramsey forensic text enclosure (hardware)
- SIM card reader (hardware)
- Paraben Device Seizure (software)
- BitPim (software)
- Susteen SecureView (software)
- EnCase and FTK (software)(*No Answer*)

- . file system
  - a. Network Forensics
  - b. **CORRECT:** Mobile Forensics Equipment
  - c. Computer Forensic Software Tools

25. -EX01

-E01 (Legacy)(*No Answer*)

- . **CORRECT:** EnCase Output Formats
  - a. Different FTK Output Formats
  - b. EEPROM

c. Network Forensics

26. look for versatility, flexibility, and robustness:

- Lab OS
- File System
- Automated Features
- Venders Reputation
- Acceptance by forensic community
- documented testing and validation

-Keep in mind what application files and operating system you'd be analyzing(*No Answer*)

. **CORRECT:** Computer Forensic and EDiscovery Tool Needs

- a. Mobile Forensics Equipment
- b. Types of The Formats ProDiscover Creates
- c. Computer Forensic Software Tools

Sr.No	Questions	Correct Answer
1.	According to the CIA Triad, which of the below-mentioned element is not considered in the triad?  a) Confidentiality b) Integrity c) Authenticity d) Availability	C
2.	CIA triad is also known as _____  a) NIC (Non-repudiation, Integrity, Confidentiality) b) AIC (Availability, Integrity, Confidentiality) c) AIN (Availability, Integrity, Non-repudiation) d) AIC (Authenticity, Integrity, Confidentiality)	B
3.	_____ of information means, only authorised users are capable of accessing the information.  a) Confidentiality b) Integrity c) Non-repudiation d) Availability	A
4.	_____ means the protection of data from modification by unknown users.  a) Confidentiality b) Integrity c) Authentication d) Non-repudiation	B
5.	When you use the word _____ it means you are protecting your data from getting disclosed.  a) Confidentiality b) Integrity c) Authentication d) Availability	A
6.	When integrity is lacking in a security system, _____ occurs.  a) Database hacking b) Data deletion c) Data tampering d) Data leakage	C
7.	Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?  a) They help understanding hacking better b) They are key elements to a security breach c) They help understand security and its components better d) They help to understand the cyber-crime better	C

8.	<p>This helps in identifying the origin of information and authentic user. This referred to here as _____</p> <p>a) Confidentiality b) Integrity c) Authenticity d) Availability</p>	C
9.	<p>Data _____ is used to ensure confidentiality.</p> <p>a) Encryption b) Locking c) Deleting d) Backup</p>	A
10.	<p>Data integrity gets compromised when _____ and _____ are taken control off.</p> <p>a) Access control, file deletion b) Network, file permission c) Access control, file permission d) Network, system</p>	C
11.	<p>_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.</p> <p>a) Network Security b) Database Security c) Information Security d) Physical Security</p>	C
12.	<p>From the options below, which of them is not a threat to information security?</p> <p>a) Disaster b) Eavesdropping c) Information leakage d) Unchanged default password</p>	D
13.	<p>Compromising confidential information comes under _____</p> <p>a) Bug b) Threat c) Vulnerability d) Attack</p>	B
14.	<p>Which of the following are not security policies?</p> <p>a)Regulatory b)Advisory c)Availability d)User Policies</p>	C

15.	Examples of User Policies is/are:  a)Password Policies b)Internet Usage c)System Use d)All of the above	D
16.	_____ Policy ensures that the organization is maintaining standards set by specific industry regulation.  a)Regulatory b)Advisory c)Availability d>User Policies	A
17.	_____ Policy is like standards rules and regulations set by the management to advise their employees on their activity or behavior  a)Regulatory b)Advisory c)Availability d>User Policies	B
18.	What defines the restrictions on employees such as usage?  a)Regulatory b)Advisory c)Availability d>User Policies	D
19.	The full form of OSI is OSI model is _____  a) Open Systems Interconnection b) Open Software Interconnection c) Open Systems Internet d) Open Software Internet	A
20.	In _____ layer, vulnerabilities are directly associated with physical access to networks and hardware.  a) physical b) data-link c) network d) application	A
21.	Loss of power and unauthorized change in the functional unit of hardware comes under problems and issues of the physical layer.  a) True b) False	A

22.	Which of the following attack can actively modify communications or data?  a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	C
23.	OSI architecture mainly focuses on:  1) Security Attack 2) Security Techniques/Mechanisms 3) Categories of Security Service  a)1 b)1 &3 c) 2& 3 d)1,2,3	D
24.	IT security department must periodically check for security logs and entries made during office hours.  a) True b) False	A
25.	Release of Message Content and Traffic analysis are type of :  a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	D
26.	If communication between 2 people is overheard by a third person without manipulation of any data, it is called as:  a) Release of Message Content-Passive Attack b) Traffic analysis -Passive Attacks c) Release of Message Content- Active Attacks d) Traffic analysis -Active Attacks	A
27.	If communication between 2 people is overheard by a third person without extraction of any data, it is called as:  a) Release of Message Content-Passive Attack b) Traffic analysis -Passive Attacks c) Release of Message Content- Active Attacks d) Traffic analysis -Active Attacks	D
28.	No modification of data is a characteristic of  a)Active Attack b)Passive Attack	A
29.	Which of the following are Active attack types	D

	a)Masquerade b)Replay c)Modification d)All of the above	
30.	_____ means when an attacker pretends to be authentic user  a)Masquerade b)Replay c)Modification d)Traffic analysis	A
31.	_____ attack is when original data is modified and malicious data is inserted  a)Masquerade b)Replay(Rewrite) c)Modification d)Traffic analysis	B
32.	When original data is changed to make it non-meaningful by attacker it is known as  a)Masquerade b)Replay c)Modification of Messages d)Traffic analysis	C
33.	Which is the type of attack when Network is made unavailable for user  a)Masquerade b)Replay c)Modification d)Denial of Service	D
34.	Modification of Data is done in:  a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	A
35.	The information that gets transformed in encryption is  a) Plain text b) Parallel text c) Encrypted text d) Decrypted text	A
36.	1. The process of transforming plain text into unreadable text.	B

	a) Decryption b) Encryption c) Network Security d) Information Hiding	
37.	A process of making the encrypted text readable again.  a) Decryption b) Encryption c) Network Security d) Information Hiding	A
38.	A unique piece of information that is used in encryption.  a) Cipher b) Plain Text c) Key d) Cipher	C
39.	Assurance that authentic user is taking part in communication is:  a)Authentication b)Authorization c)Access Control d)Auditing	A
40.	ATM pin while withdrawing money is an example of using:  a)Authentication b)Authorization c)Access Control d)Auditing	B
41.	Study of creating a d using encryption and decryption techniques.  a) Cipher b) Cryptography c) Encryption d) Decryption	B
42.	An attack in which the user receives unwanted amount of e-mails.  a) Smurfing b) Denial of service c) E-mail bombing d) Ping storm	C
43.	The process of disguising plaintext in such a way that its substance gets hidden (into what is known as cipher-text) is called _____	D

	a) cryptanalysis b) decryption c) reverse engineering d) encryption	
44.	In _____ same keys are implemented for encrypting as well as decrypting the information.  a) Symmetric Key Encryption b) Asymmetric Key Encryption c) Asymmetric Key Decryption d) Hash-based Key Encryption	A
45.	The procedure to add bits to the last block is termed as _____  a) decryption b) hashing c) tuning d) padding	D
46.	In asymmetric key cryptography, the private key is kept by _____  a) sender b) receiver c) sender and receiver d) all the connected devices to the network	B
47.	Cryptanalysis is used _____ a) to find some insecurity in a cryptographic scheme b) to increase the speed c) to encrypt the data d) to make new ciphers	A
48.	Conventional cryptography is also known as _____ or symmetric-key encryption.  a) secret-key b) public key c) protected key d) primary key	A
49.	_____ is the art & science of cracking the cipher-text without knowing the key.  a) Cracking b) Cryptanalysis c) Cryptography d) Crypto-hacking	B
50.	In _____ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.	A

- |  |  |  |
|--|--|--|
|  | <ul style="list-style-type: none"><li>a) Block Cipher</li><li>b) One-time pad</li><li>c) Hash functions</li><li>d) Vigenere Cipher</li></ul> |  |
|--|--|--|

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
((OPTION_A)) THIS IS MANDATORY OPTION	Network Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Database Security
((OPTION_C)) This is optional	Information Security
((OPTION_D)) This is optional	Physical Security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information from alteration, destruction, deletion or disclosure by unauthorised users.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a threat to information security?
((OPTION_A)) THIS IS MANDATORY OPTION	Disaster
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Eavesdropping
((OPTION_C)) This is optional	Information leakage
((OPTION_D)) This is optional	Unchanged default password
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Disaster, eavesdropping and information leakage come under information security threats whereas not changing the default password of any system, hardware or any software comes under the category of vulnerabilities that the user may pose to its system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a vulnerability to information security?
((OPTION_A))  THIS IS MANDATORY OPTION	flood
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	without deleting data, disposal of storage media
((OPTION_C))  This is optional	unchanged default password
((OPTION_D))  This is optional	latest patches and updates not done
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Compromising confidential information comes under
((OPTION_A)) THIS IS MANDATORY OPTION	Bug
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Threat
((OPTION_C)) This is optional	Vulnerability
((OPTION_D)) This is optional	Attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	Threats are anything that may cause damage or harm to a computer system, individual or any information. Compromising of confidential information means extracting out sensitive data from a system by illegal manner.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Lack of access control policy is a
((OPTION_A)) THIS IS MANDATORY OPTION	Bug
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Threat
((OPTION_C)) This is optional	Vulnerability
((OPTION_D)) This is optional	Attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Access control policies are incorporated to a security system for restricting of unauthorised access to any logical or physical system. Every security compliance program must need this as a fundamental component. Those systems which lack this feature is vulnerable.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Possible threat to any information cannot be
((OPTION_A)) THIS IS MANDATORY OPTION	reduced
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transferred
((OPTION_C)) This is optional	protected
((OPTION_D)) This is optional	ignored
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	When there lies a threat to any system, safeguards can be implemented, outsourced, distributed or transferred to some other system, protected using security tools and techniques but cannot be ignored.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	According to the CIA Triad, which of the below-mentioned element is not considered in the triad?
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authenticity
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	According to the CIA triad the three components that a security need is the Confidentiality, Integrity, Availability (as in short read as

		
CIA).		

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When you use the word _____ it means you are protecting your data from getting disclosed.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	

((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Confidentiality is what every individual prefer in terms of physical privacy as well as digital privacy. This term means our information needs to be protected from getting disclose to unauthorised parties, for which we use different security mechanisms like password protection, biometric security, OTPs (One Time Passwords) etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ means the protection of data from modification by unknown users.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	Non-repudiation
((OPTION_E)) This is optional. If optional keep empty so that system will skip	

this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	A information only seems valuable if it is correct and do not get modified during its journey in the course of arrival. The element integrity makes sure that the data sent or generated from other end is correct and is not modified by any unauthorised party in between.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When integrity is lacking in a security system, _____ occurs.
((OPTION_A)) THIS IS MANDATORY OPTION	Database hacking
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data deletion
((OPTION_C)) This is optional	Data tampering
((OPTION_D)) This is optional	Data leakage
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The term data tampering is used when integrity is compromised in any security model and checking its integrity later becomes costlier. Example: let suppose you sent \$50 to an authorised person and in between a Man in the Middle (MiTM) attack takes place and the value has tampered to \$500. This is how integrity is compromised.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	of information means, only authorised users are capable of accessing the information.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Non-repudiation
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional.	

If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Information seems useful only when right people (authorised users) access it after going through proper authenticity check. The key element availability ensures that only authorised users are able to access the information.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?
((OPTION_A)) THIS IS MANDATORY OPTION	They help understanding hacking better
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	They are key elements to a security breach
((OPTION_C)) This is optional	They help understands security and its components better
((OPTION_D)) This is optional	They help to understand the cyber-crime better
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The four elements of security viz. confidentiality, integrity, authenticity & availability helps in better understanding the pillars of security and its different components.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	This helps in identifying the origin of information and authentic user. This referred to here as
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authenticity
((OPTION_D)) This is optional	Availability
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The key element, authenticity helps in assuring the fact that the information is from the original source.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Data _____ is used to ensure confidentiality.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Locking
((OPTION_C)) This is optional	Deleting
((OPTION_D)) This is optional	Backup
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Data encryption is the method of converting plain text to cipher-text and only authorised users can decrypt the message back to plain text. This preserves the confidentiality of data

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of these is not a proper method of maintaining AUTHENTICATION?
((OPTION_A)) THIS IS MANDATORY OPTION	Biometric verification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ID and password based verification
((OPTION_C)) This is optional	2-factor authentication
((OPTION_D)) This is optional	switching off the phone
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Switching off the phone in the fear of preserving the confidentiality of data is not a proper solution for data confidentiality. Fingerprint detection, face recognition, password-based authentication, two-step verifications are some of these.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Data integrity gets compromised when _____ and _____ are taken control off.
((OPTION_A)) THIS IS MANDATORY OPTION	Access control, file deletion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Network, file permission
((OPTION_C)) This is optional	Access control, file permission
((OPTION_D)) This is optional	Network, system

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The two key ingredients that need to be kept safe are: access control & file permission in order to preserve data integrity.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	One common way to maintain data availability is
((OPTION_A)) THIS IS MANDATORY OPTION	Data clustering
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data backup
((OPTION_C)) This is optional	Data recovery
((OPTION_D)) This is optional	Data Altering

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	For preventing data from data-loss, or damage data backup can be done and stored in a different geographical location so that it can sustain its data from natural disasters & unpredictable events.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as
((OPTION_A)) THIS IS MANDATORY OPTION	Black Hat hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	White Hat Hackers
((OPTION_C)) This is optional	Grey Hat Hackers
((OPTION_D)) This is optional	Red Hat Hackers

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	White Hat Hackers are cyber security analysts and consultants who have the intent to help firms and Governments in the identification of loopholes as well as help to perform penetration tests for securing a system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the legal form of hacking based on which jobs are provided in IT industries and firms?
((OPTION_A)) THIS IS MANDATORY OPTION	Cracking
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Non ethical Hacking
((OPTION_C)) This is optional	Ethical hacking
((OPTION_D))	Hactivism

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Ethical Hacking is an ethical form of hacking done by white-hat hackers for performing penetration tests and identifying potential threats in any organizations and firms.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are "they" referred to here?
((OPTION_A)) THIS IS MANDATORY OPTION	Gray Hat Hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	White Hat Hackers
((OPTION_C)) This is optional	Hactivists
((OPTION_D))	Black Hat Hackers

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Black Hat hackers also termed as 'crackers' and are a major type of cyber criminals who take unauthorized access in user's account or system and steal sensitive data or inject malware into the system for their profit or to harm the organization.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are the combination of both white as well as black hat hackers.
((OPTION_A)) THIS IS MANDATORY OPTION	Grey Hat hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Green Hat hackers
((OPTION_C)) This is optional	Blue Hat Hackers

((OPTION_D)) This is optional	Red Hat Hacker
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Grey Hat Hackers have a blending character of both ethical as well as un-ethical hacker. They hack other's systems for fun but do not harm the system, exploits bugs and vulnerabilities in network without the knowledge of the admin or the owner.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The amateur or newbie in the field of hacking who don't have many skills about coding and in-depth working of security and hacking tools are called _____
((OPTION_A)) THIS IS MANDATORY OPTION	Sponsored Hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hactivists
((OPTION_C))	Script Kiddies

This is optional	
((OPTION_D))	Whistle Blowers
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Script Kiddies are new to hacking and at the same time do not have many interests in developing coding skills or find bugs of their own in systems; rather they prefer downloading of available tools (developed by elite hackers) and use them to break any system or network. They just try to gain attention of their friend circles.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Suicide Hackers are those _____
((OPTION_A)) THIS IS MANDATORY OPTION	who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their malicious activity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	individuals with no knowledge of codes but an expert in using hacking tools

((OPTION_C)) This is optional	who know the consequences of their hacking activities and hence try to prevent them by erasing their digital footprints
((OPTION_D)) This is optional	who are employed in an organization to do malicious activities on other firms
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Suicide hackers are those who break into any network or system with or without knowing the consequences of the cyber crime and its penalty. There are some suicide hackers who intentionally do crimes and get caught to bring their names in the headlines.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____
((OPTION_A)) THIS IS MANDATORY OPTION	State sponsored hackers
((OPTION_B)) THIS IS ALSO MANDATORY	Blue Hat Hackers

OPTION	
((OPTION_C)) This is optional	Cyber Terrorists
((OPTION_D)) This is optional	Red Hat Hackers
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Cyber Terrorists are very expert programmers and cyber criminals who hide themselves while doing malicious activities over the internet and they are smart enough to hide themselves or their tracks of action. They are hired for gaining unauthorised access to nation's data centres or break into the network of intelligence agencies.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are those individuals who maintain and handles IT security in any firm or organization.
((OPTION_A)) THIS IS MANDATORY OPTION	IT Security Engineer
((OPTION_B))	Cyber Security Interns

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Software Security Specialist
((OPTION_D)) This is optional	Security Auditor
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is an intermediary level of position of an individual in an organization or firm who builds and preserves different systems and its associated security tools of the firm of organization to which he/she belongs.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Role of security auditor is to _____
((OPTION_A)) THIS IS MANDATORY OPTION	secure the network

((OPTION_B)) THIS IS ALSO MANDATORY OPTION	probe for safety and security of organization's security components and systems
((OPTION_C)) This is optional	detects and prevents cyber attacks and threats to organization
((OPTION_D)) This is optional	does penetration testing on different web applications
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Security auditors are those who conduct auditing of various computer and network systems on an organization or company and reports the safety and security issues as well as helps in suggesting improvements or enhancements in any particular system that is threat prone.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are senior level corporate employees who have the role and responsibilities of creating and designing secured network or security structures.
((OPTION_A)) THIS IS MANDATORY	Ethical Hackers

OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Chief Technical Officer
((OPTION_C)) This is optional	IT Security Engineers
((OPTION_D)) This is optional	Security Architect
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Security architect are those senior grade employees of an organization who are in charge of building, designing, implementing and testing of secured network topologies, protocols as well as secured computers in an organization.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Governments hired some highly skilled hackers. These types of hackers are termed as _____
((OPTION_A)) THIS IS	Special Hackers

<b>MANDATORY OPTION</b>	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Government Hackers
((OPTION_C))  This is optional	Cyber Intelligence Agents
((OPTION_D))  This is optional	Nation / State sponsored hackers
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Nation / State sponsored hackers are specific individuals who are employed or hired by the government of that nation or state and protect the nation from cyber terrorists and other groups or individuals and to reveal their plans, communications and actions.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The full form of Malware is _____
((OPTION_A))	Malfunctioned Software

THIS IS MANDATORY OPTION	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Multipurpose Software
((OPTION_C))  This is optional	) Malicious Software
((OPTION_D))  This is optional	Malfunctioning of Security
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Different types of harmful software and programs that can pose threats to a system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransomware, spyware, worms, rootkits etc.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Who deploy Malwares to a system or network?

((OPTION_A)) THIS IS MANDATORY OPTION	Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Criminal organizations, gray hat hackers, Malware developers, Penetration testers
((OPTION_C)) This is optional	) Criminal organizations, Black hat hackers, software developers, cyber-terrorists
((OPTION_D)) This is optional	Criminal organizations, White hat hackers, malware developers, cyber-terrorists
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Criminal-minded organizations, groups and individuals cyber-terrorist groups, Black hat hackers, malware developers etc are those who can deploy malwares to any target system or network in order to deface that system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	_____ is a code injecting method used for attacking the database of a system / website.

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	HTML injection
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SQL Injection
((OPTION_C)) This is optional	Malicious code injection
((OPTION_D)) This is optional	XML Injection
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	SQLi (Structured Query Language Injection) is a popular attack where SQL code is targeted or injected; for breaking the web application having SQL vulnerabilities. This allows the attacker to run malicious code and take access to the database of that server.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN	This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?

CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	SQL injection
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	HTML Injection
((OPTION_C)) This is optional	Cross Site Scripting (XSS)
((OPTION_D)) This is optional	Cross Site Request Forgery (XSRF)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	XSS attack can be infused by putting the malicious code (which gets automatically run) in any comment section or feedback section of any webpage (usually a blogging page). This can hamper the reputation of a site and the attacker may place any private data or personal credentials.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	An attempt to harm, damage or cause threat to a system or network is broadly termed as _____

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A))  THIS IS MANDATORY OPTION	Cyber-crime
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Cyber Attack
((OPTION_C))  This is optional	System hijacking
((OPTION_D))  This is optional	Digital crime
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cyber attack is an umbrella term used to classify different computer & network attacks or activities such as extortion, identity theft, email hacking, digital spying, stealing hardware, mobile hacking and physical security breaching.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
((OPTION_A))  THIS IS MANDATORY OPTION	Network Security
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Database Security
((OPTION_C))  This is optional	Information Security
((OPTION_D))  This is optional	Physical Security
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information from alteration, destruction, deletion or disclosure by unauthorised users.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a vulnerability to information security?
((OPTION_A))  THIS IS MANDATORY OPTION	flood
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	without deleting data, disposal of storage media
((OPTION_C))  This is optional	unchanged default password
((OPTION_D))  This is optional	latest patches and updates not done
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a set of conventions & rules set for communicating two or more devices residing in the same network?
((OPTION_A))  THIS IS MANDATORY OPTION	Security policies
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Protocols
((OPTION_C))  This is optional	Wireless network
((OPTION_D))  This is optional	Network algorithms
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Network protocols are designed with mechanisms for identifying devices and make connections between them. In addition, some proper rules are defined as to how data packets will be sent and received.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The field that covers a variety of computer networks, both public and private, that are used in everyday jobs
((OPTION_A)) THIS IS MANDATORY OPTION	Artificial Intelligence
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ML
((OPTION_C)) This is optional	Network Security
((OPTION_D)) This is optional	IT
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Network security covers a variety of computer networks, both private and public. Everyday jobs like conducting transactions and communications among business and government agencies etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Network Security provides authentication and access control for resources.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is not an objective of network security?
((OPTION_A)) THIS IS MANDATORY OPTION	Identification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Authentication
((OPTION_C)) This is optional	Access control
((OPTION_D)) This is optional	Lock
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The Identification, Authentication and Access control are the objectives of network security. There is no such thing called lock.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of these is a part of network identification?
((OPTION_A)) THIS IS MANDATORY OPTION	UserID
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Password
((OPTION_C)) This is optional	OTP
((OPTION_D)) This is optional	fingerprint
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The answer is UserID. UserID is a part of identification. UserID can be a combination of username, user student number etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The process of verifying the identity of a user.
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Identification
((OPTION_C)) This is optional	Validation
((OPTION_D)) This is optional	Verification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	It is called an authentication. It is typically based on passwords, smart card, fingerprint, etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Security features that control that can access resources in the OS
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Identification
((OPTION_C)) This is optional	Validation
((OPTION_D)) This is optional	Access control
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Access control refers to the security features. Applications call access control to provide resources

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm in encryption is called
((OPTION_A)) THIS IS MANDATORY OPTION	Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Procedure
((OPTION_C)) This is optional	Cipher
((OPTION_D)) This is optional	Module
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	An algorithm used in encryption is referred to as a cipher. cipher is an algorithm for performing encryption or decryption

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The information that gets transformed in encryption is
((OPTION_A)) THIS IS MANDATORY OPTION	Plain text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Parallel text
((OPTION_C)) This is optional	Encrypted text
((OPTION_D)) This is optional	Decrypted text
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The text that gets transformed is called plain text. The algorithm used is called cipher

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The type of threats on the security of a computer system or network are..... i) Interruption ii) Interception iii) Modification iv) Creation v) Fabrication
((OPTION_A)) THIS IS MANDATORY OPTION	i, ii, iii and iv only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii, iii, iv and v only
((OPTION_C)) This is optional	i, ii, iii and v only
((OPTION_D)) This is optional	All i, ii, iii, iv and v
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is computer threat?
((OPTION_A))  THIS IS MANDATORY OPTION	Phishing
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Soliciting
((OPTION_C))  This is optional	DoS attack
((OPTION_D))  This is optional	stalking
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a term used in cryptography that refers to a message before encryption or after decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PLAIN TEXT
((OPTION_C)) This is optional	Original text
((OPTION_D)) This is optional	Plain script
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ is encrypted text
((OPTION_A)) THIS IS MANDATORY OPTION	cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	cipher script
((OPTION_C)) This is optional	secret text
((OPTION_D)) This is optional	secret script
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An _____ along with a key is used in the encryption
((OPTION_A)) THIS IS MANDATORY OPTION	cryptography algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption algorithm
((OPTION_C)) This is optional	encryption algorithm
((OPTION_D)) This is optional	plain text algorithm
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them.
((OPTION_A)) THIS IS MANDATORY OPTION	Availability
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	Cryptography
((OPTION_D)) This is optional	Integrity
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that information are in a format that is true and correct to its original purposes.
((OPTION_A)) THIS IS MANDATORY OPTION	Availability
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	integrity
((OPTION_D)) This is optional	cryptography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that information and resources are available to those who need them.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Availability</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Confidentiality</b>
((OPTION_C)) This is optional	<b>Cryptography</b>
((OPTION_D)) This is optional	<b>Integrity</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the process of identifying an individual, usually based on a username and password.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Authentication</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Authorization</b>
((OPTION_C)) This is optional	<b>either authentication or authorization</b>
((OPTION_D)) This is optional	<b>neither authentication nor authorization</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the process of giving individuals access to system objects based on their identity.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Authentication</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Authorization</b>
((OPTION_C)) This is optional	<b>either authentication or authorization</b>
((OPTION_D)) This is optional	<b>neither congestion control nor quality of service</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	when someone gains access to a server, website, or other sensitive data using someone else's account details called as
((OPTION_A)) THIS IS MANDATORY OPTION	Authorized access
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Access control
((OPTION_C)) This is optional	Unauthorized access
((OPTION_D)) This is optional	access
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.called as
((OPTION_A)) THIS IS MANDATORY OPTION	Thief
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	hacker
((OPTION_C)) This is optional	attacker
((OPTION_D)) This is optional	criminal
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is an action or event that might compromise the security.
((OPTION_A))  THIS IS MANDATORY OPTION	Threat
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Vulnerability
((OPTION_C))  This is optional	Protect
((OPTION_D))  This is optional	attack
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system
((OPTION_A)) THIS IS MANDATORY OPTION	threat
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Vulnerability
((OPTION_C)) This is optional	Attack
((OPTION_D)) This is optional	Protection
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is a software that operates on different OS which is used to prevent from malicious software.
((OPTION_A)) THIS IS MANDATORY OPTION	Anti virus
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	virus
((OPTION_C)) This is optional	protocol
((OPTION_D)) This is optional	risk
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is a technique that a hacker uses to stole data by a person for different purposes by psychological manipulation combined with social scenes.
((OPTION_A)) THIS IS MANDATORY OPTION	Social Engineering
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IT engineering
((OPTION_C)) This is optional	Psycology
((OPTION_D)) This is optional	Social engineering
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is a software or hardware which is used to filter network traffic based on rules.
((OPTION_A)) THIS IS MANDATORY OPTION	antivirus
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	firewall
((OPTION_C)) This is optional	protocol
((OPTION_D)) This is optional	keylogger
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not Basic Functions of Antivirus Engines
((OPTION_A)) THIS IS MANDATORY OPTION	Scanning
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity Checking
((OPTION_C)) This is optional	Interception
((OPTION_D)) This is optional	Evesdropping
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is name of antivirus
((OPTION_A))  THIS IS MANDATORY OPTION	AVG
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	PAN
((OPTION_C))  This is optional	SACK
((OPTION_D))  This is optional	FIREP
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Hacking tools that can be found very easily by everyone just by googling and they are endless.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Potential Losses due to Security Attacks doesn't involve _____
((OPTION_A)) THIS IS MANDATORY OPTION	Losing your data
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Bad usage of your computer resources
((OPTION_C)) This is optional	Reputation gain
((OPTION_D)) This is optional	Identity theft
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Reputation loss is part of it and not gain

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not malware category?
((OPTION_A))  THIS IS MANDATORY OPTION	Worms
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Viruses
((OPTION_C))  This is optional	Trojans
((OPTION_D))  This is optional	None of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	All are malware categories

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ encrypts all your data when your computer gets infected and the second is to roll back the data at a specific time you want.
((OPTION_A)) THIS IS MANDATORY OPTION	ransomware
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	firmware
((OPTION_C)) This is optional	middleware
((OPTION_D)) This is optional	Cyber ware
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	this network is created between two secure network devices like two firewalls.
((OPTION_A)) THIS IS MANDATORY OPTION	LAN
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MAN
((OPTION_C)) This is optional	VPN
((OPTION_D)) This is optional	WAN
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Virtual private network

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Name of the attack when integrity is compromised is called as _____
((OPTION_A))  THIS IS MANDATORY OPTION	Fabrication
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	interception
((OPTION_C))  This is optional	Interruption
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Attack made on confidentiality is __
((OPTION_A))  THIS IS MANDATORY OPTION	interception
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C))  This is optional	interruption
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	an attack on availability such as a denial of service attack (or DOS)
((OPTION_A))  THIS IS MANDATORY OPTION	Interruption
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Interception
((OPTION_C))  This is optional	fabrication
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An unauthorized party inserts counterfeit objects into the system and basically attacks the authenticity of the system.
((OPTION_A)) THIS IS MANDATORY OPTION	modification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C)) This is optional	interception
((OPTION_D)) This is optional	interruption
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Attack in which a network service is made degraded or unavailable for legitimate use
((OPTION_A)) THIS IS MANDATORY OPTION	Interruption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C)) This is optional	interception
((OPTION_D)) This is optional	modification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is assurance that someone cannot deny something.
((OPTION_A))  THIS IS MANDATORY OPTION	availability
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	confidentiality
((OPTION_C))  This is optional	Access control
((OPTION_D))  This is optional	Non-repudiation
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the purpose of a Denial of Service attack?
((OPTION_A))  THIS IS MANDATORY OPTION	Exploit a weakness in the TCP/IP stack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	To execute a Trojan on a system
((OPTION_C))  This is optional	To overload a system so it is no longer operational
((OPTION_D))  This is optional	To shutdown services by turning them off
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	DoS attacks force systems to stop responding by overloading the processing of the system

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What are some of the most common vulnerabilities that exist in a network or system?
((OPTION_A)) THIS IS MANDATORY OPTION	Changing manufacturer, or recommended, settings of a newly installed application.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additional unused features on commercial software packages
((OPTION_C)) This is optional	Utilizing open source application code
((OPTION_D)) This is optional	Balancing security concerns with functionality and ease of use of a system.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Linux is an open source code and considered to have greater security than the commercial Windows environment

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Sniffing is used to perform _____ fingerprinting
((OPTION_A))  THIS IS MANDATORY OPTION	Passive stack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Active stack
((OPTION_C))  This is optional	Passive banner grabbing
((OPTION_D))  This is optional	Scanned
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Passive stack fingerprinting uses sniffing technologies instead of scanning

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a principle of data security?
((OPTION_A)) THIS IS MANDATORY OPTION	Data Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following attacks is a passive attack?
((OPTION_A))  THIS IS MANDATORY OPTION	Masquerade
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Modification of message
((OPTION_C))  This is optional	Denial of service
((OPTION_D))  This is optional	Traffic analysis
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	In a passive attack, the attacker does not modify any part of the data. His attempt is only to obtain the information and not to modify it. From the mentioned options, this happens only in Traffic analysis in which the attacker monitors the pattern of transmission. The rest other options are examples of active attacks.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options correctly defines the Brute force attack?
((OPTION_A)) THIS IS MANDATORY OPTION	Brutally forcing the user to share the useful information like pins and passwords.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Trying every possible key to decrypt the message.
((OPTION_C)) This is optional	One entity pretends to be some other entity
((OPTION_D)) This is optional	The message or information is modified before sending it to the receiver.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	Integer value
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Square matrix
((OPTION_C)) This is optional	An array of characters
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems is called as
((OPTION_A)) THIS IS MANDATORY OPTION	Network security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Information security
((OPTION_C)) This is optional	Cyber security
((OPTION_D)) This is optional	Internet security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	phishing and pre-texting is part of _____
((OPTION_A)) THIS IS MANDATORY OPTION	<b>NETWORK SECURITY</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>CYBER SECURITY</b>
((OPTION_C)) This is optional	Internet security
((OPTION_D)) This is optional	Internet security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures to protect the transit data only.
((OPTION_A))  THIS IS MANDATORY OPTION	NETWORK SECURITY
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Internet security
((OPTION_C))  This is optional	Information security
((OPTION_D))  This is optional	Cyber security
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is danger for <b>Integrity</b> as well as <b>availability</b> .
((OPTION_A)) THIS IS MANDATORY OPTION	Active attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ is danger for <b>Confidentiality</b> .
((OPTION_A)) THIS IS MANDATORY OPTION	Active attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ attack attention is on detection.
((OPTION_A))  THIS IS MANDATORY OPTION	Passive attack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Active Attack
((OPTION_C))  This is optional	Both
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	in _____ attack attention is on prevention.
((OPTION_A))  THIS IS MANDATORY OPTION	Active attack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C))  This is optional	Both
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Due to ___ attack system is always damaged.
((OPTION_A))  THIS IS MANDATORY OPTION	Active
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C))  This is optional	Both active and passive
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	due to _____ attack, there is no any harm to the system.
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	Both active and passive
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ attack is tough to restrict from entering systems or networks.
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	Both active and passive
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Attack is easy to prohibited in comparison to _____ attack.
((OPTION_A))  THIS IS MANDATORY OPTION	Active,passive
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive,active
((OPTION_C))  This is optional	
((OPTION_D))  This is optional	
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not active attack
((OPTION_A)) THIS IS MANDATORY OPTION	Denial of service (DoS)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	replay
((OPTION_C)) This is optional	Trojans
((OPTION_D)) This is optional	traffic analysis
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In __ <b>attack</b> , an attacker tries to modify the content of the messages.
((OPTION_A))  THIS IS MANDATORY OPTION	Active
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C))  This is optional	
((OPTION_D))  This is optional	
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	in _____ <b>attack</b> , an attacker observes the messages, copy them and may use them for malicious purposes
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is state of being free from potential threats or dangers
((OPTION_A)) THIS IS MANDATORY OPTION	privacy
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	freedom
((OPTION_C)) This is optional	security
((OPTION_D)) This is optional	independence
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ refers to the state of being free from unwanted attention.
((OPTION_A)) THIS IS MANDATORY OPTION	Freedom
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Security
((OPTION_C)) This is optional	Privacy
((OPTION_D)) This is optional	independence
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ can be achieved without _____ but _____ cannot be achieved without _____.
((OPTION_A)) THIS IS MANDATORY OPTION	Security,privacy,privacy security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Privacy,security,security,privacy
((OPTION_C)) This is optional	Security,privacy,privacy,privacy
((OPTION_D)) This is optional	Security,security,privacy,security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ program refers to a set of protocols and regulations set in place to protect all the confidential information assets and resources that an organization collects and owns.
((OPTION_A)) THIS IS MANDATORY OPTION	Privacy
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Security
((OPTION_C)) This is optional	Security and privacy
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ program focuses on protecting only personal information such as log in credentials, passwords, etc.
((OPTION_A)) THIS IS MANDATORY OPTION	Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Privacy
((OPTION_C)) This is optional	Security and privacy
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following Algorithms does not belong to symmetric encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	3DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	RC5
((OPTION_D)) This is optional	IDEA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Assymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key?
((OPTION_A)) THIS IS MANDATORY OPTION	Not true, the message can also be decrypted with the Public Key.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A so called "one way function with back door" is applied for the encryption
((OPTION_C)) This is optional	The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key.
((OPTION_D)) This is optional	The encrypted message contains the function for decryption which identifies the Private Key.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	An one-way function is a function which a computer can calculate quickly, but whose reversal would last months or years. An one-way function with back door can be reversed with the help of a couple of additional information (the back door), but scarcely

	without this information. The information for the back door is contained in the private Key.
--	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the largest disadvantage of the symmetric Encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	More complex and therefore more time-consuming calculations.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Problem of the secure transmission of the Secret Key
((OPTION_C)) This is optional	Less secure encryption function.
((OPTION_D)) This is optional	Isn't used any more
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION))	As there is only one key in the symmetrical encryption, this must

)) This is also optional	be known by both sender and recipient and this key is sufficient to decrypt the secret message. Therefore it must be exchanged between sender and receiver in such a manner that an unauthorized person can in no case take possession of it.
--------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the principle of the encryption using a key?
((OPTION_A)) THIS IS MANDATORY OPTION	The key indicates which function is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	The key contains the secret function for encryption including parameters. Only a password can activate the key.
((OPTION_C)) This is optional	All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.
((OPTION_D)) This is optional	The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	C

E	
((EXPLANATION)) This is also optional	The encoding of a message is calculated by an algorithm. If always the same algorithm would be used, it would be easy to crack intercepted messages. However, it isn't possible to invent a new algorithm whenever the old one was cracked, therefor the possibility to parameterize algorithms is needed and this is the assignment of the key. All algorithms must be public, only the keys are secret (principle of Kerckhoff, Dutch cryptographer during 19th century).

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If the sender and receiver use different keys, the system is referred to as conventional cipher system
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Such a system is called asymmetric, two-key, or public-key cipher system

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW
((OPTION_A)) THIS IS MANDATORY OPTION	ABANDONED LOCK
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ENCRYPTED TEXT
((OPTION_C)) This is optional	ABANDONED TEXT
((OPTION_D)) This is optional	ENCRYPTED LOCK
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher uses $C = (p+3) \text{ mod } 26$ to encrypt.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Caesar Cipher is an example of
((OPTION_A)) THIS IS MANDATORY OPTION	Poly-alphabetic Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Mono-alphabetic Cipher
((OPTION_C)) This is optional	Multi-alphabetic Cipher
((OPTION_D)) This is optional	Bi-alphabetic Cipher
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis
((OPTION_A)) THIS IS MANDATORY OPTION	Random Polyalphabetic, Plaintext, Playfair
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Random Polyalphabetic, Playfair, Vignere
((OPTION_C)) This is optional	Random Polyalphabetic, Vignere, Playfair, Plaintext
((OPTION_D)) This is optional	Random Polyalphabetic, Plaintext, Beaufort, Playfair
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Random Polyalphabetic is the most resistant to frequency analysis, followed by Vignere, Playfair and then Plaintext.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-
((OPTION_A)) THIS IS MANDATORY OPTION	abqdnwewuwjphfvrrtrfznsdokvl
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	abqdmwuwjphfvyyrfznydokvl
((OPTION_C)) This is optional	tbqyrvmwuwjphfvyyrfznydokvl
((OPTION_D)) This is optional	baiuvmwuwjphfoeiyrfznydokvl
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cipher text:= $C_i = P_i + k_i \text{ mod } m \text{ (mod 26).}$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	nlazeiiblji
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nlazeiiblji
((OPTION_C)) This is optional	olaaeiiblki
((OPTION_D)) This is optional	mlaaeiiblki
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Cipher text:= $C_i = P_i + k_i \text{ mod } m \text{ (mod 26).}$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Confusion hides the relationship between the ciphertext and the plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Confusion hides the relationship between the ciphertext and the key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The S-Box is used to provide confusion, as it is dependent on the unknown key.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	false
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>The S-Box is used to provide confusion, as it is dependent on the unknown key.</p> <p>The P-Box is fixed, and there is no confusion due to it, but it provides diffusion.</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	<p>This is an example of</p> <pre> graph TD     P[P] --&gt; L1[L1]     P --&gt; R1[R1]     R1 --&gt; F1[F]     K1[K1] --&gt; F1     F1 --&gt; L2[L2]     L2 --&gt; R2[R2]     R2 --&gt; F2[F]     K2[K2] --&gt; F2     F2 --&gt; L3[L3]     L3 --&gt; Rn[Rn]     Rn --&gt; Fn[F]     Kn[Kn] --&gt; Fn     Fn --&gt; Ln[Ln]     Ln --- C[C]     </pre>
((OPTION_A)) THIS IS MANDATORY OPTION	SP Networks
((OPTION_B)) THIS IS ALSO MANDATORY	Feistel Cipher

OPTION	
((OPTION_C)) This is optional	Hash Algorithm
((OPTION_D)) This is optional	Hill Cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation
((OPTION_A)) THIS IS MANDATORY OPTION	1 and 3
((OPTION_B)) THIS IS ALSO MANDATORY	2 and 3

OPTION	
((OPTION_C)) This is optional	3 and 4
((OPTION_D)) This is optional	2 and 4
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Increase in any of the above 4 leads to slowing of the cipher algorithm i.e. more computational time will be required.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES follows
((OPTION_A)) THIS IS MANDATORY OPTION	Hash Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY	Caesars Cipher

OPTION	
((OPTION_C)) This is optional	Feistel Cipher Structure
((OPTION_D)) This is optional	SP Network
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES Algorithm Cipher System consists of _____ rounds (iterations) each with a round key
((OPTION_A)) THIS IS MANDATORY OPTION	12
((OPTION_B)) THIS IS ALSO MANDATORY	18

OPTION	
((OPTION_C)) This is optional	9
((OPTION_D)) This is optional	16
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES algorithm has a key length of
((OPTION_A)) THIS IS MANDATORY OPTION	128 Bits
((OPTION_B)) THIS IS ALSO MANDATORY	32 Bits

OPTION	
((OPTION_C)) This is optional	64 Bits
((OPTION_D)) This is optional	16 Bits
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	56 bits are used, the rest 8 bits are parity bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the round key is _____ bit and the Round Input is _____ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	48, 32
((OPTION_B)) THIS IS ALSO MANDATORY	64,32

OPTION	
((OPTION_C)) This is optional	56, 24
((OPTION_D)) This is optional	32, 32
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The round key is 48 bits. The input is 32 bits

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
((OPTION_A)) THIS IS MANDATORY OPTION	Scaling of the existing bits
((OPTION_B)) THIS IS ALSO MANDATORY	Duplication of the existing bits

<b>OPTION</b>	
((OPTION_C)) This is optional	Addition of zeros
((OPTION_D)) This is optional	Addition of ones
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits (permutation plus an expansion), that involves duplication of 16 of the bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The Initial Permutation table/matrix is of size
((OPTION_A)) THIS IS MANDATORY OPTION	16x8
((OPTION_B)) THIS IS ALSO MANDATORY	12x8

OPTION	
((OPTION_C)) This is optional	8x8
((OPTION_D)) This is optional	4x8
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	There are 64 bits to permute and this requires a 8x8 matrix.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The number of unique substitution boxes in DES after the 48 bit XOR operation are
((OPTION_A)) THIS IS MANDATORY OPTION	8
((OPTION_B)) THIS IS ALSO MANDATORY	4

OPTION	
((OPTION_C)) This is optional	6
((OPTION_D)) This is optional	12
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	IP-1 is the first step and the last step is IP during decryption.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A preferable cryptographic algorithm should have a good avalanche effect.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Thus statement is true as a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the size(in bits) of the key in the SDES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	24
((OPTION_B)) THIS IS ALSO MANDATORY	16

OPTION	
((OPTION_C)) This is optional	20
((OPTION_D)) This is optional	10
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The size of the key in the SDES algorithm is 10 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	GCD(a,b) is the same as GCD( a , b ).
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is true. $\gcd(60,24) = \gcd(60,-24) = 12$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	882
((OPTION_B)) THIS IS ALSO MANDATORY	770

OPTION	
((OPTION_C)) This is optional	1078
((OPTION_D)) This is optional	1225
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	$\text{GCD}(1160718174, 316258250) = 1078$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	$\text{GCD}(102947526, 239821932) = 6.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	13
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	17
((OPTION_D)) This is optional	7
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	$\text{GCD}(8376238, 1921023) = 13.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 1234 mod 4321 is
((OPTION_A)) THIS IS MANDATORY OPTION	3239
((OPTION_B)) THIS IS ALSO MANDATORY	3213

OPTION	
((OPTION_C)) This is optional	3242
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The multiplicative Inverse of 1234 mod 4321 is 3239.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 550 mod 1769 is
((OPTION_A)) THIS IS MANDATORY OPTION	434
((OPTION_B)) THIS IS ALSO MANDATORY	224

OPTION	
((OPTION_C)) This is optional	550
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The multiplicative Inverse of 550 mod 1769 is 550.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	<p><b>You are supposed to use hill cipher for encryption technique. You are provided with the following matrix,</b></p> $A = \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix}$ <p><b>Is the given matrix 'A', a valid key to be used for encryption?</b></p>
((OPTION_A)) THIS IS MANDATORY OPTION	Yes
((OPTION_B))	No

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Can't be determined
((OPTION_D)) This is optional	Data insufficient
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>For choosing any square matrix as a key, it should be taken care that the matrix is invertible, i.e. its inverse must exist.</p> <p>Here, in this case,</p> $  A   = 0$ <p>Therefore, it means that 'A' is not an invertible matrix. Hence matrix 'A' cannot be chosen as a key matrix for encryption in the <a href="#">Hill cipher</a>.</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	The input text is divided into two parts: one being left half and another one being right half.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Swapping of the left and right halves are performed after each round.
((OPTION_C)) This is optional	The plain text is converted into a matrix form first
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The fiestal structure does not require the conversion of the plain text into matrix form at any of its steps.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Among the following given options, chose the strongest encryption technique

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	DES ( Data Encryption Standard))
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Double DES
((OPTION_C)) This is optional	Triple DES
((OPTION_D)) This is optional	AES (Advance Encryption Standard)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	It has been proved that the AES performs much better than the all the other DES, whether it be single DES or series of DES.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	<p><b>Consider the following steps,</b></p> <ul style="list-style-type: none"> <li>i. Substitution bytes</li> <li>ii. Shift Rows</li> </ul>

IMAGES ALSO	<p>iii. Mix columns iv. Add round key</p> <p><b>The above steps are performed in each round of which of the following ciphers?</b></p>
((OPTION_A))  THIS IS MANDATORY OPTION	Rail fence cipher
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Data Encryption Standard (DES)
((OPTION_C))  This is optional	Advance Encryption Standard (AES)
((OPTION_D))  This is optional	None of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ algorithm transforms ciphertext to plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _____ cipher replaces one character with another character.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ cipher reorders the plaintext characters to create a ciphertext.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
((OPTION_A)) THIS IS MANDATORY OPTION	man-in-the-middle
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ciphertext attack
((OPTION_C)) This is optional	plaintext attack
((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the receiver uses the _____ key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either a or b
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES is a(n) _____ method adopted by the U.S. government.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	either (a) or (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ECB and CBC are _____ ciphers.
((OPTION_A)) THIS IS MANDATORY OPTION	block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	stream
((OPTION_C)) This is optional	field
((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ cipher, the same key is used by both the sender and receiver.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the sender uses the_____key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a(n) _____ cipher, a pair of keys is used.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	2
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	AES uses a _____ bit block size and a key size of _____ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	128; 128 or 256
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64; 128 or 192
((OPTION_C)) This is optional	256; 128, 192, or 256
((OPTION_D)) This is optional	128; 128, 192, or 256
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	It uses a 128-bit block size and a key size of 128, 192, or 256 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Like DES, AES also uses Feistel Structure.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES does not use a Feistel structure. Instead, each full round consists of four separate functions: -byte substitution -Permutation -arithmetic operations over a finite field, and -XOR with a key.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The 4x4 byte matrices in the AES algorithm are called
((OPTION_A)) THIS IS MANDATORY OPTION	States
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Words
((OPTION_C)) This is optional	Transitions
((OPTION_D)) This is optional	Permutations
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is a type of substitution cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	poly alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition cipher
((OPTION_C)) This is optional	Columnar cipher
((OPTION_D)) This is optional	Rail fence cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In substitution cipher the plain text is replaced by cipher text according to a fixed rule. There are two types of substitution cipher- Mono alphabetic and Poly alphabetic cipher.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following correctly defines poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	a substitution based cipher which uses multiple substitution at different positions
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a substitution based cipher which uses fixed substitution over entire message
((OPTION_C)) This is optional	a transposition based cipher which uses multiple substitution at different positions
((OPTION_D)) This is optional	A transposition based cipher which uses fixed substitution over entire message
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Poly alphabetic cipher is a type of substitution cipher. It uses multiple substitution at different positions in order to cipher the plain text.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a type of poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Rotor cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hill cipher
((OPTION_C)) This is optional	One time pad cipher
((OPTION_D)) This is optional	Affine cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	In poly alphabetic cipher each symbol of plain text is replaced by a different cipher text regardless of its occurrence. Out of the given options, only affine cipher is not a poly alphabetic cipher.

((MARKS)) QUESTION IS OF	2
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	We are provided the plain text "SUN". You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2?
((OPTION_A)) THIS IS MANDATORY OPTION	UWP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	NUS
((OPTION_C)) This is optional	WUP
((OPTION_D)) This is optional	QSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>In the Caesar cipher technique, the encryption is performed as follows,</p> $E(P, K) = (P + K) \text{ mod } 26$ <p>Therefore,</p> $E(S, 2) = (18 + 2) \text{ mod } 26 = 20 = U$ $E(U, 2) = (20 + 2) \text{ mod } 26 = 22 = W$ $E(N, 2) = (13 + 2) \text{ mod } 26 = 15 = P$ <p>Hence, the ciphertext is "UWP".</p>

--	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?
((OPTION_A)) THIS IS MANDATORY OPTION	<u>Hill Cipher</u>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<u>Playfair cipher</u>
((OPTION_C)) This is optional	Both a and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also	The hill cipher includes a square matrix as the key, and in Playfair cipher, we create a 5X5 matrix using the given key string. Hence,

optional	both these ciphers include the use of matrices.
----------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Playfair cipher is an example of _____
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C)) This is optional	transposition cipher
((OPTION_D)) This is optional	additive cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	Playfair cipher is a substitution cipher. It falls under the category of poly alphabetic cipher as it uses multiple substitution at different positions in order to cipher the plain text.
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Encryption in Playfair cipher is done using _
((OPTION_A)) THIS IS MANDATORY OPTION	a 5x5 table
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a 13x2 table
((OPTION_C)) This is optional	vigenere table
((OPTION_D)) This is optional	a 6x6 table
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A

((EXPLANATION)) This is also optional	
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the plain text corresponding to cipher text "BPKYFS" if playfair cipher is used with keyword as "SECRET" (assuming j is combined with i)?
((OPTION_A))  THIS IS MANDATORY OPTION	INDIAN
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	WORLD
((OPTION_C))  This is optional	DOLLAR
((OPTION_D))  This is optional	HELLO
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C

((EXPLANATION)) This is also optional	To decrypt the message we follow the reverse procedure. The table is formed in the same manner. Applying this we get the plain text to be "DOLLAR".
---------------------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair are identical?
((OPTION_A)) THIS IS MANDATORY OPTION	then that pair is neglected
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a null(or x) is added in between the letters
((OPTION_C)) This is optional	one of the identical letter is replaced by some other letter
((OPTION_D)) This is optional	then both of the letters are replaced by the letter appearing just next in the row
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	In playfair cipher if the letters in a pair are identical then a null is added in between the letters. Any letter can be used as a null as long as that letter is not the one being repeated.
---------------------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same row?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter at the corner of the row
((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	If the letters in a pair appear in same row then they are replaced by the letters appearing immediately right to them respectively. If the element to be replaced appears at the corner of the row then we wrap around to the left side of that row.
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the ciphered text if the string “SANFOUNDRY” is given as input to the code of playfair cipher with keyword as “SECRET” (assuming j is combined with i)?
((OPTION_A)) THIS IS MANDATORY OPTION	ZHQAPNPAFR
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AHQAPNPAFR
((OPTION_C)) This is optional	HAQAPNPAFR
((OPTION_D)) This is optional	QHAAPNPAFR
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	B

E	
((EXPLANATION)) This is also optional	<p>For encrypting the plain text using playfair cipher we use a <math>5 \times 5</math> table that is constructed by using keyword. Then we apply rules for encryption in order to get the ciphered text. Table is given as under-</p> <p>S E C R T</p> <p>A B D F G</p> <p>H I K L M</p> <p>N O P Q U</p> <p>V W X Y Z</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letters at the corner of the row
((OPTION_D))	that pair is neglected

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	If the letters in a pair appear in the same column then they are replaced by the letters appearing immediately below them respectively. If the element to be replaced appears at the corner of the column then we wrap around to the top side of that column.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair does not appear in same row or column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter of the same row at the corner of the rectangle defined by the original pair respectively

((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	If the letters in a pair does not appear in same row or column then they are replaced by the letters of the same row at the corner of the rectangle defined by the original pair respectively. The order of letters should be maintained.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Columnar cipher falls under the category of?
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C))	additive cipher

This is optional	
((OPTION_D))	Transposition cipher
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Columnar cipher is a transposition cipher. It falls under the category of transposition cipher as it encrypts the plain text by rearranging its letters.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following ciphered text would have NOT used transposition cipher for encryption of the plain text “CIPHER”?
((OPTION_A)) THIS IS MANDATORY OPTION	EPIHRC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	EHIPCR
((OPTION_C))	DTIPRC

This is optional	
((OPTION_D))	HRIPEC
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	We know that transposition cipher encrypts the plain text by shuffling the letters of the plain text. So out of the given options, only “DTIPRC” does not have the same set of letters as “CIPHER”.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many columns do we need to have in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	4
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	5
((OPTION_C))	6

This is optional	
((OPTION_D))	7
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So in this case it will be equal to 6.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the encrypted text corresponding to plain text “CLASSIFIED” using columnar transposition cipher with a keyword as “GAMES”?
((OPTION_A)) THIS IS MANDATORY OPTION	LFDSIASECI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SECIAISDFL
((OPTION_C))	CILFAISESD

This is optional																					
((OPTION_D))	IFSECIAISD																				
This is optional																					
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option																					
((CORRECT_CH OICE)) Either A or B or C or D or E	D																				
((EXPLANATION )) This is also optional	<p>For encrypting using columnar cipher we have to arrange the letters of the plain text in a table which has the same number of columns as the letters of the keyword. Then the letters of the keyword are arranged in alphabetical order and we read along each column.</p> <table style="margin-left: auto; margin-right: auto;"> <tr><td>3</td><td>1</td><td>4</td><td>2</td><td>5</td></tr> <tr><td>G</td><td>A</td><td>M</td><td>E</td><td>S</td></tr> <tr><td>C</td><td>L</td><td>A</td><td>S</td><td>S</td></tr> <tr><td>I</td><td>F</td><td>I</td><td>E</td><td>D</td></tr> </table> <p>So the ciphered text will be “IFSECIAISD”.</p>	3	1	4	2	5	G	A	M	E	S	C	L	A	S	S	I	F	I	E	D
3	1	4	2	5																	
G	A	M	E	S																	
C	L	A	S	S																	
I	F	I	E	D																	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many rows will the letters of the plain text occupy in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B))	2

THIS IS ALSO MANDATORY OPTION																			
((OPTION_C)) This is optional	3																		
((OPTION_D)) This is optional	4																		
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option																			
((CORRECT_CHOICE)) Either A or B or C or D or E	B																		
((EXPLANATION)) This is also optional	<p>Explanation: The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So when we will write the letters of the plain text row wise then there will be 2 rows of plain text in this case. The table is shown below :-</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td>S</td><td>E</td><td>C</td><td>R</td><td>E</td><td>T</td> </tr> <tr> <td>1</td><td>S</td><td>A</td><td>N</td><td>F</td><td>O</td><td>U</td> </tr> <tr> <td>2</td><td>N</td><td>D</td><td>R</td><td>Y</td> </tr> </table>	S	E	C	R	E	T	1	S	A	N	F	O	U	2	N	D	R	Y
S	E	C	R	E	T														
1	S	A	N	F	O	U													
2	N	D	R	Y															

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following statement is not true regarding columnar transposition cipher?
((OPTION_A)) THIS IS	probability of error is high while deciphering

<b>MANDATORY OPTION</b>	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	it cannot be combined with other ciphers
((OPTION_C))  This is optional	it is a traditional symmetric cipher
((OPTION_D))  This is optional	it is a weak cipher
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Although columnar transposition cipher is a weak cipher in itself. But it can be combined with other substitution ciphers so as to improve its security. The probability of error remains high while decoding columnar cipher as it is a lengthy process

<b>((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)</b>	1
<b>((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</b>	_____ is another data hiding technique which can be used in conjunction with cryptography for the extra-secure method of protecting data.
<b>((OPTION_A))</b>	Cryptography

THIS IS MANDATORY OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Steganography
((OPTION_C)) This is optional	Tomography
((OPTION_D)) This is optional	Chorography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Steganography is the technique of hiding data in another raw data. Steganography is another data hiding technique which can be used in conjunction with cryptography for an extra-secure method of protecting data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((OPTION_A))  THIS IS MANDATORY OPTION	Cryptography
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C))  This is optional	Steganography
((OPTION_D))  This is optional	Chorography
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Steganography helps in hiding any form of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _____ tool permits security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((OPTION_A)) THIS IS MANDATORY OPTION	Cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C)) This is optional	Chorography
((OPTION_D)) This is optional	Steganography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	A steganography tool is a software tool that permits a security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The main motive for using steganography is that hackers or other users can hide a secret message behind a _____

((OPTION_A)) THIS IS MANDATORY OPTION	special file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ordinary file
((OPTION_C)) This is optional	program file
((OPTION_D)) This is optional	encrypted file
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	The main motive for using steganography is that hackers or other users can hide a secret message behind ordinary files. Some steganography tools are SSuite Picsel, rSteg etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	People will normally think it as a normal/regular file and your secret message will pass on without any _____

((OPTION_A)) THIS IS MANDATORY OPTION	Suspicion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	cracking
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Steganography techniques help hackers or other users to conceal covert message behind regular files. People will normally think it as a normal/regular file and your secret message will pass on without any suspicion.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	By using _____ you can diminish the chance of data leakage

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C)) This is optional	Chorography
((OPTION_D)) This is optional	Steganography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Hackers or other cyber criminals target ordinary files to hide different data or information within another data file. By using steganography, you can diminish the chance of data leakage.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Which of the following is a mode of operation for the Block ciphers in cryptography?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Electronic Code Book (ECB)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Cipher Block Chaining (CBC)
((OPTION_C)) This is optional	Counter (CTR) mode
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	For which of the following should EBC (Electronic Code Book) process not be used for encryption?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	For large block sizes
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	For fixed block sizes
((OPTION_C)) This is optional	For small block sizes
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	It is preferred that the block size in the ECB technique must be greater than 64 bits. If not, the text is padded to make it of the required length. This is due to some particular words and phrases that may be reused again often so that the same repetitive part of ciphertext can emerge as mixed.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	Which of the following is the main disadvantage of the ECB (Electronic Code Book)?

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	It requires large block size
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Padding is done to make the plain text divisible into blocks of fixed size
((OPTION_C)) This is optional	It is prone to cryptanalysis since there is a direct relationship between plain text and cipher text.
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	In <u>ECB</u> , there lies a direct relation between the plain text and the ciphertext. Therefore, it is easy for an outsider to break the encryption logic and steal the data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options is not correct according to the definition of the Cipher Block Chaining (CBC)?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC is a mode of operation for stream ciphers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Initialization vector (IV) is used in CBC in the initial phase.
((OPTION_C)) This is optional	It has better resistive nature towards cryptanalysis than ECB
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<a href="#">CBC</a> which stands for Cipher Block chaining is a mode of operation for block ciphers and not for stream ciphers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following modes of operations can be followed for both stream ciphers as well as block ciphers?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC (Cipher Block Chaining)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ECB (Electronic Code Book)
((OPTION_C)) This is optional	CFB (Cipher text Feed Back)
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	<b>CFB</b> is primarily a mode to derive some characteristics of a stream cipher from a block cipher on the cryptography in cryptoanalysis.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

<p>((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</p>	<p>All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES?</p> <ul style="list-style-type: none"> <li>i. Substitution bytes</li> <li>ii. Shift rows</li> <li>iii. Mix columns</li> <li>iv. Add round key</li> </ul>
<p>((OPTION_A)) THIS IS MANDATORY OPTION</p>	<p>i</p>
<p>((OPTION_B)) THIS IS ALSO MANDATORY OPTION</p>	<p>iii</p>
<p>((OPTION_C)) This is optional</p>	<p>All of the mentioned</p>
<p>((OPTION_D)) This is optional</p>	<p>None of the mentioned</p>
<p>((OPTION_E)) This is optional. If optional keep empty so that system will skip this option</p>	
<p>((CORRECT_CHOICE)) Either A or B or C or D or E</p>	<p>B</p>
<p>((EXPLANATION)) This is also optional</p>	<p>In the AES algorithm, the MIX COLUMN operation is performed in all the rounds except the final round of the algorithm.</p>

<p>((MARKS))</p>	<p>1</p>
------------------	----------

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"The number of rounds in the AES algorithm depends upon the key size being used." Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	128 key size: 10 rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	192 key size: 12 rounds
((OPTION_C)) This is optional	256 key size: 14 rounds
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS))	2
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Avalanche effect
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Completeness
((OPTION_C)) This is optional	Both a. and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS))	2
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For the AES-128 algorithm there are _____ similar rounds and _____ round is different.
((OPTION_A)) THIS IS MANDATORY OPTION	2 pair of 5 similar rounds ; every alternate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	9 ; the last
((OPTION_C)) This is optional	8 ; the first and last
((OPTION_D)) This is optional	10 ; no
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS))	1
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the 4 operations are false for each round in the AES algorithm? i) Substitute Bytes ii) Shift Columns iii) Mix Rows iv) XOR Key
((OPTION_A)) THIS IS MANDATORY OPTION	i) only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii) iii) and iv)
((OPTION_C)) This is optional	ii) and iii)
((OPTION_D)) This is optional	only iv
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES rounds involve substitute bytes, shift rows, mix columns and addition of round key.

((MARKS))	1
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	There is an addition of round key before the start of the AES round algorithms.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In AES the final round contains only three transformations, and there is an initial single transformation (Add Round Key) before the first round which can be considered Round 0. Each transformation takes 4x4 matrixes as input and produces a 4x4 matrix as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1																
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the Shifted Row transformation for the matrix bellow?  <table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>6B</td><td>77</td><td>A4</td><td>6B</td></tr> <tr> <td>AD</td><td>01</td><td>F0</td><td>63</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	FE	72	2B	D7	6B	77	A4	6B	AD	01	F0	63	30	D7	AF	FE
FE	72	2B	D7														
6B	77	A4	6B														
AD	01	F0	63														
30	D7	AF	FE														
((OPTION_A))  THIS IS MANDATORY OPTION	<table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>6B</td><td>77</td><td>A4</td><td>6B</td></tr> <tr> <td>AD</td><td>01</td><td>F0</td><td>63</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	FE	72	2B	D7	6B	77	A4	6B	AD	01	F0	63	30	D7	AF	FE
FE	72	2B	D7														
6B	77	A4	6B														
AD	01	F0	63														
30	D7	AF	FE														
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	<table border="1"> <tr> <td>72</td><td>2B</td><td>D7</td><td>FE</td></tr> <tr> <td>A4</td><td>6B</td><td>6B</td><td>77</td></tr> <tr> <td>63</td><td>AD</td><td>01</td><td>F0</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	72	2B	D7	FE	A4	6B	6B	77	63	AD	01	F0	30	D7	AF	FE
72	2B	D7	FE														
A4	6B	6B	77														
63	AD	01	F0														
30	D7	AF	FE														
((OPTION_C))  This is optional	<table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>77</td><td>A4</td><td>6B</td><td>6B</td></tr> <tr> <td>F0</td><td>63</td><td>AD</td><td>01</td></tr> <tr> <td>FE</td><td>30</td><td>D7</td><td>AF</td></tr> </table>	FE	72	2B	D7	77	A4	6B	6B	F0	63	AD	01	FE	30	D7	AF
FE	72	2B	D7														
77	A4	6B	6B														
F0	63	AD	01														
FE	30	D7	AF														
((OPTION_D))  This is optional	<table border="1"> <tr> <td>D7</td><td>FE</td><td>72</td><td>2B</td></tr> <tr> <td>A4</td><td>6B</td><td>6B</td><td>77</td></tr> <tr> <td>01</td><td>AD</td><td>63</td><td>F0</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	D7	FE	72	2B	A4	6B	6B	77	01	AD	63	F0	30	D7	AF	FE
D7	FE	72	2B														
A4	6B	6B	77														
01	AD	63	F0														
30	D7	AF	FE														

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The Shift Rows transformation consists of: -Not shifting the first row of the state array at all. -Circularly shifting the second row by one byte to the left. -Circularly shifting the third row by two bytes to the left, and -Circularly shifting the last row by three bytes to the left.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not weak key in DES
((OPTION_A)) THIS IS MANDATORY OPTION	0x0101010101010101
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0xEFABFEFEFEFEFEFE
((OPTION_C)) This is optional	0x1F1F1F1F0E0E0E0E
((OPTION_D))	0xFFFFFFFFFFFFFF

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple-DES has _____ keys.
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	2
((OPTION_C)) This is optional	5
((OPTION_D))	4

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a encryption technique which uses two instance of DES on same plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	Double DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tripple DES
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ attack which can be used to break through double DES.
((OPTION_A)) THIS IS MANDATORY OPTION	Brute force
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	meet-in-the middle
((OPTION_C)) This is optional	Timing
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple DES involve __
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption, Decryption, Decryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption ,Encryption, Encryption
((OPTION_C)) This is optional	Decryption ,Encryption, Decryption
((OPTION_D))	Encryption, Decryption, Encryption

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ involves feeding the successive output blocks from the underlying block cipher back to it
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	OFB
((OPTION_D))	CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is counter-based version of CFB mode without the feedback
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	counter
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below mode is independent of previous output
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	CFB
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Errors get propagated in all modes except ___and ___
((OPTION_A)) THIS IS MANDATORY OPTION	ECB,COUNTER
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC,COUNTER
((OPTION_C)) This is optional	CFB,COUNTER
((OPTION_D))	OFB,CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Patterns are not preserved in ___ mode
((OPTION_A)) THIS IS MANDATORY OPTION	CBC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CFB
((OPTION_C)) This is optional	Both CBC and CFB
((OPTION_D))	ECB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A small change in plaintext results in the very great change in the cipher text indicates which characteristic
((OPTION_A)) THIS IS MANDATORY OPTION	completeness
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Strong key
((OPTION_C)) This is optional	Avalanche effect
((OPTION_D))	All of the above

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ ciphers, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of cipher text.
((OPTION_A)) THIS IS MANDATORY OPTION	Block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Stream
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	More number of _____ provide more secure system in feistel cipher.
((OPTION_A)) THIS IS MANDATORY OPTION	rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	keys
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	Function
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes..

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In public key cryptosystem _____ keys are used for encryption and decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	Same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Different
((OPTION_C)) This is optional	Encryption Keys
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	In conventional cryptosystem, same keys are used for encryption and decryption where as in public key cryptosystem different keys are used.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In public key cryptosystem which is kept as public?
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption keys
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption keys
((OPTION_C)) This is optional	Encryption & Decryption keys
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	In public key cryptosystem, the encryption keys are kept as public where as decryption keys are kept as secret.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Public key cryptosystem uses same key for both encryption and decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which should be kept as a secret in public key cryptosystem?
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption key
((OPTION_C)) This is optional	Encryption & Decryption key
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	In public key cryptosystem, Encryption is done using public key . decryption key needs to be kept as a secret.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Euler's totient function is determined by
((OPTION_A)) THIS IS MANDATORY OPTION	$pq$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(p-1)(q-1)$
((OPTION_C)) This is optional	$(p+1)(q+1)$
((OPTION_D)) This is optional	$p/q$
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	The Euler's totient function is determined by $(p-1)(q-1)$ , where p and q are kept hidden.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?
((OPTION_A))  THIS IS MANDATORY OPTION	p and q should be divisible by $\Phi(n)$
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	p and q should be co-prime
((OPTION_C))  This is optional	p and q should be prime
((OPTION_D))  This is optional	p/q should give no remainder
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	'p' and 'q' should have large random values which are both prime numbers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, $\Phi(n) = \text{_____}$ in terms of p and q.
((OPTION_A)) THIS IS MANDATORY OPTION	(p)/(q)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	(p)(q)
((OPTION_C)) This is optional	(p-1)(q-1)
((OPTION_D)) This is optional	(p+1)(q+1)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	$\Phi(n) = (p-1)(q-1).$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, we select a value 'e' such that it lies between 0 and $\Phi(n)$ and it is relatively prime to $\Phi(n)$ .
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	$\gcd(e, \Phi(n))=1$ ; and $1 < e < \Phi(n)$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 19$ and choose $e=17$ . Apply RSA algorithm where message=5 and find the cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	C=80
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	C=92
((OPTION_C)) This is optional	C=56
((OPTION_D)) This is optional	C=23
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 209.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 19$ and choose $d=17$ . Apply RSA algorithm where Cipher message=80 and thus find the plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	54
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	43
((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	24
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	$n = pq = 11 \times 19 = 209$ . $C=M^e \text{ mod } n ; C=5^{17} \text{ mod } 209 ; C = 80 \text{ mod } 209$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	$n = 35; e = 5; C = 10$ . What is the plaintext (use RSA) ?
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	7
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Use RSA system to decrypt and get PT = 5.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 17$ and choose $e=7$ . Apply RSA algorithm where PT message=88 and thus find the CT.
((OPTION_A)) THIS IS MANDATORY OPTION	23
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64
((OPTION_C)) This is optional	11
((OPTION_D)) This is optional	54
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 187$ . $C=M^e \text{ mod } n ; C=88^7 \text{ mod } 187 ; C = 11 \text{ mod } 187$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 17$ and choose $e=7$ . Apply RSA algorithm where Cipher message=11 and thus find the plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	88
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	122
((OPTION_C)) This is optional	143
((OPTION_D)) This is optional	111
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 187$ . $C=M^e \text{ mod } n ; C=11^{23} \text{ mod } 187 ; C = 88 \text{ mod } 187$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an RSA system the public key of a given user is $e = 31$ , $n = 3599$ . What is the private key of this user?
((OPTION_A))  THIS IS MANDATORY OPTION	3031
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	2412
((OPTION_C))  This is optional	2432
((OPTION_D))  This is optional	1023
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	By trial and error, we determine that $p = 59$ and $q = 61$ . Hence $f(n) = 58 \times 60 = 3480$ . Then, using the extended Euclidean algorithm, we find that the multiplicative inverse of 31 modulo $f(n)$ is 3031

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Compute private key (d, p, q) given public key (e=23, n=233 ´ 241=56,153).
((OPTION_A)) THIS IS MANDATORY OPTION	35212
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	12543
((OPTION_C)) This is optional	19367
((OPTION_D)) This is optional	32432
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Since n=233 ´ 241=56,153, p=233 and q=241 $f(n) = (p - 1)(q - 1) = 55,680$ Using Extended Euclidean algorithm, we obtain $d = 23^{-1} \text{ mod } 55680 = 19,367.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a RSA cryptosystem a particular A uses two prime numbers $p = 13$ and $q = 17$ to generate her public and private keys. If the public key of A is 35. Then the private key of A is _____.
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	13
((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	17
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In an RSA cryptosystem, for public key: $\text{GCD}(\phi(n), e) = 1$ And, for private key:

	$(e * d) \bmod \phi(n) = 1$ Where, $\phi(n) = (p - 1)*(q - 1) = (13 - 1)(17 - 1) = 12 * 16 = 192$ Such that $1 < e, d < \phi(n)$ Therefore, the private key is: $(35 * d) \bmod \phi(n) = 1$ $d = 11$
--	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the RSA public key cryptosystem, which one of the following numbers will always be largest?
((OPTION_A)) THIS IS MANDATORY OPTION	E
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	N
((OPTION_C)) This is optional	P
((OPTION_D)) This is optional	Q
((OPTION_E)) This is optional. If optional keep empty so that system will skip	

this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	The number n is generated as the product of the two large prime numbers p and q. Therefore, n must always be greater than both p and q. Furthermore, it is an algorithm constraint that e must be chosen such that e is smaller than n. Therefore, in RSA cryptography n is always the largest of the four variables shown in the options to this question.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If Richard wants to send an encrypted message to Sue using a public key cryptosystem, which key does he use to encrypt the message?
((OPTION_A)) THIS IS MANDATORY OPTION	Richard's public key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Richard's private key
((OPTION_C)) This is optional	Sue's public key
((OPTION_D)) This is optional	Sue's private key
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Richard must encrypt the message using Sue's public key so that Sue can decrypt it using her private key. If he encrypted the message with his own public key, the recipient would need to know Richard's private key to decrypt the message. If he encrypted it with his own private key, any user could decrypt the message using Richard's freely available public key. Richard could not encrypt the message using Sue's private key because he does not have access to it. If he did, any user could decrypt it using Sue's freely available public key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Acme Widgets currently uses a 1,024-bit RSA encryption standard companywide. The company plans to convert from RSA to an elliptic curve cryptosystem. If it wishes to maintain the same cryptographic strength, what ECC key length should it use?
((OPTION_A)) THIS IS MANDATORY OPTION	160 bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	512 bits
((OPTION_C)) This is optional	1,024 bits
((OPTION_D)) This is optional	2,048 bits

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The elliptic curve cryptosystem requires significantly shorter keys to achieve encryption that would be the same strength as encryption achieved with the RSA encryption algorithm. A 1,024-bit RSA key is cryptographically equivalent to a 160-bit elliptic curve cryptosystem key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Richard received an encrypted message sent to him from Sue. Which key should he use to decrypt the message?
((OPTION_A)) THIS IS MANDATORY OPTION	Richard's public key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Richard's private key
((OPTION_C)) This is optional	Sue's public key
((OPTION_D)) This is optional	Sue's private key

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Sue would have encrypted the message using Richard's public key. Therefore, Richard needs to use the complementary key in the key pair, his private key, to decrypt the message.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	One commonly used public-key cryptography method is the _____ algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	RSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RAS
((OPTION_C)) This is optional	RSA
((OPTION_D)) This is optional	RAA

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
((OPTION_A)) THIS IS MANDATORY OPTION	man-in-the-middle
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ciphertext attack
((OPTION_C)) This is optional	plaintext attack
((OPTION_D)) This is optional	none of the above

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the objective of Diffie-Hellman key exchange?
((OPTION_A)) THIS IS MANDATORY OPTION	To protect encrypted data from man-in-the-middle attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	To perform mutual authentication on both sides
((OPTION_C)) This is optional	To prove to another party that one holds a secret key without revealing it
((OPTION_D)) This is optional	To establish a shared secret key on both sides

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The security of RSA encryption relies on which assumption?
((OPTION_A)) THIS IS MANDATORY OPTION	It is computationally infeasible to compute a GCD of two large numbers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	It is computationally infeasible to factor a large number.
((OPTION_C)) This is optional	It is computationally infeasible to test whether a large number is prime.
((OPTION_D)) This is optional	It is computationally infeasible to compute a square modulo n.

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	All of the above
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is asymmetric cryptography?
((OPTION_A)) THIS IS MANDATORY OPTION	ECC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	Both ECC and RSA
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below requires less hardware capacity because of less key size
((OPTION_A)) THIS IS MANDATORY OPTION	ECC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	DES
((OPTION_D)) This is optional	AES

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Diffie Hellman is _____
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption algorithm
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	D-H is key exchange algorithm

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Timing attack on RSA can be avoided by __
((OPTION_A)) THIS IS MANDATORY OPTION	Padding extra bits in message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Adding delays
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below algorithm is used in cryptocurrency?
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AES
((OPTION_C)) This is optional	ECC
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When a hash function is used to provide message authentication, the hash function value is called to as:
((OPTION_A)) THIS IS MANDATORY OPTION	Message Field
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Message Digest
((OPTION_C)) This is optional	Message Score
((OPTION_D)) This is optional	Message Leap

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	We know that the hash function providing message authentication is referred to as message digest in cryptography.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following are used to create a message digest  a. RSA b. SHA-1 c. DES d. MD5
((OPTION_A)) THIS IS MANDATORY OPTION	A&B
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	B&C
((OPTION_C)) This is optional	A&C

((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	They are Message digest algorithm

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the output of a cryptographic hash function?
((OPTION_A)) THIS IS MANDATORY OPTION	A variable set of bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A fixed set of bits, derived from one-way mathematical operations
((OPTION_C)) This is optional	An output which may be easily discovered by an adversary

((OPTION_D)) This is optional	Outputs of such functions are of no importance
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message digest algorithms are primarily used to provide _____
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Authentication
((OPTION_C)) This is optional	inegrity

((OPTION_D)) This is optional	authorization
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a message digest algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IDEA
((OPTION_C)) This is optional	MD5

((OPTION_D)) This is optional	RSA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message _____ means that the data must arrive at the receiver exactly as sent.
((OPTION_A)) THIS IS MANDATORY OPTION	confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	integrity
((OPTION_C)) This is optional	authentication

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
((OPTION_A)) THIS IS MANDATORY OPTION	confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	integrity
((OPTION_C)) This is optional	authentication

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ function creates a message digest out of a message
((OPTION_A)) THIS IS MANDATORY OPTION	encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	hash

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ is a trusted third party that assigns a symmetric key to two parties.
((OPTION_A)) THIS IS MANDATORY OPTION	Public directory
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Certificate authority
((OPTION_C)) This is optional	Both

((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature provides _____.
((OPTION_A)) THIS IS MANDATORY OPTION	authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nonrepudiation
((OPTION_C)) This is optional	both (a) and (b)

((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A digital signature needs a(n) _____ system
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)

((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ is a federal or state organization that binds a public key to an entity and issues a certificate.
((OPTION_A)) THIS IS MANDATORY OPTION	KDC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Kerberos
((OPTION_C)) This is optional	CA

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	means that a sender must not be able to deny sending a message that he sent.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication

((OPTION_D)) This is optional	Nonrepudiation
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Kerberos is a popular session key creator protocol that requires an authentication server and a ticket-granting server.
((OPTION_A)) THIS IS MANDATORY OPTION	KDC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Kerberos
((OPTION_C)) This is optional	CA

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The MD5 is a message digest algorithm developed by
((OPTION_A)) THIS IS MANDATORY OPTION	Ron Rivest.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	WhiteField Diffie.
((OPTION_C)) This is optional	Martin Hellman.

((OPTION_D)) This is optional	Diffie-Hellman.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 is quite fast and produces _____ message digests
((OPTION_A)) THIS IS MANDATORY OPTION	512 bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	1024 bits
((OPTION_C)) This is optional	128 bits

((OPTION_D)) This is optional	64 bits
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The first step of MD5 is
((OPTION_A)) THIS IS MANDATORY OPTION	add padding bits to original messsge
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	adding append length bits
((OPTION_C)) This is optional	divide the input into 512 bit blocks

((OPTION_D)) This is optional	compression
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In MD5, the process block divides the 512 bits into _____ sub blocks.
((OPTION_A)) THIS IS MANDATORY OPTION	16
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	24
((OPTION_C)) This is optional	32

((OPTION_D)) This is optional	84
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which financial institutions have a relationship with merchants for processing payment card authorizations and payments?
((OPTION_A)) THIS IS MANDATORY OPTION	Issuer
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Acquirer
((OPTION_C)) This is optional	Merchant

((OPTION_D)) This is optional	Dealer
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following contains the order information such as which items are being purchased?
((OPTION_A)) THIS IS MANDATORY OPTION	PI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	OI
((OPTION_C)) This is optional	MD

((OPTION_D)) This is optional	DS
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Payment information can be encrypted by using _____.
((OPTION_A)) THIS IS MANDATORY OPTION	customer's private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	merchant public key
((OPTION_C)) This is optional	one-time session key.

((OPTION_D)) This is optional	customer's public key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature envelope is decrypted by using _____.
((OPTION_A)) THIS IS MANDATORY OPTION	merchant private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	payment's private key
((OPTION_C)) This is optional	payment public key

((OPTION_D)) This is optional	merchant's public key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ will ensure the merchant and their payment information
((OPTION_A)) THIS IS MANDATORY OPTION	Digital certificate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Merchant
((OPTION_C)) This is optional	Dual signature

((OPTION_D)) This is optional	Certificate authority
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SET provides an authentication with the help of _____
((OPTION_A)) THIS IS MANDATORY OPTION	dual signature
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	digital certificate
((OPTION_C)) This is optional	payment's public key

((OPTION_D)) This is optional	payment's private key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are very crucial for success of RSA algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	Integers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Prime numbers
((OPTION_C)) This is optional	Negative number

((OPTION_D)) This is optional	Fraction
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ acts as financial institutions who provides a payment card to a card holder
((OPTION_A)) THIS IS MANDATORY OPTION	payment gateway
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	card holder
((OPTION_C)) This is optional	acquirer

((OPTION_D)) This is optional	issuer
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	ISSUER means Bank

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Who will be responsible for processing the payment from the customer's account to the merchant account?
((OPTION_A)) THIS IS MANDATORY OPTION	Acquirer
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Merchant
((OPTION_C)) This is optional	Issuer

((OPTION_D)) This is optional	Payment gateway
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The cardholder combines the PIMD and OIMD and hashes them together to form
((OPTION_A)) THIS IS MANDATORY OPTION	OPMD
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	POMD
((OPTION_C)) This is optional	MD

((OPTION_D)) This is optional	DS
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which process will ensure that the issues of the credit card is an approved transactions?
((OPTION_A)) THIS IS MANDATORY OPTION	Payment capture
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Payment authorization
((OPTION_C)) This is optional	Purchase request

((OPTION_D)) This is optional	Purchase reply
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is used for hiding the payment information from the merchant.
((OPTION_A)) THIS IS MANDATORY OPTION	SET
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	SHTTP

((OPTION_D)) This is optional	TSP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A __word buffer is used to compute the message digest in MD5
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4
((OPTION_C)) This is optional	5

((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	4 WORD A,B,C,D

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In MD5, the message is <b>padded</b> so that its length is divisible by ____
((OPTION_A)) THIS IS MANDATORY OPTION	32
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	128
((OPTION_C)) This is optional	512

((OPTION_D)) This is optional	1024
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 should meet requirements:
((OPTION_A)) THIS IS MANDATORY OPTION	It is impossible to generate two inputs that cannot produce the same hash function
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	It is impossible to generate a message having the same hash value
((OPTION_C)) This is optional	Both of the above

((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 takes an input of ___ size and produces an output if a 128-bit hash value
((OPTION_A)) THIS IS MANDATORY OPTION	Any
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Multiple of 512
((OPTION_C)) This is optional	Multiple of 128

((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following best describes sniffing?
((OPTION_A)) THIS IS MANDATORY OPTION	Gathering packets to locate IP addresses, in order to initiate a session hijacking attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Analyzing packets in order to locate the sequence number to start a session hijack
((OPTION_C)) This is optional	Monitoring TCP sessions in order to initiate a session-hijacking attack

((OPTION_D)) This is optional	Locating a host susceptible to a session-hijack attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Sniffing is usually used to locate the sequence number, which is necessary for a session hijack.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The secret key between members needs to be created as a _____ key when two members contact Kerberos system
((OPTION_A)) THIS IS MANDATORY OPTION	Public
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Session
((OPTION_C))	complimentary

This is optional	
((OPTION_D))	None of these
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The main components of Kerberos are:
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Ticket granting server
((OPTION_C))	database

This is optional	
((OPTION_D))	All of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ performs the initial authentication and ticket for Ticket Granting Service
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Ticket granting server
((OPTION_C))	Database

This is optional	
((OPTION_D))	Kerberos
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The Authentication Server verifies access right of users in __
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TG server
((OPTION_C))	Database

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ issues the ticket for the Server
((OPTION_A)) THIS IS MANDATORY OPTION	AS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TGS
((OPTION_C))	DB

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Kerberos is primarily used for _____
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C))	confidentiality

This is optional	
((OPTION_D))	authorization
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The KDC encrypts the TGT with a password that only the _____ knows.
((OPTION_A)) THIS IS MANDATORY OPTION	AS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TGS
((OPTION_C))	Server

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Because no one else needs to be able to see the contents.  It's for the server to keep track of the client

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The essence of Kerberos' system is _____.
((OPTION_A)) THIS IS MANDATORY OPTION	One way authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity

((OPTION_C)) This is optional	Mutual authentication
((OPTION_D)) This is optional	Public authentication
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not an element/field of the X.509 certificates?
((OPTION_A)) THIS IS MANDATORY OPTION	Issuer Name
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Serial Modifier

((OPTION_C)) This is optional	Issuer unique Identifier
((OPTION_D)) This is optional	Signature
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	X.509 certificate recommends which cryptographic algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	DES

((OPTION_C)) This is optional	AES
((OPTION_D)) This is optional	Rabin
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The standard used in digital certificates that defines its structure, fields, and Values is
((OPTION_A)) THIS IS MANDATORY OPTION	Kerberos
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	End to end encryption

((OPTION_C)) This is optional	X.509
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	X.509 Certificates includes
((OPTION_A)) THIS IS MANDATORY OPTION	Version
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	signature algorithm identifier

((OPTION_C)) This is optional	period of validity
((OPTION_D)) This is optional	extension fields
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	All of the above
((CORRECT_CH OICE)) Either A or B or C or D or E	E
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ defines a framework for the provision of authentication services by the X.500 directory
((OPTION_A)) THIS IS MANDATORY OPTION	X.509
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	X.508

((OPTION_C)) This is optional	X.505
((OPTION_D)) This is optional	X.609
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A digital signature is a mathematical technique used to validate the _____ and _____ of a message, software or digital document
((OPTION_A)) THIS IS MANDATORY OPTION	Authenticity, integrity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity, confidentiality

((OPTION_C)) This is optional	Integrity,non-repudiation
((OPTION_D)) This is optional	Authenticity,confidentiality
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature involves ____ and ____
((OPTION_A)) THIS IS MANDATORY OPTION	Signature verification ,validation
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Signature creation,verification

((OPTION_C)) This is optional	Signature creation,deletion
((OPTION_D)) This is optional	Signature validation,modification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message digest is computed by applying hash function on the message and then message digest is encrypted using _____ key of sender to form the digital signature.
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public

((OPTION_C)) This is optional	Session
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In digital signature , Receiver decrypts the digital signature using the _____ key of sender
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public

((OPTION_C)) This is optional	Secret
((OPTION_D)) This is optional	Session
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In digital signature, The message digest computed by ___ and the message digest (got by decryption on digital signature) need to be ___ for ensuring integrity
((OPTION_A)) THIS IS MANDATORY OPTION	Receiver,same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Receiver,different

((OPTION_C)) This is optional	Sender,same
((OPTION_D)) This is optional	Sender,different
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.
((OPTION_A)) THIS IS MANDATORY OPTION	Digital certificate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Digital signature

((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature follows _____
((OPTION_A)) THIS IS MANDATORY OPTION	Digital Signature Standard (DSS)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	X.509 standard format

((OPTION_C)) This is optional	Both of the above
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In diffie-hellman algorithm, if Alice and Bob wish to communicate with each other, they first agree between them a large prime number n, and ____ g
((OPTION_A)) THIS IS MANDATORY OPTION	Generator
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Small prime number

((OPTION_C)) This is optional	Natural number
((OPTION_D)) This is optional	Factorial
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm if $X_a$ is private key of user then public key is calculated by ____
((OPTION_A)) THIS IS MANDATORY OPTION	$g^{X_a} \text{ mod } n$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$n^{X_a} \text{ mod } n$

((OPTION_C)) This is optional	$g^n \bmod p$
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm, ____ keys of each other should be known
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Session

((OPTION_C)) This is optional	Public
((OPTION_D)) This is optional	No
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm,shared secret key is calculated by ____
((OPTION_A)) THIS IS MANDATORY OPTION	$(g^a \text{ mod } n)^b \text{ mod } n$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(g^b \text{ mod } n)^a \text{ mod } n$

((OPTION_C)) This is optional	Both of the above
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm, the resulting shared secret will be the ___ every time
((OPTION_A)) THIS IS MANDATORY OPTION	Same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Different

((OPTION_C)) This is optional	Maybe same
((OPTION_D)) This is optional	Can't say
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ the first widely used method of safely developing and exchanging keys over an insecure channel
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSS

((OPTION_C)) This is optional	Diffie Hellman
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4

((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value $q = 17$ and primitive root $= 5$ . If Alice's secret key is 4 and Bob's secret key is 6, what is the shared secret key they exchanged?
((OPTION_A)) THIS IS MANDATORY OPTION	16
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	17

((OPTION_C)) This is optional	18
((OPTION_D)) This is optional	19
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Each round of MD5 consist of ____ operations
((OPTION_A)) THIS IS MANDATORY OPTION	14
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	15

((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	18
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Each buffer of MD5 algorithm is ____ bit long
((OPTION_A))  THIS IS MANDATORY OPTION	32
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	64

((OPTION_C)) This is optional	128
((OPTION_D)) This is optional	512
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	RSA is _____ cryptography
((OPTION_A)) THIS IS MANDATORY OPTION	Asymmetric
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key

((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Value generated by hash function is referred as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Message digest
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hash

((OPTION_C)) This is optional	MAC
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not service of digital signature
((OPTION_A))  THIS IS MANDATORY OPTION	Authentication to message
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Data integrity

((OPTION_C)) This is optional	Non-repudiation
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ digitally signs this entire information and includes digital signature in the certificate
((OPTION_A)) THIS IS MANDATORY OPTION	CA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	KDC

((OPTION_C)) This is optional	PKI
((OPTION_D)) This is optional	DB
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA ,e is used as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key

((OPTION_C)) This is optional	Euler's totient
((OPTION_D)) This is optional	Session key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, d is referred as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key
((OPTION_C)) This is optional	Totient function
((OPTION_D)) This is optional	Session key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Collection of protocol designed by IETF
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Operation in Tunnel mode
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec protects information in
((OPTION_A)) THIS IS MANDATORY OPTION	transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec in which mode does not protect IP header
((OPTION_A)) THIS IS MANDATORY OPTION	transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which mode is used when we need host to host protection
((OPTION_A)) THIS IS MANDATORY OPTION	Transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec protects the whole IP packets
((OPTION_A)) THIS IS MANDATORY OPTION	Transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec defines two protocol
((OPTION_A)) THIS IS MANDATORY OPTION	AH, SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PGP, ASP
((OPTION_C)) This is optional	AH, ESP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Authentication at the IP header
((OPTION_A)) THIS IS MANDATORY OPTION	AH
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ECP
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	SSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IT PROVIDES AUTHENTICATION OR ENCRYPTION OR BOTH FOR PACKET AT IP LEVEL
((OPTION_A)) THIS IS MANDATORY OPTION	AH
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ESP
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	SSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSEC USES A SET OF SA CALLED
((OPTION_A)) THIS IS MANDATORY OPTION	SAD
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SAB
((OPTION_C)) This is optional	SADB
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Protocol to provide security for inbound and outbound
((OPTION_A)) THIS IS MANDATORY OPTION	SA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CA
((OPTION_C)) This is optional	KDC
((OPTION_D)) This is optional	IKE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE creates SA for
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PGP
((OPTION_C)) This is optional	IPSec
((OPTION_D)) This is optional	VP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE based on other how many protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Two
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Three
((OPTION_C)) This is optional	Four
((OPTION_D)) This is optional	five
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE uses
((OPTION_A)) THIS IS MANDATORY OPTION	OAKLEY
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SKEME
((OPTION_C)) This is optional	ISKAMP
((OPTION_D)) This is optional	ALL ABOVE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Network is used in an organization
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Semi private
((OPTION_D)) This is optional	Semi publik
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Private network that uses an internet model
((OPTION_A)) THIS IS MANDATORY OPTION	intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is a network that allows authorized access from outside
((OPTION_A)) THIS IS MANDATORY OPTION	Intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Internet authorities have reserved address for
((OPTION_A)) THIS IS MANDATORY OPTION	Intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is provides privacy for LAN
((OPTION_A)) THIS IS MANDATORY OPTION	VPP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	VNP
((OPTION_C)) This is optional	VNN
((OPTION_D)) This is optional	VPN
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IT PROVIDES END TO END SECURITY FOR APPLICATION
((OPTION_A)) THIS IS MANDATORY OPTION	DATA LINK
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	NETWORK
((OPTION_C)) This is optional	TRANSPORT
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is actually an IETF version on
((OPTION_A)) THIS IS MANDATORY OPTION	TLS, TSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL. TLS
((OPTION_C)) This is optional	TLS, SSL
((OPTION_D)) This is optional	SSL,SLT
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Provides security at the transport layer
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To provide security and compression
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Can receive application data from any application layer protocol
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SSL provides
((OPTION_A)) THIS IS MANDATORY OPTION	Integrity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	Compression
((OPTION_D)) This is optional	All above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SSI session
((OPTION_A)) THIS IS MANDATORY OPTION	List of protocol
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Cipher suit
((OPTION_C)) This is optional	List of keys
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cryptographic algorithem and secrets are sent with the message IN
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	TLS
((OPTION_D)) This is optional	PGP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Security protocol for email security is
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Was invented by Phil Zimmerman
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSI
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Provides security, integration, authentication in email
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSI
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Method to transfer secure message
((OPTION_A)) THIS IS MANDATORY OPTION	cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	cryptoanalysis
((OPTION_C)) This is optional	both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is the original message before transmission
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Plain text
((OPTION_C)) This is optional	Secret text
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is the message after transmission
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Plain text
((OPTION_C)) This is optional	Secret text
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm transforms plaintext to ciphertext
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm transforms cipher text to plain text
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A combination of encryption and decryption algorithm is called
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Secret
((OPTION_C)) This is optional	Key
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cipher operates on
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	secret
((OPTION_C)) This is optional	Key
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The same key used by both the sender and receiver
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The key is called as secret key
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A pair of keys used in
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An asymmetric key cipher the sender uses the key
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An asymmetric key cipher the receiver uses the key
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A cipher replaces one character with another
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Monoalphabetic and polyalphabetic cipher are
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The simplest monoalphabetic cipher is
((OPTION_A)) THIS IS MANDATORY OPTION	Transposition
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additive
((OPTION_C)) This is optional	Shift
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Ceasar cipher that has key of 3
((OPTION_A)) THIS IS MANDATORY OPTION	Transposition
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additive
((OPTION_C)) This is optional	Shift
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The cipher reorders the plain text to create the ciphertext
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a keyless substitution To define the relationship between input and output stream
((OPTION_A)) THIS IS MANDATORY OPTION	S box
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	P box
((OPTION_C)) This is optional	T box
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a keyless transposition To define the relationship between input and output stream
((OPTION_A)) THIS IS MANDATORY OPTION	S box
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	P box
((OPTION_C)) This is optional	T box
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cipher made of a combination of different simple cipher
((OPTION_A)) THIS IS MANDATORY OPTION	Round
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Circle
((OPTION_C)) This is optional	Square
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES is an method
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES has an Round
((OPTION_A)) THIS IS MANDATORY OPTION	14
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	15
((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES functions has components
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	3
((OPTION_C)) This is optional	4
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES uses a key generaterto generater to generate sixteen ---round key
((OPTION_A)) THIS IS MANDATORY OPTION	32 bit
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	48 bit
((OPTION_C)) This is optional	54 bit
((OPTION_D)) This is optional	42 bit
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES was designed to increase the size of DES key
((OPTION_A)) THIS IS MANDATORY OPTION	Double
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tripal
((OPTION_C)) This is optional	Quadrupal
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Algorithm uses a 128 bit block of data
((OPTION_A)) THIS IS MANDATORY OPTION	AEE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AED
((OPTION_C)) This is optional	AER
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	AES has how many different combinations
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	3
((OPTION_C)) This is optional	4
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ECB and CBC are ciphers
((OPTION_A)) THIS IS MANDATORY OPTION	Block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Stream
((OPTION_C)) This is optional	Field
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Public key cryptographic algorithm is
((OPTION_A)) THIS IS MANDATORY OPTION	RSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RAS
((OPTION_C)) This is optional	RSA
((OPTION_D)) This is optional	RAA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	AC
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	it provides a one time session key for two parties
((OPTION_A)) THIS IS MANDATORY OPTION	Diffie hellman
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	DES
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	TELNET is an abbreviation of
((OPTION_A)) THIS IS MANDATORY OPTION	Terminal network
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Telephone network
((OPTION_C)) This is optional	Telecommunication network
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	TELNET is a client server application program for
((OPTION_A)) THIS IS MANDATORY OPTION	Specific purpose
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	General purpose
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Users logs in to local time sharing system is called
((OPTION_A)) THIS IS MANDATORY OPTION	Local
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Remote
((OPTION_C)) This is optional	Temporary
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To access remote machine need a login
((OPTION_A)) THIS IS MANDATORY OPTION	Local
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Remote
((OPTION_C)) This is optional	Temporary
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	NVT uses two set of character
((OPTION_A)) THIS IS MANDATORY OPTION	Sending, receiving
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Request, reply
((OPTION_C)) This is optional	Data, control
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For data NVT uses ASCII with the highest order bit set
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0
((OPTION_C)) This is optional	A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For data NVT uses ASCII with the highest order bit set
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0
((OPTION_C)) This is optional	A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The server uses -----port
((OPTION_A)) THIS IS MANDATORY OPTION	Wellknown
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Emperor
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To distinguish data from characters
((OPTION_A)) THIS IS MANDATORY OPTION	ICA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IAC
((OPTION_C)) This is optional	AIC
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	the echoing is done by the client in the mode
((OPTION_A)) THIS IS MANDATORY OPTION	Default
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Character
((OPTION_C)) This is optional	Line
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP uses a service of
((OPTION_A)) THIS IS MANDATORY OPTION	UDP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IP
((OPTION_C)) This is optional	TCP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP control and data connection are
((OPTION_A))  THIS IS MANDATORY OPTION	21, 22
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	20,21
((OPTION_C))  This is optional	21,20
((OPTION_D))  This is optional	none
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP is the service type used by IP protocol because
((OPTION_A)) THIS IS MANDATORY OPTION	Maximise throughput
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Minimize delay
((OPTION_C)) This is optional	Minimize error
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For control connection FTP use a character set of
((OPTION_A)) THIS IS MANDATORY OPTION	Regular ASCII
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	EBCDIC
((OPTION_C)) This is optional	NVT ASCII
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During FTP session the control connection is opened
((OPTION_A)) THIS IS MANDATORY OPTION	Exactly once
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Exactly twice
((OPTION_C)) This is optional	Many times
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During FTP session the control connection is opened
((OPTION_A)) THIS IS MANDATORY OPTION	Exactly once
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Exactly twice
((OPTION_C)) This is optional	Many times
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP files are types of an attribute called
((OPTION_A)) THIS IS MANDATORY OPTION	File types
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structures
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP there are three types of -----,stream, blocked and compression
((OPTION_A)) THIS IS MANDATORY OPTION	File types
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structurs
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP and image defines an attribute called
((OPTION_A)) THIS IS MANDATORY OPTION	File type
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structure
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP when we -----, it is copied from the server to client
((OPTION_A)) THIS IS MANDATORY OPTION	Retrieve a file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Retrieve a list
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP when we -----, it is copied from the client to server
((OPTION_A)) THIS IS MANDATORY OPTION	Retrieve a file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Store a file
((OPTION_C)) This is optional	Retrieve a lise
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is a part of a local hard drive, a special file with permission restriction
((OPTION_A)) THIS IS MANDATORY OPTION	A message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A response
((OPTION_C)) This is optional	An agent
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and the receiver on the same system we need
((OPTION_A)) THIS IS MANDATORY OPTION	One UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA
((OPTION_C)) This is optional	One UA and one MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and receiver are on the different system, we need
((OPTION_A)) THIS IS MANDATORY OPTION	One MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA
((OPTION_C)) This is optional	Two UA and one pair of MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender is connected to the mail server via a LAN or WAN, we need
((OPTION_A)) THIS IS MANDATORY OPTION	Two MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA and two pairs of MTA
((OPTION_C)) This is optional	Two UA and a pair of MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and receiver are connected to the mail server via a LAN or WAN, we need
((OPTION_A)) THIS IS MANDATORY OPTION	Two UA, two pair of MTA, a pair of MAA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA and two pair of MTA
((OPTION_C)) This is optional	Two UA, two pair of MTA, two pair of MAA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	It provides a service to the user to make the process of sending and receiving message
((OPTION_A)) THIS IS MANDATORY OPTION	MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MAA
((OPTION_C)) This is optional	UA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following services is not provided by UA
((OPTION_A))  THIS IS MANDATORY OPTION	Composing message
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Reading message
((OPTION_C))  This is optional	Reply message
((OPTION_D))  This is optional	ALL are
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	There are two types of user agents
((OPTION_A)) THIS IS MANDATORY OPTION	Command driven, data driven
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Command driven, GUI based
((OPTION_C)) This is optional	Command based and data based
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	It contains the sender address, receiver address and other information
((OPTION_A)) THIS IS MANDATORY OPTION	Message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Envelop
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The message contains
((OPTION_A)) THIS IS MANDATORY OPTION	Header, envelop
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Header, body
((OPTION_C)) This is optional	Envelop, body
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the internet, the email address contains two parts
((OPTION_A)) THIS IS MANDATORY OPTION	Local part, domain name
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Global part, domain name
((OPTION_C)) This is optional	Label, domain name
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is a supplementary protocol that allow Non ASCII data to be sent through email
((OPTION_A)) THIS IS MANDATORY OPTION	JPEG
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MPEG
((OPTION_C)) This is optional	MIME
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The actual email transfer is done through
((OPTION_A)) THIS IS MANDATORY OPTION	UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MTA
((OPTION_C)) This is optional	MAA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Protocol that defines a MTA client and server in the internet is called
((OPTION_A)) THIS IS MANDATORY OPTION	SMTP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SNMP
((OPTION_C)) This is optional	TELNET
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The process of transferring a mail message occurs in-----phase
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4
((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SMTP is --- protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Pull
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Push
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

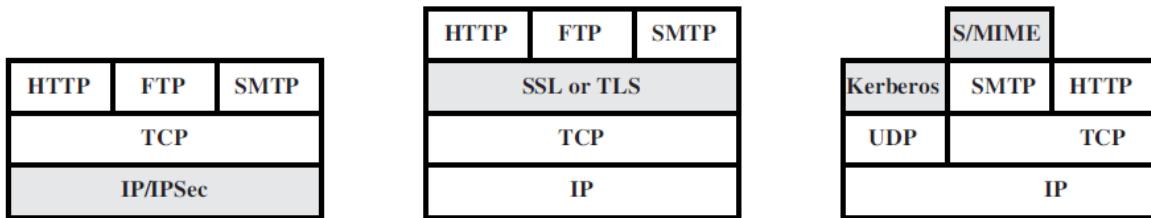
((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The third stage in a email transfer need a ---protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Pull
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Push
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The third stage in an email transfer uses an ----protocol
((OPTION_A)) THIS IS MANDATORY OPTION	UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MTA
((OPTION_C)) This is optional	MAA
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Currently two message asses protocol are available
((OPTION_A)) THIS IS MANDATORY OPTION	POP3, IMAP2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	POP4,IMAP1
((OPTION_C)) This is optional	POP3, IMAP4
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

## Unit 4

### 1. Secure Socket Layer Protocol



1. In the above figure from left to right, the correct order of the shaded levels are

- a) Network level, Application level, Transport level
- b) Application level, Network level, Transport level
- c) Transport level, Application level, Network level
- d) Network level, Transport level, Application level

Answer: d

Explanation: IP/IPSec is the Network level, SSL or TLS is the Transport Level, Kerberos and S/MIME are the Application level.

2. In the above figure, which of the above shaded block is transparent to end users and applications?

- a) IP/IPSec
- b) SSL
- c) Kerberos
- d) S/MIME

Answer: a

Explanation: IP/IPSec is the Network layer which is transparent to end users and applications.

3. In terms of Web Security Threats, “Impersonation of another user” is a Passive Attack.

- a) True
- b) False

Answer: b

Explanation: Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a website that is supposed to be restricted. Active attacks include impersonating another user, altering messages in transit between client and server, altering information on a website.

4. Which one of the following is not a higher –layer SSL protocol?

- a) Alert Protocol
- b) Handshake Protocol
- c) Alarm Protocol

d) Change Cipher Spec Protocol

Answer: c

Explanation: Three higher –layer protocols are defined as part of SSL: The Handshake Protocol, The Change Cipher Spec Protocol and The Alert Protocol.

5. In the SSL Protocol, each upper layer message if fragmented into a maximum of \_\_\_\_\_ bytes.

- a)  $2^{16}$
- b)  $2^{32}$
- c)  $2^{14}$
- d)  $2^{12}$

Answer: c

Explanation: In the fragmentation process we obtain blocks of  $2^{14}$  bytes which is compressed in the next step.

6. The full form of SSL is

- a) Serial Session Layer
- b) Secure Socket Layer
- c) Session Secure Layer
- d) Series Socket Layer

Answer: b

Explanation: SSL stands for Secure Sockets Layer.

7. Which protocol is used to convey SSL related alerts to the peer entity?

- a) Alert Protocol
- b) Handshake Protocol
- c) Upper-Layer Protocol
- d) Change Cipher Spec Protocol

Answer: a

Explanation: The Alert protocol is used to convey SSL related alerts to the peer entity.

8. Which protocol consists of only 1 bit?

- a) Alert Protocol
- b) Handshake Protocol
- c) Upper-Layer Protocol
- d) Change Cipher Spec Protocol

Answer: d

Explanation: The change cipher spec protocol is bit long.

9. Which protocol is used for the purpose of copying the pending state into the current state?

- a) Alert Protocol
- b) Handshake Protocol
- c) Upper-Layer Protocol

d) Change Cipher Spec Protocol

Answer: d

Explanation: The Change Cipher Spec Protocol is used for this action.

10. In the alert protocol the first byte takes the value 1 or 2 which corresponds to \_\_\_\_\_ and \_\_\_\_\_ respectively.

- a) Select, Alarm
- b) Alert, Alarm
- c) Warning, Alarm
- d) Warning, Fatal

Answer: d

Explanation: The first byte takes the value warning(1) or fatal(2) to convey the severity of the message.

## 2. Pretty good privacy (PGP), S/MIME, SET

1. Pretty good privacy (PGP) security system uses

- a) Public key cryptosystem
- b) Private key cryptosystem
- c) Public & Private key cryptosystem
- d) None of the mentioned

Answer: c

Explanation: PGP uses many encryption techniques such as private key cryptosystem and also public key cryptosystem.

2. Data compression includes

- a) Removal of redundant character
- b) Uniform distribution of characters
- c) Removal of redundant character & Uniform distribution of characters
- d) None of the mentioned

Answer: c

Explanation: Data compression removes redundant character strings in a file and produces a more uniform distribution of characters.

3. PGP offers \_\_\_\_\_ block ciphers for message encryption.

- a) Triple-DES
- b) CAST
- c) IDEA
- d) All of the mentioned

Answer: d

Explanation: Pretty good privacy security system offers three block ciphers for message encryption – Triple-DES, IDEA and CAST.

4. What is the key size allowed in PGP?

- a) 1024-1056
- b) 1024-4056
- c) 1024-4096
- d) 1024-2048

Answer: c

Explanation: Pretty good privacy security system allows 1024 to 4096 bits of key size.

5. Which of the following is not a secured mail transferring methodology?

- a) POP3
- b) SSMTP
- c) Mail using PGP
- d) S/MIME

Answer: a

Explanation: POP (Post Office Protocol) is a simple protocol which fetches the updated mail stored for you by the server. S/MIME (Secure/Multipurpose Internet Mail Extensions), SSMTP (Secure-Simple Mail Transfer Protocol), and PGP (Pretty Good Privacy) are examples of protocols and methods for secure mailing.

6. HTTPS is abbreviated as \_\_\_\_\_

- a) Hypertexts Transfer Protocol Secured
- b) Secured Hyper Text Transfer Protocol
- c) Hyperlinked Text Transfer Protocol Secured
- d) Hyper Text Transfer Protocol Secure

Answer: d

Explanation: Hyper Text Transfer Protocol Secure (HTTPS) is a security protocol which maintains security when data is sent from browser to server and vice versa. It denotes that all communication setup between the browser and the server is encrypted.

7. SSL primarily focuses on \_\_\_\_\_

- a) integrity and authenticity
- b) integrity and non-repudiation
- c) authenticity and privacy
- d) confidentiality and integrity

Answer: a

Explanation: SSL primarily focuses on maintaining the integrity of the data. Also, it maintains authenticity which helps the customers feel secure to communicate over the internet.

8. In SSL, what is used for authenticating a message?

- a) MAC (Message Access Code)
- b) MAC (Message Authentication Code)

- c) MAC (Machine Authentication Code)
- d) MAC (Machine Access Code)

Answer: b

Explanation: For authenticating in SSL, a short message known as MAC (Message Authentication Code) is used for authenticating a message; where both the sender & the receiver need to implement the same key in order to start communicating.

9. \_\_\_\_\_ is used for encrypting data at network level.

- a) IPSec
- b) HTTPS
- c) SMTP
- d) S/MIME

Answer: a

Explanation: IPSec (Secure Internet Protocol) is used for securing data at the network level by using 3 different protocols. These are Encapsulating Secure Payload (ESP), Authentication Header, and Internet Key Exchange (IKE).

10. S/MIME is abbreviated as \_\_\_\_\_

- a) Secure/Multimedia Internet Mailing Extensions
- b) Secure/Multipurpose Internet Mailing Extensions
- c) Secure/Multimedia Internet Mail Extensions
- d) Secure/Multipurpose Internet Mail Extensions

Answer: d

Explanation: Secure/Multipurpose Internet Mail Extensions is the most popular protocol used to send encrypted messages that are digitally signed. In this protocol, the encryption is done with a digital sign in them.

11. S/MIME stands for \_\_\_\_\_.

- a. standard multipurpose internet mail extensions.
- b. secure multipurpose internet mail extensions.
- c. secure multipurpose international mail extensions.
- d. standard multipurpose international mail extensions.

Answer: B.

12. \_\_\_\_\_ uniquely identifies the MIME entities uniquely with reference to multiple contexts.

- a. Content description.
- b. Content -id.
- c. Content type.
- d. Content transfer encoding.

Answer: B.

13. The processed S/MIME along with security related data is called as \_\_\_\_\_.

- a. public key cryptography standard.
- b. private key cryptography standard.
- c. S/MIME.

d. MIME.

Answer: A.

14. In S/MIME, MLA stands for \_\_\_\_\_.

- a. mailing list agent.
- b. multipurpose list agent.
- c. mail lock agent.
- d. message link agent.

Answer: A.

15. The cryptography algorithms used in S/MIME are \_\_\_\_\_.

- a. IDEA.
- b. RC4.
- c. RSA,DES-3.
- d. RC5.

Answer: C.

16. The \_\_\_\_\_ acts as financial institutions who provides a payment card to a card holder.

- a. payment gateway.
- b. card holder.
- c. acquirer.
- d. issuer.

Answer: D.

17. Who will be responsible for processing the payment from the customer's account to the merchant account?

- a. Acquirer.
- b. Merchant.
- c. Issuer.
- d. Payment gateway.

Answer: D.

18. The cardholder combines the PIMD and OIMD and hashes them together to form \_\_\_\_\_.

- a. OPMD.
- b. POMD.
- c. MD.
- d. DS.

Answer: B.

19. Which process will ensure that the issues of the credit card is an approved transactions?

- a. Payment capture.
- b. Payment authorization.
- c. Purchase request.
- d. Purchase reply.

Answer: B.

20. \_\_\_\_\_ is used for hiding the payment information from the merchant.

- a. SET.
- b. SSL.
- c. SHTTP.
- d. TSP.

Answer: A.

### **3.IPSEC**

1. IPSec is designed to provide security at the \_\_\_\_\_

- a) Transport layer
- b) Network layer
- c) Application layer
- d) Session layer

Answer: b

Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. In the TCP/IP model, it provides security at the IP layer i.e. the network layer.

2. In tunnel mode, IPSec protects the \_\_\_\_\_

- a) Entire IP packet
- b) IP header
- c) IP payload
- d) IP trailer

Answer: a

Explanation: In the tunnel mode, IPSec adds control bits into the packets to encrypt the entire packet between the IPSec endpoints. Using encryption, it provides secure communication between the two endpoints.

3. Which component is included in IP security?

- a) Authentication Header (AH)
- b) Encapsulating Security Payload (ESP)
- c) Internet key Exchange (IKE)
- d) All of the mentioned

Answer: d

Explanation: AH ensures that there is no retransmission of data from an unauthorized source, and protects against data tampering. ESP provides with content protection and ensures that there is integrity and confidentiality for the message. IKE is used to make sure that only the intended sender and receiver can access the message.

4. Pretty good privacy (PGP) is used in \_\_\_\_\_

- a) Browser security
- b) Email security
- c) FTP security

d) WiFi security

Answer: b

Explanation: PGP is an encryption method used in e-mail security to encrypt and decrypt the content of an e-mail transmitted over the internet. It makes sure that the message cannot be stolen by other unauthorized users.

5. PGP encrypts data by using a block cipher called \_\_\_\_\_

- a) International data encryption algorithm
- b) Private data encryption algorithm
- c) Internet data encryption algorithm
- d) Local data encryption algorithm

Answer: a

Explanation: The IDEA was designed in 1991 by Xuejia Lai and James Massey. Before IDEA, PGP used the cipher method BassOmatic.

## VPN

1. A \_\_\_\_\_ is an extension of an enterprise's private intranet across a public network such as the internet, creating a secure private connection.

- a) VNP
- b) VPN
- c) VSN
- d) VSPN

Answer: b

Explanation: VPN provides enhanced security and online anonymity to users on the internet. It is also used to unblock websites that are unavailable in certain regions.

2. When were VPNs introduced into the commercial world?

- a) Early 80's
- b) Late 80's
- c) Early 90's
- d) Late 90's

Answer: d

Explanation: VPNs were first introduced in the year 1996. Then as the internet started to get popularized, the need for connection security increased. VPN was a great solution to this, and that's when VPNs were implemented in the commercial world.

3. What protocol is NOT used in the operation of a VPN?

- a) PPTP
- b) IPsec
- c) YMUM
- d) L2TP

Answer: c

Explanation: PPTP is a tunneling protocol which was initially used for the creation of VPNs.

IPSec is used in encrypting the traffic flowing in the VPN. L2TP is used to tunnel all the L2 traffic on the VPN.

4. Which of the following statements is NOT true concerning VPNs?

- a) Financially rewarding compared to leased lines
- b) Allows remote workers to access corporate data
- c) Allows LAN-to-LAN connectivity over public networks
- d) Is the backbone of the Internet

Answer: d

Explanation: VPNs are not the backbone of the Internet as they are just a method to create private intranets on the internet. They are used for enhancing the connection security for the users.

5. Traffic in a VPN is NOT \_\_\_\_\_

- a) Invisible from public networks
- b) Logically separated from other traffic
- c) Accessible from unauthorized public networks
- d) Restricted to a single protocol in IPsec

Answer: c

Explanation: Traffic in a VPN is not accessible from any unauthorized public networks because it is secured with the masking IP address. This provides the benefit of access to blocked resources to the users.

6. VPNs are financially speaking \_\_\_\_\_

- a) Always more expensive than leased lines
- b) Always cheaper than leased lines
- c) Usually cheaper than leased lines
- d) Usually more expensive than leased lines

7. Which layer 3 protocols can be transmitted over an L2TP VPN?

- a) Only IP
- b) Only IPX
- c) Only ICMP
- d) IP and IPX

Answer: d

Explanation: L2TP stands for Layer 2 Tunneling Protocol. It is used to tunnel all the L2 traffic on an IP network and is able to transmit network layer's IP and IPX protocol data.

8. ESP (Encapsulating Security Protocol) is defined in which of the following standards?

- a) IPsec
- b) PPTP
- c) PPP
- d) L2TP

Answer: a

Explanation: ESP is a security component of IPSec. ESP provides content protection and

ensures that there is integrity and confidentiality of the message. The other security components of IPSec are Authentication Header and Internet Key Exchange.

9. L2F was developed by which company?

- a) Microsoft
- b) Cisco
- c) Blizzard Entertainment
- d) IETF

Answer: b

Explanation: L2F stands for Layer 2 Forwarding protocol. It was designed by Cisco to tunnel PPP traffic, helping create VPNs over the internet.

10. Which layer of the OSI reference model does PPTP work at?

- a) Layer 1
- b) Layer 2
- c) Layer 3
- d) Layer 4

Answer: b

Explanation: PPTP stands for Point-to-Point Tunneling Protocol. PPTP is a tunneling protocol that was primitively used to create VPNs. It is no longer used for VPNs due to the lack of security it provides.

11. Which layer of the OSI reference model does IPsec work at?

- a) Layer 1
- b) Layer 2
- c) Layer 3
- d) Layer 4

Answer: c

Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. It operates in the network layer.

1 . \_\_\_\_\_ is a collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level.

- A. IPSec
- B. SSL
- C. PGP
- D. none of the above

Correct Answer :

**IPSec**

[View Answer](#)

2 . \_\_\_\_\_ operates in the transport mode or the tunnel mode.

- A. IPSec
- B. SSL
- C. PGP
- D. none of the above

Correct Answer :

**IPSec**

3 . In the \_\_\_\_\_ mode, IPSec protects information delivered from the transport layer to the network layer.

- A. transport
- B. tunnel
- C. either (a) or (b)
- D. neither (a) nor (b)

Correct Answer :

**transport**

[View Answer](#)

4 . IPSec in the \_\_\_\_\_ mode does not protect the IP header.

- A. transport
- B. tunnel
- C. either (a) or (b)
- D. neither (a) nor (b)

Correct Answer :

**transport**

"|

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
((OPTION_A)) THIS IS MANDATORY OPTION	Network Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Database Security
((OPTION_C)) This is optional	Information Security
((OPTION_D)) This is optional	Physical Security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information from alteration, destruction, deletion or disclosure by unauthorised users.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a threat to information security?
((OPTION_A)) THIS IS MANDATORY OPTION	Disaster
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Eavesdropping
((OPTION_C)) This is optional	Information leakage
((OPTION_D)) This is optional	Unchanged default password
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Disaster, eavesdropping and information leakage come under information security threats whereas not changing the default password of any system, hardware or any software comes under the category of vulnerabilities that the user may pose to its system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a vulnerability to information security?
((OPTION_A))  THIS IS MANDATORY OPTION	flood
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	without deleting data, disposal of storage media
((OPTION_C))  This is optional	unchanged default password
((OPTION_D))  This is optional	latest patches and updates not done
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Compromising confidential information comes under
((OPTION_A)) THIS IS MANDATORY OPTION	Bug
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Threat
((OPTION_C)) This is optional	Vulnerability
((OPTION_D)) This is optional	Attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	Threats are anything that may cause damage or harm to a computer system, individual or any information. Compromising of confidential information means extracting out sensitive data from a system by illegal manner.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Lack of access control policy is a
((OPTION_A)) THIS IS MANDATORY OPTION	Bug
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Threat
((OPTION_C)) This is optional	Vulnerability
((OPTION_D)) This is optional	Attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Access control policies are incorporated to a security system for restricting of unauthorised access to any logical or physical system. Every security compliance program must need this as a fundamental component. Those systems which lack this feature is vulnerable.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Possible threat to any information cannot be
((OPTION_A)) THIS IS MANDATORY OPTION	reduced
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transferred
((OPTION_C)) This is optional	protected
((OPTION_D)) This is optional	ignored
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	When there lies a threat to any system, safeguards can be implemented, outsourced, distributed or transferred to some other system, protected using security tools and techniques but cannot be ignored.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	According to the CIA Triad, which of the below-mentioned element is not considered in the triad?
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authenticity
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	According to the CIA triad the three components that a security need is the Confidentiality, Integrity, Availability (as in short read as

		
CIA).		

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When you use the word _____ it means you are protecting your data from getting disclosed.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	

((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Confidentiality is what every individual prefer in terms of physical privacy as well as digital privacy. This term means our information needs to be protected from getting disclose to unauthorised parties, for which we use different security mechanisms like password protection, biometric security, OTPs (One Time Passwords) etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ means the protection of data from modification by unknown users.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	Non-repudiation
((OPTION_E)) This is optional. If optional keep empty so that system will skip	

this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	A information only seems valuable if it is correct and do not get modified during its journey in the course of arrival. The element integrity makes sure that the data sent or generated from other end is correct and is not modified by any unauthorised party in between.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When integrity is lacking in a security system, _____ occurs.
((OPTION_A)) THIS IS MANDATORY OPTION	Database hacking
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data deletion
((OPTION_C)) This is optional	Data tampering
((OPTION_D)) This is optional	Data leakage
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The term data tampering is used when integrity is compromised in any security model and checking its integrity later becomes costlier. Example: let suppose you sent \$50 to an authorised person and in between a Man in the Middle (MiTM) attack takes place and the value has tampered to \$500. This is how integrity is compromised.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	of information means, only authorised users are capable of accessing the information.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Non-repudiation
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional.	

If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Information seems useful only when right people (authorised users) access it after going through proper authenticity check. The key element availability ensures that only authorised users are able to access the information.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?
((OPTION_A)) THIS IS MANDATORY OPTION	They help understanding hacking better
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	They are key elements to a security breach
((OPTION_C)) This is optional	They help understands security and its components better
((OPTION_D)) This is optional	They help to understand the cyber-crime better
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The four elements of security viz. confidentiality, integrity, authenticity & availability helps in better understanding the pillars of security and its different components.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	This helps in identifying the origin of information and authentic user. This referred to here as
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authenticity
((OPTION_D)) This is optional	Availability
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The key element, authenticity helps in assuring the fact that the information is from the original source.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Data _____ is used to ensure confidentiality.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Locking
((OPTION_C)) This is optional	Deleting
((OPTION_D)) This is optional	Backup
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Data encryption is the method of converting plain text to cipher-text and only authorised users can decrypt the message back to plain text. This preserves the confidentiality of data

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of these is not a proper method of maintaining AUTHENTICATION?
((OPTION_A)) THIS IS MANDATORY OPTION	Biometric verification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ID and password based verification
((OPTION_C)) This is optional	2-factor authentication
((OPTION_D)) This is optional	switching off the phone
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Switching off the phone in the fear of preserving the confidentiality of data is not a proper solution for data confidentiality. Fingerprint detection, face recognition, password-based authentication, two-step verifications are some of these.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Data integrity gets compromised when _____ and _____ are taken control off.
((OPTION_A)) THIS IS MANDATORY OPTION	Access control, file deletion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Network, file permission
((OPTION_C)) This is optional	Access control, file permission
((OPTION_D)) This is optional	Network, system

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The two key ingredients that need to be kept safe are: access control & file permission in order to preserve data integrity.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	One common way to maintain data availability is
((OPTION_A)) THIS IS MANDATORY OPTION	Data clustering
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data backup
((OPTION_C)) This is optional	Data recovery
((OPTION_D)) This is optional	Data Altering

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	For preventing data from data-loss, or damage data backup can be done and stored in a different geographical location so that it can sustain its data from natural disasters & unpredictable events.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as
((OPTION_A)) THIS IS MANDATORY OPTION	Black Hat hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	White Hat Hackers
((OPTION_C)) This is optional	Grey Hat Hackers
((OPTION_D)) This is optional	Red Hat Hackers

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	White Hat Hackers are cyber security analysts and consultants who have the intent to help firms and Governments in the identification of loopholes as well as help to perform penetration tests for securing a system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the legal form of hacking based on which jobs are provided in IT industries and firms?
((OPTION_A)) THIS IS MANDATORY OPTION	Cracking
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Non ethical Hacking
((OPTION_C)) This is optional	Ethical hacking
((OPTION_D))	Hactivism

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Ethical Hacking is an ethical form of hacking done by white-hat hackers for performing penetration tests and identifying potential threats in any organizations and firms.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are "they" referred to here?
((OPTION_A)) THIS IS MANDATORY OPTION	Gray Hat Hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	White Hat Hackers
((OPTION_C)) This is optional	Hactivists
((OPTION_D))	Black Hat Hackers

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Black Hat hackers also termed as 'crackers' and are a major type of cyber criminals who take unauthorized access in user's account or system and steal sensitive data or inject malware into the system for their profit or to harm the organization.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are the combination of both white as well as black hat hackers.
((OPTION_A)) THIS IS MANDATORY OPTION	Grey Hat hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Green Hat hackers
((OPTION_C)) This is optional	Blue Hat Hackers

((OPTION_D)) This is optional	Red Hat Hacker
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Grey Hat Hackers have a blending character of both ethical as well as un-ethical hacker. They hack other's systems for fun but do not harm the system, exploits bugs and vulnerabilities in network without the knowledge of the admin or the owner.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The amateur or newbie in the field of hacking who don't have many skills about coding and in-depth working of security and hacking tools are called _____
((OPTION_A)) THIS IS MANDATORY OPTION	Sponsored Hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hactivists
((OPTION_C))	Script Kiddies

This is optional	
((OPTION_D))	Whistle Blowers
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Script Kiddies are new to hacking and at the same time do not have many interests in developing coding skills or find bugs of their own in systems; rather they prefer downloading of available tools (developed by elite hackers) and use them to break any system or network. They just try to gain attention of their friend circles.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Suicide Hackers are those _____
((OPTION_A)) THIS IS MANDATORY OPTION	who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their malicious activity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	individuals with no knowledge of codes but an expert in using hacking tools

((OPTION_C)) This is optional	who know the consequences of their hacking activities and hence try to prevent them by erasing their digital footprints
((OPTION_D)) This is optional	who are employed in an organization to do malicious activities on other firms
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Suicide hackers are those who break into any network or system with or without knowing the consequences of the cyber crime and its penalty. There are some suicide hackers who intentionally do crimes and get caught to bring their names in the headlines.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____
((OPTION_A)) THIS IS MANDATORY OPTION	State sponsored hackers
((OPTION_B)) THIS IS ALSO MANDATORY	Blue Hat Hackers

OPTION	
((OPTION_C)) This is optional	Cyber Terrorists
((OPTION_D)) This is optional	Red Hat Hackers
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Cyber Terrorists are very expert programmers and cyber criminals who hide themselves while doing malicious activities over the internet and they are smart enough to hide themselves or their tracks of action. They are hired for gaining unauthorised access to nation's data centres or break into the network of intelligence agencies.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are those individuals who maintain and handles IT security in any firm or organization.
((OPTION_A)) THIS IS MANDATORY OPTION	IT Security Engineer
((OPTION_B))	Cyber Security Interns

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Software Security Specialist
((OPTION_D)) This is optional	Security Auditor
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is an intermediary level of position of an individual in an organization or firm who builds and preserves different systems and its associated security tools of the firm of organization to which he/she belongs.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Role of security auditor is to _____
((OPTION_A)) THIS IS MANDATORY OPTION	secure the network

((OPTION_B)) THIS IS ALSO MANDATORY OPTION	probe for safety and security of organization's security components and systems
((OPTION_C)) This is optional	detects and prevents cyber attacks and threats to organization
((OPTION_D)) This is optional	does penetration testing on different web applications
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Security auditors are those who conduct auditing of various computer and network systems on an organization or company and reports the safety and security issues as well as helps in suggesting improvements or enhancements in any particular system that is threat prone.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are senior level corporate employees who have the role and responsibilities of creating and designing secured network or security structures.
((OPTION_A)) THIS IS MANDATORY	Ethical Hackers

OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Chief Technical Officer
((OPTION_C)) This is optional	IT Security Engineers
((OPTION_D)) This is optional	Security Architect
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Security architect are those senior grade employees of an organization who are in charge of building, designing, implementing and testing of secured network topologies, protocols as well as secured computers in an organization.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Governments hired some highly skilled hackers. These types of hackers are termed as _____
((OPTION_A)) THIS IS	Special Hackers

<b>MANDATORY OPTION</b>	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Government Hackers
((OPTION_C))  This is optional	Cyber Intelligence Agents
((OPTION_D))  This is optional	Nation / State sponsored hackers
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Nation / State sponsored hackers are specific individuals who are employed or hired by the government of that nation or state and protect the nation from cyber terrorists and other groups or individuals and to reveal their plans, communications and actions.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The full form of Malware is _____
((OPTION_A))	Malfunctioned Software

THIS IS MANDATORY OPTION	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Multipurpose Software
((OPTION_C))  This is optional	) Malicious Software
((OPTION_D))  This is optional	Malfunctioning of Security
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Different types of harmful software and programs that can pose threats to a system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransomware, spyware, worms, rootkits etc.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Who deploy Malwares to a system or network?

((OPTION_A)) THIS IS MANDATORY OPTION	Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Criminal organizations, gray hat hackers, Malware developers, Penetration testers
((OPTION_C)) This is optional	) Criminal organizations, Black hat hackers, software developers, cyber-terrorists
((OPTION_D)) This is optional	Criminal organizations, White hat hackers, malware developers, cyber-terrorists
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Criminal-minded organizations, groups and individuals cyber-terrorist groups, Black hat hackers, malware developers etc are those who can deploy malwares to any target system or network in order to deface that system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	_____ is a code injecting method used for attacking the database of a system / website.

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	HTML injection
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SQL Injection
((OPTION_C)) This is optional	Malicious code injection
((OPTION_D)) This is optional	XML Injection
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	SQLi (Structured Query Language Injection) is a popular attack where SQL code is targeted or injected; for breaking the web application having SQL vulnerabilities. This allows the attacker to run malicious code and take access to the database of that server.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN	This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?

CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	SQL injection
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	HTML Injection
((OPTION_C)) This is optional	Cross Site Scripting (XSS)
((OPTION_D)) This is optional	Cross Site Request Forgery (XSRF)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	XSS attack can be infused by putting the malicious code (which gets automatically run) in any comment section or feedback section of any webpage (usually a blogging page). This can hamper the reputation of a site and the attacker may place any private data or personal credentials.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	An attempt to harm, damage or cause threat to a system or network is broadly termed as _____

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A))  THIS IS MANDATORY OPTION	Cyber-crime
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Cyber Attack
((OPTION_C))  This is optional	System hijacking
((OPTION_D))  This is optional	Digital crime
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cyber attack is an umbrella term used to classify different computer & network attacks or activities such as extortion, identity theft, email hacking, digital spying, stealing hardware, mobile hacking and physical security breaching.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
((OPTION_A)) THIS IS MANDATORY OPTION	Network Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Database Security
((OPTION_C)) This is optional	Information Security
((OPTION_D)) This is optional	Physical Security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information from alteration, destruction, deletion or disclosure by unauthorised users.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a vulnerability to information security?
((OPTION_A))  THIS IS MANDATORY OPTION	flood
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	without deleting data, disposal of storage media
((OPTION_C))  This is optional	unchanged default password
((OPTION_D))  This is optional	latest patches and updates not done
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a set of conventions & rules set for communicating two or more devices residing in the same network?
((OPTION_A))  THIS IS MANDATORY OPTION	Security policies
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Protocols
((OPTION_C))  This is optional	Wireless network
((OPTION_D))  This is optional	Network algorithms
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Network protocols are designed with mechanisms for identifying devices and make connections between them. In addition, some proper rules are defined as to how data packets will be sent and received.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The field that covers a variety of computer networks, both public and private, that are used in everyday jobs
((OPTION_A)) THIS IS MANDATORY OPTION	Artificial Intelligence
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ML
((OPTION_C)) This is optional	Network Security
((OPTION_D)) This is optional	IT
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Network security covers a variety of computer networks, both private and public. Everyday jobs like conducting transactions and communications among business and government agencies etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Network Security provides authentication and access control for resources.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is not an objective of network security?
((OPTION_A)) THIS IS MANDATORY OPTION	Identification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Authentication
((OPTION_C)) This is optional	Access control
((OPTION_D)) This is optional	Lock
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The Identification, Authentication and Access control are the objectives of network security. There is no such thing called lock.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of these is a part of network identification?
((OPTION_A)) THIS IS MANDATORY OPTION	UserID
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Password
((OPTION_C)) This is optional	OTP
((OPTION_D)) This is optional	fingerprint
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The answer is UserID. UserID is a part of identification. UserID can be a combination of username, user student number etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The process of verifying the identity of a user.
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Identification
((OPTION_C)) This is optional	Validation
((OPTION_D)) This is optional	Verification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	It is called an authentication. It is typically based on passwords, smart card, fingerprint, etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Security features that control that can access resources in the OS
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Identification
((OPTION_C)) This is optional	Validation
((OPTION_D)) This is optional	Access control
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Access control refers to the security features. Applications call access control to provide resources

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm in encryption is called
((OPTION_A)) THIS IS MANDATORY OPTION	Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Procedure
((OPTION_C)) This is optional	Cipher
((OPTION_D)) This is optional	Module
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	An algorithm used in encryption is referred to as a cipher. cipher is an algorithm for performing encryption or decryption

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The information that gets transformed in encryption is
((OPTION_A)) THIS IS MANDATORY OPTION	Plain text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Parallel text
((OPTION_C)) This is optional	Encrypted text
((OPTION_D)) This is optional	Decrypted text
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The text that gets transformed is called plain text. The algorithm used is called cipher

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The type of threats on the security of a computer system or network are..... i) Interruption ii) Interception iii) Modification iv) Creation v) Fabrication
((OPTION_A)) THIS IS MANDATORY OPTION	i, ii, iii and iv only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii, iii, iv and v only
((OPTION_C)) This is optional	i, ii, iii and v only
((OPTION_D)) This is optional	All i, ii, iii, iv and v
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is computer threat?
((OPTION_A))  THIS IS MANDATORY OPTION	Phishing
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Soliciting
((OPTION_C))  This is optional	DoS attack
((OPTION_D))  This is optional	stalking
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a term used in cryptography that refers to a message before encryption or after decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PLAIN TEXT
((OPTION_C)) This is optional	Original text
((OPTION_D)) This is optional	Plain script
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ is encrypted text
((OPTION_A)) THIS IS MANDATORY OPTION	cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	cipher script
((OPTION_C)) This is optional	secret text
((OPTION_D)) This is optional	secret script
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An _____ along with a key is used in the encryption
((OPTION_A)) THIS IS MANDATORY OPTION	cryptography algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption algorithm
((OPTION_C)) This is optional	encryption algorithm
((OPTION_D)) This is optional	plain text algorithm
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them.
((OPTION_A)) THIS IS MANDATORY OPTION	Availability
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	Cryptography
((OPTION_D)) This is optional	Integrity
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that information are in a format that is true and correct to its original purposes.
((OPTION_A)) THIS IS MANDATORY OPTION	Availability
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	integrity
((OPTION_D)) This is optional	cryptography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that information and resources are available to those who need them.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Availability</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Confidentiality</b>
((OPTION_C)) This is optional	<b>Cryptography</b>
((OPTION_D)) This is optional	<b>Integrity</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the process of identifying an individual, usually based on a username and password.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Authentication</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Authorization</b>
((OPTION_C)) This is optional	<b>either authentication or authorization</b>
((OPTION_D)) This is optional	<b>neither authentication nor authorization</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the process of giving individuals access to system objects based on their identity.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Authentication</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Authorization</b>
((OPTION_C)) This is optional	<b>either authentication or authorization</b>
((OPTION_D)) This is optional	<b>neither congestion control nor quality of service</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	when someone gains access to a server, website, or other sensitive data using someone else's account details called as
((OPTION_A)) THIS IS MANDATORY OPTION	Authorized access
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Access control
((OPTION_C)) This is optional	Unauthorized access
((OPTION_D)) This is optional	access
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.called as
((OPTION_A)) THIS IS MANDATORY OPTION	Thief
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	hacker
((OPTION_C)) This is optional	attacker
((OPTION_D)) This is optional	criminal
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is an action or event that might compromise the security.
((OPTION_A))  THIS IS MANDATORY OPTION	Threat
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Vulnerability
((OPTION_C))  This is optional	Protect
((OPTION_D))  This is optional	attack
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system
((OPTION_A)) THIS IS MANDATORY OPTION	threat
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Vulnerability
((OPTION_C)) This is optional	Attack
((OPTION_D)) This is optional	Protection
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is a software that operates on different OS which is used to prevent from malicious software.
((OPTION_A)) THIS IS MANDATORY OPTION	Anti virus
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	virus
((OPTION_C)) This is optional	protocol
((OPTION_D)) This is optional	risk
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is a technique that a hacker uses to stole data by a person for different purposes by psychological manipulation combined with social scenes.
((OPTION_A)) THIS IS MANDATORY OPTION	Social Engineering
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IT engineering
((OPTION_C)) This is optional	Psycology
((OPTION_D)) This is optional	Social engineering
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is a software or hardware which is used to filter network traffic based on rules.
((OPTION_A)) THIS IS MANDATORY OPTION	antivirus
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	firewall
((OPTION_C)) This is optional	protocol
((OPTION_D)) This is optional	keylogger
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not Basic Functions of Antivirus Engines
((OPTION_A)) THIS IS MANDATORY OPTION	Scanning
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity Checking
((OPTION_C)) This is optional	Interception
((OPTION_D)) This is optional	Evesdropping
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is name of antivirus
((OPTION_A))  THIS IS MANDATORY OPTION	AVG
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	PAN
((OPTION_C))  This is optional	SACK
((OPTION_D))  This is optional	FIREP
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Hacking tools that can be found very easily by everyone just by googling and they are endless.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Potential Losses due to Security Attacks doesn't involve _____
((OPTION_A)) THIS IS MANDATORY OPTION	Losing your data
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Bad usage of your computer resources
((OPTION_C)) This is optional	Reputation gain
((OPTION_D)) This is optional	Identity theft
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Reputation loss is part of it and not gain

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not malware category?
((OPTION_A))  THIS IS MANDATORY OPTION	Worms
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Viruses
((OPTION_C))  This is optional	Trojans
((OPTION_D))  This is optional	None of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	All are malware categories

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ encrypts all your data when your computer gets infected and the second is to roll back the data at a specific time you want.
((OPTION_A)) THIS IS MANDATORY OPTION	ransomware
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	firmware
((OPTION_C)) This is optional	middleware
((OPTION_D)) This is optional	Cyber ware
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	this network is created between two secure network devices like two firewalls.
((OPTION_A)) THIS IS MANDATORY OPTION	LAN
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MAN
((OPTION_C)) This is optional	VPN
((OPTION_D)) This is optional	WAN
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Virtual private network

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Name of the attack when integrity is compromised is called as _____
((OPTION_A))  THIS IS MANDATORY OPTION	Fabrication
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	interception
((OPTION_C))  This is optional	Interruption
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Attack made on confidentiality is __
((OPTION_A))  THIS IS MANDATORY OPTION	interception
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C))  This is optional	interruption
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	an attack on availability such as a denial of service attack (or DOS)
((OPTION_A))  THIS IS MANDATORY OPTION	Interruption
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Interception
((OPTION_C))  This is optional	fabrication
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An unauthorized party inserts counterfeit objects into the system and basically attacks the authenticity of the system.
((OPTION_A)) THIS IS MANDATORY OPTION	modification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C)) This is optional	interception
((OPTION_D)) This is optional	interruption
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Attack in which a network service is made degraded or unavailable for legitimate use
((OPTION_A)) THIS IS MANDATORY OPTION	Interruption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C)) This is optional	interception
((OPTION_D)) This is optional	modification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is assurance that someone cannot deny something.
((OPTION_A))  THIS IS MANDATORY OPTION	availability
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	confidentiality
((OPTION_C))  This is optional	Access control
((OPTION_D))  This is optional	Non-repudiation
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the purpose of a Denial of Service attack?
((OPTION_A))  THIS IS MANDATORY OPTION	Exploit a weakness in the TCP/IP stack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	To execute a Trojan on a system
((OPTION_C))  This is optional	To overload a system so it is no longer operational
((OPTION_D))  This is optional	To shutdown services by turning them off
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	DoS attacks force systems to stop responding by overloading the processing of the system

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What are some of the most common vulnerabilities that exist in a network or system?
((OPTION_A)) THIS IS MANDATORY OPTION	Changing manufacturer, or recommended, settings of a newly installed application.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additional unused features on commercial software packages
((OPTION_C)) This is optional	Utilizing open source application code
((OPTION_D)) This is optional	Balancing security concerns with functionality and ease of use of a system.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Linux is an open source code and considered to have greater security than the commercial Windows environment

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Sniffing is used to perform _____ fingerprinting
((OPTION_A))  THIS IS MANDATORY OPTION	Passive stack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Active stack
((OPTION_C))  This is optional	Passive banner grabbing
((OPTION_D))  This is optional	Scanned
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Passive stack fingerprinting uses sniffing technologies instead of scanning

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a principle of data security?
((OPTION_A)) THIS IS MANDATORY OPTION	Data Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following attacks is a passive attack?
((OPTION_A))  THIS IS MANDATORY OPTION	Masquerade
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Modification of message
((OPTION_C))  This is optional	Denial of service
((OPTION_D))  This is optional	Traffic analysis
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	In a passive attack, the attacker does not modify any part of the data. His attempt is only to obtain the information and not to modify it. From the mentioned options, this happens only in Traffic analysis in which the attacker monitors the pattern of transmission. The rest other options are examples of active attacks.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options correctly defines the Brute force attack?
((OPTION_A)) THIS IS MANDATORY OPTION	Brutally forcing the user to share the useful information like pins and passwords.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Trying every possible key to decrypt the message.
((OPTION_C)) This is optional	One entity pretends to be some other entity
((OPTION_D)) This is optional	The message or information is modified before sending it to the receiver.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	Integer value
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Square matrix
((OPTION_C)) This is optional	An array of characters
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems is called as
((OPTION_A)) THIS IS MANDATORY OPTION	Network security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Information security
((OPTION_C)) This is optional	Cyber security
((OPTION_D)) This is optional	Internet security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	phishing and pre-texting is part of _____
((OPTION_A)) THIS IS MANDATORY OPTION	<b>NETWORK SECURITY</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>CYBER SECURITY</b>
((OPTION_C)) This is optional	Internet security
((OPTION_D)) This is optional	Internet security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures to protect the transit data only.
((OPTION_A))  THIS IS MANDATORY OPTION	NETWORK SECURITY
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Internet security
((OPTION_C))  This is optional	Information security
((OPTION_D))  This is optional	Cyber security
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is danger for <b>Integrity</b> as well as <b>availability</b> .
((OPTION_A)) THIS IS MANDATORY OPTION	Active attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ is danger for <b>Confidentiality</b> .
((OPTION_A)) THIS IS MANDATORY OPTION	Active attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ attack attention is on detection.
((OPTION_A))  THIS IS MANDATORY OPTION	Passive attack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Active Attack
((OPTION_C))  This is optional	Both
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	in _____ attack attention is on prevention.
((OPTION_A))  THIS IS MANDATORY OPTION	Active attack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C))  This is optional	Both
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Due to ___ attack system is always damaged.
((OPTION_A))  THIS IS MANDATORY OPTION	Active
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C))  This is optional	Both active and passive
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	due to _____ attack, there is no any harm to the system.
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	Both active and passive
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ attack is tough to restrict from entering systems or networks.
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	Both active and passive
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Attack is easy to prohibited in comparison to _____ attack.
((OPTION_A))  THIS IS MANDATORY OPTION	Active,passive
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive,active
((OPTION_C))  This is optional	
((OPTION_D))  This is optional	
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not active attack
((OPTION_A)) THIS IS MANDATORY OPTION	Denial of service (DoS)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	replay
((OPTION_C)) This is optional	Trojans
((OPTION_D)) This is optional	traffic analysis
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In __ <b>attack</b> , an attacker tries to modify the content of the messages.
((OPTION_A))  THIS IS MANDATORY OPTION	Active
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C))  This is optional	
((OPTION_D))  This is optional	
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	in _____ <b>attack</b> , an attacker observes the messages, copy them and may use them for malicious purposes
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is state of being free from potential threats or dangers
((OPTION_A)) THIS IS MANDATORY OPTION	privacy
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	freedom
((OPTION_C)) This is optional	security
((OPTION_D)) This is optional	independence
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ refers to the state of being free from unwanted attention.
((OPTION_A)) THIS IS MANDATORY OPTION	Freedom
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Security
((OPTION_C)) This is optional	Privacy
((OPTION_D)) This is optional	independence
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ can be achieved without _____ but _____ cannot be achieved without _____.
((OPTION_A)) THIS IS MANDATORY OPTION	Security,privacy,privacy security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Privacy,security,security,privacy
((OPTION_C)) This is optional	Security,privacy,privacy,privacy
((OPTION_D)) This is optional	Security,security,privacy,security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ program refers to a set of protocols and regulations set in place to protect all the confidential information assets and resources that an organization collects and owns.
((OPTION_A)) THIS IS MANDATORY OPTION	Privacy
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Security
((OPTION_C)) This is optional	Security and privacy
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ program focuses on protecting only personal information such as log in credentials, passwords, etc.
((OPTION_A)) THIS IS MANDATORY OPTION	Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Privacy
((OPTION_C)) This is optional	Security and privacy
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
((OPTION_A)) THIS IS MANDATORY OPTION	Network Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Database Security
((OPTION_C)) This is optional	Information Security
((OPTION_D)) This is optional	Physical Security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information from alteration, destruction, deletion or disclosure by unauthorised users.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a threat to information security?
((OPTION_A)) THIS IS MANDATORY OPTION	Disaster
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Eavesdropping
((OPTION_C)) This is optional	Information leakage
((OPTION_D)) This is optional	Unchanged default password
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Disaster, eavesdropping and information leakage come under information security threats whereas not changing the default password of any system, hardware or any software comes under the category of vulnerabilities that the user may pose to its system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a vulnerability to information security?
((OPTION_A))  THIS IS MANDATORY OPTION	flood
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	without deleting data, disposal of storage media
((OPTION_C))  This is optional	unchanged default password
((OPTION_D))  This is optional	latest patches and updates not done
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Compromising confidential information comes under
((OPTION_A)) THIS IS MANDATORY OPTION	Bug
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Threat
((OPTION_C)) This is optional	Vulnerability
((OPTION_D)) This is optional	Attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	Threats are anything that may cause damage or harm to a computer system, individual or any information. Compromising of confidential information means extracting out sensitive data from a system by illegal manner.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Lack of access control policy is a
((OPTION_A)) THIS IS MANDATORY OPTION	Bug
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Threat
((OPTION_C)) This is optional	Vulnerability
((OPTION_D)) This is optional	Attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Access control policies are incorporated to a security system for restricting of unauthorised access to any logical or physical system. Every security compliance program must need this as a fundamental component. Those systems which lack this feature is vulnerable.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Possible threat to any information cannot be
((OPTION_A)) THIS IS MANDATORY OPTION	reduced
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transferred
((OPTION_C)) This is optional	protected
((OPTION_D)) This is optional	ignored
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	When there lies a threat to any system, safeguards can be implemented, outsourced, distributed or transferred to some other system, protected using security tools and techniques but cannot be ignored.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	According to the CIA Triad, which of the below-mentioned element is not considered in the triad?
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authenticity
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	According to the CIA triad the three components that a security need is the Confidentiality, Integrity, Availability (as in short read as

		
CIA).		

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When you use the word _____ it means you are protecting your data from getting disclosed.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	

((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Confidentiality is what every individual prefer in terms of physical privacy as well as digital privacy. This term means our information needs to be protected from getting disclose to unauthorised parties, for which we use different security mechanisms like password protection, biometric security, OTPs (One Time Passwords) etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ means the protection of data from modification by unknown users.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	Non-repudiation
((OPTION_E)) This is optional. If optional keep empty so that system will skip	

this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	A information only seems valuable if it is correct and do not get modified during its journey in the course of arrival. The element integrity makes sure that the data sent or generated from other end is correct and is not modified by any unauthorised party in between.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When integrity is lacking in a security system, _____ occurs.
((OPTION_A)) THIS IS MANDATORY OPTION	Database hacking
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data deletion
((OPTION_C)) This is optional	Data tampering
((OPTION_D)) This is optional	Data leakage
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The term data tampering is used when integrity is compromised in any security model and checking its integrity later becomes costlier. Example: let suppose you sent \$50 to an authorised person and in between a Man in the Middle (MiTM) attack takes place and the value has tampered to \$500. This is how integrity is compromised.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	of information means, only authorised users are capable of accessing the information.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Non-repudiation
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional.	

If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Information seems useful only when right people (authorised users) access it after going through proper authenticity check. The key element availability ensures that only authorised users are able to access the information.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?
((OPTION_A)) THIS IS MANDATORY OPTION	They help understanding hacking better
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	They are key elements to a security breach
((OPTION_C)) This is optional	They help understands security and its components better
((OPTION_D)) This is optional	They help to understand the cyber-crime better
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The four elements of security viz. confidentiality, integrity, authenticity & availability helps in better understanding the pillars of security and its different components.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	This helps in identifying the origin of information and authentic user. This referred to here as
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authenticity
((OPTION_D)) This is optional	Availability
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The key element, authenticity helps in assuring the fact that the information is from the original source.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Data _____ is used to ensure confidentiality.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Locking
((OPTION_C)) This is optional	Deleting
((OPTION_D)) This is optional	Backup
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Data encryption is the method of converting plain text to cipher-text and only authorised users can decrypt the message back to plain text. This preserves the confidentiality of data

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of these is not a proper method of maintaining AUTHENTICATION?
((OPTION_A)) THIS IS MANDATORY OPTION	Biometric verification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ID and password based verification
((OPTION_C)) This is optional	2-factor authentication
((OPTION_D)) This is optional	switching off the phone
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Switching off the phone in the fear of preserving the confidentiality of data is not a proper solution for data confidentiality. Fingerprint detection, face recognition, password-based authentication, two-step verifications are some of these.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Data integrity gets compromised when _____ and _____ are taken control off.
((OPTION_A)) THIS IS MANDATORY OPTION	Access control, file deletion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Network, file permission
((OPTION_C)) This is optional	Access control, file permission
((OPTION_D)) This is optional	Network, system

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The two key ingredients that need to be kept safe are: access control & file permission in order to preserve data integrity.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	One common way to maintain data availability is
((OPTION_A)) THIS IS MANDATORY OPTION	Data clustering
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data backup
((OPTION_C)) This is optional	Data recovery
((OPTION_D)) This is optional	Data Altering

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	For preventing data from data-loss, or damage data backup can be done and stored in a different geographical location so that it can sustain its data from natural disasters & unpredictable events.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as
((OPTION_A)) THIS IS MANDATORY OPTION	Black Hat hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	White Hat Hackers
((OPTION_C)) This is optional	Grey Hat Hackers
((OPTION_D)) This is optional	Red Hat Hackers

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	White Hat Hackers are cyber security analysts and consultants who have the intent to help firms and Governments in the identification of loopholes as well as help to perform penetration tests for securing a system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the legal form of hacking based on which jobs are provided in IT industries and firms?
((OPTION_A)) THIS IS MANDATORY OPTION	Cracking
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Non ethical Hacking
((OPTION_C)) This is optional	Ethical hacking
((OPTION_D))	Hactivism

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Ethical Hacking is an ethical form of hacking done by white-hat hackers for performing penetration tests and identifying potential threats in any organizations and firms.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are "they" referred to here?
((OPTION_A)) THIS IS MANDATORY OPTION	Gray Hat Hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	White Hat Hackers
((OPTION_C)) This is optional	Hactivists
((OPTION_D))	Black Hat Hackers

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Black Hat hackers also termed as 'crackers' and are a major type of cyber criminals who take unauthorized access in user's account or system and steal sensitive data or inject malware into the system for their profit or to harm the organization.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are the combination of both white as well as black hat hackers.
((OPTION_A)) THIS IS MANDATORY OPTION	Grey Hat hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Green Hat hackers
((OPTION_C)) This is optional	Blue Hat Hackers

((OPTION_D)) This is optional	Red Hat Hacker
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Grey Hat Hackers have a blending character of both ethical as well as un-ethical hacker. They hack other's systems for fun but do not harm the system, exploits bugs and vulnerabilities in network without the knowledge of the admin or the owner.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The amateur or newbie in the field of hacking who don't have many skills about coding and in-depth working of security and hacking tools are called _____
((OPTION_A)) THIS IS MANDATORY OPTION	Sponsored Hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hactivists
((OPTION_C))	Script Kiddies

This is optional	
((OPTION_D))	Whistle Blowers
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Script Kiddies are new to hacking and at the same time do not have many interests in developing coding skills or find bugs of their own in systems; rather they prefer downloading of available tools (developed by elite hackers) and use them to break any system or network. They just try to gain attention of their friend circles.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Suicide Hackers are those _____
((OPTION_A)) THIS IS MANDATORY OPTION	who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their malicious activity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	individuals with no knowledge of codes but an expert in using hacking tools

((OPTION_C)) This is optional	who know the consequences of their hacking activities and hence try to prevent them by erasing their digital footprints
((OPTION_D)) This is optional	who are employed in an organization to do malicious activities on other firms
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Suicide hackers are those who break into any network or system with or without knowing the consequences of the cyber crime and its penalty. There are some suicide hackers who intentionally do crimes and get caught to bring their names in the headlines.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____
((OPTION_A)) THIS IS MANDATORY OPTION	State sponsored hackers
((OPTION_B)) THIS IS ALSO MANDATORY	Blue Hat Hackers

OPTION	
((OPTION_C)) This is optional	Cyber Terrorists
((OPTION_D)) This is optional	Red Hat Hackers
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Cyber Terrorists are very expert programmers and cyber criminals who hide themselves while doing malicious activities over the internet and they are smart enough to hide themselves or their tracks of action. They are hired for gaining unauthorised access to nation's data centres or break into the network of intelligence agencies.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are those individuals who maintain and handles IT security in any firm or organization.
((OPTION_A)) THIS IS MANDATORY OPTION	IT Security Engineer
((OPTION_B))	Cyber Security Interns

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Software Security Specialist
((OPTION_D)) This is optional	Security Auditor
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is an intermediary level of position of an individual in an organization or firm who builds and preserves different systems and its associated security tools of the firm of organization to which he/she belongs.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Role of security auditor is to _____
((OPTION_A)) THIS IS MANDATORY OPTION	secure the network

((OPTION_B)) THIS IS ALSO MANDATORY OPTION	probe for safety and security of organization's security components and systems
((OPTION_C)) This is optional	detects and prevents cyber attacks and threats to organization
((OPTION_D)) This is optional	does penetration testing on different web applications
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Security auditors are those who conduct auditing of various computer and network systems on an organization or company and reports the safety and security issues as well as helps in suggesting improvements or enhancements in any particular system that is threat prone.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are senior level corporate employees who have the role and responsibilities of creating and designing secured network or security structures.
((OPTION_A)) THIS IS MANDATORY	Ethical Hackers

OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Chief Technical Officer
((OPTION_C)) This is optional	IT Security Engineers
((OPTION_D)) This is optional	Security Architect
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Security architect are those senior grade employees of an organization who are in charge of building, designing, implementing and testing of secured network topologies, protocols as well as secured computers in an organization.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Governments hired some highly skilled hackers. These types of hackers are termed as _____
((OPTION_A)) THIS IS	Special Hackers

<b>MANDATORY OPTION</b>	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Government Hackers
((OPTION_C))  This is optional	Cyber Intelligence Agents
((OPTION_D))  This is optional	Nation / State sponsored hackers
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Nation / State sponsored hackers are specific individuals who are employed or hired by the government of that nation or state and protect the nation from cyber terrorists and other groups or individuals and to reveal their plans, communications and actions.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The full form of Malware is _____
((OPTION_A))	Malfunctioned Software

THIS IS MANDATORY OPTION	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Multipurpose Software
((OPTION_C))  This is optional	) Malicious Software
((OPTION_D))  This is optional	Malfunctioning of Security
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Different types of harmful software and programs that can pose threats to a system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransomware, spyware, worms, rootkits etc.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Who deploy Malwares to a system or network?

((OPTION_A)) THIS IS MANDATORY OPTION	Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Criminal organizations, gray hat hackers, Malware developers, Penetration testers
((OPTION_C)) This is optional	) Criminal organizations, Black hat hackers, software developers, cyber-terrorists
((OPTION_D)) This is optional	Criminal organizations, White hat hackers, malware developers, cyber-terrorists
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Criminal-minded organizations, groups and individuals cyber-terrorist groups, Black hat hackers, malware developers etc are those who can deploy malwares to any target system or network in order to deface that system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	_____ is a code injecting method used for attacking the database of a system / website.

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	HTML injection
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SQL Injection
((OPTION_C)) This is optional	Malicious code injection
((OPTION_D)) This is optional	XML Injection
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	SQLi (Structured Query Language Injection) is a popular attack where SQL code is targeted or injected; for breaking the web application having SQL vulnerabilities. This allows the attacker to run malicious code and take access to the database of that server.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN	This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?

CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	SQL injection
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	HTML Injection
((OPTION_C)) This is optional	Cross Site Scripting (XSS)
((OPTION_D)) This is optional	Cross Site Request Forgery (XSRF)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	XSS attack can be infused by putting the malicious code (which gets automatically run) in any comment section or feedback section of any webpage (usually a blogging page). This can hamper the reputation of a site and the attacker may place any private data or personal credentials.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	An attempt to harm, damage or cause threat to a system or network is broadly termed as _____

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A))  THIS IS MANDATORY OPTION	Cyber-crime
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Cyber Attack
((OPTION_C))  This is optional	System hijacking
((OPTION_D))  This is optional	Digital crime
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cyber attack is an umbrella term used to classify different computer & network attacks or activities such as extortion, identity theft, email hacking, digital spying, stealing hardware, mobile hacking and physical security breaching.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
((OPTION_A)) THIS IS MANDATORY OPTION	Network Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Database Security
((OPTION_C)) This is optional	Information Security
((OPTION_D)) This is optional	Physical Security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information from alteration, destruction, deletion or disclosure by unauthorised users.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a vulnerability to information security?
((OPTION_A))  THIS IS MANDATORY OPTION	flood
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	without deleting data, disposal of storage media
((OPTION_C))  This is optional	unchanged default password
((OPTION_D))  This is optional	latest patches and updates not done
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a set of conventions & rules set for communicating two or more devices residing in the same network?
((OPTION_A))  THIS IS MANDATORY OPTION	Security policies
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Protocols
((OPTION_C))  This is optional	Wireless network
((OPTION_D))  This is optional	Network algorithms
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Network protocols are designed with mechanisms for identifying devices and make connections between them. In addition, some proper rules are defined as to how data packets will be sent and received.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The field that covers a variety of computer networks, both public and private, that are used in everyday jobs
((OPTION_A)) THIS IS MANDATORY OPTION	Artificial Intelligence
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ML
((OPTION_C)) This is optional	Network Security
((OPTION_D)) This is optional	IT
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Network security covers a variety of computer networks, both private and public. Everyday jobs like conducting transactions and communications among business and government agencies etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Network Security provides authentication and access control for resources.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is not an objective of network security?
((OPTION_A)) THIS IS MANDATORY OPTION	Identification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Authentication
((OPTION_C)) This is optional	Access control
((OPTION_D)) This is optional	Lock
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The Identification, Authentication and Access control are the objectives of network security. There is no such thing called lock.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of these is a part of network identification?
((OPTION_A)) THIS IS MANDATORY OPTION	UserID
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Password
((OPTION_C)) This is optional	OTP
((OPTION_D)) This is optional	fingerprint
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The answer is UserID. UserID is a part of identification. UserID can be a combination of username, user student number etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The process of verifying the identity of a user.
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Identification
((OPTION_C)) This is optional	Validation
((OPTION_D)) This is optional	Verification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	It is called an authentication. It is typically based on passwords, smart card, fingerprint, etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Security features that control that can access resources in the OS
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Identification
((OPTION_C)) This is optional	Validation
((OPTION_D)) This is optional	Access control
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Access control refers to the security features. Applications call access control to provide resources

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm in encryption is called
((OPTION_A)) THIS IS MANDATORY OPTION	Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Procedure
((OPTION_C)) This is optional	Cipher
((OPTION_D)) This is optional	Module
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	An algorithm used in encryption is referred to as a cipher. cipher is an algorithm for performing encryption or decryption

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The information that gets transformed in encryption is
((OPTION_A)) THIS IS MANDATORY OPTION	Plain text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Parallel text
((OPTION_C)) This is optional	Encrypted text
((OPTION_D)) This is optional	Decrypted text
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The text that gets transformed is called plain text. The algorithm used is called cipher

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The type of threats on the security of a computer system or network are..... i) Interruption ii) Interception iii) Modification iv) Creation v) Fabrication
((OPTION_A)) THIS IS MANDATORY OPTION	i, ii, iii and iv only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii, iii, iv and v only
((OPTION_C)) This is optional	i, ii, iii and v only
((OPTION_D)) This is optional	All i, ii, iii, iv and v
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is computer threat?
((OPTION_A))  THIS IS MANDATORY OPTION	Phishing
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Soliciting
((OPTION_C))  This is optional	DoS attack
((OPTION_D))  This is optional	stalking
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a term used in cryptography that refers to a message before encryption or after decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PLAIN TEXT
((OPTION_C)) This is optional	Original text
((OPTION_D)) This is optional	Plain script
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ is encrypted text
((OPTION_A)) THIS IS MANDATORY OPTION	cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	cipher script
((OPTION_C)) This is optional	secret text
((OPTION_D)) This is optional	secret script
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An _____ along with a key is used in the encryption
((OPTION_A)) THIS IS MANDATORY OPTION	cryptography algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption algorithm
((OPTION_C)) This is optional	encryption algorithm
((OPTION_D)) This is optional	plain text algorithm
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them.
((OPTION_A)) THIS IS MANDATORY OPTION	Availability
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	Cryptography
((OPTION_D)) This is optional	Integrity
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that information are in a format that is true and correct to its original purposes.
((OPTION_A)) THIS IS MANDATORY OPTION	Availability
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	integrity
((OPTION_D)) This is optional	cryptography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that information and resources are available to those who need them.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Availability</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Confidentiality</b>
((OPTION_C)) This is optional	<b>Cryptography</b>
((OPTION_D)) This is optional	<b>Integrity</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the process of identifying an individual, usually based on a username and password.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Authentication</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Authorization</b>
((OPTION_C)) This is optional	<b>either authentication or authorization</b>
((OPTION_D)) This is optional	<b>neither authentication nor authorization</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the process of giving individuals access to system objects based on their identity.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Authentication</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Authorization</b>
((OPTION_C)) This is optional	<b>either authentication or authorization</b>
((OPTION_D)) This is optional	<b>neither congestion control nor quality of service</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	when someone gains access to a server, website, or other sensitive data using someone else's account details called as
((OPTION_A)) THIS IS MANDATORY OPTION	Authorized access
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Access control
((OPTION_C)) This is optional	Unauthorized access
((OPTION_D)) This is optional	access
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.called as
((OPTION_A)) THIS IS MANDATORY OPTION	Thief
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	hacker
((OPTION_C)) This is optional	attacker
((OPTION_D)) This is optional	criminal
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is an action or event that might compromise the security.
((OPTION_A))  THIS IS MANDATORY OPTION	Threat
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Vulnerability
((OPTION_C))  This is optional	Protect
((OPTION_D))  This is optional	attack
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system
((OPTION_A)) THIS IS MANDATORY OPTION	threat
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Vulnerability
((OPTION_C)) This is optional	Attack
((OPTION_D)) This is optional	Protection
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is a software that operates on different OS which is used to prevent from malicious software.
((OPTION_A)) THIS IS MANDATORY OPTION	Anti virus
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	virus
((OPTION_C)) This is optional	protocol
((OPTION_D)) This is optional	risk
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is a technique that a hacker uses to stole data by a person for different purposes by psychological manipulation combined with social scenes.
((OPTION_A)) THIS IS MANDATORY OPTION	Social Engineering
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IT engineering
((OPTION_C)) This is optional	Psycology
((OPTION_D)) This is optional	Social engineering
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is a software or hardware which is used to filter network traffic based on rules.
((OPTION_A)) THIS IS MANDATORY OPTION	antivirus
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	firewall
((OPTION_C)) This is optional	protocol
((OPTION_D)) This is optional	keylogger
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not Basic Functions of Antivirus Engines
((OPTION_A)) THIS IS MANDATORY OPTION	Scanning
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity Checking
((OPTION_C)) This is optional	Interception
((OPTION_D)) This is optional	Evesdropping
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is name of antivirus
((OPTION_A))  THIS IS MANDATORY OPTION	AVG
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	PAN
((OPTION_C))  This is optional	SACK
((OPTION_D))  This is optional	FIREP
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Hacking tools that can be found very easily by everyone just by googling and they are endless.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Potential Losses due to Security Attacks doesn't involve _____
((OPTION_A)) THIS IS MANDATORY OPTION	Losing your data
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Bad usage of your computer resources
((OPTION_C)) This is optional	Reputation gain
((OPTION_D)) This is optional	Identity theft
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Reputation loss is part of it and not gain

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not malware category?
((OPTION_A))  THIS IS MANDATORY OPTION	Worms
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Viruses
((OPTION_C))  This is optional	Trojans
((OPTION_D))  This is optional	None of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	All are malware categories

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ encrypts all your data when your computer gets infected and the second is to roll back the data at a specific time you want.
((OPTION_A)) THIS IS MANDATORY OPTION	ransomware
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	firmware
((OPTION_C)) This is optional	middleware
((OPTION_D)) This is optional	Cyber ware
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	this network is created between two secure network devices like two firewalls.
((OPTION_A)) THIS IS MANDATORY OPTION	LAN
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MAN
((OPTION_C)) This is optional	VPN
((OPTION_D)) This is optional	WAN
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Virtual private network

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Name of the attack when integrity is compromised is called as _____
((OPTION_A))  THIS IS MANDATORY OPTION	Fabrication
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	interception
((OPTION_C))  This is optional	Interruption
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Attack made on confidentiality is __
((OPTION_A))  THIS IS MANDATORY OPTION	interception
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C))  This is optional	interruption
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	an attack on availability such as a denial of service attack (or DOS)
((OPTION_A))  THIS IS MANDATORY OPTION	Interruption
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Interception
((OPTION_C))  This is optional	fabrication
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An unauthorized party inserts counterfeit objects into the system and basically attacks the authenticity of the system.
((OPTION_A)) THIS IS MANDATORY OPTION	modification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C)) This is optional	interception
((OPTION_D)) This is optional	interruption
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Attack in which a network service is made degraded or unavailable for legitimate use
((OPTION_A)) THIS IS MANDATORY OPTION	Interruption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C)) This is optional	interception
((OPTION_D)) This is optional	modification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is assurance that someone cannot deny something.
((OPTION_A))  THIS IS MANDATORY OPTION	availability
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	confidentiality
((OPTION_C))  This is optional	Access control
((OPTION_D))  This is optional	Non-repudiation
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the purpose of a Denial of Service attack?
((OPTION_A))  THIS IS MANDATORY OPTION	Exploit a weakness in the TCP/IP stack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	To execute a Trojan on a system
((OPTION_C))  This is optional	To overload a system so it is no longer operational
((OPTION_D))  This is optional	To shutdown services by turning them off
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	DoS attacks force systems to stop responding by overloading the processing of the system

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What are some of the most common vulnerabilities that exist in a network or system?
((OPTION_A)) THIS IS MANDATORY OPTION	Changing manufacturer, or recommended, settings of a newly installed application.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additional unused features on commercial software packages
((OPTION_C)) This is optional	Utilizing open source application code
((OPTION_D)) This is optional	Balancing security concerns with functionality and ease of use of a system.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Linux is an open source code and considered to have greater security than the commercial Windows environment

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Sniffing is used to perform _____ fingerprinting
((OPTION_A))  THIS IS MANDATORY OPTION	Passive stack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Active stack
((OPTION_C))  This is optional	Passive banner grabbing
((OPTION_D))  This is optional	Scanned
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Passive stack fingerprinting uses sniffing technologies instead of scanning

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a principle of data security?
((OPTION_A)) THIS IS MANDATORY OPTION	Data Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following attacks is a passive attack?
((OPTION_A))  THIS IS MANDATORY OPTION	Masquerade
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Modification of message
((OPTION_C))  This is optional	Denial of service
((OPTION_D))  This is optional	Traffic analysis
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	In a passive attack, the attacker does not modify any part of the data. His attempt is only to obtain the information and not to modify it. From the mentioned options, this happens only in Traffic analysis in which the attacker monitors the pattern of transmission. The rest other options are examples of active attacks.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options correctly defines the Brute force attack?
((OPTION_A)) THIS IS MANDATORY OPTION	Brutally forcing the user to share the useful information like pins and passwords.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Trying every possible key to decrypt the message.
((OPTION_C)) This is optional	One entity pretends to be some other entity
((OPTION_D)) This is optional	The message or information is modified before sending it to the receiver.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	Integer value
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Square matrix
((OPTION_C)) This is optional	An array of characters
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems is called as
((OPTION_A)) THIS IS MANDATORY OPTION	Network security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Information security
((OPTION_C)) This is optional	Cyber security
((OPTION_D)) This is optional	Internet security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	phishing and pre-texting is part of _____
((OPTION_A)) THIS IS MANDATORY OPTION	<b>NETWORK SECURITY</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>CYBER SECURITY</b>
((OPTION_C)) This is optional	Internet security
((OPTION_D)) This is optional	Internet security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures to protect the transit data only.
((OPTION_A))  THIS IS MANDATORY OPTION	NETWORK SECURITY
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Internet security
((OPTION_C))  This is optional	Information security
((OPTION_D))  This is optional	Cyber security
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is danger for <b>Integrity</b> as well as <b>availability</b> .
((OPTION_A)) THIS IS MANDATORY OPTION	Active attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ is danger for <b>Confidentiality</b> .
((OPTION_A)) THIS IS MANDATORY OPTION	Active attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ attack attention is on detection.
((OPTION_A))  THIS IS MANDATORY OPTION	Passive attack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Active Attack
((OPTION_C))  This is optional	Both
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	in _____ attack attention is on prevention.
((OPTION_A))  THIS IS MANDATORY OPTION	Active attack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C))  This is optional	Both
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Due to ___ attack system is always damaged.
((OPTION_A))  THIS IS MANDATORY OPTION	Active
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C))  This is optional	Both active and passive
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	due to _____ attack, there is no any harm to the system.
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	Both active and passive
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ attack is tough to restrict from entering systems or networks.
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	Both active and passive
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Attack is easy to prohibited in comparison to _____ attack.
((OPTION_A))  THIS IS MANDATORY OPTION	Active,passive
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive,active
((OPTION_C))  This is optional	
((OPTION_D))  This is optional	
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not active attack
((OPTION_A)) THIS IS MANDATORY OPTION	Denial of service (DoS)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	replay
((OPTION_C)) This is optional	Trojans
((OPTION_D)) This is optional	traffic analysis
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In __ <b>attack</b> , an attacker tries to modify the content of the messages.
((OPTION_A))  THIS IS MANDATORY OPTION	Active
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C))  This is optional	
((OPTION_D))  This is optional	
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	in _____ <b>attack</b> , an attacker observes the messages, copy them and may use them for malicious purposes
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is state of being free from potential threats or dangers
((OPTION_A)) THIS IS MANDATORY OPTION	privacy
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	freedom
((OPTION_C)) This is optional	security
((OPTION_D)) This is optional	independence
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ refers to the state of being free from unwanted attention.
((OPTION_A)) THIS IS MANDATORY OPTION	Freedom
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Security
((OPTION_C)) This is optional	Privacy
((OPTION_D)) This is optional	independence
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ can be achieved without _____ but _____ cannot be achieved without _____.
((OPTION_A)) THIS IS MANDATORY OPTION	Security,privacy,privacy security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Privacy,security,security,privacy
((OPTION_C)) This is optional	Security,privacy,privacy,privacy
((OPTION_D)) This is optional	Security,security,privacy,security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ program refers to a set of protocols and regulations set in place to protect all the confidential information assets and resources that an organization collects and owns.
((OPTION_A)) THIS IS MANDATORY OPTION	Privacy
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Security
((OPTION_C)) This is optional	Security and privacy
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ program focuses on protecting only personal information such as log in credentials, passwords, etc.
((OPTION_A)) THIS IS MANDATORY OPTION	Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Privacy
((OPTION_C)) This is optional	Security and privacy
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following Algorithms does not belong to symmetric encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	3DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	RC5
((OPTION_D)) This is optional	IDEA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Assymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key?
((OPTION_A)) THIS IS MANDATORY OPTION	Not true, the message can also be decrypted with the Public Key.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A so called "one way function with back door" is applied for the encryption
((OPTION_C)) This is optional	The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key.
((OPTION_D)) This is optional	The encrypted message contains the function for decryption which identifies the Private Key.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	An one-way function is a function which a computer can calculate quickly, but whose reversal would last months or years. An one-way function with back door can be reversed with the help of a couple of additional information (the back door), but scarcely

	without this information. The information for the back door is contained in the private Key.
--	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the largest disadvantage of the symmetric Encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	More complex and therefore more time-consuming calculations.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Problem of the secure transmission of the Secret Key
((OPTION_C)) This is optional	Less secure encryption function.
((OPTION_D)) This is optional	Isn't used any more
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION))	As there is only one key in the symmetrical encryption, this must

)) This is also optional	be known by both sender and recipient and this key is sufficient to decrypt the secret message. Therefore it must be exchanged between sender and receiver in such a manner that an unauthorized person can in no case take possession of it.
--------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the principle of the encryption using a key?
((OPTION_A)) THIS IS MANDATORY OPTION	The key indicates which function is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	The key contains the secret function for encryption including parameters. Only a password can activate the key.
((OPTION_C)) This is optional	All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.
((OPTION_D)) This is optional	The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	C

E	
((EXPLANATION)) This is also optional	The encoding of a message is calculated by an algorithm. If always the same algorithm would be used, it would be easy to crack intercepted messages. However, it isn't possible to invent a new algorithm whenever the old one was cracked, therefor the possibility to parameterize algorithms is needed and this is the assignment of the key. All algorithms must be public, only the keys are secret (principle of Kerckhoff, Dutch cryptographer during 19th century).

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If the sender and receiver use different keys, the system is referred to as conventional cipher system
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Such a system is called asymmetric, two-key, or public-key cipher system

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW
((OPTION_A)) THIS IS MANDATORY OPTION	ABANDONED LOCK
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ENCRYPTED TEXT
((OPTION_C)) This is optional	ABANDONED TEXT
((OPTION_D)) This is optional	ENCRYPTED LOCK
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher uses $C = (p+3) \text{ mod } 26$ to encrypt.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Caesar Cipher is an example of
((OPTION_A)) THIS IS MANDATORY OPTION	Poly-alphabetic Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Mono-alphabetic Cipher
((OPTION_C)) This is optional	Multi-alphabetic Cipher
((OPTION_D)) This is optional	Bi-alphabetic Cipher
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis
((OPTION_A)) THIS IS MANDATORY OPTION	Random Polyalphabetic, Plaintext, Playfair
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Random Polyalphabetic, Playfair, Vignere
((OPTION_C)) This is optional	Random Polyalphabetic, Vignere, Playfair, Plaintext
((OPTION_D)) This is optional	Random Polyalphabetic, Plaintext, Beaufort, Playfair
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Random Polyalphabetic is the most resistant to frequency analysis, followed by Vignere, Playfair and then Plaintext.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-
((OPTION_A)) THIS IS MANDATORY OPTION	abqdnwewuwjphfvrrtrfznsdokvl
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	abqdmwuwjphfvyyrfznydokvl
((OPTION_C)) This is optional	tbqryvmwuwjphfvyyrfznydokvl
((OPTION_D)) This is optional	baiuvmwuwjphfoeiyrfznydokvl
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cipher text:= $C_i = P_i + k_i \text{ mod } m \text{ (mod 26).}$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	nlazeiiblji
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nlazeiiblji
((OPTION_C)) This is optional	olaaeiiblki
((OPTION_D)) This is optional	mlaaeiiblki
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Cipher text:= $C_i = P_i + k_i \text{ mod } m \text{ (mod 26).}$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Confusion hides the relationship between the ciphertext and the plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Confusion hides the relationship between the ciphertext and the key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The S-Box is used to provide confusion, as it is dependent on the unknown key.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	false
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>The S-Box is used to provide confusion, as it is dependent on the unknown key.</p> <p>The P-Box is fixed, and there is no confusion due to it, but it provides diffusion.</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	<p>This is an example of</p> <pre> graph TD     P[P] --&gt; L1[L1]     P --&gt; R1[R1]     L1 --&gt; F1[F]     F1 --&gt; R1     R1 --&gt; L2[L2]     R1 --&gt; R2[R2]     L2 --&gt; F2[F]     F2 --&gt; R2     R2 --&gt; Ln[Ln]     R2 --&gt; Rn[Rn]     Ln --&gt; Fn[F]     Fn --&gt; Rn     Rn --&gt; C[C]     </pre>
((OPTION_A)) THIS IS MANDATORY OPTION	SP Networks
((OPTION_B)) THIS IS ALSO MANDATORY	Feistel Cipher

OPTION	
((OPTION_C)) This is optional	Hash Algorithm
((OPTION_D)) This is optional	Hill Cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation
((OPTION_A)) THIS IS MANDATORY OPTION	1 and 3
((OPTION_B)) THIS IS ALSO MANDATORY	2 and 3

OPTION	
((OPTION_C)) This is optional	3 and 4
((OPTION_D)) This is optional	2 and 4
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Increase in any of the above 4 leads to slowing of the cipher algorithm i.e. more computational time will be required.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES follows
((OPTION_A)) THIS IS MANDATORY OPTION	Hash Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY	Caesars Cipher

OPTION	
((OPTION_C)) This is optional	Feistel Cipher Structure
((OPTION_D)) This is optional	SP Network
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES Algorithm Cipher System consists of _____ rounds (iterations) each with a round key
((OPTION_A)) THIS IS MANDATORY OPTION	12
((OPTION_B)) THIS IS ALSO MANDATORY	18

OPTION	
((OPTION_C)) This is optional	9
((OPTION_D)) This is optional	16
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES algorithm has a key length of
((OPTION_A)) THIS IS MANDATORY OPTION	128 Bits
((OPTION_B)) THIS IS ALSO MANDATORY	32 Bits

OPTION	
((OPTION_C)) This is optional	64 Bits
((OPTION_D)) This is optional	16 Bits
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	56 bits are used, the rest 8 bits are parity bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the round key is _____ bit and the Round Input is _____ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	48, 32
((OPTION_B)) THIS IS ALSO MANDATORY	64,32

OPTION	
((OPTION_C)) This is optional	56, 24
((OPTION_D)) This is optional	32, 32
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The round key is 48 bits. The input is 32 bits

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
((OPTION_A)) THIS IS MANDATORY OPTION	Scaling of the existing bits
((OPTION_B)) THIS IS ALSO MANDATORY	Duplication of the existing bits

<b>OPTION</b>	
((OPTION_C)) This is optional	Addition of zeros
((OPTION_D)) This is optional	Addition of ones
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits (permutation plus an expansion), that involves duplication of 16 of the bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The Initial Permutation table/matrix is of size
((OPTION_A)) THIS IS MANDATORY OPTION	16x8
((OPTION_B)) THIS IS ALSO MANDATORY	12x8

OPTION	
((OPTION_C)) This is optional	8x8
((OPTION_D)) This is optional	4x8
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	There are 64 bits to permute and this requires a 8x8 matrix.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The number of unique substitution boxes in DES after the 48 bit XOR operation are
((OPTION_A)) THIS IS MANDATORY OPTION	8
((OPTION_B)) THIS IS ALSO MANDATORY	4

OPTION	
((OPTION_C)) This is optional	6
((OPTION_D)) This is optional	12
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	IP-1 is the first step and the last step is IP during decryption.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A preferable cryptographic algorithm should have a good avalanche effect.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Thus statement is true as a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the size(in bits) of the key in the SDES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	24
((OPTION_B)) THIS IS ALSO MANDATORY	16

OPTION	
((OPTION_C)) This is optional	20
((OPTION_D)) This is optional	10
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The size of the key in the SDES algorithm is 10 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	GCD(a,b) is the same as GCD( a , b ).
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is true. $\gcd(60,24) = \gcd(60,-24) = 12$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	882
((OPTION_B)) THIS IS ALSO MANDATORY	770

OPTION	
((OPTION_C)) This is optional	1078
((OPTION_D)) This is optional	1225
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	$\text{GCD}(1160718174, 316258250) = 1078$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	$\text{GCD}(102947526, 239821932) = 6.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	13
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	17
((OPTION_D)) This is optional	7
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	$\text{GCD}(8376238, 1921023) = 13.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 1234 mod 4321 is
((OPTION_A)) THIS IS MANDATORY OPTION	3239
((OPTION_B)) THIS IS ALSO MANDATORY	3213

OPTION	
((OPTION_C)) This is optional	3242
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The multiplicative Inverse of 1234 mod 4321 is 3239.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 550 mod 1769 is
((OPTION_A)) THIS IS MANDATORY OPTION	434
((OPTION_B)) THIS IS ALSO MANDATORY	224

OPTION	
((OPTION_C)) This is optional	550
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The multiplicative Inverse of 550 mod 1769 is 550.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	<p><b>You are supposed to use hill cipher for encryption technique. You are provided with the following matrix,</b></p> $A = \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix}$ <p><b>Is the given matrix 'A', a valid key to be used for encryption?</b></p>
((OPTION_A)) THIS IS MANDATORY OPTION	Yes
((OPTION_B))	No

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Can't be determined
((OPTION_D)) This is optional	Data insufficient
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>For choosing any square matrix as a key, it should be taken care that the matrix is invertible, i.e. its inverse must exist.</p> <p>Here, in this case,</p> $  A   = 0$ <p>Therefore, it means that 'A' is not an invertible matrix. Hence matrix 'A' cannot be chosen as a key matrix for encryption in the <a href="#">Hill cipher</a>.</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	The input text is divided into two parts: one being left half and another one being right half.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Swapping of the left and right halves are performed after each round.
((OPTION_C)) This is optional	The plain text is converted into a matrix form first
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The fiestal structure does not require the conversion of the plain text into matrix form at any of its steps.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Among the following given options, chose the strongest encryption technique

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	DES ( Data Encryption Standard))
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Double DES
((OPTION_C)) This is optional	Triple DES
((OPTION_D)) This is optional	AES (Advance Encryption Standard)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	It has been proved that the AES performs much better than the all the other DES, whether it be single DES or series of DES.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	<p><b>Consider the following steps,</b></p> <ul style="list-style-type: none"> <li>i. Substitution bytes</li> <li>ii. Shift Rows</li> </ul>

IMAGES ALSO	<p>iii. Mix columns iv. Add round key</p> <p><b>The above steps are performed in each round of which of the following ciphers?</b></p>
((OPTION_A))  THIS IS MANDATORY OPTION	Rail fence cipher
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Data Encryption Standard (DES)
((OPTION_C))  This is optional	Advance Encryption Standard (AES)
((OPTION_D))  This is optional	None of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ algorithm transforms ciphertext to plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _____ cipher replaces one character with another character.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ cipher reorders the plaintext characters to create a ciphertext.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
((OPTION_A)) THIS IS MANDATORY OPTION	man-in-the-middle
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ciphertext attack
((OPTION_C)) This is optional	plaintext attack
((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the receiver uses the _____ key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either a or b
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES is a(n) _____ method adopted by the U.S. government.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	either (a) or (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ECB and CBC are _____ ciphers.
((OPTION_A))  THIS IS MANDATORY OPTION	block
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	stream
((OPTION_C))  This is optional	field
((OPTION_D))  This is optional	none of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ cipher, the same key is used by both the sender and receiver.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the sender uses the_____key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a(n) _____ cipher, a pair of keys is used.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	2
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	AES uses a _____ bit block size and a key size of _____ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	128; 128 or 256
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64; 128 or 192
((OPTION_C)) This is optional	256; 128, 192, or 256
((OPTION_D)) This is optional	128; 128, 192, or 256
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	It uses a 128-bit block size and a key size of 128, 192, or 256 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Like DES, AES also uses Feistel Structure.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES does not use a Feistel structure. Instead, each full round consists of four separate functions: -byte substitution -Permutation -arithmetic operations over a finite field, and -XOR with a key.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The 4x4 byte matrices in the AES algorithm are called
((OPTION_A)) THIS IS MANDATORY OPTION	States
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Words
((OPTION_C)) This is optional	Transitions
((OPTION_D)) This is optional	Permutations
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is a type of substitution cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	poly alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition cipher
((OPTION_C)) This is optional	Columnar cipher
((OPTION_D)) This is optional	Rail fence cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In substitution cipher the plain text is replaced by cipher text according to a fixed rule. There are two types of substitution cipher- Mono alphabetic and Poly alphabetic cipher.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following correctly defines poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	a substitution based cipher which uses multiple substitution at different positions
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a substitution based cipher which uses fixed substitution over entire message
((OPTION_C)) This is optional	a transposition based cipher which uses multiple substitution at different positions
((OPTION_D)) This is optional	A transposition based cipher which uses fixed substitution over entire message
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Poly alphabetic cipher is a type of substitution cipher. It uses multiple substitution at different positions in order to cipher the plain text.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a type of poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Rotor cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hill cipher
((OPTION_C)) This is optional	One time pad cipher
((OPTION_D)) This is optional	Affine cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	In poly alphabetic cipher each symbol of plain text is replaced by a different cipher text regardless of its occurrence. Out of the given options, only affine cipher is not a poly alphabetic cipher.

((MARKS)) QUESTION IS OF	2
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	We are provided the plain text "SUN". You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2?
((OPTION_A)) THIS IS MANDATORY OPTION	UWP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	NUS
((OPTION_C)) This is optional	WUP
((OPTION_D)) This is optional	QSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>In the Caesar cipher technique, the encryption is performed as follows,</p> $E(P, K) = (P + K) \text{ mod } 26$ <p>Therefore,</p> $E(S, 2) = (18 + 2) \text{ mod } 26 = 20 = U$ $E(U, 2) = (20 + 2) \text{ mod } 26 = 22 = W$ $E(N, 2) = (13 + 2) \text{ mod } 26 = 15 = P$ <p>Hence, the ciphertext is "UWP".</p>

--	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?
((OPTION_A)) THIS IS MANDATORY OPTION	<u>Hill Cipher</u>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<u>Playfair cipher</u>
((OPTION_C)) This is optional	Both a and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also	The hill cipher includes a square matrix as the key, and in Playfair cipher, we create a 5X5 matrix using the given key string. Hence,

optional	both these ciphers include the use of matrices.
----------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Playfair cipher is an example of _____
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C)) This is optional	transposition cipher
((OPTION_D)) This is optional	additive cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	Playfair cipher is a substitution cipher. It falls under the category of poly alphabetic cipher as it uses multiple substitution at different positions in order to cipher the plain text.
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Encryption in Playfair cipher is done using _
((OPTION_A)) THIS IS MANDATORY OPTION	a 5x5 table
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a 13x2 table
((OPTION_C)) This is optional	vigenere table
((OPTION_D)) This is optional	a 6x6 table
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A

((EXPLANATION)) This is also optional	
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the plain text corresponding to cipher text "BPKYFS" if playfair cipher is used with keyword as "SECRET" (assuming j is combined with i)?
((OPTION_A))  THIS IS MANDATORY OPTION	INDIAN
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	WORLD
((OPTION_C))  This is optional	DOLLAR
((OPTION_D))  This is optional	HELLO
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C

((EXPLANATION)) This is also optional	To decrypt the message we follow the reverse procedure. The table is formed in the same manner. Applying this we get the plain text to be "DOLLAR".
---------------------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair are identical?
((OPTION_A)) THIS IS MANDATORY OPTION	then that pair is neglected
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a null(or x) is added in between the letters
((OPTION_C)) This is optional	one of the identical letter is replaced by some other letter
((OPTION_D)) This is optional	then both of the letters are replaced by the letter appearing just next in the row
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	In playfair cipher if the letters in a pair are identical then a null is added in between the letters. Any letter can be used as a null as long as that letter is not the one being repeated.
---------------------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same row?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter at the corner of the row
((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	If the letters in a pair appear in same row then they are replaced by the letters appearing immediately right to them respectively. If the element to be replaced appears at the corner of the row then we wrap around to the left side of that row.
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the ciphered text if the string “SANFOUNDRY” is given as input to the code of playfair cipher with keyword as “SECRET” (assuming j is combined with i)?
((OPTION_A)) THIS IS MANDATORY OPTION	ZHQAPNPAFR
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AHQAPNPAFR
((OPTION_C)) This is optional	HAQAPNPAFR
((OPTION_D)) This is optional	QHAAPNPAFR
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	B

E	
((EXPLANATION)) This is also optional	<p>For encrypting the plain text using playfair cipher we use a <math>5 \times 5</math> table that is constructed by using keyword. Then we apply rules for encryption in order to get the ciphered text. Table is given as under-</p> <p>S E C R T</p> <p>A B D F G</p> <p>H I K L M</p> <p>N O P Q U</p> <p>V W X Y Z</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letters at the corner of the row
((OPTION_D))	that pair is neglected

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	If the letters in a pair appear in the same column then they are replaced by the letters appearing immediately below them respectively. If the element to be replaced appears at the corner of the column then we wrap around to the top side of that column.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair does not appear in same row or column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter of the same row at the corner of the rectangle defined by the original pair respectively

((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	If the letters in a pair does not appear in same row or column then they are replaced by the letters of the same row at the corner of the rectangle defined by the original pair respectively. The order of letters should be maintained.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Columnar cipher falls under the category of?
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C))	additive cipher

This is optional	
((OPTION_D)) This is optional	Transposition cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Columnar cipher is a transposition cipher. It falls under the category of transposition cipher as it encrypts the plain text by rearranging its letters.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following ciphered text would have NOT used transposition cipher for encryption of the plain text "CIPHER"?
((OPTION_A)) THIS IS MANDATORY OPTION	EPIHRC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	EHIPCR
((OPTION_C))	DTIPRC

This is optional	
((OPTION_D))	HRIPEC
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	We know that transposition cipher encrypts the plain text by shuffling the letters of the plain text. So out of the given options, only “DTIPRC” does not have the same set of letters as “CIPHER”.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many columns do we need to have in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	4
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	5
((OPTION_C))	6

This is optional	
((OPTION_D))	7
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So in this case it will be equal to 6.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the encrypted text corresponding to plain text “CLASSIFIED” using columnar transposition cipher with a keyword as “GAMES”?
((OPTION_A)) THIS IS MANDATORY OPTION	LFDSIASECI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SECIAISDFL
((OPTION_C))	CILFAISESD

This is optional																					
((OPTION_D))	IFSECIAISD																				
This is optional																					
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option																					
((CORRECT_CH OICE)) Either A or B or C or D or E	D																				
((EXPLANATION )) This is also optional	<p>For encrypting using columnar cipher we have to arrange the letters of the plain text in a table which has the same number of columns as the letters of the keyword. Then the letters of the keyword are arranged in alphabetical order and we read along each column.</p> <table style="margin-left: auto; margin-right: auto;"> <tr><td>3</td><td>1</td><td>4</td><td>2</td><td>5</td></tr> <tr><td>G</td><td>A</td><td>M</td><td>E</td><td>S</td></tr> <tr><td>C</td><td>L</td><td>A</td><td>S</td><td>S</td></tr> <tr><td>I</td><td>F</td><td>I</td><td>E</td><td>D</td></tr> </table> <p>So the ciphered text will be “IFSECIAISD”.</p>	3	1	4	2	5	G	A	M	E	S	C	L	A	S	S	I	F	I	E	D
3	1	4	2	5																	
G	A	M	E	S																	
C	L	A	S	S																	
I	F	I	E	D																	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many rows will the letters of the plain text occupy in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B))	2

THIS IS ALSO MANDATORY OPTION																			
((OPTION_C)) This is optional	3																		
((OPTION_D)) This is optional	4																		
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option																			
((CORRECT_CHOICE)) Either A or B or C or D or E	B																		
((EXPLANATION)) This is also optional	<p>Explanation: The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So when we will write the letters of the plain text row wise then there will be 2 rows of plain text in this case. The table is shown below :-</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td>S</td><td>E</td><td>C</td><td>R</td><td>E</td><td>T</td> </tr> <tr> <td>1</td><td>S</td><td>A</td><td>N</td><td>F</td><td>O</td><td>U</td> </tr> <tr> <td>2</td><td>N</td><td>D</td><td>R</td><td>Y</td> </tr> </table>	S	E	C	R	E	T	1	S	A	N	F	O	U	2	N	D	R	Y
S	E	C	R	E	T														
1	S	A	N	F	O	U													
2	N	D	R	Y															

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following statement is not true regarding columnar transposition cipher?
((OPTION_A)) THIS IS	probability of error is high while deciphering

<b>MANDATORY OPTION</b>	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	it cannot be combined with other ciphers
((OPTION_C))  This is optional	it is a traditional symmetric cipher
((OPTION_D))  This is optional	it is a weak cipher
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Although columnar transposition cipher is a weak cipher in itself. But it can be combined with other substitution ciphers so as to improve its security. The probability of error remains high while decoding columnar cipher as it is a lengthy process

<b>((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)</b>	1
<b>((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</b>	_____ is another data hiding technique which can be used in conjunction with cryptography for the extra-secure method of protecting data.
<b>((OPTION_A))</b>	Cryptography

THIS IS MANDATORY OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Steganography
((OPTION_C)) This is optional	Tomography
((OPTION_D)) This is optional	Chorography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Steganography is the technique of hiding data in another raw data. Steganography is another data hiding technique which can be used in conjunction with cryptography for an extra-secure method of protecting data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((OPTION_A))  THIS IS MANDATORY OPTION	Cryptography
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C))  This is optional	Steganography
((OPTION_D))  This is optional	Chorography
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Steganography helps in hiding any form of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _____ tool permits security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((OPTION_A))  THIS IS MANDATORY OPTION	Cryptography
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C))  This is optional	Chorography
((OPTION_D))  This is optional	Steganography
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	A steganography tool is a software tool that permits a security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The main motive for using steganography is that hackers or other users can hide a secret message behind a _____

((OPTION_A)) THIS IS MANDATORY OPTION	special file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ordinary file
((OPTION_C)) This is optional	program file
((OPTION_D)) This is optional	encrypted file
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	The main motive for using steganography is that hackers or other users can hide a secret message behind ordinary files. Some steganography tools are SSuite Picsel, rSteg etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	People will normally think it as a normal/regular file and your secret message will pass on without any _____

((OPTION_A)) THIS IS MANDATORY OPTION	Suspicion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	cracking
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Steganography techniques help hackers or other users to conceal covert message behind regular files. People will normally think it as a normal/regular file and your secret message will pass on without any suspicion.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	By using _____ you can diminish the chance of data leakage

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C)) This is optional	Chorography
((OPTION_D)) This is optional	Steganography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Hackers or other cyber criminals target ordinary files to hide different data or information within another data file. By using steganography, you can diminish the chance of data leakage.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Which of the following is a mode of operation for the Block ciphers in cryptography?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Electronic Code Book (ECB)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Cipher Block Chaining (CBC)
((OPTION_C)) This is optional	Counter (CTR) mode
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	For which of the following should EBC (Electronic Code Book) process not be used for encryption?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	For large block sizes
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	For fixed block sizes
((OPTION_C)) This is optional	For small block sizes
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	It is preferred that the block size in the ECB technique must be greater than 64 bits. If not, the text is padded to make it of the required length. This is due to some particular words and phrases that may be reused again often so that the same repetitive part of ciphertext can emerge as mixed.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	Which of the following is the main disadvantage of the ECB (Electronic Code Book)?

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	It requires large block size
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Padding is done to make the plain text divisible into blocks of fixed size
((OPTION_C)) This is optional	It is prone to cryptanalysis since there is a direct relationship between plain text and cipher text.
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	In <u>ECB</u> , there lies a direct relation between the plain text and the ciphertext. Therefore, it is easy for an outsider to break the encryption logic and steal the data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options is not correct according to the definition of the Cipher Block Chaining (CBC)?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC is a mode of operation for stream ciphers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Initialization vector (IV) is used in CBC in the initial phase.
((OPTION_C)) This is optional	It has better resistive nature towards cryptanalysis than ECB
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<a href="#">CBC</a> which stands for Cipher Block chaining is a mode of operation for block ciphers and not for stream ciphers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following modes of operations can be followed for both stream ciphers as well as block ciphers?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC (Cipher Block Chaining)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ECB (Electronic Code Book)
((OPTION_C)) This is optional	CFB (Cipher text Feed Back)
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	<b>CFB</b> is primarily a mode to derive some characteristics of a stream cipher from a block cipher on the cryptography in cryptoanalysis.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

<p>((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</p>	<p>All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES?</p> <ul style="list-style-type: none"> <li>i. Substitution bytes</li> <li>ii. Shift rows</li> <li>iii. Mix columns</li> <li>iv. Add round key</li> </ul>
<p>((OPTION_A)) THIS IS MANDATORY OPTION</p>	<p>i</p>
<p>((OPTION_B)) THIS IS ALSO MANDATORY OPTION</p>	<p>iii</p>
<p>((OPTION_C)) This is optional</p>	<p>All of the mentioned</p>
<p>((OPTION_D)) This is optional</p>	<p>None of the mentioned</p>
<p>((OPTION_E)) This is optional. If optional keep empty so that system will skip this option</p>	
<p>((CORRECT_CHOICE)) Either A or B or C or D or E</p>	<p>B</p>
<p>((EXPLANATION)) This is also optional</p>	<p>In the AES algorithm, the MIX COLUMN operation is performed in all the rounds except the final round of the algorithm.</p>

<p>((MARKS))</p>	<p>1</p>
------------------	----------

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"The number of rounds in the AES algorithm depends upon the key size being used." Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	128 key size: 10 rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	192 key size: 12 rounds
((OPTION_C)) This is optional	256 key size: 14 rounds
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS))	2
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Avalanche effect
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Completeness
((OPTION_C)) This is optional	Both a. and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS))	2
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For the AES-128 algorithm there are _____ similar rounds and _____ round is different.
((OPTION_A)) THIS IS MANDATORY OPTION	2 pair of 5 similar rounds ; every alternate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	9 ; the last
((OPTION_C)) This is optional	8 ; the first and last
((OPTION_D)) This is optional	10 ; no
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS))	1
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the 4 operations are false for each round in the AES algorithm? i) Substitute Bytes ii) Shift Columns iii) Mix Rows iv) XOR Key
((OPTION_A)) THIS IS MANDATORY OPTION	i) only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii) iii) and iv)
((OPTION_C)) This is optional	ii) and iii)
((OPTION_D)) This is optional	only iv
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES rounds involve substitute bytes, shift rows, mix columns and addition of round key.

((MARKS))	1
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	There is an addition of round key before the start of the AES round algorithms.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In AES the final round contains only three transformations, and there is an initial single transformation (Add Round Key) before the first round which can be considered Round 0. Each transformation takes 4x4 matrixes as input and produces a 4x4 matrix as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1																
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the Shifted Row transformation for the matrix bellow?  <table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>6B</td><td>77</td><td>A4</td><td>6B</td></tr> <tr> <td>AD</td><td>01</td><td>F0</td><td>63</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	FE	72	2B	D7	6B	77	A4	6B	AD	01	F0	63	30	D7	AF	FE
FE	72	2B	D7														
6B	77	A4	6B														
AD	01	F0	63														
30	D7	AF	FE														
((OPTION_A))  THIS IS MANDATORY OPTION	<table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>6B</td><td>77</td><td>A4</td><td>6B</td></tr> <tr> <td>AD</td><td>01</td><td>F0</td><td>63</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	FE	72	2B	D7	6B	77	A4	6B	AD	01	F0	63	30	D7	AF	FE
FE	72	2B	D7														
6B	77	A4	6B														
AD	01	F0	63														
30	D7	AF	FE														
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	<table border="1"> <tr> <td>72</td><td>2B</td><td>D7</td><td>FE</td></tr> <tr> <td>A4</td><td>6B</td><td>6B</td><td>77</td></tr> <tr> <td>63</td><td>AD</td><td>01</td><td>F0</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	72	2B	D7	FE	A4	6B	6B	77	63	AD	01	F0	30	D7	AF	FE
72	2B	D7	FE														
A4	6B	6B	77														
63	AD	01	F0														
30	D7	AF	FE														
((OPTION_C))  This is optional	<table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>77</td><td>A4</td><td>6B</td><td>6B</td></tr> <tr> <td>F0</td><td>63</td><td>AD</td><td>01</td></tr> <tr> <td>FE</td><td>30</td><td>D7</td><td>AF</td></tr> </table>	FE	72	2B	D7	77	A4	6B	6B	F0	63	AD	01	FE	30	D7	AF
FE	72	2B	D7														
77	A4	6B	6B														
F0	63	AD	01														
FE	30	D7	AF														
((OPTION_D))  This is optional	<table border="1"> <tr> <td>D7</td><td>FE</td><td>72</td><td>2B</td></tr> <tr> <td>A4</td><td>6B</td><td>6B</td><td>77</td></tr> <tr> <td>01</td><td>AD</td><td>63</td><td>F0</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	D7	FE	72	2B	A4	6B	6B	77	01	AD	63	F0	30	D7	AF	FE
D7	FE	72	2B														
A4	6B	6B	77														
01	AD	63	F0														
30	D7	AF	FE														

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The Shift Rows transformation consists of: -Not shifting the first row of the state array at all. -Circularly shifting the second row by one byte to the left. -Circularly shifting the third row by two bytes to the left, and -Circularly shifting the last row by three bytes to the left.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not weak key in DES
((OPTION_A)) THIS IS MANDATORY OPTION	0x0101010101010101
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0xEFABFEFEFEFEFEFE
((OPTION_C)) This is optional	0x1F1F1F1F0E0E0E0E
((OPTION_D))	0xFFFFFFFFFFFFFF

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple-DES has _____ keys.
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	2
((OPTION_C)) This is optional	5
((OPTION_D))	4

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a encryption technique which uses two instance of DES on same plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	Double DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tripple DES
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ attack which can be used to break through double DES.
((OPTION_A)) THIS IS MANDATORY OPTION	Brute force
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	meet-in-the middle
((OPTION_C)) This is optional	Timing
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple DES involve __
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption, Decryption, Decryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption ,Encryption, Encryption
((OPTION_C)) This is optional	Decryption ,Encryption, Decryption
((OPTION_D))	Encryption, Decryption, Encryption

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ involves feeding the successive output blocks from the underlying block cipher back to it
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	OFB
((OPTION_D))	CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is counter-based version of CFB mode without the feedback
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	counter
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below mode is independent of previous output
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	CFB
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Errors get propagated in all modes except ___and ___
((OPTION_A)) THIS IS MANDATORY OPTION	ECB,COUNTER
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC,COUNTER
((OPTION_C)) This is optional	CFB,COUNTER
((OPTION_D))	OFB,CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Patterns are not preserved in ___ mode
((OPTION_A)) THIS IS MANDATORY OPTION	CBC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CFB
((OPTION_C)) This is optional	Both CBC and CFB
((OPTION_D))	ECB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A small change in plaintext results in the very great change in the cipher text indicates which characteristic
((OPTION_A)) THIS IS MANDATORY OPTION	completeness
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Strong key
((OPTION_C)) This is optional	Avalanche effect
((OPTION_D))	All of the above

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ ciphers, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of cipher text.
((OPTION_A)) THIS IS MANDATORY OPTION	Block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Stream
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	More number of _____ provide more secure system in feistel cipher.
((OPTION_A)) THIS IS MANDATORY OPTION	rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	keys
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	Function
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes..

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following Algorithms does not belong to symmetric encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	3DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	RC5
((OPTION_D)) This is optional	IDEA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Assymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key?
((OPTION_A)) THIS IS MANDATORY OPTION	Not true, the message can also be decrypted with the Public Key.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A so called "one way function with back door" is applied for the encryption
((OPTION_C)) This is optional	The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key.
((OPTION_D)) This is optional	The encrypted message contains the function for decryption which identifies the Private Key.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	An one-way function is a function which a computer can calculate quickly, but whose reversal would last months or years. An one-way function with back door can be reversed with the help of a couple of additional information (the back door), but scarcely

	without this information. The information for the back door is contained in the private Key.
--	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the largest disadvantage of the symmetric Encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	More complex and therefore more time-consuming calculations.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Problem of the secure transmission of the Secret Key
((OPTION_C)) This is optional	Less secure encryption function.
((OPTION_D)) This is optional	Isn't used any more
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION))	As there is only one key in the symmetrical encryption, this must

)) This is also optional	be known by both sender and recipient and this key is sufficient to decrypt the secret message. Therefore it must be exchanged between sender and receiver in such a manner that an unauthorized person can in no case take possession of it.
--------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the principle of the encryption using a key?
((OPTION_A)) THIS IS MANDATORY OPTION	The key indicates which function is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	The key contains the secret function for encryption including parameters. Only a password can activate the key.
((OPTION_C)) This is optional	All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.
((OPTION_D)) This is optional	The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	C

E	
((EXPLANATION)) This is also optional	The encoding of a message is calculated by an algorithm. If always the same algorithm would be used, it would be easy to crack intercepted messages. However, it isn't possible to invent a new algorithm whenever the old one was cracked, therefor the possibility to parameterize algorithms is needed and this is the assignment of the key. All algorithms must be public, only the keys are secret (principle of Kerckhoff, Dutch cryptographer during 19th century).

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If the sender and receiver use different keys, the system is referred to as conventional cipher system
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Such a system is called asymmetric, two-key, or public-key cipher system

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW
((OPTION_A)) THIS IS MANDATORY OPTION	ABANDONED LOCK
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ENCRYPTED TEXT
((OPTION_C)) This is optional	ABANDONED TEXT
((OPTION_D)) This is optional	ENCRYPTED LOCK
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher uses $C = (p+3) \text{ mod } 26$ to encrypt.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Caesar Cipher is an example of
((OPTION_A)) THIS IS MANDATORY OPTION	Poly-alphabetic Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Mono-alphabetic Cipher
((OPTION_C)) This is optional	Multi-alphabetic Cipher
((OPTION_D)) This is optional	Bi-alphabetic Cipher
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis
((OPTION_A)) THIS IS MANDATORY OPTION	Random Polyalphabetic, Plaintext, Playfair
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Random Polyalphabetic, Playfair, Vignere
((OPTION_C)) This is optional	Random Polyalphabetic, Vignere, Playfair, Plaintext
((OPTION_D)) This is optional	Random Polyalphabetic, Plaintext, Beaufort, Playfair
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Random Polyalphabetic is the most resistant to frequency analysis, followed by Vignere, Playfair and then Plaintext.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-
((OPTION_A)) THIS IS MANDATORY OPTION	abqdnwewuwjphfvrrtrfznsdokvl
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	abqdmwuwjphfvyyrfznydokvl
((OPTION_C)) This is optional	tbqyrvmwuwjphfvyyrfznydokvl
((OPTION_D)) This is optional	baiuvmwuwjphfoeiyrfznydokvl
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cipher text:= $C_i = P_i + k_i \text{ mod } m \text{ (mod 26).}$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	nlazeiiblji
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nlazeiiblji
((OPTION_C)) This is optional	olaaeiiblki
((OPTION_D)) This is optional	mlaaeiiblki
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Cipher text:= $C_i = P_i + k_i \text{ mod } m \text{ (mod 26).}$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Confusion hides the relationship between the ciphertext and the plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Confusion hides the relationship between the ciphertext and the key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The S-Box is used to provide confusion, as it is dependent on the unknown key.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	false
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>The S-Box is used to provide confusion, as it is dependent on the unknown key.</p> <p>The P-Box is fixed, and there is no confusion due to it, but it provides diffusion.</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	<p>This is an example of</p> <pre> graph TD     P[P] --&gt; L1[L1]     P --&gt; R1[R1]     R1 --&gt; F1[F]     K1[K1] --&gt; F1     F1 --&gt; L2[L2]     L2 --&gt; R2[R2]     R2 --&gt; F2[F]     K2[K2] --&gt; F2     F2 --&gt; L3[L3]     L3 --&gt; Rn[Rn]     Rn --&gt; Fn[F]     Kn[Kn] --&gt; Fn     Fn --&gt; Ln[Ln]     Ln --- C[C]     </pre>
((OPTION_A)) THIS IS MANDATORY OPTION	SP Networks
((OPTION_B)) THIS IS ALSO MANDATORY	Feistel Cipher

OPTION	
((OPTION_C)) This is optional	Hash Algorithm
((OPTION_D)) This is optional	Hill Cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation
((OPTION_A)) THIS IS MANDATORY OPTION	1 and 3
((OPTION_B)) THIS IS ALSO MANDATORY	2 and 3

OPTION	
((OPTION_C)) This is optional	3 and 4
((OPTION_D)) This is optional	2 and 4
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Increase in any of the above 4 leads to slowing of the cipher algorithm i.e. more computational time will be required.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES follows
((OPTION_A)) THIS IS MANDATORY OPTION	Hash Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY	Caesars Cipher

OPTION	
((OPTION_C)) This is optional	Feistel Cipher Structure
((OPTION_D)) This is optional	SP Network
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES Algorithm Cipher System consists of _____ rounds (iterations) each with a round key
((OPTION_A)) THIS IS MANDATORY OPTION	12
((OPTION_B)) THIS IS ALSO MANDATORY	18

OPTION	
((OPTION_C)) This is optional	9
((OPTION_D)) This is optional	16
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES algorithm has a key length of
((OPTION_A)) THIS IS MANDATORY OPTION	128 Bits
((OPTION_B)) THIS IS ALSO MANDATORY	32 Bits

OPTION	
((OPTION_C)) This is optional	64 Bits
((OPTION_D)) This is optional	16 Bits
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	56 bits are used, the rest 8 bits are parity bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the round key is _____ bit and the Round Input is _____ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	48, 32
((OPTION_B)) THIS IS ALSO MANDATORY	64,32

OPTION	
((OPTION_C)) This is optional	56, 24
((OPTION_D)) This is optional	32, 32
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The round key is 48 bits. The input is 32 bits

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
((OPTION_A)) THIS IS MANDATORY OPTION	Scaling of the existing bits
((OPTION_B)) THIS IS ALSO MANDATORY	Duplication of the existing bits

<b>OPTION</b>	
((OPTION_C)) This is optional	Addition of zeros
((OPTION_D)) This is optional	Addition of ones
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits (permutation plus an expansion), that involves duplication of 16 of the bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The Initial Permutation table/matrix is of size
((OPTION_A)) THIS IS MANDATORY OPTION	16x8
((OPTION_B)) THIS IS ALSO MANDATORY	12x8

OPTION	
((OPTION_C)) This is optional	8x8
((OPTION_D)) This is optional	4x8
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	There are 64 bits to permute and this requires a 8x8 matrix.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The number of unique substitution boxes in DES after the 48 bit XOR operation are
((OPTION_A)) THIS IS MANDATORY OPTION	8
((OPTION_B)) THIS IS ALSO MANDATORY	4

OPTION	
((OPTION_C)) This is optional	6
((OPTION_D)) This is optional	12
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	IP-1 is the first step and the last step is IP during decryption.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A preferable cryptographic algorithm should have a good avalanche effect.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Thus statement is true as a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the size(in bits) of the key in the SDES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	24
((OPTION_B)) THIS IS ALSO MANDATORY	16

OPTION	
((OPTION_C)) This is optional	20
((OPTION_D)) This is optional	10
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The size of the key in the SDES algorithm is 10 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	GCD(a,b) is the same as GCD( a , b ).
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is true. $\gcd(60,24) = \gcd(60,-24) = 12$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	882
((OPTION_B)) THIS IS ALSO MANDATORY	770

OPTION	
((OPTION_C)) This is optional	1078
((OPTION_D)) This is optional	1225
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	$\text{GCD}(1160718174, 316258250) = 1078$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	$\text{GCD}(102947526, 239821932) = 6.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	13
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	17
((OPTION_D)) This is optional	7
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	$\text{GCD}(8376238, 1921023) = 13.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 1234 mod 4321 is
((OPTION_A)) THIS IS MANDATORY OPTION	3239
((OPTION_B)) THIS IS ALSO MANDATORY	3213

OPTION	
((OPTION_C)) This is optional	3242
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The multiplicative Inverse of 1234 mod 4321 is 3239.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 550 mod 1769 is
((OPTION_A)) THIS IS MANDATORY OPTION	434
((OPTION_B)) THIS IS ALSO MANDATORY	224

OPTION	
((OPTION_C)) This is optional	550
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The multiplicative Inverse of 550 mod 1769 is 550.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	<p><b>You are supposed to use hill cipher for encryption technique. You are provided with the following matrix,</b></p> $A = \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix}$ <p><b>Is the given matrix 'A', a valid key to be used for encryption?</b></p>
((OPTION_A)) THIS IS MANDATORY OPTION	Yes
((OPTION_B))	No

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Can't be determined
((OPTION_D)) This is optional	Data insufficient
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>For choosing any square matrix as a key, it should be taken care that the matrix is invertible, i.e. its inverse must exist.</p> <p>Here, in this case,</p> $  A   = 0$ <p>Therefore, it means that 'A' is not an invertible matrix. Hence matrix 'A' cannot be chosen as a key matrix for encryption in the <a href="#">Hill cipher</a>.</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	The input text is divided into two parts: one being left half and another one being right half.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Swapping of the left and right halves are performed after each round.
((OPTION_C)) This is optional	The plain text is converted into a matrix form first
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The fiestal structure does not require the conversion of the plain text into matrix form at any of its steps.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Among the following given options, chose the strongest encryption technique

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	DES ( Data Encryption Standard))
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Double DES
((OPTION_C)) This is optional	Triple DES
((OPTION_D)) This is optional	AES (Advance Encryption Standard)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	It has been proved that the AES performs much better than the all the other DES, whether it be single DES or series of DES.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	<p><b>Consider the following steps,</b></p> <ul style="list-style-type: none"> <li>i. Substitution bytes</li> <li>ii. Shift Rows</li> </ul>

IMAGES ALSO	<p>iii. Mix columns iv. Add round key</p> <p><b>The above steps are performed in each round of which of the following ciphers?</b></p>
((OPTION_A))  THIS IS MANDATORY OPTION	Rail fence cipher
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Data Encryption Standard (DES)
((OPTION_C))  This is optional	Advance Encryption Standard (AES)
((OPTION_D))  This is optional	None of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ algorithm transforms ciphertext to plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _____ cipher replaces one character with another character.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ cipher reorders the plaintext characters to create a ciphertext.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
((OPTION_A)) THIS IS MANDATORY OPTION	man-in-the-middle
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ciphertext attack
((OPTION_C)) This is optional	plaintext attack
((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the receiver uses the _____ key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either a or b
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES is a(n) _____ method adopted by the U.S. government.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	either (a) or (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ECB and CBC are _____ ciphers.
((OPTION_A))  THIS IS MANDATORY OPTION	block
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	stream
((OPTION_C))  This is optional	field
((OPTION_D))  This is optional	none of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ cipher, the same key is used by both the sender and receiver.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the sender uses the_____key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a(n) _____ cipher, a pair of keys is used.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	2
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	AES uses a _____ bit block size and a key size of _____ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	128; 128 or 256
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64; 128 or 192
((OPTION_C)) This is optional	256; 128, 192, or 256
((OPTION_D)) This is optional	128; 128, 192, or 256
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	It uses a 128-bit block size and a key size of 128, 192, or 256 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Like DES, AES also uses Feistel Structure.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES does not use a Feistel structure. Instead, each full round consists of four separate functions: -byte substitution -Permutation -arithmetic operations over a finite field, and -XOR with a key.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The 4x4 byte matrices in the AES algorithm are called
((OPTION_A)) THIS IS MANDATORY OPTION	States
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Words
((OPTION_C)) This is optional	Transitions
((OPTION_D)) This is optional	Permutations
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is a type of substitution cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	poly alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition cipher
((OPTION_C)) This is optional	Columnar cipher
((OPTION_D)) This is optional	Rail fence cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In substitution cipher the plain text is replaced by cipher text according to a fixed rule. There are two types of substitution cipher- Mono alphabetic and Poly alphabetic cipher.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following correctly defines poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	a substitution based cipher which uses multiple substitution at different positions
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a substitution based cipher which uses fixed substitution over entire message
((OPTION_C)) This is optional	a transposition based cipher which uses multiple substitution at different positions
((OPTION_D)) This is optional	A transposition based cipher which uses fixed substitution over entire message
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Poly alphabetic cipher is a type of substitution cipher. It uses multiple substitution at different positions in order to cipher the plain text.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a type of poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Rotor cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hill cipher
((OPTION_C)) This is optional	One time pad cipher
((OPTION_D)) This is optional	Affine cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	In poly alphabetic cipher each symbol of plain text is replaced by a different cipher text regardless of its occurrence. Out of the given options, only affine cipher is not a poly alphabetic cipher.

((MARKS)) QUESTION IS OF	2
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	We are provided the plain text "SUN". You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2?
((OPTION_A)) THIS IS MANDATORY OPTION	UWP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	NUS
((OPTION_C)) This is optional	WUP
((OPTION_D)) This is optional	QSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>In the Caesar cipher technique, the encryption is performed as follows,</p> $E(P, K) = (P + K) \bmod 26$ <p>Therefore,</p> $E(S, 2) = (18 + 2) \bmod 26 = 20 = U$ $E(U, 2) = (20 + 2) \bmod 26 = 22 = W$ $E(N, 2) = (13 + 2) \bmod 26 = 15 = P$ <p>Hence, the ciphertext is "UWP".</p>

--	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?
((OPTION_A)) THIS IS MANDATORY OPTION	<u>Hill Cipher</u>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<u>Playfair cipher</u>
((OPTION_C)) This is optional	Both a and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also	The hill cipher includes a square matrix as the key, and in Playfair cipher, we create a 5X5 matrix using the given key string. Hence,

optional	both these ciphers include the use of matrices.
----------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Playfair cipher is an example of _____
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C)) This is optional	transposition cipher
((OPTION_D)) This is optional	additive cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	Playfair cipher is a substitution cipher. It falls under the category of poly alphabetic cipher as it uses multiple substitution at different positions in order to cipher the plain text.
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Encryption in Playfair cipher is done using _
((OPTION_A)) THIS IS MANDATORY OPTION	a 5x5 table
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a 13x2 table
((OPTION_C)) This is optional	vigenere table
((OPTION_D)) This is optional	a 6x6 table
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A

((EXPLANATION)) This is also optional	
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the plain text corresponding to cipher text "BPKYFS" if playfair cipher is used with keyword as "SECRET" (assuming j is combined with i)?
((OPTION_A))  THIS IS MANDATORY OPTION	INDIAN
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	WORLD
((OPTION_C))  This is optional	DOLLAR
((OPTION_D))  This is optional	HELLO
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C

((EXPLANATION)) This is also optional	To decrypt the message we follow the reverse procedure. The table is formed in the same manner. Applying this we get the plain text to be "DOLLAR".
---------------------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair are identical?
((OPTION_A)) THIS IS MANDATORY OPTION	then that pair is neglected
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a null(or x) is added in between the letters
((OPTION_C)) This is optional	one of the identical letter is replaced by some other letter
((OPTION_D)) This is optional	then both of the letters are replaced by the letter appearing just next in the row
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	In playfair cipher if the letters in a pair are identical then a null is added in between the letters. Any letter can be used as a null as long as that letter is not the one being repeated.
---------------------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same row?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter at the corner of the row
((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	If the letters in a pair appear in same row then they are replaced by the letters appearing immediately right to them respectively. If the element to be replaced appears at the corner of the row then we wrap around to the left side of that row.
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the ciphered text if the string “SANFOUNDRY” is given as input to the code of playfair cipher with keyword as “SECRET” (assuming j is combined with i)?
((OPTION_A)) THIS IS MANDATORY OPTION	ZHQAPNPAFR
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AHQAPNPAFR
((OPTION_C)) This is optional	HAQAPNPAFR
((OPTION_D)) This is optional	QHAAPNPAFR
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	B

E	
((EXPLANATION)) This is also optional	<p>For encrypting the plain text using playfair cipher we use a <math>5 \times 5</math> table that is constructed by using keyword. Then we apply rules for encryption in order to get the ciphered text. Table is given as under-</p> <p>S E C R T</p> <p>A B D F G</p> <p>H I K L M</p> <p>N O P Q U</p> <p>V W X Y Z</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letters at the corner of the row
((OPTION_D))	that pair is neglected

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	If the letters in a pair appear in the same column then they are replaced by the letters appearing immediately below them respectively. If the element to be replaced appears at the corner of the column then we wrap around to the top side of that column.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair does not appear in same row or column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter of the same row at the corner of the rectangle defined by the original pair respectively

((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	If the letters in a pair does not appear in same row or column then they are replaced by the letters of the same row at the corner of the rectangle defined by the original pair respectively. The order of letters should be maintained.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Columnar cipher falls under the category of?
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C))	additive cipher

This is optional	
((OPTION_D)) This is optional	Transposition cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Columnar cipher is a transposition cipher. It falls under the category of transposition cipher as it encrypts the plain text by rearranging its letters.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following ciphered text would have NOT used transposition cipher for encryption of the plain text “CIPHER”?
((OPTION_A)) THIS IS MANDATORY OPTION	EPIHRC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	EHIPCR
((OPTION_C))	DTIPRC

This is optional	
((OPTION_D))	HRIPEC
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	We know that transposition cipher encrypts the plain text by shuffling the letters of the plain text. So out of the given options, only “DTIPRC” does not have the same set of letters as “CIPHER”.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many columns do we need to have in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	4
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	5
((OPTION_C))	6

This is optional	
((OPTION_D))	7
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So in this case it will be equal to 6.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the encrypted text corresponding to plain text “CLASSIFIED” using columnar transposition cipher with a keyword as “GAMES”?
((OPTION_A)) THIS IS MANDATORY OPTION	LFDSIASECI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SECIAISDFL
((OPTION_C))	CILFAISESD

This is optional																					
((OPTION_D))	IFSECIAISD																				
This is optional																					
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option																					
((CORRECT_CH OICE)) Either A or B or C or D or E	D																				
((EXPLANATION )) This is also optional	<p>For encrypting using columnar cipher we have to arrange the letters of the plain text in a table which has the same number of columns as the letters of the keyword. Then the letters of the keyword are arranged in alphabetical order and we read along each column.</p> <table style="margin-left: auto; margin-right: auto;"> <tr><td>3</td><td>1</td><td>4</td><td>2</td><td>5</td></tr> <tr><td>G</td><td>A</td><td>M</td><td>E</td><td>S</td></tr> <tr><td>C</td><td>L</td><td>A</td><td>S</td><td>S</td></tr> <tr><td>I</td><td>F</td><td>I</td><td>E</td><td>D</td></tr> </table> <p>So the ciphered text will be “IFSECIAISD”.</p>	3	1	4	2	5	G	A	M	E	S	C	L	A	S	S	I	F	I	E	D
3	1	4	2	5																	
G	A	M	E	S																	
C	L	A	S	S																	
I	F	I	E	D																	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many rows will the letters of the plain text occupy in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B))	2

THIS IS ALSO MANDATORY OPTION																			
((OPTION_C)) This is optional	3																		
((OPTION_D)) This is optional	4																		
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option																			
((CORRECT_CHOICE)) Either A or B or C or D or E	B																		
((EXPLANATION)) This is also optional	<p>Explanation: The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So when we will write the letters of the plain text row wise then there will be 2 rows of plain text in this case. The table is shown below :-</p> <table style="margin-left: auto; margin-right: auto;"> <tr> <td>S</td><td>E</td><td>C</td><td>R</td><td>E</td><td>T</td> </tr> <tr> <td>1</td><td>S</td><td>A</td><td>N</td><td>F</td><td>O</td><td>U</td> </tr> <tr> <td>2</td><td>N</td><td>D</td><td>R</td><td>Y</td> </tr> </table>	S	E	C	R	E	T	1	S	A	N	F	O	U	2	N	D	R	Y
S	E	C	R	E	T														
1	S	A	N	F	O	U													
2	N	D	R	Y															

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following statement is not true regarding columnar transposition cipher?
((OPTION_A)) THIS IS	probability of error is high while deciphering

<b>MANDATORY OPTION</b>	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	it cannot be combined with other ciphers
((OPTION_C))  This is optional	it is a traditional symmetric cipher
((OPTION_D))  This is optional	it is a weak cipher
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Although columnar transposition cipher is a weak cipher in itself. But it can be combined with other substitution ciphers so as to improve its security. The probability of error remains high while decoding columnar cipher as it is a lengthy process

<b>((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)</b>	1
<b>((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</b>	_____ is another data hiding technique which can be used in conjunction with cryptography for the extra-secure method of protecting data.
<b>((OPTION_A))</b>	Cryptography

THIS IS MANDATORY OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Steganography
((OPTION_C)) This is optional	Tomography
((OPTION_D)) This is optional	Chorography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Steganography is the technique of hiding data in another raw data. Steganography is another data hiding technique which can be used in conjunction with cryptography for an extra-secure method of protecting data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((OPTION_A))  THIS IS MANDATORY OPTION	Cryptography
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C))  This is optional	Steganography
((OPTION_D))  This is optional	Chorography
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Steganography helps in hiding any form of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _____ tool permits security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((OPTION_A))  THIS IS MANDATORY OPTION	Cryptography
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C))  This is optional	Chorography
((OPTION_D))  This is optional	Steganography
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	A steganography tool is a software tool that permits a security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The main motive for using steganography is that hackers or other users can hide a secret message behind a _____

((OPTION_A))  THIS IS MANDATORY OPTION	special file
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	ordinary file
((OPTION_C))  This is optional	program file
((OPTION_D))  This is optional	encrypted file
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	The main motive for using steganography is that hackers or other users can hide a secret message behind ordinary files. Some steganography tools are SSuite Picsel, rSteg etc.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	People will normally think it as a normal/regular file and your secret message will pass on without any _____

((OPTION_A)) THIS IS MANDATORY OPTION	Suspicion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	cracking
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Steganography techniques help hackers or other users to conceal covert message behind regular files. People will normally think it as a normal/regular file and your secret message will pass on without any suspicion.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	By using _____ you can diminish the chance of data leakage

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C)) This is optional	Chorography
((OPTION_D)) This is optional	Steganography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Hackers or other cyber criminals target ordinary files to hide different data or information within another data file. By using steganography, you can diminish the chance of data leakage.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Which of the following is a mode of operation for the Block ciphers in cryptography?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Electronic Code Book (ECB)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Cipher Block Chaining (CBC)
((OPTION_C)) This is optional	Counter (CTR) mode
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	For which of the following should EBC (Electronic Code Book) process not be used for encryption?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	For large block sizes
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	For fixed block sizes
((OPTION_C)) This is optional	For small block sizes
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	It is preferred that the block size in the ECB technique must be greater than 64 bits. If not, the text is padded to make it of the required length. This is due to some particular words and phrases that may be reused again often so that the same repetitive part of ciphertext can emerge as mixed.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	Which of the following is the main disadvantage of the ECB (Electronic Code Book)?

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	It requires large block size
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Padding is done to make the plain text divisible into blocks of fixed size
((OPTION_C)) This is optional	It is prone to cryptanalysis since there is a direct relationship between plain text and cipher text.
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	In <u>ECB</u> , there lies a direct relation between the plain text and the ciphertext. Therefore, it is easy for an outsider to break the encryption logic and steal the data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options is not correct according to the definition of the Cipher Block Chaining (CBC)?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC is a mode of operation for stream ciphers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Initialization vector (IV) is used in CBC in the initial phase.
((OPTION_C)) This is optional	It has better resistive nature towards cryptanalysis than ECB
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<a href="#">CBC</a> which stands for Cipher Block chaining is a mode of operation for block ciphers and not for stream ciphers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following modes of operations can be followed for both stream ciphers as well as block ciphers?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC (Cipher Block Chaining)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ECB (Electronic Code Book)
((OPTION_C)) This is optional	CFB (Cipher text Feed Back)
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	<b>CFB</b> is primarily a mode to derive some characteristics of a stream cipher from a block cipher on the cryptography in cryptoanalysis.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

<p>((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</p>	<p>All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES?</p> <ul style="list-style-type: none"> <li>i. Substitution bytes</li> <li>ii. Shift rows</li> <li>iii. Mix columns</li> <li>iv. Add round key</li> </ul>
<p>((OPTION_A)) THIS IS MANDATORY OPTION</p>	<p>i</p>
<p>((OPTION_B)) THIS IS ALSO MANDATORY OPTION</p>	<p>iii</p>
<p>((OPTION_C)) This is optional</p>	<p>All of the mentioned</p>
<p>((OPTION_D)) This is optional</p>	<p>None of the mentioned</p>
<p>((OPTION_E)) This is optional. If optional keep empty so that system will skip this option</p>	
<p>((CORRECT_CHOICE)) Either A or B or C or D or E</p>	<p>B</p>
<p>((EXPLANATION)) This is also optional</p>	<p>In the AES algorithm, the MIX COLUMN operation is performed in all the rounds except the final round of the algorithm.</p>

<p>((MARKS))</p>	<p>1</p>
------------------	----------

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"The number of rounds in the AES algorithm depends upon the key size being used." Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	128 key size: 10 rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	192 key size: 12 rounds
((OPTION_C)) This is optional	256 key size: 14 rounds
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS))	2
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Avalanche effect
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Completeness
((OPTION_C)) This is optional	Both a. and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS))	2
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For the AES-128 algorithm there are _____ similar rounds and _____ round is different.
((OPTION_A)) THIS IS MANDATORY OPTION	2 pair of 5 similar rounds ; every alternate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	9 ; the last
((OPTION_C)) This is optional	8 ; the first and last
((OPTION_D)) This is optional	10 ; no
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS))	1
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the 4 operations are false for each round in the AES algorithm? i) Substitute Bytes ii) Shift Columns iii) Mix Rows iv) XOR Key
((OPTION_A)) THIS IS MANDATORY OPTION	i) only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii) iii) and iv)
((OPTION_C)) This is optional	ii) and iii)
((OPTION_D)) This is optional	only iv
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES rounds involve substitute bytes, shift rows, mix columns and addition of round key.

((MARKS))	1
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	There is an addition of round key before the start of the AES round algorithms.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In AES the final round contains only three transformations, and there is an initial single transformation (Add Round Key) before the first round which can be considered Round 0. Each transformation takes 4x4 matrixes as input and produces a 4x4 matrix as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1																
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the Shifted Row transformation for the matrix bellow?  <table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>6B</td><td>77</td><td>A4</td><td>6B</td></tr> <tr> <td>AD</td><td>01</td><td>F0</td><td>63</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	FE	72	2B	D7	6B	77	A4	6B	AD	01	F0	63	30	D7	AF	FE
FE	72	2B	D7														
6B	77	A4	6B														
AD	01	F0	63														
30	D7	AF	FE														
((OPTION_A))  THIS IS MANDATORY OPTION	<table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>6B</td><td>77</td><td>A4</td><td>6B</td></tr> <tr> <td>AD</td><td>01</td><td>F0</td><td>63</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	FE	72	2B	D7	6B	77	A4	6B	AD	01	F0	63	30	D7	AF	FE
FE	72	2B	D7														
6B	77	A4	6B														
AD	01	F0	63														
30	D7	AF	FE														
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	<table border="1"> <tr> <td>72</td><td>2B</td><td>D7</td><td>FE</td></tr> <tr> <td>A4</td><td>6B</td><td>6B</td><td>77</td></tr> <tr> <td>63</td><td>AD</td><td>01</td><td>F0</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	72	2B	D7	FE	A4	6B	6B	77	63	AD	01	F0	30	D7	AF	FE
72	2B	D7	FE														
A4	6B	6B	77														
63	AD	01	F0														
30	D7	AF	FE														
((OPTION_C))  This is optional	<table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>77</td><td>A4</td><td>6B</td><td>6B</td></tr> <tr> <td>F0</td><td>63</td><td>AD</td><td>01</td></tr> <tr> <td>FE</td><td>30</td><td>D7</td><td>AF</td></tr> </table>	FE	72	2B	D7	77	A4	6B	6B	F0	63	AD	01	FE	30	D7	AF
FE	72	2B	D7														
77	A4	6B	6B														
F0	63	AD	01														
FE	30	D7	AF														
((OPTION_D))  This is optional	<table border="1"> <tr> <td>D7</td><td>FE</td><td>72</td><td>2B</td></tr> <tr> <td>A4</td><td>6B</td><td>6B</td><td>77</td></tr> <tr> <td>01</td><td>AD</td><td>63</td><td>F0</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	D7	FE	72	2B	A4	6B	6B	77	01	AD	63	F0	30	D7	AF	FE
D7	FE	72	2B														
A4	6B	6B	77														
01	AD	63	F0														
30	D7	AF	FE														

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The Shift Rows transformation consists of: -Not shifting the first row of the state array at all. -Circularly shifting the second row by one byte to the left. -Circularly shifting the third row by two bytes to the left, and -Circularly shifting the last row by three bytes to the left.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not weak key in DES
((OPTION_A)) THIS IS MANDATORY OPTION	0x0101010101010101
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0xEFABFEFEFEFEFEFE
((OPTION_C)) This is optional	0x1F1F1F1F0E0E0E0E
((OPTION_D))	0xFFFFFFFFFFFFFF

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple-DES has _____ keys.
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	2
((OPTION_C)) This is optional	5
((OPTION_D))	4

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a encryption technique which uses two instance of DES on same plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	Double DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tripple DES
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ attack which can be used to break through double DES.
((OPTION_A)) THIS IS MANDATORY OPTION	Brute force
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	meet-in-the middle
((OPTION_C)) This is optional	Timing
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple DES involve __
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption, Decryption, Decryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption ,Encryption, Encryption
((OPTION_C)) This is optional	Decryption ,Encryption, Decryption
((OPTION_D))	Encryption, Decryption, Encryption

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ involves feeding the successive output blocks from the underlying block cipher back to it
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	OFB
((OPTION_D))	CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is counter-based version of CFB mode without the feedback
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	counter
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below mode is independent of previous output
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	CFB
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Errors get propagated in all modes except ___and ___
((OPTION_A)) THIS IS MANDATORY OPTION	ECB,COUNTER
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC,COUNTER
((OPTION_C)) This is optional	CFB,COUNTER
((OPTION_D))	OFB,CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Patterns are not preserved in ___ mode
((OPTION_A)) THIS IS MANDATORY OPTION	CBC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CFB
((OPTION_C)) This is optional	Both CBC and CFB
((OPTION_D))	ECB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A small change in plaintext results in the very great change in the cipher text indicates which characteristic
((OPTION_A)) THIS IS MANDATORY OPTION	completeness
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Strong key
((OPTION_C)) This is optional	Avalanche effect
((OPTION_D))	All of the above

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ ciphers, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of cipher text.
((OPTION_A)) THIS IS MANDATORY OPTION	Block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Stream
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	More number of _____ provide more secure system in feistel cipher.
((OPTION_A)) THIS IS MANDATORY OPTION	rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	keys
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	Function
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes..

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In public key cryptosystem _____ keys are used for encryption and decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	Same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Different
((OPTION_C)) This is optional	Encryption Keys
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	In conventional cryptosystem, same keys are used for encryption and decryption where as in public key cryptosystem different keys are used.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In public key cryptosystem which is kept as public?
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption keys
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption keys
((OPTION_C)) This is optional	Encryption & Decryption keys
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	In public key cryptosystem, the encryption keys are kept as public where as decryption keys are kept as secret.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Public key cryptosystem uses same key for both encryption and decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which should be kept as a secret in public key cryptosystem?
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption key
((OPTION_C)) This is optional	Encryption & Decryption key
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	In public key cryptosystem, Encryption is done using public key . decryption key needs to be kept as a secret.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Euler's totient function is determined by
((OPTION_A)) THIS IS MANDATORY OPTION	$pq$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(p-1)(q-1)$
((OPTION_C)) This is optional	$(p+1)(q+1)$
((OPTION_D)) This is optional	$p/q$
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	The Euler's totient function is determined by $(p-1)(q-1)$ , where p and q are kept hidden.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?
((OPTION_A))  THIS IS MANDATORY OPTION	p and q should be divisible by $\Phi(n)$
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	p and q should be co-prime
((OPTION_C))  This is optional	p and q should be prime
((OPTION_D))  This is optional	p/q should give no remainder
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	'p' and 'q' should have large random values which are both prime numbers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, $\Phi(n) = \text{_____}$ in terms of p and q.
((OPTION_A)) THIS IS MANDATORY OPTION	(p)/(q)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	(p)(q)
((OPTION_C)) This is optional	(p-1)(q-1)
((OPTION_D)) This is optional	(p+1)(q+1)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	$\Phi(n) = (p-1)(q-1).$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, we select a value 'e' such that it lies between 0 and $\Phi(n)$ and it is relatively prime to $\Phi(n)$ .
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	$\gcd(e, \Phi(n))=1$ ; and $1 < e < \Phi(n)$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 19$ and choose $e=17$ . Apply RSA algorithm where message=5 and find the cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	C=80
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	C=92
((OPTION_C)) This is optional	C=56
((OPTION_D)) This is optional	C=23
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 209.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 19$ and choose $d=17$ . Apply RSA algorithm where Cipher message=80 and thus find the plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	54
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	43
((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	24
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	$n = pq = 11 \times 19 = 209$ . $C=M^e \text{ mod } n ; C=5^{17} \text{ mod } 209 ; C = 80 \text{ mod } 209$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	$n = 35; e = 5; C = 10$ . What is the plaintext (use RSA) ?
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	7
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Use RSA system to decrypt and get PT = 5.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 17$ and choose $e=7$ . Apply RSA algorithm where PT message=88 and thus find the CT.
((OPTION_A)) THIS IS MANDATORY OPTION	23
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64
((OPTION_C)) This is optional	11
((OPTION_D)) This is optional	54
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 187$ . $C=M^e \text{ mod } n ; C=88^7 \text{ mod } 187 ; C = 11 \text{ mod } 187$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 17$ and choose $e=7$ . Apply RSA algorithm where Cipher message=11 and thus find the plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	88
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	122
((OPTION_C)) This is optional	143
((OPTION_D)) This is optional	111
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 187$ . $C=M^e \text{ mod } n ; C=11^{23} \text{ mod } 187 ; C = 88 \text{ mod } 187$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an RSA system the public key of a given user is $e = 31$ , $n = 3599$ . What is the private key of this user?
((OPTION_A))  THIS IS MANDATORY OPTION	3031
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	2412
((OPTION_C))  This is optional	2432
((OPTION_D))  This is optional	1023
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	By trial and error, we determine that $p = 59$ and $q = 61$ . Hence $f(n) = 58 \times 60 = 3480$ . Then, using the extended Euclidean algorithm, we find that the multiplicative inverse of 31 modulo $f(n)$ is 3031

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Compute private key (d, p, q) given public key (e=23, n=233 ´ 241=56,153).
((OPTION_A)) THIS IS MANDATORY OPTION	35212
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	12543
((OPTION_C)) This is optional	19367
((OPTION_D)) This is optional	32432
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Since n=233 ´ 241=56,153, p=233 and q=241 $f(n) = (p - 1)(q - 1) = 55,680$ Using Extended Euclidean algorithm, we obtain $d = 23^{-1} \text{ mod } 55680 = 19,367.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a RSA cryptosystem a particular A uses two prime numbers $p = 13$ and $q = 17$ to generate her public and private keys. If the public key of A is 35. Then the private key of A is _____.
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	13
((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	17
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In an RSA cryptosystem, for public key: $\text{GCD}(\phi(n), e) = 1$ And, for private key:

	$(e * d) \bmod \phi(n) = 1$ Where, $\phi(n) = (p - 1)*(q - 1) = (13 - 1)(17 - 1) = 12 * 16 = 192$ Such that $1 < e, d < \phi(n)$ Therefore, the private key is: $(35 * d) \bmod \phi(n) = 1$ $d = 11$
--	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the RSA public key cryptosystem, which one of the following numbers will always be largest?
((OPTION_A)) THIS IS MANDATORY OPTION	E
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	N
((OPTION_C)) This is optional	P
((OPTION_D)) This is optional	Q
((OPTION_E)) This is optional. If optional keep empty so that system will skip	

this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	The number n is generated as the product of the two large prime numbers p and q. Therefore, n must always be greater than both p and q. Furthermore, it is an algorithm constraint that e must be chosen such that e is smaller than n. Therefore, in RSA cryptography n is always the largest of the four variables shown in the options to this question.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If Richard wants to send an encrypted message to Sue using a public key cryptosystem, which key does he use to encrypt the message?
((OPTION_A)) THIS IS MANDATORY OPTION	Richard's public key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Richard's private key
((OPTION_C)) This is optional	Sue's public key
((OPTION_D)) This is optional	Sue's private key
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Richard must encrypt the message using Sue's public key so that Sue can decrypt it using her private key. If he encrypted the message with his own public key, the recipient would need to know Richard's private key to decrypt the message. If he encrypted it with his own private key, any user could decrypt the message using Richard's freely available public key. Richard could not encrypt the message using Sue's private key because he does not have access to it. If he did, any user could decrypt it using Sue's freely available public key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Acme Widgets currently uses a 1,024-bit RSA encryption standard companywide. The company plans to convert from RSA to an elliptic curve cryptosystem. If it wishes to maintain the same cryptographic strength, what ECC key length should it use?
((OPTION_A)) THIS IS MANDATORY OPTION	160 bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	512 bits
((OPTION_C)) This is optional	1,024 bits
((OPTION_D)) This is optional	2,048 bits

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The elliptic curve cryptosystem requires significantly shorter keys to achieve encryption that would be the same strength as encryption achieved with the RSA encryption algorithm. A 1,024-bit RSA key is cryptographically equivalent to a 160-bit elliptic curve cryptosystem key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Richard received an encrypted message sent to him from Sue. Which key should he use to decrypt the message?
((OPTION_A)) THIS IS MANDATORY OPTION	Richard's public key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Richard's private key
((OPTION_C)) This is optional	Sue's public key
((OPTION_D)) This is optional	Sue's private key

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Sue would have encrypted the message using Richard's public key. Therefore, Richard needs to use the complementary key in the key pair, his private key, to decrypt the message.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	One commonly used public-key cryptography method is the _____ algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	RSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RAS
((OPTION_C)) This is optional	RSA
((OPTION_D)) This is optional	RAA

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
((OPTION_A)) THIS IS MANDATORY OPTION	man-in-the-middle
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ciphertext attack
((OPTION_C)) This is optional	plaintext attack
((OPTION_D)) This is optional	none of the above

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the objective of Diffie-Hellman key exchange?
((OPTION_A)) THIS IS MANDATORY OPTION	To protect encrypted data from man-in-the-middle attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	To perform mutual authentication on both sides
((OPTION_C)) This is optional	To prove to another party that one holds a secret key without revealing it
((OPTION_D)) This is optional	To establish a shared secret key on both sides

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The security of RSA encryption relies on which assumption?
((OPTION_A)) THIS IS MANDATORY OPTION	It is computationally infeasible to compute a GCD of two large numbers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	It is computationally infeasible to factor a large number.
((OPTION_C)) This is optional	It is computationally infeasible to test whether a large number is prime.
((OPTION_D)) This is optional	It is computationally infeasible to compute a square modulo n.

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	All of the above
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is asymmetric cryptography?
((OPTION_A)) THIS IS MANDATORY OPTION	ECC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	Both ECC and RSA
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below requires less hardware capacity because of less key size
((OPTION_A)) THIS IS MANDATORY OPTION	ECC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	DES
((OPTION_D)) This is optional	AES

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Diffie Hellman is _____
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption algorithm
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	D-H is key exchange algorithm

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Timing attack on RSA can be avoided by __
((OPTION_A)) THIS IS MANDATORY OPTION	Padding extra bits in message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Adding delays
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below algorithm is used in cryptocurrency?
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AES
((OPTION_C)) This is optional	ECC
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When a hash function is used to provide message authentication, the hash function value is called to as:
((OPTION_A)) THIS IS MANDATORY OPTION	Message Field
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Message Digest
((OPTION_C)) This is optional	Message Score
((OPTION_D)) This is optional	Message Leap

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	We know that the hash function providing message authentication is referred to as message digest in cryptography.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following are used to create a message digest  a. RSA b. SHA-1 c. DES d. MD5
((OPTION_A)) THIS IS MANDATORY OPTION	A&B
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	B&C
((OPTION_C)) This is optional	A&C

((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	They are Message digest algorithm

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the output of a cryptographic hash function?
((OPTION_A)) THIS IS MANDATORY OPTION	A variable set of bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A fixed set of bits, derived from one-way mathematical operations
((OPTION_C)) This is optional	An output which may be easily discovered by an adversary

((OPTION_D)) This is optional	Outputs of such functions are of no importance
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message digest algorithms are primarily used to provide _____
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Authentication
((OPTION_C)) This is optional	inegrity

((OPTION_D)) This is optional	authorization
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a message digest algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IDEA
((OPTION_C)) This is optional	MD5

((OPTION_D)) This is optional	RSA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message _____ means that the data must arrive at the receiver exactly as sent.
((OPTION_A)) THIS IS MANDATORY OPTION	confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	integrity
((OPTION_C)) This is optional	authentication

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
((OPTION_A)) THIS IS MANDATORY OPTION	confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	integrity
((OPTION_C)) This is optional	authentication

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ function creates a message digest out of a message
((OPTION_A)) THIS IS MANDATORY OPTION	encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	hash

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ is a trusted third party that assigns a symmetric key to two parties.
((OPTION_A)) THIS IS MANDATORY OPTION	Public directory
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Certificate authority
((OPTION_C)) This is optional	Both

((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature provides _____.
((OPTION_A)) THIS IS MANDATORY OPTION	authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nonrepudiation
((OPTION_C)) This is optional	both (a) and (b)

((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A digital signature needs a(n) _____ system
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)

((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ is a federal or state organization that binds a public key to an entity and issues a certificate.
((OPTION_A)) THIS IS MANDATORY OPTION	KDC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Kerberos
((OPTION_C)) This is optional	CA

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	means that a sender must not be able to deny sending a message that he sent.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication

((OPTION_D)) This is optional	Nonrepudiation
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Kerberos is a popular session key creator protocol that requires an authentication server and a ticket-granting server.
((OPTION_A)) THIS IS MANDATORY OPTION	KDC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Kerberos
((OPTION_C)) This is optional	CA

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The MD5 is a message digest algorithm developed by
((OPTION_A)) THIS IS MANDATORY OPTION	Ron Rivest.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	WhiteField Diffie.
((OPTION_C)) This is optional	Martin Hellman.

((OPTION_D)) This is optional	Diffie-Hellman.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 is quite fast and produces _____ message digests
((OPTION_A)) THIS IS MANDATORY OPTION	512 bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	1024 bits
((OPTION_C)) This is optional	128 bits

((OPTION_D)) This is optional	64 bits
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The first step of MD5 is
((OPTION_A)) THIS IS MANDATORY OPTION	add padding bits to original messsge
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	adding append length bits
((OPTION_C)) This is optional	divide the input into 512 bit blocks

((OPTION_D)) This is optional	compression
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In MD5, the process block divides the 512 bits into _____ sub blocks.
((OPTION_A)) THIS IS MANDATORY OPTION	16
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	24
((OPTION_C)) This is optional	32

((OPTION_D)) This is optional	84
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which financial institutions have a relationship with merchants for processing payment card authorizations and payments?
((OPTION_A)) THIS IS MANDATORY OPTION	Issuer
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Acquirer
((OPTION_C)) This is optional	Merchant

((OPTION_D)) This is optional	Dealer
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following contains the order information such as which items are being purchased?
((OPTION_A)) THIS IS MANDATORY OPTION	PI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	OI
((OPTION_C)) This is optional	MD

((OPTION_D)) This is optional	DS
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Payment information can be encrypted by using _____.
((OPTION_A)) THIS IS MANDATORY OPTION	customer's private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	merchant public key
((OPTION_C)) This is optional	one-time session key.

((OPTION_D)) This is optional	customer's public key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature envelope is decrypted by using _____.
((OPTION_A)) THIS IS MANDATORY OPTION	merchant private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	payment's private key
((OPTION_C)) This is optional	payment public key

((OPTION_D)) This is optional	merchant's public key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ will ensure the merchant and their payment information
((OPTION_A)) THIS IS MANDATORY OPTION	Digital certificate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Merchant
((OPTION_C)) This is optional	Dual signature

((OPTION_D)) This is optional	Certificate authority
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SET provides an authentication with the help of _____
((OPTION_A)) THIS IS MANDATORY OPTION	dual signature
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	digital certificate
((OPTION_C)) This is optional	payment's public key

((OPTION_D)) This is optional	payment's private key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are very crucial for success of RSA algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	Integers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Prime numbers
((OPTION_C)) This is optional	Negative number

((OPTION_D)) This is optional	Fraction
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ acts as financial institutions who provides a payment card to a card holder
((OPTION_A)) THIS IS MANDATORY OPTION	payment gateway
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	card holder
((OPTION_C)) This is optional	acquirer

((OPTION_D)) This is optional	issuer
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	ISSUER means Bank

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Who will be responsible for processing the payment from the customer's account to the merchant account?
((OPTION_A)) THIS IS MANDATORY OPTION	Acquirer
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Merchant
((OPTION_C)) This is optional	Issuer

((OPTION_D)) This is optional	Payment gateway
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The cardholder combines the PIMD and OIMD and hashes them together to form
((OPTION_A)) THIS IS MANDATORY OPTION	OPMD
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	POMD
((OPTION_C)) This is optional	MD

((OPTION_D)) This is optional	DS
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which process will ensure that the issues of the credit card is an approved transactions?
((OPTION_A)) THIS IS MANDATORY OPTION	Payment capture
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Payment authorization
((OPTION_C)) This is optional	Purchase request

((OPTION_D)) This is optional	Purchase reply
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is used for hiding the payment information from the merchant.
((OPTION_A)) THIS IS MANDATORY OPTION	SET
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	SHTTP

((OPTION_D)) This is optional	TSP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A __word buffer is used to compute the message digest in MD5
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4
((OPTION_C)) This is optional	5

((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	4 WORD A,B,C,D

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In MD5, the message is <b>padded</b> so that its length is divisible by ____
((OPTION_A)) THIS IS MANDATORY OPTION	32
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	128
((OPTION_C)) This is optional	512

((OPTION_D)) This is optional	1024
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 should meet requirements:
((OPTION_A)) THIS IS MANDATORY OPTION	It is impossible to generate two inputs that cannot produce the same hash function
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	It is impossible to generate a message having the same hash value
((OPTION_C)) This is optional	Both of the above

((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 takes an input of ___ size and produces an output if a 128-bit hash value
((OPTION_A)) THIS IS MANDATORY OPTION	Any
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Multiple of 512
((OPTION_C)) This is optional	Multiple of 128

((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following best describes sniffing?
((OPTION_A)) THIS IS MANDATORY OPTION	Gathering packets to locate IP addresses, in order to initiate a session hijacking attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Analyzing packets in order to locate the sequence number to start a session hijack
((OPTION_C)) This is optional	Monitoring TCP sessions in order to initiate a session-hijacking attack

((OPTION_D)) This is optional	Locating a host susceptible to a session-hijack attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Sniffing is usually used to locate the sequence number, which is necessary for a session hijack.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The secret key between members needs to be created as a _____ key when two members contact Kerberos system
((OPTION_A)) THIS IS MANDATORY OPTION	Public
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Session
((OPTION_C))	complimentary

This is optional	
((OPTION_D))	None of these
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The main components of Kerberos are:
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Ticket granting server
((OPTION_C))	database

This is optional	
((OPTION_D))	All of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ performs the initial authentication and ticket for Ticket Granting Service
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Ticket granting server
((OPTION_C))	Database

This is optional	
((OPTION_D))	Kerberos
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The Authentication Server verifies access right of users in __
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TG server
((OPTION_C))	Database

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ issues the ticket for the Server
((OPTION_A)) THIS IS MANDATORY OPTION	AS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TGS
((OPTION_C))	DB

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Kerberos is primarily used for _____
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C))	confidentiality

This is optional	
((OPTION_D))	authorization
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The KDC encrypts the TGT with a password that only the _____ knows.
((OPTION_A)) THIS IS MANDATORY OPTION	AS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TGS
((OPTION_C))	Server

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Because no one else needs to be able to see the contents.  It's for the server to keep track of the client

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The essence of Kerberos' system is _____.
((OPTION_A)) THIS IS MANDATORY OPTION	One way authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity

((OPTION_C)) This is optional	Mutual authentication
((OPTION_D)) This is optional	Public authentication
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not an element/field of the X.509 certificates?
((OPTION_A)) THIS IS MANDATORY OPTION	Issuer Name
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Serial Modifier

((OPTION_C)) This is optional	Issuer unique Identifier
((OPTION_D)) This is optional	Signature
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	X.509 certificate recommends which cryptographic algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	DES

((OPTION_C)) This is optional	AES
((OPTION_D)) This is optional	Rabin
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The standard used in digital certificates that defines its structure, fields, and Values is
((OPTION_A)) THIS IS MANDATORY OPTION	Kerberos
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	End to end encryption

((OPTION_C)) This is optional	X.509
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	X.509 Certificates includes
((OPTION_A)) THIS IS MANDATORY OPTION	Version
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	signature algorithm identifier

((OPTION_C)) This is optional	period of validity
((OPTION_D)) This is optional	extension fields
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	All of the above
((CORRECT_CH OICE)) Either A or B or C or D or E	E
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ defines a framework for the provision of authentication services by the X.500 directory
((OPTION_A)) THIS IS MANDATORY OPTION	X.509
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	X.508

((OPTION_C)) This is optional	X.505
((OPTION_D)) This is optional	X.609
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A digital signature is a mathematical technique used to validate the _____ and _____ of a message, software or digital document
((OPTION_A)) THIS IS MANDATORY OPTION	Authenticity, integrity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity, confidentiality

((OPTION_C)) This is optional	Integrity,non-repudiation
((OPTION_D)) This is optional	Authenticity,confidentiality
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature involves ____ and ____
((OPTION_A)) THIS IS MANDATORY OPTION	Signature verification ,validation
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Signature creation,verification

((OPTION_C)) This is optional	Signature creation,deletion
((OPTION_D)) This is optional	Signature validation,modification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message digest is computed by applying hash function on the message and then message digest is encrypted using _____ key of sender to form the digital signature.
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public

((OPTION_C)) This is optional	Session
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In digital signature , Receiver decrypts the digital signature using the _____ key of sender
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public

((OPTION_C)) This is optional	Secret
((OPTION_D)) This is optional	Session
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In digital signature, The message digest computed by ___ and the message digest (got by decryption on digital signature) need to be ___ for ensuring integrity
((OPTION_A)) THIS IS MANDATORY OPTION	Receiver,same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Receiver,different

((OPTION_C)) This is optional	Sender,same
((OPTION_D)) This is optional	Sender,different
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.
((OPTION_A)) THIS IS MANDATORY OPTION	Digital certificate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Digital signature

((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature follows _____
((OPTION_A)) THIS IS MANDATORY OPTION	Digital Signature Standard (DSS)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	X.509 standard format

((OPTION_C)) This is optional	Both of the above
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In diffie-hellman algorithm, if Alice and Bob wish to communicate with each other, they first agree between them a large prime number n, and ____ g
((OPTION_A)) THIS IS MANDATORY OPTION	Generator
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Small prime number

((OPTION_C)) This is optional	Natural number
((OPTION_D)) This is optional	Factorial
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm if $X_a$ is private key of user then public key is calculated by ____
((OPTION_A)) THIS IS MANDATORY OPTION	$g^{X_a} \text{ mod } n$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$n^{X_a} \text{ mod } n$

((OPTION_C)) This is optional	$g^n \bmod p$
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm, ____ keys of each other should be known
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Session

((OPTION_C)) This is optional	Public
((OPTION_D)) This is optional	No
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm,shared secret key is calculated by ____
((OPTION_A)) THIS IS MANDATORY OPTION	$(g^a \text{ mod } n)^b \text{ mod } n$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(g^b \text{ mod } n)^a \text{ mod } n$

((OPTION_C)) This is optional	Both of the above
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm, the resulting shared secret will be the ___ every time
((OPTION_A)) THIS IS MANDATORY OPTION	Same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Different

((OPTION_C)) This is optional	Maybe same
((OPTION_D)) This is optional	Can't say
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ the first widely used method of safely developing and exchanging keys over an insecure channel
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSS

((OPTION_C)) This is optional	Diffie Hellman
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4

((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value $q = 17$ and primitive root $= 5$ . If Alice's secret key is 4 and Bob's secret key is 6, what is the shared secret key they exchanged?
((OPTION_A)) THIS IS MANDATORY OPTION	16
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	17

((OPTION_C)) This is optional	18
((OPTION_D)) This is optional	19
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Each round of MD5 consist of ____ operations
((OPTION_A)) THIS IS MANDATORY OPTION	14
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	15

((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	18
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Each buffer of MD5 algorithm is ____ bit long
((OPTION_A))  THIS IS MANDATORY OPTION	32
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	64

((OPTION_C)) This is optional	128
((OPTION_D)) This is optional	512
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	RSA is _____ cryptography
((OPTION_A)) THIS IS MANDATORY OPTION	Asymmetric
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key

((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Value generated by hash function is referred as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Message digest
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hash

((OPTION_C)) This is optional	MAC
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not service of digital signature
((OPTION_A))  THIS IS MANDATORY OPTION	Authentication to message
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Data integrity

((OPTION_C)) This is optional	Non-repudiation
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ digitally signs this entire information and includes digital signature in the certificate
((OPTION_A)) THIS IS MANDATORY OPTION	CA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	KDC

((OPTION_C)) This is optional	PKI
((OPTION_D)) This is optional	DB
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA ,e is used as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key

((OPTION_C)) This is optional	Euler's totient
((OPTION_D)) This is optional	Session key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, d is referred as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key
((OPTION_C)) This is optional	Totient function
((OPTION_D)) This is optional	Session key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

1.	<p>Asymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key?</p> <ol style="list-style-type: none"> <li>1. Not true, the message can also be decrypted with the Public Key.</li> <li>2. A so called "one way function with back door" is applied for the encryption.</li> <li>3. The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key.</li> <li>4. The encrypted message contains the function for decryption which identifies the Private Key.</li> </ol>	2
2.	<p>In which way does the Combined Encryption combine symmetric and asymmetric encryption?</p> <ol style="list-style-type: none"> <li>1. First, the message is encrypted with symmetric encryption and afterwards it is encrypted asymmetrically together with the key.</li> <li>2. The secret key is symmetrically transmitted, the message itself asymmetrically.</li> <li>3. First, the message is encrypted with asymmetric encryption and afterwards it is encrypted symmetrically together with the key.</li> <li>4. The secret key is asymmetrically transmitted, the message itself symmetrically.</li> </ol>	4
3.	<p>Which is the largest disadvantage of the symmetric Encryption?</p> <ol style="list-style-type: none"> <li>1. More complex and therefore more time-consuming calculations.</li> <li>2. Problem of the secure transmission of the Secret Key.</li> <li>3. Less secure encryption function.</li> <li>4. Isn't used any more.</li> </ol>	2
4.	<p>Which is the principle of the encryption using a key?</p> <ol style="list-style-type: none"> <li>1. The key indicates which function is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.</li> <li>2. The key contains the secret function for encryption including parameters. Only a password can activate the key.</li> <li>3. All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.</li> <li>4. The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.</li> </ol>	3
5.	<p>A substitution cipher substitutes one symbol with</p> <ol style="list-style-type: none"> <li>1. Keys</li> <li>2. Others</li> <li>3. Multi Parties</li> <li>4. Single Party</li> </ol>	2

6.	An asymmetric-key (or public-key) cipher uses  1. 1 Key 2. 2 Key 3. 3 Key 4. 4 Key	2
7.	A straight permutation cipher or a straight P-box has the same number of inputs as  1. cipher 2. Frames 3. Outputs 4. Bits	3
8.	We use Cryptography term to transforming messages to make them secure and immune to  1. Change 2. Idle 3. Attacks 4. Defend	3
9.	The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not  1. Authenticated 2. Joined 3. Submit 4. Separate	1
10.	The cryptography algorithms (ciphers) are divided into  1. two groups 2. four groups 3. one single group 4. None	1
11.	The shift cipheris sometimes referred to as the  1. Caesar cipher 2. Julia cipher 3. plain cipher 4. All of them	1

12.	<p>One commonly used public-key cryptography method is the _____ algorithm.</p> <ol style="list-style-type: none"> <li>1. RSS</li> <li>2. RAS</li> <li>3. RSA</li> <li>4. RAA</li> </ol>	3
13.	<p>A(n) _____ algorithm transforms cipher text to plaintext.</p> <ol style="list-style-type: none"> <li>1. encryption</li> <li>2. decryption</li> <li>3. either (a) or (b)</li> <li>4. neither (a) nor (b)</li> </ol>	2
14.	<p>The _____ method provides a one-time session key for two parties.</p> <ol style="list-style-type: none"> <li>1. Diffie-Hellman</li> <li>2. RSA</li> <li>3. DES</li> <li>4. AES</li> </ol>	1
15.	<p>A(n) _____ is a keyless substitution cipher with N inputs and M outputs that uses a formula to define the relationship between the input stream and the output stream.</p> <ol style="list-style-type: none"> <li>1. S-box</li> <li>2. P-box</li> <li>3. T-box</li> <li>4. none of the above</li> </ol>	1
16.	<p>A _____ cipher replaces one character with another character.</p> <ol style="list-style-type: none"> <li>1. substitution</li> <li>2. transposition</li> <li>3. either (a) or (b)</li> <li>4. neither (a) nor (b)</li> </ol>	1
17.	<p>The _____ cipher reorders the plaintext characters to create a ciphertext.</p> <ol style="list-style-type: none"> <li>1. substitution</li> <li>2. transposition</li> <li>3. either (a) or (b)</li> <li>4. neither (a) nor (b)</li> </ol>	2

18.	<p>_____ is a round cipher based on the Rijndael algorithm that uses a 128-bit block of data.</p> <ol style="list-style-type: none"> <li>1. AEE</li> <li>2. AED</li> <li>3. AER</li> <li>4. AES</li> </ol>	4
19.	<p>The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.</p> <ol style="list-style-type: none"> <li>1. man-in-the-middle</li> <li>2. ciphertext attack</li> <li>3. plaintext attack</li> <li>4. none of the above</li> </ol>	1
20.	<p>A combination of an encryption algorithm and a decryption algorithm is called a _____.</p> <ol style="list-style-type: none"> <li>1. cipher</li> <li>2. secret</li> <li>3. key</li> <li>4. none of the above</li> </ol>	1
21.	<p>AES has _____ different configurations.</p> <ol style="list-style-type: none"> <li>1. two</li> <li>2. three</li> <li>3. four</li> <li>4. five</li> </ol>	3
22.	<p>DES is a(n) _____ method adopted by the U.S. government.</p> <ol style="list-style-type: none"> <li>1. symmetric-key</li> <li>2. asymmetric-key</li> <li>3. either (a) or (b)</li> <li>4. neither (a) nor (b)</li> </ol>	1
23.	<p>DES uses a key generator to generate sixteen _____ round keys.</p> <p>A) 32-bit</p> <p>B) 48-bit</p> <p>C) 54-bit</p> <p>D) 42-bit</p>	2

24.	The Caesar cipher is a _____ cipher that has a key of 3.  1. transposition 2. additive 3. shift 4. none of the above	3
25.	ECB and CBC are _____ ciphers.  1. block 2. stream 3. field 4. none of the above	1
26.	A(n) _____ is a keyless transposition cipher with N inputs and M outputs that uses a table to define the relationship between the input stream and the output stream.  1. S-box 2. P-box 3. T-box 4. none of the above	2
27.	_____ DES was designed to increase the size of the DES key.  1. Double 2. Triple 3. Quadruple 4. none of the above	2
28.	DES has an initial and final permutation block and _____ rounds.  1. 14 2. 15 3. 16 4. none of the above	3
29.	The DES function has _____ components.  A) 2 B) 3 C) 4 D) 5	3

30.	In a(n) _____ cipher, the same key is used by both the sender and receiver.  1. symmetric-key 2. asymmetric-key 3. either (a) or (b) 4. neither (a) nor (b)	1
31.	The _____ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26.  1. transposition 2. additive 3. shift 4. none of the above	3
32.	In a(n) _____, the key is called the secret key.  1. symmetric-key 2. asymmetric-key 3. either (a) or (b) 4. neither (a) nor (b)	1
33.	RSA stands for:  1. Rivest Shamirand Adleman 2. Rock Shane and Amozen 3. Rivest Shane and Amozen 4. Rock Shamir and Adleman	1
34.	The S-Box is used to provide confusion, as it is dependent on the unknown key. 1. True 2. False	1
35.	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits. 1. True 2. False	2
36.	In the DES algorithm the round key is _____ bit and the Round Input is _____ bits. 1. 48, 32 2. 64,32 3. 56, 24 4. 32, 32	1

37.	<p>In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____</p> <ol style="list-style-type: none"> <li>1. Scaling of the existing bits</li> <li>2. Duplication of the existing bits</li> <li>3. Addition of zeros</li> <li>4. Addition of ones</li> </ol>	1
38.	<p>The Initial Permutation table/matrix is of size</p> <ol style="list-style-type: none"> <li>1. <math>16 \times 8</math></li> <li>2. <math>12 \times 8</math></li> <li>3. <math>8 \times 8</math></li> <li>4. <math>4 \times 8</math></li> </ol>	3
39.	<p>In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.</p> <ol style="list-style-type: none"> <li>1. True</li> <li>2. False</li> </ol>	2
40.	<p>AES uses a _____ bit block size and a key size of _____ bits.</p> <ol style="list-style-type: none"> <li>1. 128; 128 or 256</li> <li>2. 64; 128 or 192</li> <li>3. 256; 128, 192, or 256</li> <li>4. 128; 128, 192, or 256</li> </ol>	4
41.	<p>SHA-1 produces a hash value of</p> <ol style="list-style-type: none"> <li>1. 256 bits</li> <li>2. 160 bits</li> <li>3. 180 bits</li> <li>4. 128 bits</li> </ol>	2
42.	<p>The big-endian format is one in which</p> <ol style="list-style-type: none"> <li>1. the least significant byte is stored in the low-address byte position</li> <li>2. the least significant byte is stored in the high-address byte position</li> <li>3. the most significant byte is stored in the high-address byte position</li> <li>4. the most significant byte is stored in the low-address byte position</li> </ol>	4
43.	<p>Caesar Cipher is an example of</p> <ol style="list-style-type: none"> <li>1 Poly-alphabetic Cipher</li> <li>2 Mono-alphabetic Cipher</li> <li>3 Multi-alphabetic Cipher</li> <li>4 Bi-alphabetic Cipher</li> </ol>	2

44.	<p>DES using 56 bits</p> <ol style="list-style-type: none"> <li>1. Cannot be broken in given time using presently available computers.</li> <li>2. Can be broken only if algorithm is known using even slow computers.</li> <li>3. Can be broken by presently available high speed computers.</li> <li>4. It is impossible to break.</li> </ol>	3
45.	<p>Triple DES</p> <ol style="list-style-type: none"> <li>1. Cannot be broken in given time using presently available computers.</li> <li>2. Can be broken only if algorithm is known using even slow computers.</li> <li>3. Can be broken by presently available high speed computers.</li> <li>4. It is impossible to break.</li> </ol>	1
46.	<p>The Acronym DES stands for</p> <ol style="list-style-type: none"> <li>1. Digital Evaluation System.</li> <li>2. Digital Encryption System.</li> <li>3. Digital Encryption Standard.</li> <li>4. Double Encryption System.</li> </ol>	2
47.	<p>The Acronym AES stands for</p> <ol style="list-style-type: none"> <li>1. Advanced Encryption Standard</li> <li>2. Advanced Encryption System.</li> <li>3. Advanced Evaluation System.</li> <li>4. Advanced Evaluation Standard</li> </ol>	1
48.	<p>Triple DES</p> <ol style="list-style-type: none"> <li>1. Is a Symmetric Key Encryption method.</li> <li>2. Guarantees Excellent Security</li> <li>3. Is implementable as hardware VLSI chip.</li> <li>4. Is a public key encryption method</li> </ol>	2



((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Collection of protocol designed by IETF
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Operation in Tunnel mode
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec protects information in
((OPTION_A)) THIS IS MANDATORY OPTION	transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec in which mode does not protect IP header
((OPTION_A)) THIS IS MANDATORY OPTION	transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which mode is used when we need host to host protection
((OPTION_A)) THIS IS MANDATORY OPTION	Transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec protects the whole IP packets
((OPTION_A)) THIS IS MANDATORY OPTION	Transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec defines two protocol
((OPTION_A)) THIS IS MANDATORY OPTION	AH, SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PGP, ASP
((OPTION_C)) This is optional	AH, ESP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Authentication at the IP header
((OPTION_A)) THIS IS MANDATORY OPTION	AH
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ECP
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	SSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IT PROVIDES AUTHENTICATION OR ENCRYPTION OR BOTH FOR PACKET AT IP LEVEL
((OPTION_A)) THIS IS MANDATORY OPTION	AH
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ESP
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	SSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSEC USES A SET OF SA CALLED
((OPTION_A)) THIS IS MANDATORY OPTION	SAD
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SAB
((OPTION_C)) This is optional	SADB
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Protocol to provide security for inbound and outbound
((OPTION_A)) THIS IS MANDATORY OPTION	SA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CA
((OPTION_C)) This is optional	KDC
((OPTION_D)) This is optional	IKE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE creates SA for
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PGP
((OPTION_C)) This is optional	IPSec
((OPTION_D)) This is optional	VP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE based on other how many protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Two
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Three
((OPTION_C)) This is optional	Four
((OPTION_D)) This is optional	five
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE uses
((OPTION_A)) THIS IS MANDATORY OPTION	OAKLEY
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SKEME
((OPTION_C)) This is optional	ISKAMP
((OPTION_D)) This is optional	ALL ABOVE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Network is used in an organization
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Semi private
((OPTION_D)) This is optional	Semi publik
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Private network that uses an internet model
((OPTION_A)) THIS IS MANDATORY OPTION	intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is a network that allows authorized access from outside
((OPTION_A)) THIS IS MANDATORY OPTION	Intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Internet authorities have reserved address for
((OPTION_A)) THIS IS MANDATORY OPTION	Intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is provides privacy for LAN
((OPTION_A)) THIS IS MANDATORY OPTION	VPP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	VNP
((OPTION_C)) This is optional	VNN
((OPTION_D)) This is optional	VPN
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IT PROVIDES END TO END SECURITY FOR APPLICATION
((OPTION_A)) THIS IS MANDATORY OPTION	DATA LINK
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	NETWORK
((OPTION_C)) This is optional	TRANSPORT
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is actually an IETF version on
((OPTION_A)) THIS IS MANDATORY OPTION	TLS, TSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL. TLS
((OPTION_C)) This is optional	TLS, SSL
((OPTION_D)) This is optional	SSL,SLT
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Provides security at the transport layer
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To provide security and compression
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Can receive application data from any application layer protocol
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SSL provides
((OPTION_A)) THIS IS MANDATORY OPTION	Integrity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	Compression
((OPTION_D)) This is optional	All above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SSI session
((OPTION_A)) THIS IS MANDATORY OPTION	List of protocol
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Cipher suit
((OPTION_C)) This is optional	List of keys
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cryptographic algorithem and secrets are sent with the message IN
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	TLS
((OPTION_D)) This is optional	PGP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Security protocol for email security is
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Was invented by Phil Zimmerman
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSI
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Provides security, integration, authentication in email
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSI
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Method to transfer secure message
((OPTION_A)) THIS IS MANDATORY OPTION	cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	cryptoanalysis
((OPTION_C)) This is optional	both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is the original message before transmission
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Plain text
((OPTION_C)) This is optional	Secret text
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is the message after transmission
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Plain text
((OPTION_C)) This is optional	Secret text
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm transforms plaintext to ciphertext
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm transforms cipher text to plain text
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A combination of encryption and decryption algorithm is called
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Secret
((OPTION_C)) This is optional	Key
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cipher operates on
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	secret
((OPTION_C)) This is optional	Key
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The same key used by both the sender and receiver
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The key is called as secret key
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A pair of keys used in
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An asymmetric key cipher the sender uses the key
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An asymmetric key cipher the receiver uses the key
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A cipher replaces one character with another
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Monoalphabetic and polyalphabetic cipher are
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The simplest monoalphabetic cipher is
((OPTION_A)) THIS IS MANDATORY OPTION	Transposition
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additive
((OPTION_C)) This is optional	Shift
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Ceasar cipher that has key of 3
((OPTION_A)) THIS IS MANDATORY OPTION	Transposition
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additive
((OPTION_C)) This is optional	Shift
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The cipher reorders the plain text to create the ciphertext
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a keyless substitution To define the relationship between input and output stream
((OPTION_A)) THIS IS MANDATORY OPTION	S box
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	P box
((OPTION_C)) This is optional	T box
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a keyless transposition To define the relationship between input and output stream
((OPTION_A)) THIS IS MANDATORY OPTION	S box
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	P box
((OPTION_C)) This is optional	T box
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cipher made of a combination of different simple cipher
((OPTION_A)) THIS IS MANDATORY OPTION	Round
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Circle
((OPTION_C)) This is optional	Square
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES is an method
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES has an Round
((OPTION_A)) THIS IS MANDATORY OPTION	14
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	15
((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES functions has componenets
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	3
((OPTION_C)) This is optional	4
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES uses a key generaterto generater to generate sixteen ---round key
((OPTION_A)) THIS IS MANDATORY OPTION	32 bit
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	48 bit
((OPTION_C)) This is optional	54 bit
((OPTION_D)) This is optional	42 bit
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES was designed to increase the size of DES key
((OPTION_A)) THIS IS MANDATORY OPTION	Double
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tripal
((OPTION_C)) This is optional	Quadrupal
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Algorithm uses a 128 bit block of data
((OPTION_A)) THIS IS MANDATORY OPTION	AEE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AED
((OPTION_C)) This is optional	AER
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	AES has how many different combinations
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	3
((OPTION_C)) This is optional	4
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ECB and CBC are ciphers
((OPTION_A)) THIS IS MANDATORY OPTION	Block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Stream
((OPTION_C)) This is optional	Field
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Public key cryptographic algorithm is
((OPTION_A)) THIS IS MANDATORY OPTION	RSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RAS
((OPTION_C)) This is optional	RSA
((OPTION_D)) This is optional	RAA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	AC
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	it provides a one time session key for two parties
((OPTION_A)) THIS IS MANDATORY OPTION	Diffie hellman
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	DES
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	TELNET is an abbreviation of
((OPTION_A)) THIS IS MANDATORY OPTION	Terminal network
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Telephone network
((OPTION_C)) This is optional	Telecommunication network
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	TELNET is a client server application program for
((OPTION_A)) THIS IS MANDATORY OPTION	Specific purpose
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	General purpose
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Users logs in to local time sharing system is called
((OPTION_A)) THIS IS MANDATORY OPTION	Local
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Remote
((OPTION_C)) This is optional	Temporary
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To access remote machine need a login
((OPTION_A)) THIS IS MANDATORY OPTION	Local
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Remote
((OPTION_C)) This is optional	Temporary
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	NVT uses two set of character
((OPTION_A)) THIS IS MANDATORY OPTION	Sending, receiving
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Request, reply
((OPTION_C)) This is optional	Data, control
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For data NVT uses ASCII with the highest order bit set
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0
((OPTION_C)) This is optional	A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For data NVT uses ASCII with the highest order bit set
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0
((OPTION_C)) This is optional	A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The server uses -----port
((OPTION_A)) THIS IS MANDATORY OPTION	Wellknown
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Emperor
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To distinguish data from characters
((OPTION_A)) THIS IS MANDATORY OPTION	ICA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IAC
((OPTION_C)) This is optional	AIC
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	the echoing is done by the client in the mode
((OPTION_A)) THIS IS MANDATORY OPTION	Default
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Character
((OPTION_C)) This is optional	Line
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP uses a service of
((OPTION_A)) THIS IS MANDATORY OPTION	UDP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IP
((OPTION_C)) This is optional	TCP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP control and data connection are
((OPTION_A))  THIS IS MANDATORY OPTION	21, 22
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	20,21
((OPTION_C))  This is optional	21,20
((OPTION_D))  This is optional	none
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP is the service type used by IP protocol because
((OPTION_A)) THIS IS MANDATORY OPTION	Maximise throughput
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Minimize delay
((OPTION_C)) This is optional	Minimize error
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For control connection FTP use a character set of
((OPTION_A)) THIS IS MANDATORY OPTION	Regular ASCII
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	EBCDIC
((OPTION_C)) This is optional	NVT ASCII
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During FTP session the control connection is opened
((OPTION_A)) THIS IS MANDATORY OPTION	Exactly once
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Exactly twice
((OPTION_C)) This is optional	Many times
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During FTP session the control connection is opened
((OPTION_A)) THIS IS MANDATORY OPTION	Exactly once
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Exactly twice
((OPTION_C)) This is optional	Many times
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP files are types of an attribute called
((OPTION_A)) THIS IS MANDATORY OPTION	File types
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structures
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP there are three types of -----,stream, blocked and compression
((OPTION_A)) THIS IS MANDATORY OPTION	File types
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structurs
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP and image defines an attribute called
((OPTION_A)) THIS IS MANDATORY OPTION	File type
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structure
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP when we -----, it is copied from the server to client
((OPTION_A)) THIS IS MANDATORY OPTION	Retrieve a file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Retrieve a list
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP when we -----, it is copied from the client to server
((OPTION_A)) THIS IS MANDATORY OPTION	Retrieve a file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Store a file
((OPTION_C)) This is optional	Retrieve a lise
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is a part of a local hard drive, a special file with permission restriction
((OPTION_A)) THIS IS MANDATORY OPTION	A message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A response
((OPTION_C)) This is optional	An agent
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and the receiver on the same system we need
((OPTION_A)) THIS IS MANDATORY OPTION	One UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA
((OPTION_C)) This is optional	One UA and one MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and receiver are on the different system, we need
((OPTION_A)) THIS IS MANDATORY OPTION	One MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA
((OPTION_C)) This is optional	Two UA and one pair of MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender is connected to the mail server via a LAN or WAN, we need
((OPTION_A)) THIS IS MANDATORY OPTION	Two MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA and two pairs of MTA
((OPTION_C)) This is optional	Two UA and a pair of MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and receiver are connected to the mail server via a LAN or WAN, we need
((OPTION_A)) THIS IS MANDATORY OPTION	Two UA, two pair of MTA, a pair of MAA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA and two pair of MTA
((OPTION_C)) This is optional	Two UA, two pair of MTA, two pair of MAA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	It provides a service to the user to make the process of sending and receiving message
((OPTION_A)) THIS IS MANDATORY OPTION	MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MAA
((OPTION_C)) This is optional	UA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following services is not provided by UA
((OPTION_A))  THIS IS MANDATORY OPTION	Composing message
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Reading message
((OPTION_C))  This is optional	Reply message
((OPTION_D))  This is optional	ALL are
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	There are two types of user agents
((OPTION_A)) THIS IS MANDATORY OPTION	Command driven, data driven
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Command driven, GUI based
((OPTION_C)) This is optional	Command based and data based
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	It contains the sender address, receiver address and other information
((OPTION_A)) THIS IS MANDATORY OPTION	Message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Envelop
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The message contains
((OPTION_A)) THIS IS MANDATORY OPTION	Header, envelop
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Header, body
((OPTION_C)) This is optional	Envelop, body
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the internet, the email address contains two parts
((OPTION_A)) THIS IS MANDATORY OPTION	Local part, domain name
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Global part, domain name
((OPTION_C)) This is optional	Label, domain name
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is a supplementary protocol that allow Non ASCII data to be sent through email
((OPTION_A)) THIS IS MANDATORY OPTION	JPEG
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MPEG
((OPTION_C)) This is optional	MIME
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The actual email transfer is done through
((OPTION_A)) THIS IS MANDATORY OPTION	UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MTA
((OPTION_C)) This is optional	MAA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Protocol that defines a MTA client and server in the internet is called
((OPTION_A)) THIS IS MANDATORY OPTION	SMTP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SNMP
((OPTION_C)) This is optional	TELNET
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The process of transferring a mail message occurs in-----phase
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4
((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SMTP is --- protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Pull
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Push
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The third stage in a email transfer need a ---protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Pull
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Push
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The third stage in an email transfer uses an ----protocol
((OPTION_A)) THIS IS MANDATORY OPTION	UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MTA
((OPTION_C)) This is optional	MAA
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Currently two message asses protocol are available
((OPTION_A)) THIS IS MANDATORY OPTION	POP3, IMAP2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	POP4,IMAP1
((OPTION_C)) This is optional	POP3, IMAP4
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

This sheet is for 1 Mark questions							
S.r No	Question	Image	a	b	c	d	Correct Answer
1	_____ is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction.		a) Network Security a) Cloud workload protection platforms a) Bug	b) Database Security b) Cloud security b) Threat	c) Information Security c) AWS c) Vulnerability	d) Physical Security d) One Drive d) Attack	c a b
2	_____ platforms are used for safety and protection of information in the cloud.						
3	Compromising confidential information comes under _____						
4	An attempt to harm, damage or cause threat to a system or network is broadly termed as _____		a) Cyber-crime a) Triangle	b) Cyber Attack b) Diagonal	c) System hijacking c) Ellipse	d) Digital crime d) Circle	b a
5	The CIA triad is often represented by which of the following?						
6	Related to information security, confidentiality is the opposite of which of the following?		a) Closure	b) Disclosure	c) Disaster	d) Disposal	b
7	When you use the word _____ it means you are protecting your data from getting disclosed.		a) Confidentiality a) Confidentiality	b) Integrity b) Integrity	c) Authentication c) Authentication	d) Availability d) Non-repudiation	a b
8	_____ means the protection of data from modification by unknown users.						
9	_____ of information means, only authorized users are capable of accessing the information.		a) Confidentiality	b) Integrity	c) Non-repudiation	d) Availability	d
10	This helps in identifying the origin of information and authentic user. This referred to here as _____		a) Confidentiality a) Encryption	b) Integrity b) Locking b) Open Systems Interconnections	c) Authenticity c) Decryption	d) Availability d) Backup d) Open Standard Interconnections	c a
11	Data _____ is used to ensure confidentiality.						
12	What does OSI stand for in the OSI Security Architecture?		a) Open System Interface		c) Open Source Initiative		b
13	A company requires its users to change passwords every month. This improves the _____ of the network.		a) Performance	b) Reliability	c) Security	d) None of the above	c
14	Release of message contents and Traffic analysis are two types of _____ attacks.		a) Active Attack a) Cipher script	b) Modification of Attack b) Cipher text	c) Passive attack c) Secret text	d) DoS Attack d) Secret script	c b
15	The _____ is encrypted text.		NTLM	MITM	NetBIOS	SMB	
16	What type of attack uses a fraudulent server with a relay address?						
17	Which of the following Algorithms not belong to symmetric encryption			RSA	RC5	IDEA	b
18	Which is the largest disadvantage of the symmetric Encryption?				More complex and therefore Problem of the security	Less secure encryption function	b
19	In cryptography, what is cipher?					Isn't used any more.	
20	In asymmetric key cryptography, the private key is kept by _____		algorithm for performing encryption	both algorithm for performing decryption			a
21	Which one of the following algorithm is not used in asymmetric-key cryptography?		sender	message receiver	sender and receiver	all the connected devices	b
22	In cryptography, the order of the letters in a message is rearranged by _____		rsa algorithm		diffie-hellman algorithm	electronic code book algorithm	c
23	What is data encryption standard (DES)?		transpositional ciphers	substitution ciphers	both transpositional ciphers	a quadratic ciphers	a
24	A asymmetric-key (or public key ) cipher uses		block cipher	stream cipher	bit cipher	byte cipher	a
25	In asymmetric key cryptography, the two keys e and d, have special relationship to _____		1 key	2 key	3 key	4 key	b
26	In asymmetric key cryptography, the two keys e and d, have special relationship to _____		others	data	keys	each other	d
27	_____ is the process or mechanism used for converting ordinary plain text into garbled non-human readable text & vice-versa.		Malware Analysis	Exploit writing	Reverse engineering	Cryptography	d
28	_____ is a means of storing & transmitting information in a specific format so that only those for whom it is planned can understand or process it.						b
29	4. Cryptographic algorithms are based on mathematical algorithms where these algorithms use _____ for a secure transformation of data.		secret key	external programs	add-ons	secondary key	a
30	Conventional cryptography is also known as _____ or symmetric-key encryption.		secret-key decryption	public key hashing	protected key tuning	primary key padding	a d
31	The procedure to add bits to the last block is termed as _____						b
32	How many rounds does the AES-192 perform?		10 symmetric key encryption algorithm	12	14	16	
	ECC encryption system is _____				asymmetric key encr not an encryption algorithm	block cipher method	

33	_____ function creates a message digest out of a message.						
34	Extensions to the X.509 certificates were added in version _____						
35	A digital signature needs _____ system						
36	"Elliptic curve cryptography follows the associative property."						
37	ECC stands for						
38	When a hash function is used to provide message authentication, the hash function value is referred to as						
39	Message authentication code is also known as						
40	The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user's public key.						
41	The DSS signature uses which hash algorithm?						
42	What is the size of the RSA signature hash after the MD5 and SHA-1 processing?						
43	In the handshake protocol which is the message type first sent between client and server ?						
44	One commonly used public-key cryptography method is the _____ algorithm.						
45	he _____ method provides a one-time session key for two parties.						
46	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.						
47	In the handshake protocol which is the message type first sent between client and server ?						
48	1. VPN is abbreviated as _____						
49	_____ provides an isolated tunnel across a public network for sending and receiving data privately as if the computing devices were directly connected to the private network.						
50	Which of the statements are not true to classify VPN systems?						
51	What types of protocols are used in VPNs?						
52	VPNs uses encryption techniques to maintain security and privacy while communicating remotely via public network.						
53	There are _____ types of VPNs.						
54	_____ type of VPNs are used for home private and secure connectivity.						
55	Which types of VPNs are used for corporate connectivity across companies residing in different geographical location?						
56	Site-to-Site VPN architecture is also known as _____						
57	There are _____ types of VPN protocols.						
58	IPSec is designed to provide security at the _____						
59	In tunnel mode, IPSec protects the _____						
60	Pretty good privacy (PGP) is used in _____						
61	PGP encrypts data by using a block cipher called _____						
62	IKE creates SAs for _____.						
63	_____ provides either authentication or encryption, or both, for packets at the IP level.						
64	A _____ network is used inside an organization.						
65	SSL provides _____.						
		encryption	decryption	hash	none of the above	c	
		symmetric-key TRUE	asymmetric-key FALSE	either (a) or (b)	neither (a) nor (b)	c b a	
		Elliptic curve cryptography	Enhanced curve crypt	Elliptic cone crypt	Eclipse curve cryptograph	a	
		Message Field	Message Digest	Message Score	Message Leap	d	
		key code	hash code	keyed hash function	message key hash functio	b	
		TRUE	FALSE				
		MD5 42 bytes	SHA-2 32 bytes	SHA-1 36 bytes	Does not use hash algoritl 48 bytes	b c c	
		server_hello RSS Diffie-Hellman	client_hello RAS RSA	hello_request RSA DES	certificate_request RAA AES	b c a	
		man-in-the-middle	ciphertext attack	plaintext attack	none of the above	a	
		server_hello	client_hello	hello_request	certificate_request	b	
		Visual Private Network	Virtual Protocol Netw	Virtual Private Network	Virtual Protocol Networki	c	
		Visual Private Network	Virtual Protocol Netw	Virtual Protocol Networking	Virtual Private Network	d	
		Protocols used for tunnelling	Whether VPNs are pr	Securing the network from bc	Levels of security provide	c	
		Application level protocols	Tunnelling protocols	Network protocols	Mailing protocols	a	
		TRUE	False			a	
		Remote access VPNs	Site-to-site VPNs	Peer-to-Peer VPNs	Router-to-router VPNs	b a	
		Remote access VPNs	Site-to-site VPNs	Peer-to-Peer VPNs	Country-to-country VPNs	b	
		Remote connection based \ Peer-to-Peer VPNs	Extranet based VPN		Country-to-country VPNs	c	
		3	4	5	6	d b a b	
		Transport layer Entire IP packet Browser security	Network layer IP header Email security Private data	Application layer IP payload FTP security	Session layer IP trailer WiFi security		
		International data encryption algorithm SSL AH private	encryption algorithm PGP ESP public	Internet data encryption algorithm IPSec PGP semi-private	Local data encryption algorithm VP SSL semi-public	a c b a	
		message integrity	confidentiality	compression	all of the above	d	

66	IKE uses _____	Oakley	SKEME	ISAKMP	all of the above	d
67	In _____, there is a single path from the fully trusted authority to any certificate.	X509	PGP	KDC	none of the above	a
68	A _____ provides privacy for LANs that must communicate through the global Internet.	VPP	VNP	VNN	VPN	d
69	_____ uses the idea of certificate trust levels.	X509	PGP	KDC	none of the above	b
70	_____ provides privacy, integrity, and authentication in e-mail.	IPSec	SSL	PGP	none of the above	c
71	In _____, there can be multiple paths from fully or partially trusted authorities.	X509	PGP	KDC	none of the above	b
72	_____ provides authentication at the IP level.	AH	ESP	PGP	SSL	a
73	In _____, the cryptographic algorithms and secrets are sent with the message.	IPSec	SSL	TLS	PGP	d
74	_____ was invented by Phil Zimmerman.	IPSec	SSL	PGP	none of the above	c
75	ISAKMP stands for _____	Internet system Association and Key Management Packet	Association and Key Management	Interchange System And Key Protocol	Internet Security Association and Key Modeling Protocol	b
76	PGP makes use of which cryptographic algorithm?	DES	AES	RSA	Rabin	c
77	What is the key size allowed in PGP?	1024-1056	1024-4056	1024-4096	1024-2048	c
78	In SSL, what is used for authenticating a message?	MAC (Message Access Code)	Authentication	MAC (Machine Code)	MAC (Machine Access Code)	b
79	S/MIME is abbreviated as _____	Secure/Multimedia Internet Mailing Extensions	Secure/Multipurpos e Internet Mailing Extensions	Secure/Multimedia Internet Mail Extensions	Secure/Multipurpose Internet Mail Extensions	d
80	Security Measures Needed to protect _____ during their transmission	file	Data	packet	All of above	b
81	_____ means knowledge obtained from investigation, study , intelligence new ,facts .	Security	Data	Information	None of These	c
82	Prevention of the unauthorised used of Resources refers too?	Data Integrity	Data confidentiality	Access Control	None of these	c
83	Protection against Denial by one of these parties in a communication refers to?	Non-Repudiation	Data integrity	Authentication	None of these	a
84	Which One of them is Passive attack?	Denial of Service	modify message in transit	Replay previous message	obtain message contain	d
85	What is lying of IP address called as?	IP Spoofing	IP Scamming	IP Lying	None Of theses	a
86	What is full form of DDoS?	Derived Denial of service	Distributed Denial of service	Denial of service	None of these	b
87	A hacker guessing suggested password to a program is call as?	Password Guessing	Dictionary Attack	Default password attack	None of these	c
88	Symmetric key encryption is also called as?	public key Encryption	Private Key Encryption	Both of these	None of these	b
89	Conversion of Cypher text to plain text?	Encryption	Decryption	Simple text	none of these	b
90	is used to create the organisation's overall security program.	program policy	purpose	security	none of these	a
91	An act of protecting information from unauthorised discloser to an entity.-	integrity	availability	confidentiality	none of these	c
92	A way to ensure that the entity is indeed what it claims to be.-	Authentication	Accountability	identification	security	a
93	The _____ model is 7 layer architecture where each layer is having some specific functionality to perform.	TCP	OSI	OIS	none of these	b
94	The full form of OSI is OSI model_____.	open systems interconnection	open software interconnection	open connection	open system internet	a
95	The technique in which when one character is replaced by another Character is called as?	Transposition	Substitution	Combinational	None of these	b
96	Conversion of plain text into Cipher text is called as _____.	Encryption	Decryption	Hidden Text	none of above	a
97	In Symmetric schemes requires both parties to share how many secret key?	one	two	three	four	a
98	Blum Blum Shub Generator is based on which Algorithm?	Private key	Public key	both a & b	none of these	b
99	In DES step both LPT and RPT undergoes in how much key Rounds?		8	16	32	64
100	What is the 4th step in DES Algorithm?	key transformation	S-box Substitution	P-box Permutation	Expansion permutation	c
101	In AES in which Round Subkeys are Generated from Original key for each round?	Key Expansion	Initial Round	Finale Round	none of these	a
102	AES stands for?	Authorized Encryption Standard	Advance Encryption Standard	Advance Encryption Strategy	none of these	b
103	Which of them is type of Cipher?	Stream Cipher	Block Cipher	both of Them	none of these	c
104	The message which is not understandable is called as?	Cipher Text	plain text	Hidden text	both a & c	a

105	The _____ is a polygraphic substitution cipher based on linear algebra.	Hill cipher	playfair cipher	Affine cipher	none of these	a
106	_____ is the practice of concealing a message within another message,image or file.	steganography	cryptography	cipher	receiver	a
107	In asymmetric key cryptography, the private key is kept by _____	sender	receiver	sender and receiver	none of these	b
108	What is data encryption standard (DES)?	block cipher	stream cipher	bit cipher	byte cipher	a
109	In cryptography the original message before being transform is called	simple text	plain text	empty text	filled text	b
110	An asymmetric-key (or public-key) cipher uses	1 key	2 key	3 key	4 key	a
111	In Asymmetric-Key Cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if the message is	Short	Flat	Long	Thin	c
112	The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not	Authenticated	Joined	Submit	Separate	a
113	In Asymmetric-Key Cryptography, the two keys, e and d, have a special relationship to	other	Data	Keys	Each other	d
114	For RSA to work, the value of P must be less than the value of	p	q	n	r	c
115	In RSA, $\Phi(n) = \text{_____}$ in terms of p and q.	(p)/(q)	(p)(q)	(p-1)(q-1)	(p+1)(q+1)	c
116	In RSA, we select a value 'e' such that it lies between 0 and $\Phi(n)$ and it is relatively prime to $\Phi(n)$ .	TRUE	FALSE			b
117	RSA is also a stream cipher like Merkel-Hellman.	TRUE	FALSE			a
118	USENET falls under which category of public key sharing?	public announcement	publicly available directory	public key authority	public key certificate	a
119	PGP makes use of which cryptographic algorithm?	RSA	AES	DES	ROBIN	a
120	Public key cryptography also called as _____	Asymmetric key cryptography	Symmetric key cryptography	Both a and b	None of the above	a
121	ECC stands for	Elliptic Curve Cryptography	Elliptic Cryptography Curve	Error Correcting Code	None of the above	a
122	Diffie-Hellman algorithm is widely known as _____	Key exchange algorithm	key agreement algorithm	only a	Both a and b	d
123	Hash function is used for _____	Message authentication	Digital Signature	Both a and b	only a	c
124	RSA algorithm is best example of _____	Asymmetric key cryptography	Symmetric key cryptography	Elliptic Curve Cryptography	All of the above	a
125	IPSec is designed to provide security at the _____	Transport layer	Network layer	Application layer	Session layer	b
126	In tunnel mode, IPSec protects the _____	Entire IP packet	IP header	IP payload	IP trailer	a
127	HTTPS is abbreviated as _____	Hypertext Transfer Protocol Secured	Secured Hyper Text Transfer Protocol	Hyperlinked Text Transfer Protocol Secured	Hyper Text Transfer Protocol Secure	d
128	An attempt to make a computer resource unavailable to its intended users is called _____	Denial-of-service attack	Virus attack	Worms attack	Botnet process	a
129	SSL primarily focuses on _____	integrity and authenticity	integrity and non-repudiation	authenticity and privacy	confidentiality and integrity	a
130	Pretty good privacy (PGP) is used in _____	Browser security	Email security	WiFi security	FTP security	b
131	_____ is used for encrypting data at network level	IPSec	HTTPS	SMTP	S/MIME	a
132	WPA2 is used for security in _____	Ethernet	Wi-Fi	Bluetooth	E-mail	b
133	Which of the following is not a strong security protocol	SSL	HTTP	SMTP	SFTP	c
134	TSL (Transport Layer Security) is a cryptographic protocol used for securing HTTP/HTTPS based connection.	TRUE	FALSE			a
135	IPSec operates in..... different modes		3	2	4	5 b
136	length of the IPv4 address is ....	32 bits	64 bits	16 bits	128 bit	a
137	Internet Key Exchange has .... phases and modes of operations		4	3	2	5 c
138	PGP is abbreviated as	Pretty Good Privacy	Pretty Good Policy	Policy Good Privacy	Pretty Good Protection	a
139	SET stands for	Set Electronic Transaction	Transaction	Simple Electronic Transaction	none of the above	b
140	Transport layer Protocol consists of ... main components		2	1	3	4 a
141	length of the IPv6 address is ....	32 bits	64 bits	16 bits	128 bit	b
142	SSL provides _____.	message integrity	confidentiality	compression	all of the above	d
143	IPSec provides ....protocols for network layer		7	3	1	4 a
144	length of the IPv6 header is....	64 bits	16 bits	32 bits	8 bits	c

## Question Bank for Information and Cyber Security (ICS)

### 1. Why would a hacker use a proxy server?

- A. To create a stronger connection with the target.
- B. To create a ghost server on the network.
- C. To obtain a remote access connection.
- D. To hide malicious activity on the network.

**Correct Answer – D**

**Explanation –** Proxy servers exist to act as an intermediary between the hacker and the target and services to keep the hacker anonymous to the network.

### 2. What type of symmetric key algorithm using a streaming cipher to encrypt information?

- A. RC4
- B. Blowfish
- C. SHA
- D. MD5

**Correct Answer – A**

**Explanation –** RC4 uses streaming ciphers.

### 3. Which of the following is not a factor in securing the environment against an attack on security?

- A. The education of the attacker
- B. The system configuration
- C. The network architecture
- D. The business strategy of the company
- E. The level of access provided to employees

**Correct Answer – D**

**Explanation –** All of the answers are factors supporting the exploitation or prevention of an attack. The business strategy may provide the motivation for a potential attack, but by itself will not influence the outcome.

### 4. What type of attack uses a fraudulent server with a relay address?

- A. NTLM
- B. MITM
- C. NetBIOS
- D. SMB

**Correct Answer – B**

**Explanation –** MITM (Man in the Middle) attacks create a server with a relay address. It is used in SMB relay attacks.

### 5. What port is used to connect to the Active Directory in Windows 2000?

- A. 80
- B. 445
- C. 139
- D. 389

**Correct Answer – D**

**Explanation –** The Active Directory Administration Tool used for a Windows 2000 LDAP client uses port 389 to connect to the Active Directory service.

### 6. To hide information inside a picture, what technology is used?

- A. Rootkits
- B. Bitmapping

- C. Steganography
- D. Image Rendering

**Correct Answer – C**

**Explanation** – Steganography is the right answer and can be used to hide information in pictures, music, or videos.

**7. Which phase of hacking performs actual attack on a network or system?**

- A. Reconnaissance
- B. Maintaining Access
- C. Scanning
- D. Gaining Access

**Correct Answer – D**

**Explanation** – In the process of hacking, actual attacks are performed when gaining access, or ownership, of the network or system. Reconnaissance and Scanning are information gathering steps to identify the best possible action for staging the attack. Maintaining access attempts to prolong the attack.

**8. Attempting to gain access to a network using an employee's credentials is called the mode of ethical hacking.**

- A. Local networking
- B. Social engineering
- C. Physical entry
- D. Remote networking

**Correct Answer – A**

**Explanation** – Local networking uses an employee's credentials, or access rights, to gain access to the network. Physical entry uses credentials to gain access to the physical IT infrastructure.

**9. Which Federal Code applies the consequences of hacking activities that disrupt subway transit systems?**

- A. Electronic Communications Interception of Oral Communications
- B. 18 U.S.C. § 1029
- C. Cyber Security Enhancement Act 2002
- D. 18 U.S.C. § 1030

**Correct Answer – C**

**Explanation** – The Cyber Security Enhancement Act 2002 deals with life sentences for hackers who recklessly endanger the lives of others, specifically transportation systems.

**10. Which of the following is not a typical characteristic of an ethical hacker?**

- A. Excellent knowledge of Windows.
- B. Understands the process of exploiting network vulnerabilities.
- C. Patience, persistence and perseverance.
- D. Has the highest level of security for the organization.

**Correct Answer – D**

**Explanation** – Each answer has validity as a characteristic of an ethical hacker. Though having the highest security clearance is ideal, it is not always the case in an organization.

**11. What is the proper command to perform an Nmap XMAS scan every 15seconds?**

- A. nmap -sX -sneaky
- B. nmap -sX -paranoid
- C. nmap -sX -aggressive
- D. nmap -sX -polite

**Correct Answer – A**

**Explanation** – SX is used to identify a xmas scan, while sneaky performs scans 15 seconds apart.

**12. What type of rootkit will patch, hook, or replace the version of system call in order to hide information?**

- A. Library level rootkits
- B. Kernel level rootkits
- C. System level rootkits
- D. Application level rootkits

**Correct Answer – A**

**Explanation** – Library leve rootkits is the correct answer. Kerel level focuses on replaceing specific code while application level will concentrate on modifying the behavior of the application or replacing application binaries. The type, system level, does not exist for rootkits.

**13. What is the purpose of a Denial of Service attack?**

- A. Exploit a weakness in the TCP/IP stack
- B. To execute a Trojan on a system
- C. To overload a system so it is no longer operational
- D. To shutdown services by turning them off

**Correct Answer – C**

**Explanation** – DoS attacks force systems to stop responding by overloading the processing of the system.

**14. What are some of the most common vulnerabilities that exist in a network or system?**

- A. Changing manufacturer, or recommended, settings of a newly installed application.
- B. Additional unused features on commercial software packages.
- C. Utilizing open source application code
- D. Balancing security concerns with functionality and ease of use of a system.

**Correct Answer – B**

**Explanation** – Linux is an open source code and considered to have greater security than the commercial Windows environment. Balancing security. Ease of use and functionality can open vulnerabilities that already exist. Manufacturer settings, or default settings, may provide basic protection against hacking threats, but need to change to provide advance support. The unused features of application code provide an excellent opportunity to attack and cover the attack.

**15. What is the sequence of a TCP connection?**

- A. SYN-ACK-FIN
- B. SYN-SYN ACK-ACK
- C. SYN-ACK
- D. SYN-SYN-ACK

**Correct Answer – B**

**Explanation** – A three-handed connection of TCP will start with a SYN packet followed by a SYN-ACK packet. A final ACK packet will complete the connection.

**16. What tool can be used to perform SNMP enumeration?**

- A. DNSlookup
- B. Whois
- C. Nslookup
- D. IP Network Browser

**Correct Answer – D**

**Explanation** – SNMPPUtil and IP Network Browser is SNMP enumeration tool

**17. Which ports should be blocked to prevent null session enumeration?**

- A. Ports 120 and 445
- B. Ports 135 and 136
- C. Ports 110 and 137
- D. Ports 135 and 139

**Correct Answer – D**

**Explanation** – Port 139 is the NetBIOS Session port typically can provide large amounts of information using APIs to connect to the system. Other ports that can be blocked in 135, 137,138, and 445.

**18. The first phase of hacking an IT system is compromise of which foundation of security?**

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Authentication

**Correct Answer – B**

**Explanation** – Reconnaissance is about gathering confidential information, such as usernames and passwords.

**19. How is IP address spoofing detected?**

- A. Installing and configuring a IDS that can read the IP header
- B. Comparing the TTL values of the actual and spoofed addresses
- C. Implementing a firewall to the network
- D. Identify all TCP sessions that are initiated but does not complete successfully

**Correct Answer – B**

**Explanation** – IP address spoofing is detectable by comparing TTL values of the actual and spoofed IP addresses

**20. Why would a ping sweep be used?**

- A. To identify live systems
- B. To locate live systems
- C. To identify open ports
- D. To locate firewalls

**Correct Answer – A**

**Explanation** – A ping sweep is intended to identify live systems. Once an active system is found on the network, other information may be distinguished, including location. Open ports and firewalls.

**21. What are the port states determined by Nmap?**

- A. Active, inactive, standby
- B. Open, half-open, closed
- C. Open, filtered, unfiltered
- D. Active, closed, unused

**Correct Answer – C**

**Explanation** – Nmap determines that ports are open, filtered, or unfiltered.

**22. What port does Telnet use?**

- A. 22
- B. 80
- C. 20
- D. 23

**Correct Answer – D**

**Explanation** – Telnet uses port 23.

**23. Which of the following will allow footprinting to be conducted without detection?**

- A. PingSweep
- B. Traceroute
- C. War Dialers
- D. ARIN

**Correct Answer – D**

**Explanation** – ARIN is a publicly accessible database, which has information that could be valuable. Because it is public, any attempt to obtain information in the database would go undetected.

**24. Performing hacking activities with the intent on gaining visibility for an unfair situation is called \_\_\_\_\_.**

- A. Cracking
- B. Analysis
- C. Hacktivism
- D. Exploitation

**Correct Answer – C**

**Explanation** – Hacktivism is the act of malicious hacking for a cause or purpose.

**25. What is the most important activity in system hacking?**

- A. Information gathering
- B. Cracking passwords
- C. Escalating privileges
- D. Covering tracks

**Correct Answer – B**

**Explanation** – Passwords are a key component to access a system, making cracking the password the most important part of system hacking.

**26. A packet with no flags set is which type of scan?**

- A. TCP
- B. XMAS
- C. IDLE
- D. NULL

**Correct Answer – D**

**Explanation** – A NULL scan has no flags set.

**27. Sniffing is used to perform \_\_\_\_\_ fingerprinting.**

- A. Passive stack
- B. Active stack
- C. Passive banner grabbing
- D. Scanned

**Correct Answer – A**

**Explanation** – Passive stack fingerprinting uses sniffing technologies instead of scanning.

**28. Phishing is a form of \_\_\_\_\_.**

- A. Spamming
- B. Identify Theft
- C. Impersonation
- D. Scanning

**Correct Answer – C**

**Explanation** – Phishing is typically a potential attacker posing, or impersonating, a financial institution

**29. Why would HTTP Tunneling be used?**

- A. To identify proxy servers
- B. Web activity is not scanned
- C. To bypass a firewall
- D. HTTP is a easy protocol to work with

**Correct Answer – C**

**Explanation** – HTTP Tunneling is used to bypass the IDS and firewalls present on a network.

**30. Which Nmap scan is does not completely open a TCP connection?**

- A. SYN stealth scan
- B. TCP connect
- C. XMAS tree scan
- D. ACK scan

**Correct Answer – A**

**Explanation** – Also known as a “half-open scanning,” SYN stealth scan will not complete a full TCP connection.

**31. What protocol is the Active Directory database based on?**

- A. LDAP
- B. TCP
- C. SQL
- D. HTTP

**Correct Answer – A**

**Explanation** – Active4 direction in Windows 200 is based on a Lightweight Directory Access Protocol (LDAP).

**32. Services running on a system are determined by \_\_\_\_\_.**

- A. The system’s IP address.
- B. The Active Directory
- C. The system’s network name
- D. The port assigned

**Correct Answer – D**

**Explanation** – Hackers can identify services running on a system by the open ports that are found.

**33. What are the types of scanning?**

- A. Port, network, and services
- B. Network, vulnerability, and port
- C. Passive, active, and interactive
- D. Server, client, and network

**Correct Answer – B**

**Explanation** – The three types of accepted scans are port, network, and vulnerability.

**34. Enumeration is part of what phase of ethical hacking?**

- A. Reconnaissance
- B. Maintaining Access
- C. Gaining Access
- D. Scanning

**Correct Answer – C**

**Explanation** – Enumeration is a process of gaining access to the network by obtaining information on a user or system to be used during an attack.

**35. Keyloggers are a form of \_\_\_\_\_.**

- A. Spyware
- B. Shoulder surfing
- C. Trojan
- D. Social engineering

**Correct Answer – A**

**Explanation** – Keyloggers are a form of hardware or software spyware installed between the keyboard and operating system.

**36. What are hybrid attacks?**

- A. An attempt to crack passwords using words that can be found in dictionary.
- B. An attempt to crack passwords by replacing characters of a dictionary word with numbers and symbols.
- C. An attempt to crack passwords using a combination of characters, numbers, and symbols.
- D. An attempt to crack passwords by replacing characters with numbers and symbols.

**Correct Answer – B**

**Explanation** – Hybrid attacks do crack passwords that are created with replaced characters of dictionary type words.

**37. Which form of encryption does WPA use?**

- A. Shared key
- B. LEAP
- C. TKIP
- D. AES

**Correct Answer – C**

**Explanation** – TKIP is used by WPA

**38. What is the best statement for taking advantage of a weakness in the security of an IT system?**

- A. Threat
- B. Attack
- C. Exploit
- D. Vulnerability

**Correct Answer – C**

**Explanation** – A weakness in security is exploited. An attack does the exploitation. A weakness is vulnerability. A threat is a potential vulnerability.

**39. Which database is queried by Whois?**

- A. ICANN
- B. ARIN
- C. APNIC
- D. DNS

**Correct Answer – A**

**Explanation** – Who utilizes the Internet Corporation for Assigned Names and Numbers.

**40. Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?**

- A. Web-based
- B. Human-based
- C. User-based
- D. Computer-based

**Correct Answer – D**

**Explanation** – Whether using email, a fake website, or popup to entice the user, obtaining information from an individual over the Internet is a computer-based type of social engineering

**1) You are supposed to use hill cipher for encryption technique. You are provided with the following matrix,**

$$A = \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix}$$

**Is the given matrix 'A', a valid key to be used for encryption?**

- a. Yes
- b. No
- c. Can't be determined
- d. Data insufficient

**Answer:** b) No

**Explanation:**

For choosing any square matrix as a key, it should be taken care that the matrix is invertible, i.e. its inverse must exist. Here, in this case,

$$|A| = 0$$

Therefore, it means that 'A' is not an invertible matrix. Hence matrix 'A' cannot be chosen as a key matrix for encryption in the [Hill cipher](#).

**2) The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?**

- a. The input text is divided into two parts: one being left half and another one being right half.
- b. Swapping of the left and right halves are performed after each round.
- c. The plain text is converted into a matrix form first
- d. None of the above

**Answer:** c) The plain text is converted into a matrix form first

**Explanation:**

The fiestal structure does not require the conversion of the plain text into matrix form at any of its steps.

**3) Among the following given options, chose the strongest encryption technique?**

- a. DES ( Data Encryption Standard)
- b. Double DES
- c. Triple DES
- d. AES (Advance Encryption Standard)

**Answer:** d) AES (Advance Encryption Standard)

**Explanation:**

It has been proved that the AES performs much better than the all the other DES, whether it be single DES or series of DES.

**4) What is the full-form of RSA in the RSA encryption technique?**

- a. Round Security Algorithm
- b. Rivest, Shamir, Adleman
- c. Robert, Shamir, Addie
- d. None of the above

**Answer:** b) Rivest, Shamir, Adleman

**Explanation:**

The RSA algorithm was named after the three scientists who developed this technique and the name RSA is itself the abbreviation of their names: Rivest, Shamir, and Adleman.

**5) Consider the following steps,**

- i. Substitution bytes
- ii. Shift Rows
- iii. Mix columns
- iv. Add round key

**The above steps are performed in each round of which of the following ciphers?**

- a. Rail fence cipher
- b. Data Encryption Standard (DES)
- c. Advance Encryption Standard (AES)
- d. None of the above

**Answer:** c) Advance Encryption Standard (AES)

**Explanation:**

Each round of AES includes the mentioned steps.

**1) What is the block size of plain text in SHA- 512 algorithm?**

- a. 512 bits
- b. 1024 bits
- c. 2048 bits

- d. None of the above

**Answer:** b. 1024 bits

**Explanation:**

The SHA- 512 algorithm uses blocks of plain text one at a time to encrypt them into ciphertext. The size of each block in the SHA- 512 algorithm is 1024 bits.

**2) All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES?**

- i. Substitution bytes
- ii. Shift rows
- iii. Mix columns
- iv. Add round key

**Options**

- a. i.
- b. iii.
- c. All of the mentioned
- d. None of the mentioned

**Answer:** b. iii.

**Explanation:**

In the AES algorithm, the MIX COLUMN operation is performed in all the rounds except the final round of the algorithm.

**3) What does IDEA stand for in the world of cryptography?**

**or**

**The IDEA word in the IDEA algorithm is the abbreviation for which of the following?**

- a. Independent Decryption Environment Analysis
- b. International Defense Encryption Area
- c. International Data Encryption Algorithm
- d. None of the above

**Answer:** c. International Data Encryption Algorithm

**Explanation:**

The IDEA Algorithm stands for "International Data Encryption Algorithm".

**4) How many sub-keys in the total are used by the IDEA for encrypting the plain text into ciphertext?**

- a. 64 sub- keys
- b. 48 sub- keys
- c. 52 sub- keys
- d. Only one key and no subkeys

**Answer:** c. 52 sub- keys

**Explanation:**

There are a total of 8 rounds in the IDEA technique for encryption and each of them uses 6 keys. Apart from that, 4 extra keys are used in the final round that is the output transformation round. This gives us a total of 52 subkeys.

$$(8 \times 6) + 4 = 52$$

**5) "The number of rounds in the AES algorithm depends upon the key size being used."**  
**Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?**

- a. 128 key size: 10 rounds
- b. 192 key size: 12 rounds
- c. 256 key size: 14 rounds
- d. All of the above

**Answer:** d. All of the above

**Explanation:**

All the mentioned options display the correct relation between the number of rounds and the key size used in the AES algorithm.

**6) Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher?**

- a. Avalanche effect
- b. Completeness
- c. Both a. and b.
- d. None of the above

**Answer:** c. Both a. and b.

**Explanation:**

Avalanche effect and Completeness are the two characteristic properties of Block ciphers which differ them from stream ciphers.

**81. Public key encryption/decryption is not preferred because**

- a. it is slow

- b.** it is hardware/software intensive
- c.** it has a high computational load
- d.** all of the mentioned

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (d).all of the mentioned

- 82.** Which one of the following is not a public key distribution means?
- a.** Public-Key Certificates
  - b.** Hashing Certificates
  - c.** Publicly available directories
  - d.** Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (b).Hashing Certificates

- 83.** What is the PGP stand for?
- a.** Permuted Gap Permission
  - b.** Permuted Great Privacy
  - c.** Pretty Good Permission
  - d.** None of the mentioned

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (d).None of the mentioned

- 84.** PGP makes use of which cryptographic algorithm?
- a.** DES
  - b.** AES

c. RSA

d. Rabin

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (c).RSA

**85.** USENET is related to which of the following Public Key distribution schemes?

a. Public-Key Certificates

b. Public announcements

c. Publicly available directories

d. Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (b).Public announcements

**86.** Which of the following public key distribution systems is most secure?

a. Public-Key Certificates

b. Public announcements

c. Publicly available directories

d. Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (a).Public-Key Certificates

**87.** Which systems use a timestamp?

i) Public-Key Certificates

ii) Public announcements

iii) Publicly available directories

iv) Public-Key authority

a. i) and ii)

- b.** iii) and iv)
- c.** i) and iv)
- d.** iv) only

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (c).i) and iv)

- 88.** Which of these systems use timestamps as an expiration date?
- a.** Public-Key Certificates
  - b.** Public announcements
  - c.** Publicly available directories
  - d.** Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (a).Public-Key Certificates

- 89.** Which system uses a trusted third party interface?
- a.** Public-Key Certificates
  - b.** Public announcements
  - c.** Publicly available directories
  - d.** Public-Key authority

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (a).Public-Key Certificates

- 90.** Publicly Available directory is more secure than which other system?
- a.** Public-Key Certificates
  - b.** Public announcements

- c. Public-Key authority
- d. None of the mentioned

[View Answer](#) [Report](#) [Discuss](#) [Too Difficult!](#) [Search Google](#)

**Answer:** (b).Public announcements

1. A method used by an IDS that involves checking for a pattern to identify unauthorized activity.(*No Answer*)
  - a. **CORRECT:** Pattern Matching
  - b. Session Splicing
  - c. Protocol Decoding
  - d. State Table
2. A list or table of stored by a router (or switch) that controls access to and from a network. (*No Answer*)
  - . State Table
    - a. **CORRECT:** Access Control List (ACL)
    - b. Session Splicing
    - c. Packet Filter
3. An analysis method used by some IDS that looks for instances that are not considered normal behavior. (*No Answer*)
  - . Stateful Inspection
    - a. **CORRECT:** Anomaly Detection
    - b. Evasion
    - c. Pattern Matching
4. Bypassing a device, or performing another action, to attack or place malware on a target network without being detected. (*No Answer*)
  - . Packet Filter
    - a. State Table
    - b. **CORRECT:** Evasion
    - c. Honeypot

5. A type of firewall closely related to a packet filter that can track the status of a connection through use of a state table that keeps track of connection activities.(*No Answer*)
  - . Anomaly Detection
    - a. Protocol Decoding
    - b. **CORRECT:** Stateful Inspection
    - c. State Table
6. A tool that uses the monitoring of network traffic, detection of unauthorized access attempts, and notification of unauthorized access attempts to network administrator.(*No Answer*)
  - . Anomaly Detection
    - a. Access Control List (ACL)
    - b. **CORRECT:** Intrusion Detection System (IDS)
    - c. Session Splicing
7. A type of stateless inspection used in some routers and firewalls to limit flow of traffic to what is on the ACL.(*No Answer*)
  - . **CORRECT:** Packet Filter
    - a. Proxy Server
    - b. Evasion
    - c. State Table
8. A way of looking at raw packet data.(*No Answer*)
  - . Proxy Server
    - a. Session Splicing
    - b. **CORRECT:** Protocol Decoding
    - c. Pattern Matching
9. A server (or application) that intercepts the requests clients make of another server, fills the requests that it can, and then forwards the requests it can't handle on to the other server thus helping to improve performance and security.(*No Answer*)
  - . Honeypot
    - a. **CORRECT:** Proxy Server
    - b. Packet Filter
    - c. State Table

10. A table in which data about connection activity is kept by a stateful firewall.(*No Answer*)
- . Evasion
    - a. **CORRECT:** State Table
    - b. Honeypot
    - c. Proxy Server
11. Something set up on a separate network (or in DMZ) to attract hackers and lure them away from the real network; it logs keystrokes, provides other information about an attacker, and also provides warning that someone is trying to attack your network.(*No Answer*)
- . Proxy Server
    - a. State Table
    - b. Evasion
    - c. **CORRECT:** Honeypot
12. A way to change network address information in IP packet headers with a router by connecting multiple computers using one IP address connected to the Internet (or IP network) to convert many private addresses into one public address.(*No Answer*)
- . Access Control List (ACL)
    - a. **CORRECT:** Network Address Translation (NAT)
    - b. Anomaly Detection
    - c. Intrusion Detection System (IDS)
13. A method of avoiding detection by an IDS by sending portions of a request in different packets.(*No Answer*)
- . **CORRECT:** Session Splicing
    - a. Protocol Decoding
    - b. Pattern Matching
    - c. Evasion

1.

What are drawbacks of the host based IDS ?

- A.) Unselective logging of messages may increase the audit burdens
- B.) Selective logging runs the risk of missed attacks
- C.) They are very fast to detect

- D.) They have to be programmed for new patterns

**Show Answer**

**Answer: Option 'A'**

**Unselective logging of messages may increase the audit burdens**

2.

What are the different ways to classify an IDS ?

- A.) Zone based
- B.) Host & Network based
- C.) Network & Zone based
- D.) Level based

**Show Answer**

**Answer: Option 'B'**

**Host & Network based**

3.

What is major drawback of anomaly detection IDS ?

- A.) These are very slow at detection
- B.) It generates many false alarms
- C.) It doesn't detect novel attacks
- D.) None of the mentioned

**Show Answer**

**Answer: Option 'B'**

**It generates many false alarms**

4.

What are strengths of the host based IDS?

- A.) Attack verification
- B.) System specific activity
- C.) No additional hardware required
- D.) All of the mentioned

**Show Answer**

**Answer: Option 'D'**

**All of the mentioned**

5.

What are major components of intrusion detection system?

- A.) Analysis Engine
- B.) Event provider

- C.) Alert Database
- D.) All of the mentioned

**Show Answer**

**Answer: Option 'D'**

**All of the mentioned**

6.

What are strengths of the host based IDS?

- A.) Attack verification
- B.) System specific activity
- C.) No additional hardware required
- D.) All of the mentioned

**Show Answer**

**Answer: Option 'D'**

**All of the mentioned**

7.

What are characteristics of stack based IDS ?

- A.) They are integrated closely with the TCP/IP stack and watch packets
- B.) The host operating system logs in the audit information
- C.) It is programmed to interpret a certain series of packets
- D.) It models the normal usage of network as a noise characterization

**Show Answer**

**Answer: Option 'A'**

**They are integrated closely with the TCP/IP stack and watch packets**

8.

What are major components of intrusion detection system?

- A.) Analysis Engine
- B.) Event provider
- C.) Alert Database
- D.) All of the mentioned

**Show Answer**

**Answer: Option 'D'**

**All of the mentioned**

9.

What are characteristics of Network based IDS ?

- A.) They look for attack signatures in network traffic
- B.) Filter decides which traffic will not be discarded or passed
- C.) It is programmed to interpret a certain series of packet
- D.) It models the normal usage of network as a noise characterization

**Show Answer**

**Answer: Option 'A'**

**They look for attack signatures in network traffic**

10.

What are the different ways to classify an IDS ?

- A.) Zone based
- B.) Host & Network based
- C.) Network & Zone based
- D.) Level based

**Show Answer**

**Answer: Option 'B'**

**Host & Network based**

11.

What is major drawback of anomaly detection IDS ?

- A.) These are very slow at detection
- B.) It generates many false alarms
- C.) It doesn't detect novel attacks
- D.) None of the mentioned

**Show Answer**

**Answer: Option 'B'**

**It generates many false alarms**

1. -systematic tracking of incoming and outgoing traffic: to ascertain how an attack was carried out or how an event occurred on a network.

-intruders and network users often leave trail behind

-identify locations where relevant digital evidence exists

-crucial when developing data map of digital evidence(*No Answer*)

- a. SIM Cards
  - b. Windows Registry
  - c. **CORRECT: Network Forensics**
  - d. Drive Slack
2. -personal digital assistant: can be separated devices from mobile phones
- PDA houses a microprocessor, ROM, RAM, disk drive and various components
- most common PDA, although not referred to as such:IPAD(*No Answer*)
- . Partition
    - a. SIM Cards
    - b. EEPROM
    - c. **CORRECT: PDA's**
3. -a logical drive(*No Answer*)
- . EEPROM
    - a. PDA's
    - b. SIM Cards
    - c. **CORRECT: Partition**
4. - .EVE -> .DFT -> IOLogErrors
- .DD -> .DFT -> IOLogErrors -> MD5(*No Answer*)
- . Additional SIM Card Purposes
    - a. Types of The Formats ProDiscover Creates
    - b. **CORRECT: Files Found When Acquisition is Done (ProDiscover)**
    - c. Mobile Forensics Equipment
5. -allows you to create a representation of another computer on an existing physical computer.
- a virtual machine is just a few files on your hard drive: must allocate space to it; dynamic or static
- a virtual machine recognizes components of the physical machine its on: virtual OS is limited by the physical machines O/S and RAM. (*No Answer*)

- . Partition
  - a. **CORRECT:** Virtual Machine
  - b. Drive Slack
  - c. SIM Cards
- 6. Considerations
  - determine the scope of the investigation.
  - determine what the case requires
  - whether you should collect all info
  - what to do in case of scope creep
- \*the key is to start with a plan but remain flexible in the face of new evidence(*No Answer*)
- . **CORRECT:** Examination Plan
  - a. Drive Slack
  - b. Partition
  - c. SIM Cards
- 7. Can be exported as:
  - RTF ~good for thumbnails and book marks
  - TEXT~plain text(*No Answer*)
- . Drive Slack
  - a. Write Blockers
  - b. Windows Registry
  - c. **CORRECT:** ProDiscover Report
- 8. -UNIX DD~most common raw image format
  - .EVE~has case metadata information(*No Answer*)
- . EnCase Output Formats
  - a. Five Major Categories
  - b. ProDiscover Report
  - c. **CORRECT:** Types of The Formats ProDiscover Creates
- 9. -electronically erasable programmable read-only memory
  - how phones store system data

-enables service providers to reprogram phones without having to physically access memory chips

-OS is stored in ROM: nonvolatile memory(*No Answer*)

- . Partition
  - a. file system
  - b. **CORRECT: EEPROM**
  - c. SIM Cards

10. -file manipulation: file names and extensions/ hidden property

-disk manipulation: hidden partitions/bad clusters

-encryption: bit shifting/stenography(*No Answer*)

- . Windows Registry
  - a. Examination Plan
  - b. Virtual Machine
  - c. **CORRECT: Data-hiding Techniques**

11. -gives us a road map to data on a disk

-type of file system an OS used determines how data is stored on the disk(*No Answer*)

- . **CORRECT: file system**
  - a. Drive Slack
  - b. EEPROM
  - c. SIM Cards

12. -the main concerns with mobile devices are loss of power and synchronization with PC's or the cloud (wired or wireless).

-all mobile devices have volatile memory that may contain valuable information: making sure they don't lose power before you can retrieve RAM data is critical.

-isolated the device from incoming signals with one of the following options: shielded container (paint can, enclosures), use the Faraday Bag, use eight layers of anti-static bags, aluminum foil.

-if device is not isolated, the data of the device will continue to change while in custody of the specialist.(*No Answer*)

- . Additional SIM Card Purposes
  - a. Network Forensics
  - b. **CORRECT:** Acquisition Procedures for Mobile Devices
  - c. Challenges With Mobile Devices

13. -acquisition~preservation~collection

-validation~discrimination~culling

~examination~extraction~review

~reconstruction~analysis

~reporting~presentation~production(*No Answer*)

- . Network Forensics
  - a. **CORRECT:** Five Major Categories
  - b. SIM Cards
  - c. Write Blockers

14. -a database that stores hardware and software configuration information, network connections, user preferences, and setup information.

-can contain valuable info about current/past applications and user created information(*No Answer*)

- . SIM Cards
  - a. **CORRECT:** Windows Registry
  - b. file system
  - c. Write Blockers

15. -unused space in a cluster between the end of an active file and the end of a cluster. (Includes RAM slack and file slack)(*No Answer*)

- . SIM Cards
  - a. file system

- b. Write Blockers
- c. **CORRECT:** Drive Slack

16. -subscribers identity module cards

-found most commonly in GSM devices

-microprocessor and from 16KB to 4MB EEPROM

-GSM refers to mobile phones as "mobile station" and divides a station into two parts: the sim card and the mobile equipment and common network in global networks

-portability of information makes SIM cards versatile(*No Answer*)

- . EEPROM
  - a. PDA's
  - b. **CORRECT:** SIM Cards
  - c. Drive Slack

17. -EnCase (E01)

-RAW (DD)

-SMART (S01)

-Sleuth Kit (AFF)(*No Answer*)

- . Five Major Categories
  - a. **CORRECT:** Different FTK Output Formats
  - b. EnCase Output Formats
  - c. Network Forensics

18. -How long a piece of information lasts on a system versus data that must be collected and preserved before its lost, corrupted, or backed up.

Order:

- 1-live network devices (switches/routers)
- 2-live computers/laptops (RAM and processes)
- 3-live other devices (smartphones, PDA's)

4-Devices/computers already OFF

5-Removable media/cables-adapters/documents(*No Answer*)

. **CORRECT:** Order of Volatility

- a. Partition
- b. Drive Slack
- c. Network Forensics

19. -devices are 'live' computers; traditional "stand-alone OFF computers" approach may be inadequate

-devices are connected to 'live' wireless networks; traditional "disconnect" or "segregate" approach network forensics may be inadequate

-devices lack hardware, software and operating system standardization; many variables affect forensic and eDiscovery techniques and analysis results.

-devices are dynamic in location; communications and operability; computers are mostly static.*(No Answer)*

. **CORRECT:** Challenges With Mobile Devices

- a. Write Blockers
- b. Network Forensics
- c. Acquisition Procedures for Mobile Devices

20. -analog

-digital personal communications service (PC's)

-third-generation (3G and 4G): increased bandwidth

\*continuing to evolve*(No Answer)*

. Data-hiding Techniques

- a. **CORRECT:** Three Generations of Mobile Phone Technology
- b. Order of Volatility
- c. Challenges With Mobile Devices

21. -identifies the subscriber to the network

-stores personal information

-stores address books and messages

-stores service-related information(*No Answer*)

- . Five Major Categories
  - a. ProDiscover Report
  - b. **CORRECT:** Additional SIM Card Purposes
  - c. SIM Cards

22. -hardware utilized for protecting source/hard drive from data alteration/tampering while collecting, preserving, and reviewing CSI.

-prevents operating systems and computer programs from making "writes" to the hard drive being acquired, examined, or analyzed.

-write blockers sits between the suspect/source drive and your analysis computer. (It is usually a hardware device, but software based write blockers may be utilized.*(No Answer)*

- . file system
  - a. Drive Slack
  - b. SIM Cards
  - c. **CORRECT:** Write Blockers

23. primary Windows based:

-EnCase

-Forensic Tool Kit (FTK)

-ProDiscover

-OSForensics

primarily Linux based:

-Sleuth Kit and Autopsy

-Helix

-Knoppix STD

-SMART(*No Answer*)

- . Computer Forensic and EDiscovery Tool Needs

- a. **CORRECT:** Computer Forensic Software Tools
  - b. Network Forensics
  - c. Mobile Forensics Equipment
24. -SIM card readers: a combination hardware/software device used to access the SIM card. You need to be in a forensic lab equip with appropriate anti-static devices.

-general forensic procedure for SIM cards:

- 1-remove the back panel of device
- 2-remove the battery
- 3-remove the SIM card
- 4-insert the SIM card into the card reader
- 5-extract relevant information

-a variety of SIM card readers are on the market: some are forensically sound and some are not

-documenting messages that haven't been read yet is critical: use a video camera to capture each screen, if data cannot be extracted with forensic hardware/software

-mobile forensic tools and utilities:

- Ramsey forensic text enclosure (hardware)
- SIM card reader (hardware)
- Paraben Device Seizure (software)
- BitPim (software)
- Susteen SecureView (software)
- EnCase and FTK (software)(*No Answer*)

- . file system
  - a. Network Forensics
  - b. **CORRECT:** Mobile Forensics Equipment
  - c. Computer Forensic Software Tools

25. -EX01

-E01 (Legacy)(*No Answer*)

- . **CORRECT:** EnCase Output Formats
  - a. Different FTK Output Formats
  - b. EEPROM

c. Network Forensics

26. look for versatility, flexibility, and robustness:

- Lab OS
- File System
- Automated Features
- Venders Reputation
- Acceptance by forensic community
- documented testing and validation

-Keep in mind what application files and operating system you'd be analyzing(*No Answer*)

. **CORRECT:** Computer Forensic and EDiscovery Tool Needs

- a. Mobile Forensics Equipment
- b. Types of The Formats ProDiscover Creates
- c. Computer Forensic Software Tools

Sr.No	Questions	Correct Answer
1.	According to the CIA Triad, which of the below-mentioned element is not considered in the triad?  a) Confidentiality b) Integrity c) Authenticity d) Availability	C
2.	CIA triad is also known as _____  a) NIC (Non-repudiation, Integrity, Confidentiality) b) AIC (Availability, Integrity, Confidentiality) c) AIN (Availability, Integrity, Non-repudiation) d) AIC (Authenticity, Integrity, Confidentiality)	B
3.	_____ of information means, only authorised users are capable of accessing the information.  a) Confidentiality b) Integrity c) Non-repudiation d) Availability	A
4.	_____ means the protection of data from modification by unknown users.  a) Confidentiality b) Integrity c) Authentication d) Non-repudiation	B
5.	When you use the word _____ it means you are protecting your data from getting disclosed.  a) Confidentiality b) Integrity c) Authentication d) Availability	A
6.	When integrity is lacking in a security system, _____ occurs.  a) Database hacking b) Data deletion c) Data tampering d) Data leakage	C
7.	Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?  a) They help understanding hacking better b) They are key elements to a security breach c) They help understand security and its components better d) They help to understand the cyber-crime better	C

8.	<p>This helps in identifying the origin of information and authentic user. This referred to here as _____</p> <p>a) Confidentiality b) Integrity c) Authenticity d) Availability</p>	C
9.	<p>Data _____ is used to ensure confidentiality.</p> <p>a) Encryption b) Locking c) Deleting d) Backup</p>	A
10.	<p>Data integrity gets compromised when _____ and _____ are taken control off.</p> <p>a) Access control, file deletion b) Network, file permission c) Access control, file permission d) Network, system</p>	C
11.	<p>_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.</p> <p>a) Network Security b) Database Security c) Information Security d) Physical Security</p>	C
12.	<p>From the options below, which of them is not a threat to information security?</p> <p>a) Disaster b) Eavesdropping c) Information leakage d) Unchanged default password</p>	D
13.	<p>Compromising confidential information comes under _____</p> <p>a) Bug b) Threat c) Vulnerability d) Attack</p>	B
14.	<p>Which of the following are not security policies?</p> <p>a)Regulatory b)Advisory c)Availability d)User Policies</p>	C

15.	<p>Examples of User Policies is/are:</p> <ul style="list-style-type: none"> <li>a) Password Policies</li> <li>b) Internet Usage</li> <li>c) System Use</li> <li>d) All of the above</li> </ul>	D
16.	<p>_____ Policy ensures that the organization is maintaining standards set by specific industry regulation.</p> <ul style="list-style-type: none"> <li>a) Regulatory</li> <li>b) Advisory</li> <li>c) Availability</li> <li>d) User Policies</li> </ul>	A
17.	<p>_____ Policy is like standards rules and regulations set by the management to advise their employees on their activity or behavior</p> <ul style="list-style-type: none"> <li>a) Regulatory</li> <li>b) Advisory</li> <li>c) Availability</li> <li>d) User Policies</li> </ul>	B
18.	<p>What defines the restrictions on employees such as usage?</p> <ul style="list-style-type: none"> <li>a) Regulatory</li> <li>b) Advisory</li> <li>c) Availability</li> <li>d) User Policies</li> </ul>	D
19.	<p>The full form of OSI is OSI model is _____</p> <ul style="list-style-type: none"> <li>a) Open Systems Interconnection</li> <li>b) Open Software Interconnection</li> <li>c) Open Systems Internet</li> <li>d) Open Software Internet</li> </ul>	A
20.	<p>In _____ layer, vulnerabilities are directly associated with physical access to networks and hardware.</p> <ul style="list-style-type: none"> <li>a) physical</li> <li>b) data-link</li> <li>c) network</li> <li>d) application</li> </ul>	A
21.	<p>Loss of power and unauthorized change in the functional unit of hardware comes under problems and issues of the physical layer.</p> <ul style="list-style-type: none"> <li>a) True</li> <li>b) False</li> </ul>	A

22.	Which of the following attack can actively modify communications or data?  a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	C
23.	OSI architecture mainly focuses on: 1) Security Attack 2) Security Techniques/Mechanisms 3) Categories of Security Service  a)1 b)1 &3 c) 2& 3 d)1,2,3	D
24.	IT security department must periodically check for security logs and entries made during office hours.  a) True b) False	A
25.	Release of Message Content and Traffic analysis are type of :  a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	D
26.	If communication between 2 people is overheard by a third person without manipulation of any data, it is called as:  a) Release of Message Content-Passive Attack b) Traffic analysis -Passive Attacks c) Release of Message Content- Active Attacks d) Traffic analysis -Active Attacks	A
27.	If communication between 2 people is overheard by a third person without extraction of any data, it is called as:  a) Release of Message Content-Passive Attack b) Traffic analysis -Passive Attacks c) Release of Message Content- Active Attacks d) Traffic analysis -Active Attacks	D
28.	No modification of data is a characteristic of  a)Active Attack b)Passive Attack	A
29.	Which of the following are Active attack types	D

	a)Masquerade b)Replay c)Modification d)All of the above	
30.	_____ means when an attacker pretends to be authentic user  a)Masquerade b)Replay c)Modification d)Traffic analysis	A
31.	_____ attack is when original data is modified and malicious data is inserted  a)Masquerade b)Replay(Rewrite) c)Modification d)Traffic analysis	B
32.	When original data is changed to make it non-meaningful by attacker it is known as  a)Masquerade b)Replay c)Modification of Messages d)Traffic analysis	C
33.	Which is the type of attack when Network is made unavailable for user  a)Masquerade b)Replay c)Modification d)Denial of Service	D
34.	Modification of Data is done in:  a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	A
35.	The information that gets transformed in encryption is  a) Plain text b) Parallel text c) Encrypted text d) Decrypted text	A
36.	1. The process of transforming plain text into unreadable text.	B

	a) Decryption b) Encryption c) Network Security d) Information Hiding	
37.	A process of making the encrypted text readable again.  a) Decryption b) Encryption c) Network Security d) Information Hiding	A
38.	A unique piece of information that is used in encryption.  a) Cipher b) Plain Text c) Key d) Cipher	C
39.	Assurance that authentic user is taking part in communication is:  a)Authentication b)Authorization c)Access Control d)Auditing	A
40.	ATM pin while withdrawing money is an example of using:  a)Authentication b)Authorization c)Access Control d)Auditing	B
41.	Study of creating a d using encryption and decryption techniques.  a) Cipher b) Cryptography c) Encryption d) Decryption	B
42.	An attack in which the user receives unwanted amount of e-mails.  a) Smurfing b) Denial of service c) E-mail bombing d) Ping storm	C
43.	The process of disguising plaintext in such a way that its substance gets hidden (into what is known as cipher-text) is called _____	D

	a) cryptanalysis b) decryption c) reverse engineering d) encryption	
44.	In _____ same keys are implemented for encrypting as well as decrypting the information.  a) Symmetric Key Encryption b) Asymmetric Key Encryption c) Asymmetric Key Decryption d) Hash-based Key Encryption	A
45.	The procedure to add bits to the last block is termed as _____  a) decryption b) hashing c) tuning d) padding	D
46.	In asymmetric key cryptography, the private key is kept by _____  a) sender b) receiver c) sender and receiver d) all the connected devices to the network	B
47.	Cryptanalysis is used _____ a) to find some insecurity in a cryptographic scheme b) to increase the speed c) to encrypt the data d) to make new ciphers	A
48.	Conventional cryptography is also known as _____ or symmetric-key encryption.  a) secret-key b) public key c) protected key d) primary key	A
49.	_____ is the art & science of cracking the cipher-text without knowing the key.  a) Cracking b) Cryptanalysis c) Cryptography d) Crypto-hacking	B
50.	In _____ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.	A

- |  |  |  |
|--|--|--|
|  | <ul style="list-style-type: none"><li>a) Block Cipher</li><li>b) One-time pad</li><li>c) Hash functions</li><li>d) Vigenere Cipher</li></ul> |  |
|--|--|--|

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
((OPTION_A)) THIS IS MANDATORY OPTION	Network Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Database Security
((OPTION_C)) This is optional	Information Security
((OPTION_D)) This is optional	Physical Security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information from alteration, destruction, deletion or disclosure by unauthorised users.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a threat to information security?
((OPTION_A)) THIS IS MANDATORY OPTION	Disaster
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Eavesdropping
((OPTION_C)) This is optional	Information leakage
((OPTION_D)) This is optional	Unchanged default password
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Disaster, eavesdropping and information leakage come under information security threats whereas not changing the default password of any system, hardware or any software comes under the category of vulnerabilities that the user may pose to its system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a vulnerability to information security?
((OPTION_A))  THIS IS MANDATORY OPTION	flood
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	without deleting data, disposal of storage media
((OPTION_C))  This is optional	unchanged default password
((OPTION_D))  This is optional	latest patches and updates not done
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Compromising confidential information comes under
((OPTION_A)) THIS IS MANDATORY OPTION	Bug
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Threat
((OPTION_C)) This is optional	Vulnerability
((OPTION_D)) This is optional	Attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	Threats are anything that may cause damage or harm to a computer system, individual or any information. Compromising of confidential information means extracting out sensitive data from a system by illegal manner.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Lack of access control policy is a
((OPTION_A)) THIS IS MANDATORY OPTION	Bug
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Threat
((OPTION_C)) This is optional	Vulnerability
((OPTION_D)) This is optional	Attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Access control policies are incorporated to a security system for restricting of unauthorised access to any logical or physical system. Every security compliance program must need this as a fundamental component. Those systems which lack this feature is vulnerable.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Possible threat to any information cannot be
((OPTION_A)) THIS IS MANDATORY OPTION	reduced
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transferred
((OPTION_C)) This is optional	protected
((OPTION_D)) This is optional	ignored
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	When there lies a threat to any system, safeguards can be implemented, outsourced, distributed or transferred to some other system, protected using security tools and techniques but cannot be ignored.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	According to the CIA Triad, which of the below-mentioned element is not considered in the triad?
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authenticity
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	According to the CIA triad the three components that a security need is the Confidentiality, Integrity, Availability (as in short read as

		
CIA).		

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When you use the word _____ it means you are protecting your data from getting disclosed.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	

((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Confidentiality is what every individual prefer in terms of physical privacy as well as digital privacy. This term means our information needs to be protected from getting disclose to unauthorised parties, for which we use different security mechanisms like password protection, biometric security, OTPs (One Time Passwords) etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ means the protection of data from modification by unknown users.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	Non-repudiation
((OPTION_E)) This is optional. If optional keep empty so that system will skip	

this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	A information only seems valuable if it is correct and do not get modified during its journey in the course of arrival. The element integrity makes sure that the data sent or generated from other end is correct and is not modified by any unauthorised party in between.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When integrity is lacking in a security system, _____ occurs.
((OPTION_A)) THIS IS MANDATORY OPTION	Database hacking
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data deletion
((OPTION_C)) This is optional	Data tampering
((OPTION_D)) This is optional	Data leakage
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The term data tampering is used when integrity is compromised in any security model and checking its integrity later becomes costlier. Example: let suppose you sent \$50 to an authorised person and in between a Man in the Middle (MiTM) attack takes place and the value has tampered to \$500. This is how integrity is compromised.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	of information means, only authorised users are capable of accessing the information.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Non-repudiation
((OPTION_D)) This is optional	Availability
((OPTION_E)) This is optional.	

If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Information seems useful only when right people (authorised users) access it after going through proper authenticity check. The key element availability ensures that only authorised users are able to access the information.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?
((OPTION_A)) THIS IS MANDATORY OPTION	They help understanding hacking better
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	They are key elements to a security breach
((OPTION_C)) This is optional	They help understands security and its components better
((OPTION_D)) This is optional	They help to understand the cyber-crime better
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The four elements of security viz. confidentiality, integrity, authenticity & availability helps in better understanding the pillars of security and its different components.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	This helps in identifying the origin of information and authentic user. This referred to here as
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authenticity
((OPTION_D)) This is optional	Availability
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The key element, authenticity helps in assuring the fact that the information is from the original source.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Data _____ is used to ensure confidentiality.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Locking
((OPTION_C)) This is optional	Deleting
((OPTION_D)) This is optional	Backup
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Data encryption is the method of converting plain text to cipher-text and only authorised users can decrypt the message back to plain text. This preserves the confidentiality of data

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of these is not a proper method of maintaining AUTHENTICATION?
((OPTION_A)) THIS IS MANDATORY OPTION	Biometric verification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ID and password based verification
((OPTION_C)) This is optional	2-factor authentication
((OPTION_D)) This is optional	switching off the phone
((OPTION_E))	

This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Switching off the phone in the fear of preserving the confidentiality of data is not a proper solution for data confidentiality. Fingerprint detection, face recognition, password-based authentication, two-step verifications are some of these.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Data integrity gets compromised when _____ and _____ are taken control off.
((OPTION_A)) THIS IS MANDATORY OPTION	Access control, file deletion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Network, file permission
((OPTION_C)) This is optional	Access control, file permission
((OPTION_D)) This is optional	Network, system

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The two key ingredients that need to be kept safe are: access control & file permission in order to preserve data integrity.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	One common way to maintain data availability is
((OPTION_A)) THIS IS MANDATORY OPTION	Data clustering
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data backup
((OPTION_C)) This is optional	Data recovery
((OPTION_D)) This is optional	Data Altering

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	For preventing data from data-loss, or damage data backup can be done and stored in a different geographical location so that it can sustain its data from natural disasters & unpredictable events.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as
((OPTION_A)) THIS IS MANDATORY OPTION	Black Hat hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	White Hat Hackers
((OPTION_C)) This is optional	Grey Hat Hackers
((OPTION_D)) This is optional	Red Hat Hackers

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	White Hat Hackers are cyber security analysts and consultants who have the intent to help firms and Governments in the identification of loopholes as well as help to perform penetration tests for securing a system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the legal form of hacking based on which jobs are provided in IT industries and firms?
((OPTION_A)) THIS IS MANDATORY OPTION	Cracking
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Non ethical Hacking
((OPTION_C)) This is optional	Ethical hacking
((OPTION_D))	Hactivism

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Ethical Hacking is an ethical form of hacking done by white-hat hackers for performing penetration tests and identifying potential threats in any organizations and firms.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are "they" referred to here?
((OPTION_A)) THIS IS MANDATORY OPTION	Gray Hat Hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	White Hat Hackers
((OPTION_C)) This is optional	Hactivists
((OPTION_D))	Black Hat Hackers

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Black Hat hackers also termed as 'crackers' and are a major type of cyber criminals who take unauthorized access in user's account or system and steal sensitive data or inject malware into the system for their profit or to harm the organization.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are the combination of both white as well as black hat hackers.
((OPTION_A)) THIS IS MANDATORY OPTION	Grey Hat hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Green Hat hackers
((OPTION_C)) This is optional	Blue Hat Hackers

((OPTION_D)) This is optional	Red Hat Hacker
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Grey Hat Hackers have a blending character of both ethical as well as un-ethical hacker. They hack other's systems for fun but do not harm the system, exploits bugs and vulnerabilities in network without the knowledge of the admin or the owner.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The amateur or newbie in the field of hacking who don't have many skills about coding and in-depth working of security and hacking tools are called _____
((OPTION_A)) THIS IS MANDATORY OPTION	Sponsored Hackers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hactivists
((OPTION_C))	Script Kiddies

This is optional	
((OPTION_D))	Whistle Blowers
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Script Kiddies are new to hacking and at the same time do not have many interests in developing coding skills or find bugs of their own in systems; rather they prefer downloading of available tools (developed by elite hackers) and use them to break any system or network. They just try to gain attention of their friend circles.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Suicide Hackers are those _____
((OPTION_A)) THIS IS MANDATORY OPTION	who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their malicious activity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	individuals with no knowledge of codes but an expert in using hacking tools

((OPTION_C)) This is optional	who know the consequences of their hacking activities and hence try to prevent them by erasing their digital footprints
((OPTION_D)) This is optional	who are employed in an organization to do malicious activities on other firms
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Suicide hackers are those who break into any network or system with or without knowing the consequences of the cyber crime and its penalty. There are some suicide hackers who intentionally do crimes and get caught to bring their names in the headlines.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Criminal minded individuals who work for terrorist organizations and steal information of nations and other secret intelligence are _____
((OPTION_A)) THIS IS MANDATORY OPTION	State sponsored hackers
((OPTION_B)) THIS IS ALSO MANDATORY	Blue Hat Hackers

OPTION	
((OPTION_C)) This is optional	Cyber Terrorists
((OPTION_D)) This is optional	Red Hat Hackers
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Cyber Terrorists are very expert programmers and cyber criminals who hide themselves while doing malicious activities over the internet and they are smart enough to hide themselves or their tracks of action. They are hired for gaining unauthorised access to nation's data centres or break into the network of intelligence agencies.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are those individuals who maintain and handles IT security in any firm or organization.
((OPTION_A)) THIS IS MANDATORY OPTION	IT Security Engineer
((OPTION_B))	Cyber Security Interns

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Software Security Specialist
((OPTION_D)) This is optional	Security Auditor
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is an intermediary level of position of an individual in an organization or firm who builds and preserves different systems and its associated security tools of the firm of organization to which he/she belongs.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Role of security auditor is to _____
((OPTION_A)) THIS IS MANDATORY OPTION	secure the network

((OPTION_B)) THIS IS ALSO MANDATORY OPTION	probe for safety and security of organization's security components and systems
((OPTION_C)) This is optional	detects and prevents cyber attacks and threats to organization
((OPTION_D)) This is optional	does penetration testing on different web applications
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Security auditors are those who conduct auditing of various computer and network systems on an organization or company and reports the safety and security issues as well as helps in suggesting improvements or enhancements in any particular system that is threat prone.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are senior level corporate employees who have the role and responsibilities of creating and designing secured network or security structures.
((OPTION_A)) THIS IS MANDATORY	Ethical Hackers

OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Chief Technical Officer
((OPTION_C)) This is optional	IT Security Engineers
((OPTION_D)) This is optional	Security Architect
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Security architect are those senior grade employees of an organization who are in charge of building, designing, implementing and testing of secured network topologies, protocols as well as secured computers in an organization.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Governments hired some highly skilled hackers. These types of hackers are termed as _____
((OPTION_A)) THIS IS	Special Hackers

<b>MANDATORY OPTION</b>	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Government Hackers
((OPTION_C))  This is optional	Cyber Intelligence Agents
((OPTION_D))  This is optional	Nation / State sponsored hackers
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Nation / State sponsored hackers are specific individuals who are employed or hired by the government of that nation or state and protect the nation from cyber terrorists and other groups or individuals and to reveal their plans, communications and actions.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The full form of Malware is _____
((OPTION_A))	Malfunctioned Software

THIS IS MANDATORY OPTION	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Multipurpose Software
((OPTION_C))  This is optional	) Malicious Software
((OPTION_D))  This is optional	Malfunctioning of Security
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Different types of harmful software and programs that can pose threats to a system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransomware, spyware, worms, rootkits etc.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Who deploy Malwares to a system or network?

((OPTION_A)) THIS IS MANDATORY OPTION	Criminal organizations, Black hat hackers, malware developers, cyber-terrorists
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Criminal organizations, gray hat hackers, Malware developers, Penetration testers
((OPTION_C)) This is optional	) Criminal organizations, Black hat hackers, software developers, cyber-terrorists
((OPTION_D)) This is optional	Criminal organizations, White hat hackers, malware developers, cyber-terrorists
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	Criminal-minded organizations, groups and individuals cyber-terrorist groups, Black hat hackers, malware developers etc are those who can deploy malwares to any target system or network in order to deface that system.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	_____ is a code injecting method used for attacking the database of a system / website.

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	HTML injection
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SQL Injection
((OPTION_C)) This is optional	Malicious code injection
((OPTION_D)) This is optional	XML Injection
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	SQLi (Structured Query Language Injection) is a popular attack where SQL code is targeted or injected; for breaking the web application having SQL vulnerabilities. This allows the attacker to run malicious code and take access to the database of that server.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN	This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?

CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	SQL injection
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	HTML Injection
((OPTION_C)) This is optional	Cross Site Scripting (XSS)
((OPTION_D)) This is optional	Cross Site Request Forgery (XSRF)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	XSS attack can be infused by putting the malicious code (which gets automatically run) in any comment section or feedback section of any webpage (usually a blogging page). This can hamper the reputation of a site and the attacker may place any private data or personal credentials.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	An attempt to harm, damage or cause threat to a system or network is broadly termed as _____

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A))  THIS IS MANDATORY OPTION	Cyber-crime
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Cyber Attack
((OPTION_C))  This is optional	System hijacking
((OPTION_D))  This is optional	Digital crime
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cyber attack is an umbrella term used to classify different computer & network attacks or activities such as extortion, identity theft, email hacking, digital spying, stealing hardware, mobile hacking and physical security breaching.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.
((OPTION_A)) THIS IS MANDATORY OPTION	Network Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Database Security
((OPTION_C)) This is optional	Information Security
((OPTION_D)) This is optional	Physical Security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information from alteration, destruction, deletion or disclosure by unauthorised users.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	From the options below, which of them is not a vulnerability to information security?
((OPTION_A))  THIS IS MANDATORY OPTION	flood
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	without deleting data, disposal of storage media
((OPTION_C))  This is optional	unchanged default password
((OPTION_D))  This is optional	latest patches and updates not done
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a set of conventions & rules set for communicating two or more devices residing in the same network?
((OPTION_A))  THIS IS MANDATORY OPTION	Security policies
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Protocols
((OPTION_C))  This is optional	Wireless network
((OPTION_D))  This is optional	Network algorithms
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Network protocols are designed with mechanisms for identifying devices and make connections between them. In addition, some proper rules are defined as to how data packets will be sent and received.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The field that covers a variety of computer networks, both public and private, that are used in everyday jobs
((OPTION_A)) THIS IS MANDATORY OPTION	Artificial Intelligence
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ML
((OPTION_C)) This is optional	Network Security
((OPTION_D)) This is optional	IT
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Network security covers a variety of computer networks, both private and public. Everyday jobs like conducting transactions and communications among business and government agencies etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Network Security provides authentication and access control for resources.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is not an objective of network security?
((OPTION_A)) THIS IS MANDATORY OPTION	Identification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Authentication
((OPTION_C)) This is optional	Access control
((OPTION_D)) This is optional	Lock
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The Identification, Authentication and Access control are the objectives of network security. There is no such thing called lock.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of these is a part of network identification?
((OPTION_A)) THIS IS MANDATORY OPTION	UserID
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Password
((OPTION_C)) This is optional	OTP
((OPTION_D)) This is optional	fingerprint
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The answer is UserID. UserID is a part of identification. UserID can be a combination of username, user student number etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The process of verifying the identity of a user.
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Identification
((OPTION_C)) This is optional	Validation
((OPTION_D)) This is optional	Verification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	It is called an authentication. It is typically based on passwords, smart card, fingerprint, etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Security features that control that can access resources in the OS
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Identification
((OPTION_C)) This is optional	Validation
((OPTION_D)) This is optional	Access control
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Access control refers to the security features. Applications call access control to provide resources

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm in encryption is called
((OPTION_A)) THIS IS MANDATORY OPTION	Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Procedure
((OPTION_C)) This is optional	Cipher
((OPTION_D)) This is optional	Module
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	An algorithm used in encryption is referred to as a cipher. cipher is an algorithm for performing encryption or decryption

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The information that gets transformed in encryption is
((OPTION_A)) THIS IS MANDATORY OPTION	Plain text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Parallel text
((OPTION_C)) This is optional	Encrypted text
((OPTION_D)) This is optional	Decrypted text
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The text that gets transformed is called plain text. The algorithm used is called cipher

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The type of threats on the security of a computer system or network are..... i) Interruption ii) Interception iii) Modification iv) Creation v) Fabrication
((OPTION_A)) THIS IS MANDATORY OPTION	i, ii, iii and iv only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii, iii, iv and v only
((OPTION_C)) This is optional	i, ii, iii and v only
((OPTION_D)) This is optional	All i, ii, iii, iv and v
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is computer threat?
((OPTION_A))  THIS IS MANDATORY OPTION	Phishing
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Soliciting
((OPTION_C))  This is optional	DoS attack
((OPTION_D))  This is optional	stalking
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a term used in cryptography that refers to a message before encryption or after decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PLAIN TEXT
((OPTION_C)) This is optional	Original text
((OPTION_D)) This is optional	Plain script
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ is encrypted text
((OPTION_A)) THIS IS MANDATORY OPTION	cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	cipher script
((OPTION_C)) This is optional	secret text
((OPTION_D)) This is optional	secret script
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An _____ along with a key is used in the encryption
((OPTION_A)) THIS IS MANDATORY OPTION	cryptography algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption algorithm
((OPTION_C)) This is optional	encryption algorithm
((OPTION_D)) This is optional	plain text algorithm
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them.
((OPTION_A)) THIS IS MANDATORY OPTION	Availability
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	Cryptography
((OPTION_D)) This is optional	Integrity
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that information are in a format that is true and correct to its original purposes.
((OPTION_A)) THIS IS MANDATORY OPTION	Availability
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	integrity
((OPTION_D)) This is optional	cryptography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures that information and resources are available to those who need them.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Availability</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Confidentiality</b>
((OPTION_C)) This is optional	<b>Cryptography</b>
((OPTION_D)) This is optional	<b>Integrity</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the process of identifying an individual, usually based on a username and password.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Authentication</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Authorization</b>
((OPTION_C)) This is optional	<b>either authentication or authorization</b>
((OPTION_D)) This is optional	<b>neither authentication nor authorization</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is the process of giving individuals access to system objects based on their identity.
((OPTION_A)) THIS IS MANDATORY OPTION	<b>Authentication</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>Authorization</b>
((OPTION_C)) This is optional	<b>either authentication or authorization</b>
((OPTION_D)) This is optional	<b>neither congestion control nor quality of service</b>
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	when someone gains access to a server, website, or other sensitive data using someone else's account details called as
((OPTION_A)) THIS IS MANDATORY OPTION	Authorized access
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Access control
((OPTION_C)) This is optional	Unauthorized access
((OPTION_D)) This is optional	access
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.called as
((OPTION_A)) THIS IS MANDATORY OPTION	Thief
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	hacker
((OPTION_C)) This is optional	attacker
((OPTION_D)) This is optional	criminal
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is an action or event that might compromise the security.
((OPTION_A))  THIS IS MANDATORY OPTION	Threat
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Vulnerability
((OPTION_C))  This is optional	Protect
((OPTION_D))  This is optional	attack
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system
((OPTION_A)) THIS IS MANDATORY OPTION	threat
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Vulnerability
((OPTION_C)) This is optional	Attack
((OPTION_D)) This is optional	Protection
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is a software that operates on different OS which is used to prevent from malicious software.
((OPTION_A)) THIS IS MANDATORY OPTION	Anti virus
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	virus
((OPTION_C)) This is optional	protocol
((OPTION_D)) This is optional	risk
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Is a technique that a hacker uses to stole data by a person for different purposes by psychological manipulation combined with social scenes.
((OPTION_A)) THIS IS MANDATORY OPTION	Social Engineering
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IT engineering
((OPTION_C)) This is optional	Psycology
((OPTION_D)) This is optional	Social engineering
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is a software or hardware which is used to filter network traffic based on rules.
((OPTION_A)) THIS IS MANDATORY OPTION	antivirus
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	firewall
((OPTION_C)) This is optional	protocol
((OPTION_D)) This is optional	keylogger
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not Basic Functions of Antivirus Engines
((OPTION_A)) THIS IS MANDATORY OPTION	Scanning
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity Checking
((OPTION_C)) This is optional	Interception
((OPTION_D)) This is optional	Evesdropping
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is name of antivirus
((OPTION_A))  THIS IS MANDATORY OPTION	AVG
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	PAN
((OPTION_C))  This is optional	SACK
((OPTION_D))  This is optional	FIREP
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Hacking tools that can be found very easily by everyone just by googling and they are endless.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Potential Losses due to Security Attacks doesn't involve _____
((OPTION_A)) THIS IS MANDATORY OPTION	Losing your data
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Bad usage of your computer resources
((OPTION_C)) This is optional	Reputation gain
((OPTION_D)) This is optional	Identity theft
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Reputation loss is part of it and not gain

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not malware category?
((OPTION_A))  THIS IS MANDATORY OPTION	Worms
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Viruses
((OPTION_C))  This is optional	Trojans
((OPTION_D))  This is optional	None of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	All are malware categories

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ encrypts all your data when your computer gets infected and the second is to roll back the data at a specific time you want.
((OPTION_A)) THIS IS MANDATORY OPTION	ransomware
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	firmware
((OPTION_C)) This is optional	middleware
((OPTION_D)) This is optional	Cyber ware
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	this network is created between two secure network devices like two firewalls.
((OPTION_A)) THIS IS MANDATORY OPTION	LAN
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MAN
((OPTION_C)) This is optional	VPN
((OPTION_D)) This is optional	WAN
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Virtual private network

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Name of the attack when integrity is compromised is called as _____
((OPTION_A))  THIS IS MANDATORY OPTION	Fabrication
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	interception
((OPTION_C))  This is optional	Interruption
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Attack made on confidentiality is __
((OPTION_A))  THIS IS MANDATORY OPTION	interception
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C))  This is optional	interruption
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	an attack on availability such as a denial of service attack (or DOS)
((OPTION_A))  THIS IS MANDATORY OPTION	Interruption
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Interception
((OPTION_C))  This is optional	fabrication
((OPTION_D))  This is optional	modification
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An unauthorized party inserts counterfeit objects into the system and basically attacks the authenticity of the system.
((OPTION_A)) THIS IS MANDATORY OPTION	modification
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C)) This is optional	interception
((OPTION_D)) This is optional	interruption
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Attack in which a network service is made degraded or unavailable for legitimate use
((OPTION_A)) THIS IS MANDATORY OPTION	Interruption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	fabrication
((OPTION_C)) This is optional	interception
((OPTION_D)) This is optional	modification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is assurance that someone cannot deny something.
((OPTION_A))  THIS IS MANDATORY OPTION	availability
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	confidentiality
((OPTION_C))  This is optional	Access control
((OPTION_D))  This is optional	Non-repudiation
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the purpose of a Denial of Service attack?
((OPTION_A))  THIS IS MANDATORY OPTION	Exploit a weakness in the TCP/IP stack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	To execute a Trojan on a system
((OPTION_C))  This is optional	To overload a system so it is no longer operational
((OPTION_D))  This is optional	To shutdown services by turning them off
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	DoS attacks force systems to stop responding by overloading the processing of the system

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What are some of the most common vulnerabilities that exist in a network or system?
((OPTION_A)) THIS IS MANDATORY OPTION	Changing manufacturer, or recommended, settings of a newly installed application.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additional unused features on commercial software packages
((OPTION_C)) This is optional	Utilizing open source application code
((OPTION_D)) This is optional	Balancing security concerns with functionality and ease of use of a system.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Linux is an open source code and considered to have greater security than the commercial Windows environment

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Sniffing is used to perform _____ fingerprinting
((OPTION_A))  THIS IS MANDATORY OPTION	Passive stack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Active stack
((OPTION_C))  This is optional	Passive banner grabbing
((OPTION_D))  This is optional	Scanned
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Passive stack fingerprinting uses sniffing technologies instead of scanning

((MARKS)) QUESTION IS OF HOW MANY	1
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a principle of data security?
((OPTION_A)) THIS IS MANDATORY OPTION	Data Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data Integrity
((OPTION_C)) This is optional	Authentication
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY	2
---	---

MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following attacks is a passive attack?
((OPTION_A))  THIS IS MANDATORY OPTION	Masquerade
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Modification of message
((OPTION_C))  This is optional	Denial of service
((OPTION_D))  This is optional	Traffic analysis
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	In a passive attack, the attacker does not modify any part of the data. His attempt is only to obtain the information and not to modify it. From the mentioned options, this happens only in Traffic analysis in which the attacker monitors the pattern of transmission. The rest other options are examples of active attacks.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options correctly defines the Brute force attack?
((OPTION_A)) THIS IS MANDATORY OPTION	Brutally forcing the user to share the useful information like pins and passwords.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Trying every possible key to decrypt the message.
((OPTION_C)) This is optional	One entity pretends to be some other entity
((OPTION_D)) This is optional	The message or information is modified before sending it to the receiver.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	Integer value
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Square matrix
((OPTION_C)) This is optional	An array of characters
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	measures taken by any enterprise or organisation to secure its computer network and data using both hardware and software systems is called as
((OPTION_A)) THIS IS MANDATORY OPTION	Network security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Information security
((OPTION_C)) This is optional	Cyber security
((OPTION_D)) This is optional	Internet security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	phishing and pre-texting is part of _____
((OPTION_A)) THIS IS MANDATORY OPTION	<b>NETWORK SECURITY</b>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<b>CYBER SECURITY</b>
((OPTION_C)) This is optional	Internet security
((OPTION_D)) This is optional	Internet security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ ensures to protect the transit data only.
((OPTION_A)) THIS IS MANDATORY OPTION	NETWORK SECURITY
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet security
((OPTION_C)) This is optional	Information security
((OPTION_D)) This is optional	Cyber security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is danger for <b>Integrity</b> as well as <b>availability</b> .
((OPTION_A)) THIS IS MANDATORY OPTION	Active attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ is danger for <b>Confidentiality</b> .
((OPTION_A)) THIS IS MANDATORY OPTION	Active attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ attack attention is on detection.
((OPTION_A))  THIS IS MANDATORY OPTION	Passive attack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Active Attack
((OPTION_C))  This is optional	Both
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	in _____ attack attention is on prevention.
((OPTION_A))  THIS IS MANDATORY OPTION	Active attack
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive attack
((OPTION_C))  This is optional	Both
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Due to ___ attack system is always damaged.
((OPTION_A))  THIS IS MANDATORY OPTION	Active
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C))  This is optional	Both active and passive
((OPTION_D))  This is optional	None of these
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	due to _____ attack, there is no any harm to the system.
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	Both active and passive
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ attack is tough to restrict from entering systems or networks.
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	Both active and passive
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ Attack is easy to prohibited in comparison to _____ attack.
((OPTION_A))  THIS IS MANDATORY OPTION	Active,passive
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive,active
((OPTION_C))  This is optional	
((OPTION_D))  This is optional	
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not active attack
((OPTION_A)) THIS IS MANDATORY OPTION	Denial of service (DoS)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	replay
((OPTION_C)) This is optional	Trojans
((OPTION_D)) This is optional	traffic analysis
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In __ <b>attack</b> , an attacker tries to modify the content of the messages.
((OPTION_A))  THIS IS MANDATORY OPTION	Active
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C))  This is optional	
((OPTION_D))  This is optional	
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	in _____ <b>attack</b> , an attacker observes the messages, copy them and may use them for malicious purposes
((OPTION_A)) THIS IS MANDATORY OPTION	Active
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Passive
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is state of being free from potential threats or dangers
((OPTION_A)) THIS IS MANDATORY OPTION	privacy
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	freedom
((OPTION_C)) This is optional	security
((OPTION_D)) This is optional	independence
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ refers to the state of being free from unwanted attention.
((OPTION_A)) THIS IS MANDATORY OPTION	Freedom
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Security
((OPTION_C)) This is optional	Privacy
((OPTION_D)) This is optional	independence
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ can be achieved without _____ but _____ cannot be achieved without _____.
((OPTION_A)) THIS IS MANDATORY OPTION	Security,privacy,privacy security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Privacy,security,security,privacy
((OPTION_C)) This is optional	Security,privacy,privacy,privacy
((OPTION_D)) This is optional	Security,security,privacy,security
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ program refers to a set of protocols and regulations set in place to protect all the confidential information assets and resources that an organization collects and owns.
((OPTION_A)) THIS IS MANDATORY OPTION	Privacy
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Security
((OPTION_C)) This is optional	Security and privacy
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ program focuses on protecting only personal information such as log in credentials, passwords, etc.
((OPTION_A)) THIS IS MANDATORY OPTION	Security
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Privacy
((OPTION_C)) This is optional	Security and privacy
((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following Algorithms does not belong to symmetric encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	3DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	RC5
((OPTION_D)) This is optional	IDEA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Assymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key?
((OPTION_A)) THIS IS MANDATORY OPTION	Not true, the message can also be decrypted with the Public Key.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A so called "one way function with back door" is applied for the encryption
((OPTION_C)) This is optional	The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key.
((OPTION_D)) This is optional	The encrypted message contains the function for decryption which identifies the Private Key.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	An one-way function is a function which a computer can calculate quickly, but whose reversal would last months or years. An one-way function with back door can be reversed with the help of a couple of additional information (the back door), but scarcely

	without this information. The information for the back door is contained in the private Key.
--	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the largest disadvantage of the symmetric Encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	More complex and therefore more time-consuming calculations.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Problem of the secure transmission of the Secret Key
((OPTION_C)) This is optional	Less secure encryption function.
((OPTION_D)) This is optional	Isn't used any more
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION))	As there is only one key in the symmetrical encryption, this must

)) This is also optional	be known by both sender and recipient and this key is sufficient to decrypt the secret message. Therefore it must be exchanged between sender and receiver in such a manner that an unauthorized person can in no case take possession of it.
--------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the principle of the encryption using a key?
((OPTION_A)) THIS IS MANDATORY OPTION	The key indicates which function is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	The key contains the secret function for encryption including parameters. Only a password can activate the key.
((OPTION_C)) This is optional	All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.
((OPTION_D)) This is optional	The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	C

E	
((EXPLANATION)) This is also optional	The encoding of a message is calculated by an algorithm. If always the same algorithm would be used, it would be easy to crack intercepted messages. However, it isn't possible to invent a new algorithm whenever the old one was cracked, therefor the possibility to parameterize algorithms is needed and this is the assignment of the key. All algorithms must be public, only the keys are secret (principle of Kerckhoff, Dutch cryptographer during 19th century).

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If the sender and receiver use different keys, the system is referred to as conventional cipher system
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Such a system is called asymmetric, two-key, or public-key cipher system

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW
((OPTION_A)) THIS IS MANDATORY OPTION	ABANDONED LOCK
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ENCRYPTED TEXT
((OPTION_C)) This is optional	ABANDONED TEXT
((OPTION_D)) This is optional	ENCRYPTED LOCK
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher uses $C = (p+3) \text{ mod } 26$ to encrypt.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Caesar Cipher is an example of
((OPTION_A)) THIS IS MANDATORY OPTION	Poly-alphabetic Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Mono-alphabetic Cipher
((OPTION_C)) This is optional	Multi-alphabetic Cipher
((OPTION_D)) This is optional	Bi-alphabetic Cipher
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis
((OPTION_A)) THIS IS MANDATORY OPTION	Random Polyalphabetic, Plaintext, Playfair
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Random Polyalphabetic, Playfair, Vignere
((OPTION_C)) This is optional	Random Polyalphabetic, Vignere, Playfair, Plaintext
((OPTION_D)) This is optional	Random Polyalphabetic, Plaintext, Beaufort, Playfair
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Random Polyalphabetic is the most resistant to frequency analysis, followed by Vignere, Playfair and then Plaintext.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-
((OPTION_A)) THIS IS MANDATORY OPTION	abqdnwewuwjphfvrrtrfznsdokvl
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	abqdmwuwjphfvyyrfznydokvl
((OPTION_C)) This is optional	tbqyrvmwuwjphfvyyrfznydokvl
((OPTION_D)) This is optional	baiuvmwuwjphfoeiyrfznydokvl
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cipher text:= $C_i = P_i + k_i \text{ mod } m \text{ (mod 26).}$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	nlazeiiblji
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nlazeiiblji
((OPTION_C)) This is optional	olaaeiiblki
((OPTION_D)) This is optional	mlaaeiiblki
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Cipher text:= $C_i = P_i + k_i \text{ mod } m \text{ (mod 26).}$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Confusion hides the relationship between the ciphertext and the plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Confusion hides the relationship between the ciphertext and the key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The S-Box is used to provide confusion, as it is dependent on the unknown key.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	false
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>The S-Box is used to provide confusion, as it is dependent on the unknown key.</p> <p>The P-Box is fixed, and there is no confusion due to it, but it provides diffusion.</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	<p>This is an example of</p>
((OPTION_A)) THIS IS MANDATORY OPTION	SP Networks
((OPTION_B)) THIS IS ALSO MANDATORY	Feistel Cipher

OPTION	
((OPTION_C)) This is optional	Hash Algorithm
((OPTION_D)) This is optional	Hill Cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation
((OPTION_A)) THIS IS MANDATORY OPTION	1 and 3
((OPTION_B)) THIS IS ALSO MANDATORY	2 and 3

OPTION	
((OPTION_C)) This is optional	3 and 4
((OPTION_D)) This is optional	2 and 4
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Increase in any of the above 4 leads to slowing of the cipher algorithm i.e. more computational time will be required.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES follows
((OPTION_A)) THIS IS MANDATORY OPTION	Hash Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY	Caesars Cipher

OPTION	
((OPTION_C)) This is optional	Feistel Cipher Structure
((OPTION_D)) This is optional	SP Network
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES Algorithm Cipher System consists of _____ rounds (iterations) each with a round key
((OPTION_A)) THIS IS MANDATORY OPTION	12
((OPTION_B)) THIS IS ALSO MANDATORY	18

OPTION	
((OPTION_C)) This is optional	9
((OPTION_D)) This is optional	16
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES algorithm has a key length of
((OPTION_A)) THIS IS MANDATORY OPTION	128 Bits
((OPTION_B)) THIS IS ALSO MANDATORY	32 Bits

OPTION	
((OPTION_C)) This is optional	64 Bits
((OPTION_D)) This is optional	16 Bits
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	56 bits are used, the rest 8 bits are parity bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the round key is _____ bit and the Round Input is _____ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	48, 32
((OPTION_B)) THIS IS ALSO MANDATORY	64,32

OPTION	
((OPTION_C)) This is optional	56, 24
((OPTION_D)) This is optional	32, 32
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The round key is 48 bits. The input is 32 bits

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____
((OPTION_A)) THIS IS MANDATORY OPTION	Scaling of the existing bits
((OPTION_B)) THIS IS ALSO MANDATORY	Duplication of the existing bits

<b>OPTION</b>	
((OPTION_C)) This is optional	Addition of zeros
((OPTION_D)) This is optional	Addition of ones
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits (permutation plus an expansion), that involves duplication of 16 of the bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The Initial Permutation table/matrix is of size
((OPTION_A)) THIS IS MANDATORY OPTION	16x8
((OPTION_B)) THIS IS ALSO MANDATORY	12x8

OPTION	
((OPTION_C)) This is optional	8x8
((OPTION_D)) This is optional	4x8
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	There are 64 bits to permute and this requires a 8x8 matrix.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The number of unique substitution boxes in DES after the 48 bit XOR operation are
((OPTION_A)) THIS IS MANDATORY OPTION	8
((OPTION_B)) THIS IS ALSO MANDATORY	4

OPTION	
((OPTION_C)) This is optional	6
((OPTION_D)) This is optional	12
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	IP-1 is the first step and the last step is IP during decryption.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A preferable cryptographic algorithm should have a good avalanche effect.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Thus statement is true as a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the size(in bits) of the key in the SDES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	24
((OPTION_B)) THIS IS ALSO MANDATORY	16

OPTION	
((OPTION_C)) This is optional	20
((OPTION_D)) This is optional	10
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The size of the key in the SDES algorithm is 10 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	GCD(a,b) is the same as GCD( a , b ).
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is true. $\gcd(60,24) = \gcd(60,-24) = 12$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	882
((OPTION_B)) THIS IS ALSO MANDATORY	770

OPTION	
((OPTION_C)) This is optional	1078
((OPTION_D)) This is optional	1225
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	$\text{GCD}(1160718174, 316258250) = 1078$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	$\text{GCD}(102947526, 239821932) = 6.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	13
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	17
((OPTION_D)) This is optional	7
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	$\text{GCD}(8376238, 1921023) = 13.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 1234 mod 4321 is
((OPTION_A)) THIS IS MANDATORY OPTION	3239
((OPTION_B)) THIS IS ALSO MANDATORY	3213

OPTION	
((OPTION_C)) This is optional	3242
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The multiplicative Inverse of 1234 mod 4321 is 3239.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 550 mod 1769 is
((OPTION_A)) THIS IS MANDATORY OPTION	434
((OPTION_B)) THIS IS ALSO MANDATORY	224

OPTION	
((OPTION_C)) This is optional	550
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The multiplicative Inverse of 550 mod 1769 is 550.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	<p><b>You are supposed to use hill cipher for encryption technique. You are provided with the following matrix,</b></p> $A = \begin{bmatrix} 4 & 2 \\ 2 & 1 \end{bmatrix}$ <p><b>Is the given matrix 'A', a valid key to be used for encryption?</b></p>
((OPTION_A)) THIS IS MANDATORY OPTION	Yes
((OPTION_B))	No

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Can't be determined
((OPTION_D)) This is optional	Data insufficient
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>For choosing any square matrix as a key, it should be taken care that the matrix is invertible, i.e. its inverse must exist.</p> <p>Here, in this case,</p> $  A   = 0$ <p>Therefore, it means that 'A' is not an invertible matrix. Hence matrix 'A' cannot be chosen as a key matrix for encryption in the <a href="#">Hill cipher</a>.</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	The input text is divided into two parts: one being left half and another one being right half.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Swapping of the left and right halves are performed after each round.
((OPTION_C)) This is optional	The plain text is converted into a matrix form first
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The fiestal structure does not require the conversion of the plain text into matrix form at any of its steps.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Among the following given options, chose the strongest encryption technique

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	DES ( Data Encryption Standard))
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Double DES
((OPTION_C)) This is optional	Triple DES
((OPTION_D)) This is optional	AES (Advance Encryption Standard)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	It has been proved that the AES performs much better than the all the other DES, whether it be single DES or series of DES.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	<p><b>Consider the following steps,</b></p> <ul style="list-style-type: none"> <li>i. Substitution bytes</li> <li>ii. Shift Rows</li> </ul>

IMAGES ALSO	<p>iii. Mix columns iv. Add round key</p> <p><b>The above steps are performed in each round of which of the following ciphers?</b></p>
((OPTION_A))  THIS IS MANDATORY OPTION	Rail fence cipher
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Data Encryption Standard (DES)
((OPTION_C))  This is optional	Advance Encryption Standard (AES)
((OPTION_D))  This is optional	None of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2)	1
--	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ algorithm transforms ciphertext to plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _____ cipher replaces one character with another character.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ cipher reorders the plaintext characters to create a ciphertext.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
((OPTION_A)) THIS IS MANDATORY OPTION	man-in-the-middle
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ciphertext attack
((OPTION_C)) This is optional	plaintext attack
((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the receiver uses the _____ key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either a or b
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES is a(n) _____ method adopted by the U.S. government.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	either (a) or (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ECB and CBC are _____ ciphers.
((OPTION_A))  THIS IS MANDATORY OPTION	block
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	stream
((OPTION_C))  This is optional	field
((OPTION_D))  This is optional	none of the above
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ cipher, the same key is used by both the sender and receiver.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the sender uses the_____key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a(n) _____ cipher, a pair of keys is used.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	2
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	AES uses a _____ bit block size and a key size of _____ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	128; 128 or 256
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64; 128 or 192
((OPTION_C)) This is optional	256; 128, 192, or 256
((OPTION_D)) This is optional	128; 128, 192, or 256
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	It uses a 128-bit block size and a key size of 128, 192, or 256 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1
---	---

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Like DES, AES also uses Feistel Structure.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES does not use a Feistel structure. Instead, each full round consists of four separate functions: -byte substitution -Permutation -arithmetic operations over a finite field, and -XOR with a key.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The 4x4 byte matrices in the AES algorithm are called
((OPTION_A)) THIS IS MANDATORY OPTION	States
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Words
((OPTION_C)) This is optional	Transitions
((OPTION_D)) This is optional	Permutations
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is a type of substitution cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	poly alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition cipher
((OPTION_C)) This is optional	Columnar cipher
((OPTION_D)) This is optional	Rail fence cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In substitution cipher the plain text is replaced by cipher text according to a fixed rule. There are two types of substitution cipher- Mono alphabetic and Poly alphabetic cipher.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following correctly defines poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	a substitution based cipher which uses multiple substitution at different positions
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a substitution based cipher which uses fixed substitution over entire message
((OPTION_C)) This is optional	a transposition based cipher which uses multiple substitution at different positions
((OPTION_D)) This is optional	A transposition based cipher which uses fixed substitution over entire message
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Poly alphabetic cipher is a type of substitution cipher. It uses multiple substitution at different positions in order to cipher the plain text.

((MARKS)) QUESTION IS OF	1
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a type of poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Rotor cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hill cipher
((OPTION_C)) This is optional	One time pad cipher
((OPTION_D)) This is optional	Affine cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	In poly alphabetic cipher each symbol of plain text is replaced by a different cipher text regardless of its occurrence. Out of the given options, only affine cipher is not a poly alphabetic cipher.

((MARKS)) QUESTION IS OF	2
-----------------------------	---

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	We are provided the plain text "SUN". You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2?
((OPTION_A)) THIS IS MANDATORY OPTION	UWP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	NUS
((OPTION_C)) This is optional	WUP
((OPTION_D)) This is optional	QSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<p>In the Caesar cipher technique, the encryption is performed as follows,</p> $E(P, K) = (P + K) \text{ mod } 26$ <p>Therefore,</p> $E(S, 2) = (18 + 2) \text{ mod } 26 = 20 = U$ $E(U, 2) = (20 + 2) \text{ mod } 26 = 22 = W$ $E(N, 2) = (13 + 2) \text{ mod } 26 = 15 = P$ <p>Hence, the ciphertext is "UWP".</p>

--	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?
((OPTION_A)) THIS IS MANDATORY OPTION	<u>Hill Cipher</u>
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	<u>Playfair cipher</u>
((OPTION_C)) This is optional	Both a and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also	The hill cipher includes a square matrix as the key, and in Playfair cipher, we create a 5X5 matrix using the given key string. Hence,

optional	both these ciphers include the use of matrices.
----------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Playfair cipher is an example of _____
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C)) This is optional	transposition cipher
((OPTION_D)) This is optional	additive cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	Playfair cipher is a substitution cipher. It falls under the category of poly alphabetic cipher as it uses multiple substitution at different positions in order to cipher the plain text.
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Encryption in Playfair cipher is done using _
((OPTION_A)) THIS IS MANDATORY OPTION	a 5x5 table
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a 13x2 table
((OPTION_C)) This is optional	vigenere table
((OPTION_D)) This is optional	a 6x6 table
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A

((EXPLANATION)) This is also optional	
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the plain text corresponding to cipher text "BPKYFS" if playfair cipher is used with keyword as "SECRET" (assuming j is combined with i)?
((OPTION_A))  THIS IS MANDATORY OPTION	INDIAN
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	WORLD
((OPTION_C))  This is optional	DOLLAR
((OPTION_D))  This is optional	HELLO
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C

((EXPLANATION)) This is also optional	To decrypt the message we follow the reverse procedure. The table is formed in the same manner. Applying this we get the plain text to be "DOLLAR".
---------------------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair are identical?
((OPTION_A)) THIS IS MANDATORY OPTION	then that pair is neglected
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a null(or x) is added in between the letters
((OPTION_C)) This is optional	one of the identical letter is replaced by some other letter
((OPTION_D)) This is optional	then both of the letters are replaced by the letter appearing just next in the row
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	In playfair cipher if the letters in a pair are identical then a null is added in between the letters. Any letter can be used as a null as long as that letter is not the one being repeated.
---------------------------------------	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same row?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter at the corner of the row
((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	If the letters in a pair appear in same row then they are replaced by the letters appearing immediately right to them respectively. If the element to be replaced appears at the corner of the row then we wrap around to the left side of that row.
---------------------------------------	--

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the ciphered text if the string “SANFOUNDRY” is given as input to the code of playfair cipher with keyword as “SECRET” (assuming j is combined with i)?
((OPTION_A)) THIS IS MANDATORY OPTION	ZHQAPNPAFR
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AHQAPNPAFR
((OPTION_C)) This is optional	HAQAPNPAFR
((OPTION_D)) This is optional	QHAAPNPAFR
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	B

E	
((EXPLANATION)) This is also optional	<p>For encrypting the plain text using playfair cipher we use a <math>5 \times 5</math> table that is constructed by using keyword. Then we apply rules for encryption in order to get the ciphered text. Table is given as under-</p> <p>S E C R T</p> <p>A B D F G</p> <p>H I K L M</p> <p>N O P Q U</p> <p>V W X Y Z</p>

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letters at the corner of the row
((OPTION_D))	that pair is neglected

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	If the letters in a pair appear in the same column then they are replaced by the letters appearing immediately below them respectively. If the element to be replaced appears at the corner of the column then we wrap around to the top side of that column.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair does not appear in same row or column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter of the same row at the corner of the rectangle defined by the original pair respectively

((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	If the letters in a pair does not appear in same row or column then they are replaced by the letters of the same row at the corner of the rectangle defined by the original pair respectively. The order of letters should be maintained.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Columnar cipher falls under the category of?
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C))	additive cipher

This is optional	
((OPTION_D)) This is optional	Transposition cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH_OICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Columnar cipher is a transposition cipher. It falls under the category of transposition cipher as it encrypts the plain text by rearranging its letters.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following ciphered text would have NOT used transposition cipher for encryption of the plain text "CIPHER"?
((OPTION_A)) THIS IS MANDATORY OPTION	EPIHRC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	EHIPCR
((OPTION_C))	DTIPRC

This is optional	
((OPTION_D))	HRIPEC
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	We know that transposition cipher encrypts the plain text by shuffling the letters of the plain text. So out of the given options, only “DTIPRC” does not have the same set of letters as “CIPHER”.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many columns do we need to have in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	4
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	5
((OPTION_C))	6

This is optional	
((OPTION_D))	7
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So in this case it will be equal to 6.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the encrypted text corresponding to plain text “CLASSIFIED” using columnar transposition cipher with a keyword as “GAMES”?
((OPTION_A)) THIS IS MANDATORY OPTION	LFDSIASECI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SECIAISDFL
((OPTION_C))	CILFAISESD

This is optional																					
((OPTION_D))	IFSECIAISD																				
This is optional																					
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option																					
((CORRECT_CH OICE)) Either A or B or C or D or E	D																				
((EXPLANATION )) This is also optional	<p>For encrypting using columnar cipher we have to arrange the letters of the plain text in a table which has the same number of columns as the letters of the keyword. Then the letters of the keyword are arranged in alphabetical order and we read along each column.</p> <table style="margin-left: auto; margin-right: auto;"> <tr><td>3</td><td>1</td><td>4</td><td>2</td><td>5</td></tr> <tr><td>G</td><td>A</td><td>M</td><td>E</td><td>S</td></tr> <tr><td>C</td><td>L</td><td>A</td><td>S</td><td>S</td></tr> <tr><td>I</td><td>F</td><td>I</td><td>E</td><td>D</td></tr> </table> <p>So the ciphered text will be “IFSECIAISD”.</p>	3	1	4	2	5	G	A	M	E	S	C	L	A	S	S	I	F	I	E	D
3	1	4	2	5																	
G	A	M	E	S																	
C	L	A	S	S																	
I	F	I	E	D																	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many rows will the letters of the plain text occupy in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B))	2

THIS IS ALSO MANDATORY OPTION																			
((OPTION_C)) This is optional	3																		
((OPTION_D)) This is optional	4																		
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option																			
((CORRECT_CHOICE)) Either A or B or C or D or E	B																		
((EXPLANATION)) This is also optional	<p>Explanation: The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So when we will write the letters of the plain text row wise then there will be 2 rows of plain text in this case. The table is shown below :-</p> <table> <tr> <td>S</td> <td>E</td> <td>C</td> <td>R</td> <td>E</td> <td>T</td> </tr> <tr> <td>1</td> <td>S</td> <td>A</td> <td>N</td> <td>F</td> <td>O</td> <td>U</td> </tr> <tr> <td>2</td> <td>N</td> <td>D</td> <td>R</td> <td>Y</td> </tr> </table>	S	E	C	R	E	T	1	S	A	N	F	O	U	2	N	D	R	Y
S	E	C	R	E	T														
1	S	A	N	F	O	U													
2	N	D	R	Y															

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following statement is not true regarding columnar transposition cipher?
((OPTION_A)) THIS IS	probability of error is high while deciphering

<b>MANDATORY OPTION</b>	
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	it cannot be combined with other ciphers
((OPTION_C))  This is optional	it is a traditional symmetric cipher
((OPTION_D))  This is optional	it is a weak cipher
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Although columnar transposition cipher is a weak cipher in itself. But it can be combined with other substitution ciphers so as to improve its security. The probability of error remains high while decoding columnar cipher as it is a lengthy process

<b>((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)</b>	1
<b>((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</b>	_____ is another data hiding technique which can be used in conjunction with cryptography for the extra-secure method of protecting data.
<b>((OPTION_A))</b>	Cryptography

THIS IS MANDATORY OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Steganography
((OPTION_C)) This is optional	Tomography
((OPTION_D)) This is optional	Chorography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Steganography is the technique of hiding data in another raw data. Steganography is another data hiding technique which can be used in conjunction with cryptography for an extra-secure method of protecting data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((OPTION_A))  THIS IS MANDATORY OPTION	Cryptography
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C))  This is optional	Steganography
((OPTION_D))  This is optional	Chorography
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Steganography helps in hiding any form of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _____ tool permits security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((OPTION_A))  THIS IS MANDATORY OPTION	Cryptography
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C))  This is optional	Chorography
((OPTION_D))  This is optional	Steganography
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	A steganography tool is a software tool that permits a security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((MARKS))  QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The main motive for using steganography is that hackers or other users can hide a secret message behind a _____

((OPTION_A)) THIS IS MANDATORY OPTION	special file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ordinary file
((OPTION_C)) This is optional	program file
((OPTION_D)) This is optional	encrypted file
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	The main motive for using steganography is that hackers or other users can hide a secret message behind ordinary files. Some steganography tools are SSuite Picsel, rSteg etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	People will normally think it as a normal/regular file and your secret message will pass on without any _____

((OPTION_A)) THIS IS MANDATORY OPTION	Suspicion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	cracking
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Steganography techniques help hackers or other users to conceal covert message behind regular files. People will normally think it as a normal/regular file and your secret message will pass on without any suspicion.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	By using _____ you can diminish the chance of data leakage

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C)) This is optional	Chorography
((OPTION_D)) This is optional	Steganography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Hackers or other cyber criminals target ordinary files to hide different data or information within another data file. By using steganography, you can diminish the chance of data leakage.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Which of the following is a mode of operation for the Block ciphers in cryptography?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Electronic Code Book (ECB)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Cipher Block Chaining (CBC)
((OPTION_C)) This is optional	Counter (CTR) mode
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	For which of the following should EBC (Electronic Code Book) process not be used for encryption?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	For large block sizes
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	For fixed block sizes
((OPTION_C)) This is optional	For small block sizes
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	It is preferred that the block size in the ECB technique must be greater than 64 bits. If not, the text is padded to make it of the required length. This is due to some particular words and phrases that may be reused again often so that the same repetitive part of ciphertext can emerge as mixed.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	Which of the following is the main disadvantage of the ECB (Electronic Code Book)?

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	It requires large block size
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Padding is done to make the plain text divisible into blocks of fixed size
((OPTION_C)) This is optional	It is prone to cryptanalysis since there is a direct relationship between plain text and cipher text.
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	In <u>ECB</u> , there lies a direct relation between the plain text and the ciphertext. Therefore, it is easy for an outsider to break the encryption logic and steal the data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options is not correct according to the definition of the Cipher Block Chaining (CBC)?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC is a mode of operation for stream ciphers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Initialization vector (IV) is used in CBC in the initial phase.
((OPTION_C)) This is optional	It has better resistive nature towards cryptanalysis than ECB
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	<a href="#">CBC</a> which stands for Cipher Block chaining is a mode of operation for block ciphers and not for stream ciphers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following modes of operations can be followed for both stream ciphers as well as block ciphers?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC (Cipher Block Chaining)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ECB (Electronic Code Book)
((OPTION_C)) This is optional	CFB (Cipher text Feed Back)
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	<b>CFB</b> is primarily a mode to derive some characteristics of a stream cipher from a block cipher on the cryptography in cryptoanalysis.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
--	---

<p>((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</p>	<p>All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES?</p> <ul style="list-style-type: none"> <li>i. Substitution bytes</li> <li>ii. Shift rows</li> <li>iii. Mix columns</li> <li>iv. Add round key</li> </ul>
<p>((OPTION_A)) THIS IS MANDATORY OPTION</p>	<p>i</p>
<p>((OPTION_B)) THIS IS ALSO MANDATORY OPTION</p>	<p>iii</p>
<p>((OPTION_C)) This is optional</p>	<p>All of the mentioned</p>
<p>((OPTION_D)) This is optional</p>	<p>None of the mentioned</p>
<p>((OPTION_E)) This is optional. If optional keep empty so that system will skip this option</p>	
<p>((CORRECT_CHOICE)) Either A or B or C or D or E</p>	<p>B</p>
<p>((EXPLANATION)) This is also optional</p>	<p>In the AES algorithm, the MIX COLUMN operation is performed in all the rounds except the final round of the algorithm.</p>

<p>((MARKS))</p>	<p>1</p>
------------------	----------

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"The number of rounds in the AES algorithm depends upon the key size being used." Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	128 key size: 10 rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	192 key size: 12 rounds
((OPTION_C)) This is optional	256 key size: 14 rounds
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS))	2
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Avalanche effect
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Completeness
((OPTION_C)) This is optional	Both a. and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS))	2
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For the AES-128 algorithm there are _____ similar rounds and _____ round is different.
((OPTION_A)) THIS IS MANDATORY OPTION	2 pair of 5 similar rounds ; every alternate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	9 ; the last
((OPTION_C)) This is optional	8 ; the first and last
((OPTION_D)) This is optional	10 ; no
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS))	1
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the 4 operations are false for each round in the AES algorithm? i) Substitute Bytes ii) Shift Columns iii) Mix Rows iv) XOR Key
((OPTION_A)) THIS IS MANDATORY OPTION	i) only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii) iii) and iv)
((OPTION_C)) This is optional	ii) and iii)
((OPTION_D)) This is optional	only iv
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES rounds involve substitute bytes, shift rows, mix columns and addition of round key.

((MARKS))	1
-----------	---

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	There is an addition of round key before the start of the AES round algorithms.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In AES the final round contains only three transformations, and there is an initial single transformation (Add Round Key) before the first round which can be considered Round 0. Each transformation takes 4x4 matrixes as input and produces a 4x4 matrix as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1																
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the Shifted Row transformation for the matrix bellow?  <table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>6B</td><td>77</td><td>A4</td><td>6B</td></tr> <tr> <td>AD</td><td>01</td><td>F0</td><td>63</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	FE	72	2B	D7	6B	77	A4	6B	AD	01	F0	63	30	D7	AF	FE
FE	72	2B	D7														
6B	77	A4	6B														
AD	01	F0	63														
30	D7	AF	FE														
((OPTION_A))  THIS IS MANDATORY OPTION	<table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>6B</td><td>77</td><td>A4</td><td>6B</td></tr> <tr> <td>AD</td><td>01</td><td>F0</td><td>63</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	FE	72	2B	D7	6B	77	A4	6B	AD	01	F0	63	30	D7	AF	FE
FE	72	2B	D7														
6B	77	A4	6B														
AD	01	F0	63														
30	D7	AF	FE														
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	<table border="1"> <tr> <td>72</td><td>2B</td><td>D7</td><td>FE</td></tr> <tr> <td>A4</td><td>6B</td><td>6B</td><td>77</td></tr> <tr> <td>63</td><td>AD</td><td>01</td><td>F0</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	72	2B	D7	FE	A4	6B	6B	77	63	AD	01	F0	30	D7	AF	FE
72	2B	D7	FE														
A4	6B	6B	77														
63	AD	01	F0														
30	D7	AF	FE														
((OPTION_C))  This is optional	<table border="1"> <tr> <td>FE</td><td>72</td><td>2B</td><td>D7</td></tr> <tr> <td>77</td><td>A4</td><td>6B</td><td>6B</td></tr> <tr> <td>F0</td><td>63</td><td>AD</td><td>01</td></tr> <tr> <td>FE</td><td>30</td><td>D7</td><td>AF</td></tr> </table>	FE	72	2B	D7	77	A4	6B	6B	F0	63	AD	01	FE	30	D7	AF
FE	72	2B	D7														
77	A4	6B	6B														
F0	63	AD	01														
FE	30	D7	AF														
((OPTION_D))  This is optional	<table border="1"> <tr> <td>D7</td><td>FE</td><td>72</td><td>2B</td></tr> <tr> <td>A4</td><td>6B</td><td>6B</td><td>77</td></tr> <tr> <td>01</td><td>AD</td><td>63</td><td>F0</td></tr> <tr> <td>30</td><td>D7</td><td>AF</td><td>FE</td></tr> </table>	D7	FE	72	2B	A4	6B	6B	77	01	AD	63	F0	30	D7	AF	FE
D7	FE	72	2B														
A4	6B	6B	77														
01	AD	63	F0														
30	D7	AF	FE														

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The Shift Rows transformation consists of: -Not shifting the first row of the state array at all. -Circularly shifting the second row by one byte to the left. -Circularly shifting the third row by two bytes to the left, and -Circularly shifting the last row by three bytes to the left.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not weak key in DES
((OPTION_A)) THIS IS MANDATORY OPTION	0x0101010101010101
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0xEFABFEFEFEFEFEFE
((OPTION_C)) This is optional	0x1F1F1F1F0E0E0E0E
((OPTION_D))	0xFFFFFFFFFFFFFF

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple-DES has _____ keys.
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	2
((OPTION_C)) This is optional	5
((OPTION_D))	4

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a encryption technique which uses two instance of DES on same plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	Double DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tripple DES
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ attack which can be used to break through double DES.
((OPTION_A)) THIS IS MANDATORY OPTION	Brute force
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	meet-in-the middle
((OPTION_C)) This is optional	Timing
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple DES involve __
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption, Decryption, Decryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption ,Encryption, Encryption
((OPTION_C)) This is optional	Decryption ,Encryption, Decryption
((OPTION_D))	Encryption, Decryption, Encryption

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ involves feeding the successive output blocks from the underlying block cipher back to it
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	OFB
((OPTION_D))	CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is counter-based version of CFB mode without the feedback
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	counter
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below mode is independent of previous output
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	CFB
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Errors get propagated in all modes except ___and ___
((OPTION_A)) THIS IS MANDATORY OPTION	ECB,COUNTER
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC,COUNTER
((OPTION_C)) This is optional	CFB,COUNTER
((OPTION_D))	OFB,CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Patterns are not preserved in ___ mode
((OPTION_A)) THIS IS MANDATORY OPTION	CBC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CFB
((OPTION_C)) This is optional	Both CBC and CFB
((OPTION_D))	ECB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A small change in plaintext results in the very great change in the cipher text indicates which characteristic
((OPTION_A)) THIS IS MANDATORY OPTION	completeness
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Strong key
((OPTION_C)) This is optional	Avalanche effect
((OPTION_D))	All of the above

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _____ ciphers, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of cipher text.
((OPTION_A)) THIS IS MANDATORY OPTION	Block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Stream
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	More number of _____ provide more secure system in feistel cipher.
((OPTION_A)) THIS IS MANDATORY OPTION	rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	keys
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	Function
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes..

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In public key cryptosystem _____ keys are used for encryption and decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	Same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Different
((OPTION_C)) This is optional	Encryption Keys
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	In conventional cryptosystem, same keys are used for encryption and decryption where as in public key cryptosystem different keys are used.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In public key cryptosystem which is kept as public?
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption keys
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption keys
((OPTION_C)) This is optional	Encryption & Decryption keys
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	In public key cryptosystem, the encryption keys are kept as public where as decryption keys are kept as secret.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Public key cryptosystem uses same key for both encryption and decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which should be kept as a secret in public key cryptosystem?
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption key
((OPTION_C)) This is optional	Encryption & Decryption key
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	In public key cryptosystem, Encryption is done using public key . decryption key needs to be kept as a secret.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Euler's totient function is determined by
((OPTION_A)) THIS IS MANDATORY OPTION	$pq$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(p-1)(q-1)$
((OPTION_C)) This is optional	$(p+1)(q+1)$
((OPTION_D)) This is optional	$p/q$
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	The Euler's totient function is determined by $(p-1)(q-1)$ , where p and q are kept hidden.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?
((OPTION_A))  THIS IS MANDATORY OPTION	p and q should be divisible by $\Phi(n)$
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	p and q should be co-prime
((OPTION_C))  This is optional	p and q should be prime
((OPTION_D))  This is optional	p/q should give no remainder
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	'p' and 'q' should have large random values which are both prime numbers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, $\Phi(n) = \text{_____}$ in terms of p and q.
((OPTION_A)) THIS IS MANDATORY OPTION	(p)/(q)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	(p)(q)
((OPTION_C)) This is optional	(p-1)(q-1)
((OPTION_D)) This is optional	(p+1)(q+1)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	$\Phi(n) = (p-1)(q-1).$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, we select a value 'e' such that it lies between 0 and $\Phi(n)$ and it is relatively prime to $\Phi(n)$ .
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	$\gcd(e, \Phi(n))=1$ ; and $1 < e < \Phi(n)$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 19$ and choose $e=17$ . Apply RSA algorithm where message=5 and find the cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	C=80
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	C=92
((OPTION_C)) This is optional	C=56
((OPTION_D)) This is optional	C=23
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 209.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 19$ and choose $d=17$ . Apply RSA algorithm where Cipher message=80 and thus find the plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	54
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	43
((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	24
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	$n = pq = 11 \times 19 = 209$ . $C=M^e \text{ mod } n ; C=5^{17} \text{ mod } 209 ; C = 80 \text{ mod } 209$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	$n = 35; e = 5; C = 10$ . What is the plaintext (use RSA) ?
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	7
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	Use RSA system to decrypt and get PT = 5.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 17$ and choose $e=7$ . Apply RSA algorithm where PT message=88 and thus find the CT.
((OPTION_A)) THIS IS MANDATORY OPTION	23
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64
((OPTION_C)) This is optional	11
((OPTION_D)) This is optional	54
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 187$ . $C=M^e \text{ mod } n ; C=88^7 \text{ mod } 187 ; C = 11 \text{ mod } 187$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 17$ and choose $e=7$ . Apply RSA algorithm where Cipher message=11 and thus find the plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	88
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	122
((OPTION_C)) This is optional	143
((OPTION_D)) This is optional	111
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	$n = pq = 11 \times 19 = 187$ . $C=M^e \text{ mod } n ; C=11^{23} \text{ mod } 187 ; C = 88 \text{ mod } 187$ .

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an RSA system the public key of a given user is $e = 31$ , $n = 3599$ . What is the private key of this user?
((OPTION_A))  THIS IS MANDATORY OPTION	3031
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	2412
((OPTION_C))  This is optional	2432
((OPTION_D))  This is optional	1023
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	By trial and error, we determine that $p = 59$ and $q = 61$ . Hence $f(n) = 58 \times 60 = 3480$ . Then, using the extended Euclidean algorithm, we find that the multiplicative inverse of 31 modulo $f(n)$ is 3031

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Compute private key (d, p, q) given public key (e=23, n=233 ´ 241=56,153).
((OPTION_A)) THIS IS MANDATORY OPTION	35212
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	12543
((OPTION_C)) This is optional	19367
((OPTION_D)) This is optional	32432
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Since n=233 ´ 241=56,153, p=233 and q=241 $f(n) = (p - 1)(q - 1) = 55,680$ Using Extended Euclidean algorithm, we obtain $d = 23^{-1} \text{ mod } 55680 = 19,367.$

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a RSA cryptosystem a particular A uses two prime numbers $p = 13$ and $q = 17$ to generate her public and private keys. If the public key of A is 35. Then the private key of A is _____.
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	13
((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	17
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In an RSA cryptosystem, for public key: $\text{GCD}(\phi(n), e) = 1$ And, for private key:

	$(e * d) \bmod \phi(n) = 1$ Where, $\phi(n) = (p - 1)*(q - 1) = (13 - 1)(17 - 1) = 12 * 16 = 192$ Such that $1 < e, d < \phi(n)$ Therefore, the private key is: $(35 * d) \bmod \phi(n) = 1$ $d = 11$
--	---

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the RSA public key cryptosystem, which one of the following numbers will always be largest?
((OPTION_A)) THIS IS MANDATORY OPTION	E
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	N
((OPTION_C)) This is optional	P
((OPTION_D)) This is optional	Q
((OPTION_E)) This is optional. If optional keep empty so that system will skip	

this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	The number n is generated as the product of the two large prime numbers p and q. Therefore, n must always be greater than both p and q. Furthermore, it is an algorithm constraint that e must be chosen such that e is smaller than n. Therefore, in RSA cryptography n is always the largest of the four variables shown in the options to this question.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If Richard wants to send an encrypted message to Sue using a public key cryptosystem, which key does he use to encrypt the message?
((OPTION_A)) THIS IS MANDATORY OPTION	Richard's public key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Richard's private key
((OPTION_C)) This is optional	Sue's public key
((OPTION_D)) This is optional	Sue's private key
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Richard must encrypt the message using Sue's public key so that Sue can decrypt it using her private key. If he encrypted the message with his own public key, the recipient would need to know Richard's private key to decrypt the message. If he encrypted it with his own private key, any user could decrypt the message using Richard's freely available public key. Richard could not encrypt the message using Sue's private key because he does not have access to it. If he did, any user could decrypt it using Sue's freely available public key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Acme Widgets currently uses a 1,024-bit RSA encryption standard companywide. The company plans to convert from RSA to an elliptic curve cryptosystem. If it wishes to maintain the same cryptographic strength, what ECC key length should it use?
((OPTION_A)) THIS IS MANDATORY OPTION	160 bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	512 bits
((OPTION_C)) This is optional	1,024 bits
((OPTION_D)) This is optional	2,048 bits

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The elliptic curve cryptosystem requires significantly shorter keys to achieve encryption that would be the same strength as encryption achieved with the RSA encryption algorithm. A 1,024-bit RSA key is cryptographically equivalent to a 160-bit elliptic curve cryptosystem key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Richard received an encrypted message sent to him from Sue. Which key should he use to decrypt the message?
((OPTION_A)) THIS IS MANDATORY OPTION	Richard's public key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Richard's private key
((OPTION_C)) This is optional	Sue's public key
((OPTION_D)) This is optional	Sue's private key

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Sue would have encrypted the message using Richard's public key. Therefore, Richard needs to use the complementary key in the key pair, his private key, to decrypt the message.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	One commonly used public-key cryptography method is the _____ algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	RSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RAS
((OPTION_C)) This is optional	RSA
((OPTION_D)) This is optional	RAA

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
((OPTION_A)) THIS IS MANDATORY OPTION	man-in-the-middle
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ciphertext attack
((OPTION_C)) This is optional	plaintext attack
((OPTION_D)) This is optional	none of the above

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the objective of Diffie-Hellman key exchange?
((OPTION_A)) THIS IS MANDATORY OPTION	To protect encrypted data from man-in-the-middle attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	To perform mutual authentication on both sides
((OPTION_C)) This is optional	To prove to another party that one holds a secret key without revealing it
((OPTION_D)) This is optional	To establish a shared secret key on both sides

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The security of RSA encryption relies on which assumption?
((OPTION_A)) THIS IS MANDATORY OPTION	It is computationally infeasible to compute a GCD of two large numbers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	It is computationally infeasible to factor a large number.
((OPTION_C)) This is optional	It is computationally infeasible to test whether a large number is prime.
((OPTION_D)) This is optional	It is computationally infeasible to compute a square modulo n.

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	All of the above
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is asymmetric cryptography?
((OPTION_A)) THIS IS MANDATORY OPTION	ECC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	Both ECC and RSA
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below requires less hardware capacity because of less key size
((OPTION_A)) THIS IS MANDATORY OPTION	ECC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	DES
((OPTION_D)) This is optional	AES

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Diffie Hellman is _____
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption algorithm
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	D-H is key exchange algorithm

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Timing attack on RSA can be avoided by __
((OPTION_A)) THIS IS MANDATORY OPTION	Padding extra bits in message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Adding delays
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below algorithm is used in cryptocurrency?
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AES
((OPTION_C)) This is optional	ECC
((OPTION_D)) This is optional	None of these

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When a hash function is used to provide message authentication, the hash function value is called to as:
((OPTION_A)) THIS IS MANDATORY OPTION	Message Field
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Message Digest
((OPTION_C)) This is optional	Message Score
((OPTION_D)) This is optional	Message Leap

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	We know that the hash function providing message authentication is referred to as message digest in cryptography.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following are used to create a message digest  a. RSA b. SHA-1 c. DES d. MD5
((OPTION_A)) THIS IS MANDATORY OPTION	A&B
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	B&C
((OPTION_C)) This is optional	A&C

((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	They are Message digest algorithm

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the output of a cryptographic hash function?
((OPTION_A)) THIS IS MANDATORY OPTION	A variable set of bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A fixed set of bits, derived from one-way mathematical operations
((OPTION_C)) This is optional	An output which may be easily discovered by an adversary

((OPTION_D)) This is optional	Outputs of such functions are of no importance
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message digest algorithms are primarily used to provide _____
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Authentication
((OPTION_C)) This is optional	inegrity

((OPTION_D)) This is optional	authorization
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is a message digest algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IDEA
((OPTION_C)) This is optional	MD5

((OPTION_D)) This is optional	RSA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message _____ means that the data must arrive at the receiver exactly as sent.
((OPTION_A)) THIS IS MANDATORY OPTION	confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	integrity
((OPTION_C)) This is optional	authentication

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
((OPTION_A)) THIS IS MANDATORY OPTION	confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	integrity
((OPTION_C)) This is optional	authentication

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ function creates a message digest out of a message
((OPTION_A)) THIS IS MANDATORY OPTION	encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	hash

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ is a trusted third party that assigns a symmetric key to two parties.
((OPTION_A)) THIS IS MANDATORY OPTION	Public directory
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Certificate authority
((OPTION_C)) This is optional	Both

((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature provides _____.
((OPTION_A)) THIS IS MANDATORY OPTION	authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nonrepudiation
((OPTION_C)) This is optional	both (a) and (b)

((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A digital signature needs a(n) _____ system
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)

((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ is a federal or state organization that binds a public key to an entity and issues a certificate.
((OPTION_A)) THIS IS MANDATORY OPTION	KDC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Kerberos
((OPTION_C)) This is optional	CA

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	means that a sender must not be able to deny sending a message that he sent.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication

((OPTION_D)) This is optional	Nonrepudiation
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Kerberos is a popular session key creator protocol that requires an authentication server and a ticket-granting server.
((OPTION_A)) THIS IS MANDATORY OPTION	KDC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Kerberos
((OPTION_C)) This is optional	CA

((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The MD5 is a message digest algorithm developed by
((OPTION_A)) THIS IS MANDATORY OPTION	Ron Rivest.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	WhiteField Diffie.
((OPTION_C)) This is optional	Martin Hellman.

((OPTION_D)) This is optional	Diffie-Hellman.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 is quite fast and produces _____ message digests
((OPTION_A)) THIS IS MANDATORY OPTION	512 bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	1024 bits
((OPTION_C)) This is optional	128 bits

((OPTION_D)) This is optional	64 bits
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The first step of MD5 is
((OPTION_A)) THIS IS MANDATORY OPTION	add padding bits to original messsge
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	adding append length bits
((OPTION_C)) This is optional	divide the input into 512 bit blocks

((OPTION_D)) This is optional	compression
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In MD5, the process block divides the 512 bits into _____ sub blocks.
((OPTION_A)) THIS IS MANDATORY OPTION	16
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	24
((OPTION_C)) This is optional	32

((OPTION_D)) This is optional	84
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which financial institutions have a relationship with merchants for processing payment card authorizations and payments?
((OPTION_A)) THIS IS MANDATORY OPTION	Issuer
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Acquirer
((OPTION_C)) This is optional	Merchant

((OPTION_D)) This is optional	Dealer
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following contains the order information such as which items are being purchased?
((OPTION_A)) THIS IS MANDATORY OPTION	PI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	OI
((OPTION_C)) This is optional	MD

((OPTION_D)) This is optional	DS
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Payment information can be encrypted by using _____.
((OPTION_A)) THIS IS MANDATORY OPTION	customer's private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	merchant public key
((OPTION_C)) This is optional	one-time session key.

((OPTION_D)) This is optional	customer's public key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature envelope is decrypted by using _____.
((OPTION_A)) THIS IS MANDATORY OPTION	merchant private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	payment's private key
((OPTION_C)) This is optional	payment public key

((OPTION_D)) This is optional	merchant's public key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ will ensure the merchant and their payment information
((OPTION_A)) THIS IS MANDATORY OPTION	Digital certificate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Merchant
((OPTION_C)) This is optional	Dual signature

((OPTION_D)) This is optional	Certificate authority
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SET provides an authentication with the help of _____
((OPTION_A)) THIS IS MANDATORY OPTION	dual signature
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	digital certificate
((OPTION_C)) This is optional	payment's public key

((OPTION_D)) This is optional	payment's private key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ are very crucial for success of RSA algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	Integers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Prime numbers
((OPTION_C)) This is optional	Negative number

((OPTION_D)) This is optional	Fraction
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ acts as financial institutions who provides a payment card to a card holder
((OPTION_A)) THIS IS MANDATORY OPTION	payment gateway
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	card holder
((OPTION_C)) This is optional	acquirer

((OPTION_D)) This is optional	issuer
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	ISSUER means Bank

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Who will be responsible for processing the payment from the customer's account to the merchant account?
((OPTION_A)) THIS IS MANDATORY OPTION	Acquirer
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Merchant
((OPTION_C)) This is optional	Issuer

((OPTION_D)) This is optional	Payment gateway
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The cardholder combines the PIMD and OIMD and hashes them together to form
((OPTION_A)) THIS IS MANDATORY OPTION	OPMD
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	POMD
((OPTION_C)) This is optional	MD

((OPTION_D)) This is optional	DS
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which process will ensure that the issues of the credit card is an approved transactions?
((OPTION_A)) THIS IS MANDATORY OPTION	Payment capture
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Payment authorization
((OPTION_C)) This is optional	Purchase request

((OPTION_D)) This is optional	Purchase reply
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is used for hiding the payment information from the merchant.
((OPTION_A)) THIS IS MANDATORY OPTION	SET
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	SHTTP

((OPTION_D)) This is optional	TSP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A __word buffer is used to compute the message digest in MD5
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4
((OPTION_C)) This is optional	5

((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	4 WORD A,B,C,D

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In MD5, the message is <b>padded</b> so that its length is divisible by ____
((OPTION_A)) THIS IS MANDATORY OPTION	32
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	128
((OPTION_C)) This is optional	512

((OPTION_D)) This is optional	1024
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 should meet requirements:
((OPTION_A)) THIS IS MANDATORY OPTION	It is impossible to generate two inputs that cannot produce the same hash function
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	It is impossible to generate a message having the same hash value
((OPTION_C)) This is optional	Both of the above

((OPTION_D)) This is optional	None of these
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	MD5 takes an input of ___ size and produces an output if a 128-bit hash value
((OPTION_A)) THIS IS MANDATORY OPTION	Any
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Multiple of 512
((OPTION_C)) This is optional	Multiple of 128

((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following best describes sniffing?
((OPTION_A)) THIS IS MANDATORY OPTION	Gathering packets to locate IP addresses, in order to initiate a session hijacking attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Analyzing packets in order to locate the sequence number to start a session hijack
((OPTION_C)) This is optional	Monitoring TCP sessions in order to initiate a session-hijacking attack

((OPTION_D)) This is optional	Locating a host susceptible to a session-hijack attack
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Sniffing is usually used to locate the sequence number, which is necessary for a session hijack.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The secret key between members needs to be created as a _____ key when two members contact Kerberos system
((OPTION_A)) THIS IS MANDATORY OPTION	Public
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Session
((OPTION_C))	complimentary

This is optional	
((OPTION_D))	None of these
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The main components of Kerberos are:
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Ticket granting server
((OPTION_C))	database

This is optional	
((OPTION_D))	All of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _____ performs the initial authentication and ticket for Ticket Granting Service
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Ticket granting server
((OPTION_C))	Database

This is optional	
((OPTION_D))	Kerberos
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The Authentication Server verifies access right of users in __
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TG server
((OPTION_C))	Database

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ issues the ticket for the Server
((OPTION_A)) THIS IS MANDATORY OPTION	AS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TGS
((OPTION_C))	DB

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Kerberos is primarily used for _____
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C))	confidentiality

This is optional	
((OPTION_D))	authorization
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The KDC encrypts the TGT with a password that only the _____ knows.
((OPTION_A)) THIS IS MANDATORY OPTION	AS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TGS
((OPTION_C))	Server

This is optional	
((OPTION_D))	None of the above
This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	Because no one else needs to be able to see the contents.  It's for the server to keep track of the client

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The essence of Kerberos' system is _____.
((OPTION_A)) THIS IS MANDATORY OPTION	One way authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity

((OPTION_C)) This is optional	Mutual authentication
((OPTION_D)) This is optional	Public authentication
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not an element/field of the X.509 certificates?
((OPTION_A)) THIS IS MANDATORY OPTION	Issuer Name
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Serial Modifier

((OPTION_C)) This is optional	Issuer unique Identifier
((OPTION_D)) This is optional	Signature
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	X.509 certificate recommends which cryptographic algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	DES

((OPTION_C)) This is optional	AES
((OPTION_D)) This is optional	Rabin
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The standard used in digital certificates that defines its structure, fields, and Values is
((OPTION_A)) THIS IS MANDATORY OPTION	Kerberos
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	End to end encryption

((OPTION_C)) This is optional	X.509
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	X.509 Certificates includes
((OPTION_A)) THIS IS MANDATORY OPTION	Version
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	signature algorithm identifier

((OPTION_C)) This is optional	period of validity
((OPTION_D)) This is optional	extension fields
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	All of the above
((CORRECT_CH OICE)) Either A or B or C or D or E	E
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ defines a framework for the provision of authentication services by the X.500 directory
((OPTION_A)) THIS IS MANDATORY OPTION	X.509
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	X.508

((OPTION_C)) This is optional	X.505
((OPTION_D)) This is optional	X.609
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A digital signature is a mathematical technique used to validate the _____ and _____ of a message, software or digital document
((OPTION_A)) THIS IS MANDATORY OPTION	Authenticity, integrity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity, confidentiality

((OPTION_C)) This is optional	Integrity,non-repudiation
((OPTION_D)) This is optional	Authenticity,confidentiality
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature involves ____ and ____
((OPTION_A)) THIS IS MANDATORY OPTION	Signature verification ,validation
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Signature creation,verification

((OPTION_C)) This is optional	Signature creation,deletion
((OPTION_D)) This is optional	Signature validation,modification
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Message digest is computed by applying hash function on the message and then message digest is encrypted using _____ key of sender to form the digital signature.
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public

((OPTION_C)) This is optional	Session
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In digital signature , Receiver decrypts the digital signature using the _____ key of sender
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public

((OPTION_C)) This is optional	Secret
((OPTION_D)) This is optional	Session
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In digital signature, The message digest computed by ___ and the message digest (got by decryption on digital signature) need to be ___ for ensuring integrity
((OPTION_A)) THIS IS MANDATORY OPTION	Receiver,same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Receiver,different

((OPTION_C)) This is optional	Sender,same
((OPTION_D)) This is optional	Sender,different
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.
((OPTION_A)) THIS IS MANDATORY OPTION	Digital certificate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Digital signature

((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature follows _____
((OPTION_A)) THIS IS MANDATORY OPTION	Digital Signature Standard (DSS)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	X.509 standard format

((OPTION_C)) This is optional	Both of the above
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In diffie-hellman algorithm, if Alice and Bob wish to communicate with each other, they first agree between them a large prime number n, and ____ g
((OPTION_A)) THIS IS MANDATORY OPTION	Generator
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Small prime number

((OPTION_C)) This is optional	Natural number
((OPTION_D)) This is optional	Factorial
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm if $X_a$ is private key of user then public key is calculated by ____
((OPTION_A)) THIS IS MANDATORY OPTION	$g^{X_a} \text{ mod } n$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$n^{X_a} \text{ mod } n$

((OPTION_C)) This is optional	$g^n \bmod p$
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm, ____ keys of each other should be known
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Session

((OPTION_C)) This is optional	Public
((OPTION_D)) This is optional	No
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm,shared secret key is calculated by ____
((OPTION_A)) THIS IS MANDATORY OPTION	$(g^a \text{ mod } n)^b \text{ mod } n$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(g^b \text{ mod } n)^a \text{ mod } n$

((OPTION_C)) This is optional	Both of the above
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm, the resulting shared secret will be the ___ every time
((OPTION_A)) THIS IS MANDATORY OPTION	Same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Different

((OPTION_C)) This is optional	Maybe same
((OPTION_D)) This is optional	Can't say
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ the first widely used method of safely developing and exchanging keys over an insecure channel
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSS

((OPTION_C)) This is optional	Diffie Hellman
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4

((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value $q = 17$ and primitive root $= 5$ . If Alice's secret key is 4 and Bob's secret key is 6, what is the shared secret key they exchanged?
((OPTION_A)) THIS IS MANDATORY OPTION	16
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	17

((OPTION_C)) This is optional	18
((OPTION_D)) This is optional	19
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Each round of MD5 consist of ____ operations
((OPTION_A)) THIS IS MANDATORY OPTION	14
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	15

((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	18
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Each buffer of MD5 algorithm is ____ bit long
((OPTION_A))  THIS IS MANDATORY OPTION	32
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	64

((OPTION_C)) This is optional	128
((OPTION_D)) This is optional	512
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	RSA is _____ cryptography
((OPTION_A)) THIS IS MANDATORY OPTION	Asymmetric
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key

((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Value generated by hash function is referred as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Message digest
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hash

((OPTION_C)) This is optional	MAC
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))  ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not service of digital signature
((OPTION_A))  THIS IS MANDATORY OPTION	Authentication to message
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	Data integrity

((OPTION_C)) This is optional	Non-repudiation
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	___ digitally signs this entire information and includes digital signature in the certificate
((OPTION_A)) THIS IS MANDATORY OPTION	CA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	KDC

((OPTION_C)) This is optional	PKI
((OPTION_D)) This is optional	DB
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA ,e is used as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key

((OPTION_C)) This is optional	Euler's totient
((OPTION_D)) This is optional	Session key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, d is referred as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key
((OPTION_C)) This is optional	Totient function
((OPTION_D)) This is optional	Session key
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Collection of protocol designed by IETF
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Operation in Tunnel mode
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec protects information in
((OPTION_A)) THIS IS MANDATORY OPTION	transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec in which mode does not protect IP header
((OPTION_A)) THIS IS MANDATORY OPTION	transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which mode is used when we need host to host protection
((OPTION_A)) THIS IS MANDATORY OPTION	Transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec protects the whole IP packets
((OPTION_A)) THIS IS MANDATORY OPTION	Transport
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tunnel
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSec defines two protocol
((OPTION_A)) THIS IS MANDATORY OPTION	AH, SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PGP, ASP
((OPTION_C)) This is optional	AH, ESP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Authentication at the IP header
((OPTION_A)) THIS IS MANDATORY OPTION	AH
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ECP
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	SSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IT PROVIDES AUTHENTICATION OR ENCRYPTION OR BOTH FOR PACKET AT IP LEVEL
((OPTION_A)) THIS IS MANDATORY OPTION	AH
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ESP
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	SSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IPSEC USES A SET OF SA CALLED
((OPTION_A)) THIS IS MANDATORY OPTION	SAD
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SAB
((OPTION_C)) This is optional	SADB
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Protocol to provide security for inbound and outbound
((OPTION_A)) THIS IS MANDATORY OPTION	SA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CA
((OPTION_C)) This is optional	KDC
((OPTION_D)) This is optional	IKE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE creates SA for
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	PGP
((OPTION_C)) This is optional	IPSec
((OPTION_D)) This is optional	VP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE based on other how many protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Two
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Three
((OPTION_C)) This is optional	Four
((OPTION_D)) This is optional	five
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IKE uses
((OPTION_A)) THIS IS MANDATORY OPTION	OAKLEY
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SKEME
((OPTION_C)) This is optional	ISKAMP
((OPTION_D)) This is optional	ALL ABOVE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Network is used in an organization
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Semi private
((OPTION_D)) This is optional	Semi publik
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Private network that uses an internet model
((OPTION_A)) THIS IS MANDATORY OPTION	intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is a network that allows authorized access from outside
((OPTION_A)) THIS IS MANDATORY OPTION	Intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Internet authorities have reserved address for
((OPTION_A)) THIS IS MANDATORY OPTION	Intranet
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Internet
((OPTION_C)) This is optional	Extranet
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is provides privacy for LAN
((OPTION_A)) THIS IS MANDATORY OPTION	VPP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	VNP
((OPTION_C)) This is optional	VNN
((OPTION_D)) This is optional	VPN
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	IT PROVIDES END TO END SECURITY FOR APPLICATION
((OPTION_A)) THIS IS MANDATORY OPTION	DATA LINK
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	NETWORK
((OPTION_C)) This is optional	TRANSPORT
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is actually an IETF version on
((OPTION_A)) THIS IS MANDATORY OPTION	TLS, TSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL. TLS
((OPTION_C)) This is optional	TLS, SSL
((OPTION_D)) This is optional	SSL,SLT
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Provides security at the transport layer
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To provide security and compression
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Can receive application data from any application layer protocol
((OPTION_A)) THIS IS MANDATORY OPTION	SSL
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TLS
((OPTION_C)) This is optional	EITHER A OR B
((OPTION_D)) This is optional	BOTH
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SSL provides
((OPTION_A)) THIS IS MANDATORY OPTION	Integrity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Confidentiality
((OPTION_C)) This is optional	Compression
((OPTION_D)) This is optional	All above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SSI session
((OPTION_A)) THIS IS MANDATORY OPTION	List of protocol
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Cipher suit
((OPTION_C)) This is optional	List of keys
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cryptographic algorithem and secrets are sent with the message IN
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	TLS
((OPTION_D)) This is optional	PGP
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Security protocol for email security is
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Was invented by Phil Zimmerman
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSI
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Provides security, integration, authentication in email
((OPTION_A)) THIS IS MANDATORY OPTION	IPSec
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSI
((OPTION_C)) This is optional	PGP
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Method to transfer secure message
((OPTION_A)) THIS IS MANDATORY OPTION	cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	cryptoanalysis
((OPTION_C)) This is optional	both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is the original message before transmission
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Plain text
((OPTION_C)) This is optional	Secret text
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is the message after transmission
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher text
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Plain text
((OPTION_C)) This is optional	Secret text
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm transforms plaintext to ciphertext
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An algorithm transforms cipher text to plain text
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A combination of encryption and decryption algorithm is called
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Secret
((OPTION_C)) This is optional	Key
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cipher operates on
((OPTION_A)) THIS IS MANDATORY OPTION	Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	secret
((OPTION_C)) This is optional	Key
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The same key used by both the sender and receiver
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The key is called as secret key
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A pair of keys used in
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An asymmetric key cipher the sender uses the key
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	An asymmetric key cipher the receiver uses the key
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A cipher replaces one character with another
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Monoalphabetic and polyalphabetic cipher are
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The simplest monoalphabetic cipher is
((OPTION_A)) THIS IS MANDATORY OPTION	Transposition
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additive
((OPTION_C)) This is optional	Shift
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Ceasar cipher that has key of 3
((OPTION_A)) THIS IS MANDATORY OPTION	Transposition
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Additive
((OPTION_C)) This is optional	Shift
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The cipher reorders the plain text to create the ciphertext
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a keyless substitution To define the relationship between input and output stream
((OPTION_A)) THIS IS MANDATORY OPTION	S box
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	P box
((OPTION_C)) This is optional	T box
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a keyless transposition To define the relationship between input and output stream
((OPTION_A)) THIS IS MANDATORY OPTION	S box
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	P box
((OPTION_C)) This is optional	T box
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Cipher made of a combination of different simple cipher
((OPTION_A)) THIS IS MANDATORY OPTION	Round
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Circle
((OPTION_C)) This is optional	Square
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES is an method
((OPTION_A)) THIS IS MANDATORY OPTION	Symmetric key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Asymmetric key
((OPTION_C)) This is optional	Either A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES has an Round
((OPTION_A)) THIS IS MANDATORY OPTION	14
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	15
((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES functions has components
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	3
((OPTION_C)) This is optional	4
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES uses a key generaterto generater to generate sixteen ---round key
((OPTION_A)) THIS IS MANDATORY OPTION	32 bit
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	48 bit
((OPTION_C)) This is optional	54 bit
((OPTION_D)) This is optional	42 bit
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES was designed to increase the size of DES key
((OPTION_A)) THIS IS MANDATORY OPTION	Double
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tripal
((OPTION_C)) This is optional	Quadrupal
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Algorithm uses a 128 bit block of data
((OPTION_A)) THIS IS MANDATORY OPTION	AEE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AED
((OPTION_C)) This is optional	AER
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	AES has how many different combinations
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	3
((OPTION_C)) This is optional	4
((OPTION_D)) This is optional	5
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ECB and CBC are ciphers
((OPTION_A)) THIS IS MANDATORY OPTION	Block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Stream
((OPTION_C)) This is optional	Field
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Public key cryptographic algorithm is
((OPTION_A)) THIS IS MANDATORY OPTION	RSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RAS
((OPTION_C)) This is optional	RSA
((OPTION_D)) This is optional	RAA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	AC
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	it provides a one time session key for two parties
((OPTION_A)) THIS IS MANDATORY OPTION	Diffie hellman
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	DES
((OPTION_D)) This is optional	AES
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	TELNET is an abbreviation of
((OPTION_A)) THIS IS MANDATORY OPTION	Terminal network
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Telephone network
((OPTION_C)) This is optional	Telecommunication network
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	TELNET is a client server application program for
((OPTION_A)) THIS IS MANDATORY OPTION	Specific purpose
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	General purpose
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Users logs in to local time sharing system is called
((OPTION_A)) THIS IS MANDATORY OPTION	Local
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Remote
((OPTION_C)) This is optional	Temporary
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To access remote machine need a login
((OPTION_A)) THIS IS MANDATORY OPTION	Local
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Remote
((OPTION_C)) This is optional	Temporary
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	NVT uses two set of character
((OPTION_A)) THIS IS MANDATORY OPTION	Sending, receiving
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Request, reply
((OPTION_C)) This is optional	Data, control
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For data NVT uses ASCII with the highest order bit set
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0
((OPTION_C)) This is optional	A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For data NVT uses ASCII with the highest order bit set
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0
((OPTION_C)) This is optional	A or B
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The server uses -----port
((OPTION_A)) THIS IS MANDATORY OPTION	Wellknown
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Emperor
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	To distinguish data from characters
((OPTION_A)) THIS IS MANDATORY OPTION	ICA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IAC
((OPTION_C)) This is optional	AIC
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	the echoing is done by the client in the mode
((OPTION_A)) THIS IS MANDATORY OPTION	Default
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Character
((OPTION_C)) This is optional	Line
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP uses a service of
((OPTION_A)) THIS IS MANDATORY OPTION	UDP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IP
((OPTION_C)) This is optional	TCP
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP control and data connection are
((OPTION_A))  THIS IS MANDATORY OPTION	21, 22
((OPTION_B))  THIS IS ALSO MANDATORY OPTION	20,21
((OPTION_C))  This is optional	21,20
((OPTION_D))  This is optional	none
((OPTION_E))  This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP is the service type used by IP protocol because
((OPTION_A)) THIS IS MANDATORY OPTION	Maximise throughput
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Minimize delay
((OPTION_C)) This is optional	Minimize error
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For control connection FTP use a character set of
((OPTION_A)) THIS IS MANDATORY OPTION	Regular ASCII
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	EBCDIC
((OPTION_C)) This is optional	NVT ASCII
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During FTP session the control connection is opened
((OPTION_A)) THIS IS MANDATORY OPTION	Exactly once
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Exactly twice
((OPTION_C)) This is optional	Many times
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During FTP session the control connection is opened
((OPTION_A)) THIS IS MANDATORY OPTION	Exactly once
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Exactly twice
((OPTION_C)) This is optional	Many times
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	FTP files are types of an attribute called
((OPTION_A)) THIS IS MANDATORY OPTION	File types
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structures
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP there are three types of -----,stream, blocked and compression
((OPTION_A)) THIS IS MANDATORY OPTION	File types
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structurs
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP and image defines an attribute called
((OPTION_A)) THIS IS MANDATORY OPTION	File type
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data structure
((OPTION_C)) This is optional	Transmission mode
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP when we -----, it is copied from the server to client
((OPTION_A)) THIS IS MANDATORY OPTION	Retrieve a file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Retrieve a list
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In FTP when we -----, it is copied from the client to server
((OPTION_A)) THIS IS MANDATORY OPTION	Retrieve a file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Store a file
((OPTION_C)) This is optional	Retrieve a lise
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Is a part of a local hard drive, a special file with permission restriction
((OPTION_A)) THIS IS MANDATORY OPTION	A message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A response
((OPTION_C)) This is optional	An agent
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and the receiver on the same system we need
((OPTION_A)) THIS IS MANDATORY OPTION	One UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA
((OPTION_C)) This is optional	One UA and one MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and receiver are on the different system, we need
((OPTION_A)) THIS IS MANDATORY OPTION	One MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA
((OPTION_C)) This is optional	Two UA and one pair of MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender is connected to the mail server via a LAN or WAN, we need
((OPTION_A)) THIS IS MANDATORY OPTION	Two MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA and two pairs of MTA
((OPTION_C)) This is optional	Two UA and a pair of MTA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	When the sender and receiver are connected to the mail server via a LAN or WAN, we need
((OPTION_A)) THIS IS MANDATORY OPTION	Two UA, two pair of MTA, a pair of MAA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Two UA and two pair of MTA
((OPTION_C)) This is optional	Two UA, two pair of MTA, two pair of MAA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	It provides a service to the user to make the process of sending and receiving message
((OPTION_A)) THIS IS MANDATORY OPTION	MTA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MAA
((OPTION_C)) This is optional	UA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following services is not provided by UA
((OPTION_A)) THIS IS MANDATORY OPTION	Composing message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Reading message
((OPTION_C)) This is optional	Reply message
((OPTION_D)) This is optional	ALL are
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	There are two types of user agents
((OPTION_A)) THIS IS MANDATORY OPTION	Command driven, data driven
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Command driven, GUI based
((OPTION_C)) This is optional	Command based and data based
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	It contains the sender address, receiver address and other information
((OPTION_A)) THIS IS MANDATORY OPTION	Message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Envelop
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The message contains
((OPTION_A)) THIS IS MANDATORY OPTION	Header, envelop
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Header, body
((OPTION_C)) This is optional	Envelop, body
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the internet, the email address contains two parts
((OPTION_A)) THIS IS MANDATORY OPTION	Local part, domain name
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Global part, domain name
((OPTION_C)) This is optional	Label, domain name
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is a supplementary protocol that allow Non ASCII data to be sent through email
((OPTION_A)) THIS IS MANDATORY OPTION	JPEG
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MPEG
((OPTION_C)) This is optional	MIME
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The actual email transfer is done through
((OPTION_A)) THIS IS MANDATORY OPTION	UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MTA
((OPTION_C)) This is optional	MAA
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Protocol that defines a MTA client and server in the internet is called
((OPTION_A)) THIS IS MANDATORY OPTION	SMTP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SNMP
((OPTION_C)) This is optional	TELNET
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The process of transferring a mail message occurs in-----phase
((OPTION_A)) THIS IS MANDATORY OPTION	2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4
((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	D
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	SMTP is --- protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Pull
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Push
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The third stage in a email transfer need a ---protocol
((OPTION_A)) THIS IS MANDATORY OPTION	Pull
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Push
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	none
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The third stage in an email transfer uses an ----protocol
((OPTION_A)) THIS IS MANDATORY OPTION	UA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	MTA
((OPTION_C)) This is optional	MAA
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Currently two message asses protocol are available
((OPTION_A)) THIS IS MANDATORY OPTION	POP3, IMAP2
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	POP4,IMAP1
((OPTION_C)) This is optional	POP3, IMAP4
((OPTION_D)) This is optional	NONE
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or E	C
((EXPLANATION )) This is also optional	

This							
Sr No	Question	Image	a	b	c	d	Correct Answer
1	Why would a hacker use a proxy server?		To create a	To create a ghost	To obtain a remote	To hide malicious	d
2	What type of symmetric key algorithm using a streaming cipher to encrypt information?	RC4	Blowfish	SHA	MD5	a	
3	Which of the following is not a factor in securing the environment against an attack on security?		The education of the attacker	The system configuration	The network architecture	The business strategy of the company	d
4	What type of attack uses a fraudulent server with a relay address?		NTLM	MITM	NetBIOS	SMB	b
5	Which of the following is not a typical characteristic of an ethical hacker?		Excellent knowledge of Windows.	Understands the process of exploiting network vulnerabilities.	Patience, persistence and perseverance.	Has the highest level of security for the organization.	d
6	What is the proper command to perform an Nmap XMAS scan every 15seconds?		nmap -sX -sneaky	nmap -sX -paranoid	nmap -sX -aggressive	nmap -sX -polite	a
7	What type of rootkit will patch, hook, or replace the version information?		Library level rootkits	Kernel level rootkits	System level rootkits	Application level rootkits	a
8	What is the purpose of a Denial of Service attack?		Exploit a weakness in the TCP/IP stack	To execute a Trojan on a system	To overload a system so it is no longer operational	To shutdown services by turning them off	c
9	What are some of the most common vulnerabilities that exist in a network or system?		Changing manufacturer, or recommended, settings of a newly installed application.	Additional unused features on commercial software packages.	Utilizing open source application code	Balancing security concerns with functionality and ease of use of a system.	b
10	What is the sequence of a TCP connection?		SYN-ACK-FIN	SYN-SYN ACK-ACK	SYN-ACK	SYN-SYN-ACK	b
11	What tool can be used to perform SNMP enumeration?	DNSlookup	Whois	Nslookup	IP Network Browser	d	
12	Which ports should be blocked to prevent null session enumeration?		Ports 120 and 445	Ports 135 and 136	Ports 110 and 137	Ports 135 and 139	d
13	The first phase of hacking an IT system is compromise of which foundation of security?		Availability	Confidentiality	Integrity	Authentication	b
14	How is IP address spoofing detected?		Installing and configuring a IDS that can read the IP header	Comparing the TTL values of the actual and spoofed addresses	Implementing a firewall to the network	Identify all TCP sessions that are initiated but does not complete successfully	c
15	What is the most important activity in system hacking?		Information gathering	Cracking passwords	Escalating privileges	Covering tracks	b
16	DES follows		Hash Algorithm	Caesars Cipher	Feistel Cipher Structure	SP Networks	c
17	The DES Algorithm Cipher System consists of rounds (iterations) each with a round key		12	18	9	16	d
18	The DES algorithm has a key length of		128 Bits	32 Bits	64 Bits	16 Bits	c
19	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.		True	False			b
20	In the DES algorithm the round key is _____ bit and the Round Input is _____ bits.		48, 32	64,32	56, 24	32, 32	a
21	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via		Scaling of the existing bits	Duplication of the existing bits	Addition of zeros	Addition of ones	a
22	The Initial Permutation table/matrix is of size		16×8	12×8	8×8	4×8	c
23	The number of unique substitution boxes in DES after the 48 bit XOR operation are		8	4	6	12	a
24	In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.		True	False			b
25	During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.		True	False			a
26	A preferable cryptographic algorithm should have a good avalanche effect.		True	False			a
27	The number of tests required to break the DES algorithm are		2.8×1014	4.2×109	1.84×1019	7.2×1016	d
28	The number of tests required to break the Double DES algorithm are		2112	2111	2128	2119	b
29	How many keys does the Triple DES algorithm use?		2	3	2 or 3	3 or 4	c
30	In triple DES, the key size is ___ and meet in the middle attack takes ___ tests to break the key.		2192 ,2112	21,842,111	21,682,111	21,682,112	d
31	Extensions were added in which version?		1	2	3	4	c
32	The subject unique identifier of the X.509 certificates was added in which version?		1	2	3	4	b
33	Which of the following is not an element/field of the X.509 certificates?		Issuer Name	Serial Modifier	Issuer unique Identifier	Signature	b
34	Suppose that A has obtained a certificate from certification authority X1 and B has obtained certificate authority from CA X2. A can use a chain of certificates to obtain B's public key. In notation of X.509, this chain is represented in the correct order as –		X2 X1 X1 B	X1 X1 X2 A	X1 X2 X2 B	X1 X2 X2 A	c
35	Certificates generated by X that are the certificates of other CAs are Reverse Certificates.		True	False			a
36	It is desirable to revoke a certificate before it expires because		the user is no longer certified by this CA	the CA's certificate is assumed to be compromised	the user's private key is assumed to be compromised	all of the mentioned	d
37	CRL stands for		Cipher Reusable List	Certificate Revocation Language	Certificate Revocation List	Certificate Resolution Language	c
38	Which of the following is not a part of an Extension?		Extension Identifier	Extension value	Criticality Indicator	All of the mentioned constitute the Extension	d
39	The criticality indicator indicates whether an extension can be safely ignored.		True	False			a
40	Which Extension among the following does this refer to?		Subject alternative name	Issuer Alternative name	Subject directory attributes	None of the mentioned	c

41	How many handshake rounds are required in the Public-Key Distribution Scenario?		7	5	3	4	a
42	A total of seven messages are required in the Public-Key distribution scenario. However, the initial five messages need to be used only infrequently because both A and B can save the other's public key for future – a technique known as _____.		time stamping	polling	caching	squeezing	c
43	X.509 certificate recommends which cryptographic algorithm?		RSA	DES	AES	Rabin	a
44	The issuer unique identifier of the X.509 certificates was added in which version?		1	2	3	4	b
45	The period of validity consists of the date on which the certificate expires.		True	False			b
46	Which of the following is not a transport layer vulnerability?		Mishandling of undefined, poorly defined	The Vulnerability that allows "fingerprinting" & other enumeration of host information	Overloading of transport-layer mechanisms	Unauthorized network access	d
47	Which of the following is not session layer vulnerability?		Mishandling of undefined, poorly defined	Spoofing and hijacking of data based on failed authentication attempts	Passing of session-credentials allowing intercept and unauthorized use	Weak or non-existent authentication mechanisms	a
48	Failed sessions allow brute-force attacks on access credentials. This type of attacks are done in which layer of the OSI model?		Physical layer	Data-link Layer	Session layer	Presentation layer	c
49	Transmission mechanisms can be subject to spoofing & attacks based on skilled modified packets.		True	False			a
50	Which of the following is not an example of presentation layer issues?		Poor handling of unexpected input can lead to the execution of arbitrary instructions	Unintentional or ill-directed use of superficially supplied input	Cryptographic flaws in the system may get exploited to evade privacy	Weak or non-existent authentication mechanisms	a
51	Which of the following is not a vulnerability of the application layer?		Application design bugs may bypass security controls	Inadequate security controls force "all-or-nothing" approach	Logical bugs in programs may be by chance or on purpose be used for crashing programs	Overloading of transport-layer mechanisms	d
52	Which of the following is an example of Transport layer vulnerability?		weak or non-existent mechanisms for authentication	overloading of transport-layer mechanisms	poor handling of unexpected input	highly complex application security controls	b
53	Which of the following is an example of session layer vulnerability?		weak or non-existent mechanisms for authentication	overloading of transport-layer mechanisms	poor handling of unexpected input	highly complex application security controls	a
54	Which of the following is an example of presentation layer vulnerability?		weak or non-existent mechanisms for authentication	overloading of transport-layer mechanisms	highly complex application security controls	poor handling of unexpected input	d
55	Which of the following is an example of application layer vulnerability?		Cryptographic flaws lead to the privacy issue	Very complex application security controls	MAC Address Spoofing	Weak or non-existent authentication	b
56	TCP/IP is extensively used model for the World Wide Web for providing network communications which are composed of 4 layers that work together.		TRUE	FALSE			a
57	TCP/IP is composed of _____ number of layers.		2	3	4	5	c
58	Trusted TCP/IP commands have the same needs & go through the identical verification process. Which of them is not a TCP/IP command?		ftp	rexec	tcpexec	telnet	c
59	Connection authentication is offered for ensuring that the remote host has the likely Internet Protocol (IP) _____ &		address, name	address, location	network, name	network, location	a
60	Application layer sends & receives data for particular applications using Hyper Text Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).		TRUE	FALSE			a
61	TLS vulnerability is also known as Return of Bleichenbacher's Oracle Threat.		TRUE	FALSE			a
62	RoBOT is abbreviated as _____		Return of Bleichenbacher's Oracle Team	Rise of Bleichenbacher's Oracle Threat	Return of Bleichenbacher's Operational Threat	Return of Bleichenbacher's Oracle Threat	d
63	There are _____ different versions of IP popularly used.		2	3	4	5	a
64	_____ is an attack where the attacker is able to guess together with the sequence number of an in progress communication session & the port number.		TCP Spoofing	TCP Blind Spoofing	IP Spoofing	IP Blind Spoofing	b
65	_____ is an attack technique where numerous SYN packets are spoofed with a bogus source address which is then sent to an inundated server.		SYN flooding attack	ACK flooding attack	SYN & ACK flooding attack	Packet flooding attack	a
66	What are the different ways to intrude?		Buffer overflows	Unexpected combinations and unhandled input	Race conditions	All of the mentioned	d
67	What are the major components of the intrusion detection system?		Analysis Engine	Event provider	Alert Database	All of the mentioned	d
68	What are the different ways to classify an IDS?		anomaly detection	signature based misuse	stack based	all of the mentioned	d
69	What are the different ways to classify an IDS?		Zone based	Host & Network based	Network & Zone based	Level based	b
70	What are the characteristics of anomaly based IDS?		It models the normal usage of network as a noise characterization	It doesn't detect novel attacks	Anything distinct from the noise is not assumed to be intrusion activity	It detects based on signature	a
71	What is the major drawback of anomaly detection IDS?		These are very slow at detection	It generates many false alarms	It doesn't detect novel attacks	None of the mentioned	b
72	What are the characteristics of signature based IDS?		Most are based on simple pattern matching algorithms	It is programmed to interpret a certain series of packets	It models the normal usage of network as a noise characterization	Anything distinct from the noise is assumed to be intrusion activity	a

73	What are the drawbacks of signature based IDS?		They are unable to detect novel attacks	They suffer from false alarms	They have to be programmed again for every new pattern to be detected	All of the mentioned	d
74	What are the characteristics of Host based IDS?		The host operating system logs in the audit information	Logs includes logins,file opens and program executions	Logs are analysed to detect tails of intrusion	All of the mentioned	d
75	What are the drawbacks of the host based IDS?		Unselective logging of messages may increase the audit burdens	Selective logging runs the risk of missed attacks	They are very fast to detect	They have to be programmed for new patterns	a
76	Network layer firewall works as a _____	Frame filter	Packet filter	Content filter	Virus filter		b
77	Network layer firewall has two sub-categories as _____	State full firewall and stateless firewall	Bit oriented firewall and byte oriented firewall	Frame firewall and packet firewall	Frame firewall and packet firewall		a
78	A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____	Chock point	Meeting point	Firewall point	Secure point		a
79	Which of the following is / are the types of firewall?	Packet Filtering Firewall	Dual Homed Gateway Firewall	Screen Host Firewall	Dual Host Firewall		a
80	A proxy firewall filters at _____	Physical layer	Data link layer	Network layer	Application layer		d
81	A packet filter firewall filters at _____	Physical layer	Data link layer	Network layer	Application layer		c
82	What is one advantage of setting up a DMZ with two firewalls?	You can control where traffic goes in three networks	You can do stateful packet filtering	You can do load balancing	Improved network performance		c
83	What tells a firewall how to reassemble a data stream that has been divided into packets?	The source routing feature	The number in the header's identification field	The destination IP address	The header checksum field in the packet header		a
84	A stateful firewall maintains a _____ which is a list of active connections.	Routing table	Bridging table	State table	Connection table		a
85	A firewall needs to be _____ so that it can grow proportionally with the network that it protects.	Robust	Expansive	Fast	Scalable		b
86	PII stands for?	Proportionally Identifiable Information	Proportionally Information Identifiable	Personally Information Identifiable	Personally Identifiable Information		d
87	PII can be.....	sensitive or non sensitive	sensitive	non sensitive	sensitive and non sensitive		a
88	..... is a crime in which the attacker harasses a victim using electronic message	Gender based Stalking	WHOA	Cyber Stalking	PII		c
89	Cyber stalking is crime regarded in the ...	India	Uk	US	Germany		c
90	Cyber stalking is a technologically based on ....	one person	two person	three person	four person		a
91	In .....the Bureau of justice statistics in the United states released the study "Stalking Victimization in the United States".	Feb-09	Jan-10	Feb-10	Jan-09		d
92	Types of Cyber Stalker Attacks?	Stalking by stranger	Gender based Stalking	Corporate cyber stalking	All of the above		d
93	A notable example of online mob annoyance was the experience of ...	American Software developer	German Software developer	American hardware developer	German hardware developer		a
94	The crime involves and uses computer devices and internet is known as .....	Stalking by stranger	Corporate cyber stalking	Cybercrime	Cyber stalking		c
95	Cybercrime can cause....	Direct harm and indirect harm	Direct harm	Direct harm or indirect harm	Indirect harm		c
96	Cybercrime causes loss in ... each Year	Millions	Trillions	Billions	None of the above		c
97	Emergence of information Act,...	2000	2001	2002	2003		a
98	Damage to Computer System etc	Sec 66	Sec 70	Sec 43	Sec 48		c
99	Hacking compensation for Rupees 1 crore.	Sec 66	Sec 70	Sec 43	Sec 48		a
100	Attempting or securing access to computer	Sec 66	Sec 70	Sec 43	Sec 48		b
101	Not complying with directions of controller	Sec 68	Sec 70	Sec 43	Sec 74		a
102	Publishing false digital signatures	Sec 66	Sec 70	Sec 73	Sec 74		c
103	Publishing of digital signatures	Sec 66	Sec 70	Sec 73	Sec 74		d
104	...is carried on by use of unreliable websites or emails.	Phishing	Computer virus	Spoofing	Phone Phishing		c
105	By using email messages which entirely resembles the original mail messages of customers	Phishing	Computer virus	Spoofing	Phone Phishing		b

- A.Phishing
- B.Computer virus
- C.Spoofing

D.Phone Phishing

A.Phishing  
B.Computer virus  
C.Spoofing  
D.Phone Phishing

A.Phishing  
B.Computer virus  
C.Risk posed on Banks and other institutions  
D.Phone Phishing

A.Firewalls  
B.Digital Singature  
C.Synchronized password  
D.Encryption

A.Firewalls  
B.Digital Singature  
C.Synchronized password  
D.Encryption

ICS MCQ  
Unit No.1 : Security Basics

1. Message \_\_\_\_\_ means that the sender and receiver except privacy

- \*A. Confidentiality\***
- B. integrity
- C.authentication
- D.none of the above

2. Message\_\_\_\_\_ means that the must arrive at the receiver exactly as sent

- A. confidentiality
- \*B. integrity\***
- C.authentication
- D.none of the above

3. Message \_\_\_\_\_ means that the receiver insured that message coming from the intended sender, not an imposter

- A. confidentiality
- B. integrity
- \*C.authentication\***
- D.none of the above

4. \_\_\_\_\_ means that a send must not able to deny sending a message that he sent.

- A. Confidentiality
- B. Integrity
- C.Authentication
- \*D.Nonrepudiation\***

5. \_\_\_\_\_ means to prove identify of entity that tries to access the system's resources.

- A. Message authentication
- B. Entity authentication**
- C.Message confidentiality
- D.none of the above

6. What are the characteristics of CIA triangle?

- A. Confidentiality
- B. Integrity
- C. Availability
- D. All of the above**

7. Which Of The Following Malicious Program Do Not Replicate Automatically?

**A.Trojan Horse**

- B.Virus
- C.Worm
- D.Zombie

8.Which Of The Following Is A Class Of Computer Threat

**A. DoS Attacks**

- B. Phishing
- C.Stalking
- D. Soliciting

9.Which of the following is independent malicious program that need not any host program?

- A. Trap doors
- B. Trojan horse
- C. Virus
- D. Worm**

10. The first computer virus is -----

- A.Sasser
- B.Creeper**
- C.Blastar
- D.I Love You

10. VIRUS stands for

- A.Very Intelligent Result Until Source
- B.Vital Information Resource Under Siege**
- C.Viral Important Record User Searched
- D.Very Interchanged Resource Under Search

11. \_\_\_\_\_ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.

- a) Network Security
- b) Database Security
- c) Information Security**
- d) Physical Security

12. From the options below, which of them is not a vulnerability to information security?

- a) flood**
- b) without deleting data, disposal of storage media
- c) unchanged default password
- d) latest patches and

13. Compromising confidential information comes under \_\_\_\_\_

- a) Bug
- b) Threat**
- c) Vulnerability
- d) Attack

14. Possible threat to any information cannot be \_\_\_\_\_

- a) reduced
- b) transferred
- c) protected
- d) ignored**

15. In general how many key elements constitute the entire security structure?

- a) 1
- b) 2
- c) 3**
- d) 5

16. According to the CIA Triad, which of the below-mentioned element is not considered in the triad?

- a) Confidentiality
- b) Integrity
- c) Authenticity**
- d) Availability

17. This is the model designed for guiding the policies of Information security within a company, firm or organization. What is "this" referred to here?

- a) Confidentiality
- b) Non-repudiation
- c) CIA Triad**
- d) Authenticity

18. When you use the word \_\_\_\_\_ it means you are protecting your data from getting disclosed.

- a) Confidentiality**
- b) Integrity
- c) Authentication

d) Availability

19. \_\_\_\_\_ means the protection of data from modification by unknown users.

- a) Confidentiality
- b) Integrity**
- c) Authentication
- d) Non-repudiation

20. When integrity is lacking in a security system, \_\_\_\_\_ occurs.

- a) Database hacking
- b) Data deletion
- c) Data tampering**
- d) Data leakage

21. \_\_\_\_\_ of information means, only authorised users are capable of accessing the information.

- a) Confidentiality
- b) Integrity
- c) Non-repudiation
- d) Availability**

22. Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?

- a) They help understanding hacking better
- b) They are key elements to a security breach
- c) They help understand security and its components better**
- d) They help to understand the cyber-crime better

23. This helps in identifying the origin of information and authentic user. This referred to here as

- 
- a) Confidentiality
  - b) Integrity
  - c) Authenticity**
  - d) Availability

24. Data \_\_\_\_\_ is used to ensure confidentiality.

- a) Encryption**
- b) Locking
- c) Deleting
- d) Backup

25. \_\_\_\_\_ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.

- a) Network Security
- b) Database Security
- c) Information Security**
- d) Physical Security

26. From the options below, which of them is not a threat to information security?

- a) Disaster
- b) Eavesdropping
- c) Information leakage
- d) Unchanged default password**

27. In Message Confidentiality, the transmitted message must make sense to only intended

**A.Receiver**

- B.Sender
- C.Modulator
- D.Translator

28. Encryption and decryption provide secrecy, or confidentiality, but not

A.Authentication

**B.Integrity**

C.Privacy

D.All of the above

29. Select categories of computer security

- A. Cryptography
- B. Data security
- C. Computer Security
- D. Network Security
- E. All of above**

30. \_\_\_\_\_ is ensuring safe data from modification and corruption

- A. Data security**
- B. Computer Security
- C. Network Security

31. \_\_\_\_\_ is protection of data on the network during transmission or sharing

- A. Data security
- B. Computer Security
- C. Network Security**

32. The field that covers a variety of computer networks, both public and private, that are used in everyday jobs.

- a) Artificial Intelligence

- b) ML
- c) Network Security**
- d) IT

33. Network Security provides authentication and access control for resources.

- a) True**
- b) False

34. An algorithm in encryption is called \_\_\_\_\_

- a) Algorithm
- b) Procedure
- c) Cipher**
- d) Module

35. The information that gets transformed in encryption is \_\_\_\_\_

- a) Plain text**
- b) Parallel text
- c) Encrypted text
- d) Decrypted text

36. The process of transforming plain text into unreadable text.

- a) Decryption
- b) Encryption**
- c) Network Security
- d) Information Hiding

37. An algorithm used in encryption is referred to as cipher.

- a) True**
- b) False

38. A process of making the encrypted text readable again.

- a) Decryption**
- b) Encryption
- c) Network Security
- d) Information Hiding

39. A small program that changes the way a computer operates.

- a) Worm
- b) Trojan
- c) Bomb
- d) Virus**

40. A program that copies itself.

- a) Worm**
- b) Virus
- c) Trojan
- d) Bomb

41. An attack in which the site is not capable of answering valid request.

- a) Smurfing
- b) Denial of service**
- c) E-mail bombing
- d) Ping storm

42. Plain text is the data after encryption is performed.

- a) True
- b) False**

43. Attack in which a user creates a packet that appears to be something else.

- a) Smurfing
- b) Trojan
- c) E-mail bombing
- d) Spoofing**

44. \_\_\_\_\_ is a weakness that can be exploited by attackers.

- a) System with Virus
- b) System without firewall
- c) System with vulnerabilities**
- d) System with a strong password

45. \_\_\_\_\_ is the sum of all the possible points in software or system where unauthorized users can enter as well as extract data from the system.

- a) Attack vector
- b) Attack surface**
- c) Attack point
- d) Attack arena

46 Risk and vulnerabilities are the same things.

- a) True
- b) False**

47. A/An \_\_\_\_\_ is a piece of software or a segment of command that usually take advantage of a bug to cause unintended actions and behaviors.

- a) malware
- b) trojan
- c) worms

**d) exploit**

48. ISMS is abbreviated as \_\_\_\_\_

- a) Information Server Management System
- b) Information Security Management Software
- c) Internet Server Management System
- d) Information Security Management System**

49. A zero-day vulnerability is a type of vulnerability unknown to the creator or vendor of the system or software.

- a) True**
- b) False

50. Risk is intersection of Assets, threats and vulnerabilities

- A) True**
- B) False

51. Privacy is the appropriate use of users information

- A) True**
- B) False

52. Interception, interruption, modification and fabrication are system threats

- A) True**
- B) False

53. The attacker using a network of compromised devices is known as \_\_\_\_\_

- a) Internet
- b) Botnet**
- c) Telnet
- d) D-net

54. Which of the following is a form of DoS attack?

- a) Vulnerability attack
- b) Bandwidth flooding
- c) Connection flooding
- d) All of the mentioned**

55. the attacker, not just only observes data but he has direct access to it. The attacker can read and update the data without the information of any of the users.

- A) Active attack**
- B) Passive attack
- C) DoS attack

56. the data that is transmitted is modified by a third client illegally is called Active Attack.

**A)True**

B) False

57. the attacker used the identity of the authentic users and he breaks into the communication and behaves like the authentic user and grabs all the data.

**A) Masquerade**

B) Replay

C) Traffic analysis

D) DoS

58. the attacker can observe every message or data that is sent or received in the communication but he can not update or modify it is called passive attack.

**A) True**

B) False

59. Which of the following security attacks is not an active attack?

OR

Which of the following attacks is a passive attack?

A) Masquerade

B) Modification of message

C) Denial of service

**D) Traffic analysis**

60. Passive attack difficult to detect.

**A) True**

B)False

61. Active attack it affects the system

**A) True**

B) False

62.

## UNIT VI MCQ

- 1. What is Digital Forensic?
  - A. Process of using scientific knowledge in analysis and presentation of evidence in court
  - **B. The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation**
  - C. A process where we develop and test hypotheses that answer questions about digital events
  - D. Use of science or technology in the investigation and establishment of the facts or evidence in a court of law
- 2. Does database forensic include in Digital Forensic application
  - **A. True**
  - B. False
- 3. Which of the following is NOT focus of digital forensic analysis?
  - A. Authenticity
  - B. Comparison
  - **C. Proving**
  - D. Enhancement
- 4. What is the Primary Objectives of Digital Forensic for Business and Industry
  - **A.Availability of service**
  - B.Continuity of operation
  - C.Prosecution
  - D.Security
- 5. Which of the following hold the highest value of evidence in the court?
  - A. Documentary
  - B. Demonstrative
  - C. Testimonial
  - **D. Real**
- 6.Which of the following is FALSE
  - A. The digital forensic investigator must maintain absolute objectivity
  - **B. It is the investigator's job to determine someone's guilt or innocence.**
  - C. It is the investigator's responsibility to accurately report the relevant facts of a case.
  - D. The investigator must maintain strict confidentiality, discussing the results of an investigation on only a "need to know" ba
- 7. This is the model designed for guiding the policies of Information security within a company, firm or organization. What is "this" referred to here?

a) Confidentiality

b) Non-repudiation

**c) CIA Triad**

d) Authenticity

8. When you use the word \_\_\_\_ it means you are protecting your data from getting disclosed.

**a) Confidentiality**

b) Integrity

c) Authentication

d) Availability

9\_\_\_\_\_ means the protection of data from modification by unknown users.

a) Confidentiality

**b) Integrity**

c) Authentication

d) Non-repudiation

10.Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental?

a) They help understanding hacking better

b) They are key elements to a security breach

**c) They help understand security and its components better**

d) They help to understand the cyber-crime better

11 Digital forensics is all of them except:

A. Extraction of computer data.

- B. Preservation of computer data.
- C. Interpretation of computer data.
- D. Manipulation of computer data.**

12 IDIP stands for

- A. Integrated Digital Investigation Process.**
- B. Integrated Data Investigator Process.
- C. Integrated Digital Investigator Process.
- D. Independent Digital Investigator Process

13 Digital Forensics entails \_\_\_\_\_.

- A. Accessing the system's directories viewing mode and navigating through the various systems files and folders
- B. Undeleting and recovering lost files
- C. Identifying and solving computer crimes

**D. The identification, preservation, recovery, restoration and presentation of digital evidence from systems and devices**

14 What is the most significant legal issue in computer forensics?

- A. Preserving Evidence
- B. Seizing Evidence
- C. Admissibility of Evidence**
- D. Discovery of Evidence

15 Computer forensics do not involve\_\_\_\_activity.

- A. Preservation of computer data.
- B. Extraction of computer data.
- C. Manipulation of computer data.**
- D. Interpretation of computer data

16 To collect and analyze the digital evidence that was obtained from the physical investigation phase, is the goal of which phase?

- A. Physical crime investigation
- B. Digital crime investigation.**
- C. Review phase.
- D. Deployment phase.

17 \_\_\_\_\_is known as father of computer forensic.

- A. G. Palmar
- B. J. Korn
- C. Michael Anderson**
- D. S.Ciardhuain.

18 Which term refers for modifying a computer in a way which was not originally intended to view Information?

- A. Metadata
- B. Live analysis

**C. Hacking**

D. Bit Copy

18 Which of this is not a computer crime?

A. e-mail harassment

B. Falsification of data.

C. Sabotage.

**D. Identification of data**

19 You need to transmit PII via email and you want to maintain its confidentiality. Of the following choices, what is the BEST solution?

A. Use hashes.

**B. Encrypt it before sending.**

C. Protect it with a digital signature.

D. Use RAID.

20 What is the name of the IT law that India is having in the Indian legislature?

a) India's Technology (IT) Act, 2000

b) India's Digital Information Technology (DIT) Act, 2000

**c) India's Information Technology (IT) Act, 2000**

d) The Technology Act, 2008

21 In which year India's IT Act came into existence?

**a) 2000**

b) 2001

c) 2002

d) 2003

22 Under which section of IT Act, stealing any digital asset or information is written a cyber-crime.

**a) 65**

b) 65-D

c) 67

d) 70

23What type of cyber-crime, its laws and punishments does section 66 of the Indian IT Act holds?

**a) Cracking or illegally hack into any system**

b) Putting antivirus into the victim

c) Stealing data

d) Stealing hardware components

24 Attempting to gain access to a network using an employee's credentials is called the \_\_\_\_\_ mode of ethical hacking.

**A Local networking**

**B Social engineering**

**C Physical entry**

**D Remote networking**

25 Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?

**A Web-based**

**B Human-based**

**C User-based**

**D Computer-based**

26 Which phase of hacking performs actual attack on a network or system?

**A Reconnaissance**

**B Maintaining Access**

**C Scanning**

**D Gaining Access**

ICS MCQ  
Unit 2: Data Encryption Techniques and standard

1.Assymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key?

- A. Not true, the message can also be decrypted with the Public Key.
- B. **So called "one way function with back door" is applied for the encryption.**
- C. The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key.
- D. The encrypted message contains the function for decryption which identifies the Private Key.

2.In which way does the Combined Encryption combine symmetric and assymmetric encryption?

- A. First, the message is encrypted with symmetric encryption and afterwards it is encrypted assymmetrically together with the key.
- B. The secret key is symmetrically transmitted, the message itself assymmetrically.
- C. First, the message is encrypted with assymmetric encryption and afterwards it is encrypted symmetrically together with the key.
- D. **The secret key is assymmetrically transmitted, the message itself symmetrically.**

3.Which is the largest disadvantage of the symmetric Encryption?

- A. More complex and therefore more time-consuming calculations.
- B. **Problem of the secure transmission of the Secret Key.**
- C. Less secure encryption function.
- D. Isn't used any more.

4.Which of the following Algorithms belong to symmetric encryption?

- A. **3DES (TripleDES)**
- B. RSA
- C. **RC5**
- D. **IDEA**

5.Which of the following statements are correct?

- A. PGP uses assymmetric encryption.
- B. In the world wide web, primarily symmetric Encryption is used.
- C. **Symmetric encryption is applied in the transmission of PIN numbers from the EC automat to the server of the bank for example.**

**D. PGP uses combined encryption.**

6. Which is the principle of the encryption using a key?

- A. The key indicates which function is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.
- B. The key contains the secret function for encryption including parameters. Only a password can activate the key.
- C. All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.**
- D. The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.

7. \_\_\_\_\_ is the process or mechanism used for converting ordinary plain text into garbled non-human readable text & vice-versa.

- A. Malware Analysis
- B. Exploit writing
- C. Reverse engineering
- D. Cryptography**

8. \_\_\_\_\_ is a means of storing & transmitting information in a specific format so that only those for whom it is planned can understand or process it.

- A. Malware Analysis
- B. Cryptography**
- C. Reverse engineering
- D. Exploit writing

9. When plain text is converted to unreadable format, it is termed as \_\_\_\_\_

- A. rotten text
- B. raw text
- C. cipher-text**
- D. ciphen-text

10. Cryptographic algorithms are based on mathematical algorithms where these algorithms use \_\_\_\_\_ for a secure transformation of data.

- A. secret key**
- B. external programs
- C. add-ons
- D. secondary key

11. Cryptography can be divided into \_\_\_\_\_ types.

- A. 5
- B. 4
- C. 3
- D. 2**

12. Data which is easily readable & understandable without any special algorithm or method is called \_\_\_\_\_

- A. cipher-text
- B. plain text**
- C. raw text
- D. encrypted text

13. Plain text are also called \_\_\_\_\_

- a) cipher-text
- b) raw text
- c) clear-text**
- d) encrypted text

14. There are \_\_\_\_\_ types of cryptographic techniques used in general.

- a) 2
- b) 3**
- c) 4
- d) 5

15. Conventional cryptography is also known as \_\_\_\_\_ or symmetric-key encryption.

- a) secret-key**
- b) public key
- c) protected key
- d) primary key

16. Data Encryption Standard is an example of a \_\_\_\_\_ cryptosystem.

- a) conventional**
- b) public key
- c) hash key
- d) asymmetric-key

17. \_\_\_\_\_ cryptography deals with traditional characters, i.e., letters & digits directly.

- a) Modern
- b) Classic**
- c) Asymmetric
- d) Latest

18. \_\_\_\_\_ cryptography operates on binary-bit series and strings.

- a) Modern**
- b) Classic
- c) Traditional
- d) Primitive

19. \_\_\_\_\_ cryptography has always been focussing on the concept of 'security through obscurity'.

- a) Modern
- b) Asymmetric
- c) Classic**
- d) Latest

20. \_\_\_\_\_ cryptography is based on publicly known mathematically designed algorithms to encrypt the information.

- a) Modern**
- b) Classic
- c) Traditional

21. \_\_\_\_\_ is the art & science of cracking the cipher-text without knowing the key.

- a) Cracking
- b) Cryptanalysis**
- c) Cryptography
- d) Crypto-hacking

22. The process of disguising plaintext in such a way that its substance gets hidden (into what is known as cipher-text) is called \_\_\_\_\_

- a) cryptanalysis
- b) decryption
- c) reverse engineering
- d) encryption**

23. The method of reverting the encrypted text which is known as cipher text to its original form i.e. plain text is known as \_\_\_\_\_

- a) cryptanalysis
- b) decryption**
- c) reverse engineering
- d) encryption

24. Cryptography offers a set of required security services. Which of the following is not among that 4 required security services?

- a) Encryption
- b) Message Authentication codes
- c) Hash functions
- d) Steganography**

25. A cryptosystem is also termed as \_\_\_\_\_

- a) secure system
- b) cipher system**
- c) cipher-text
- d) secure algorithm

26. \_\_\_\_\_ is the mathematical procedure or algorithm which produces a cipher-text for any specified plaintext.

- a) Encryption Algorithm**
- b) Decryption Algorithm
- c) Hashing Algorithm
- d) Tuning Algorithm

27. \_\_\_\_\_ takes the plain text and the key as input for creating cipher-text.

- a) Decryption Algorithm**
- b) Hashing Algorithm
- c) Tuning Algorithm
- d) Encryption Algorithm

28. A set of all probable decryption keys are collectively termed as \_\_\_\_\_

- a) key-stack
- b) key bunch
- c) key space**
- d) key pack

29. Encryption-decryption in cryptosystem is done in \_\_\_\_\_ ways.

- a) 4
- b) 3
- c) 5
- d) 2**

30. In \_\_\_\_\_ same keys are implemented for encrypting as well as decrypting the information.

- a) Symmetric Key Encryption**
- b) Asymmetric Key Encryption
- c) Asymmetric Key Decryption
- d) Hash-based Key Encryption

31. In \_\_\_\_\_ 2 different keys are implemented for encrypting as well as decrypting that particular information.

- a) Symmetric Key Encryption
- b) Asymmetric Key Encryption**
- c) Asymmetric Key Decryption
- d) Hash-based Key Encryption

32. A set of all probable decryption keys are collectively termed as key space.

- a) True
- b) False

33. \_\_\_\_\_ is a mono-alphabetic encryption code wherein each & every letter of plain-text is replaced by another letter in creating the cipher-text.

- a) Polyalphabetic Cipher
- b) Caesar Cipher**
- c) Playfair Cipher
- d) Monoalphabetic Cipher

34. \_\_\_\_\_ is the concept that tells us about the replacement of every alphabet by another alphabet and the entire series gets 'shifted' by some fixed quantity.

- a) Rolling Cipher
- b) Shift Cipher**
- c) Playfair Cipher
- d) Block Cipher

35. \_\_\_\_\_ is a cipher formed out of substitution where for a given key-value the cipher alphabet for every plain text remains fixed all through the encryption procedure.

- a) Polyalphabetic Cipher
- b) Caesar Cipher
- c) Playfair Cipher
- d) Monoalphabetic Cipher**

36. In Playfair cipher, at first, a key table is produced. That key table is a 5 by 5 grid of alphabets which operates as the key to encrypt the plaintext.

- a) Rolling Cipher
- b) Shift Cipher
- c) Playfair Cipher**
- d) Block Cipher

37. \_\_\_\_\_ employs a text string as a key that is implemented to do a series of shifts on the plain-text.

- a) Vigenere Cipher**
- b) Shift Cipher
- c) Playfair Cipher
- d) Block Cipher

38. The \_\_\_\_\_ has piece of the keyword that has the same length as that of the plaintext.

- a) Block Cipher

- b) One-time pad**
- c) Hash functions
- d) Vigenere Cipher

39. In \_\_\_\_\_ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.

- a) Block Cipher**
- b) One-time pad
- c) Hash functions
- d) Vigenere Cipher

40. In \_\_\_\_\_ the plain-text is processed 1-bit at a time & a series of actions is carried out on it for generating one bit of cipher-text.

- a) Block Cipher
- b) One-time pad
- c) Stream cipher**
- d) Vigenere Cipher

41. The procedure to add bits to the last block is termed as \_\_\_\_\_

- a) decryption
- b) hashing
- c) tuning
- d) padding**

42. Which of the following is not an example of a block cipher?

- a) DES
- b) IDEA
- c) Caesar cipher**
- d) Twofish

43. Data Encryption Standard is implemented using the Feistel Cipher which employs 16 round of Feistel structure.

- a) DES**
- b) IDEA
- c) Caesar cipher
- d) Twofish

44. DES stands for \_\_\_\_\_

- a) Data Encryption Security
- b) Data Encrypted Standard
- c) Device Encryption Standard
- d) Data Encryption Standard**

45. \_\_\_\_\_ carries out all its calculations on bytes rather than using bits and is at least 6-times faster than 3-DES.

- a) AES
- b) DES
- c) IDEA
- d) Twofish

46. AES stands for \_\_\_\_\_

- a) Advanced Encryption Security
- b) Advanced Encryption Standard**
- c) Advanced Encrypted Standard
- d) Active Encryption Standard

47. AES is at least 6-times faster than 3-DES.

- a) True**
- b) False

48. \_\_\_\_\_ is another data hiding technique which can be used in conjunction with cryptography for the extra-secure method of protecting data.

- a) Cryptography
- b) Steganography**
- c) Tomography
- d) Chorography

49. \_\_\_\_\_ is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

- a) Cryptography
- b) Tomography
- c) Steganography**
- d) Chorography

50. Steganography follows the concept of security through obscurity.

- a) True**
- b) False

51. The word \_\_\_\_\_ is a combination of the Greek words ‘steganos’ which means “covered or concealed”, and ‘graphein’ which means “writing”.

- a) Cryptography
- b) Tomography
- c) Steganography**
- d) Chorography

52. A \_\_\_\_\_ tool permits security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

- a) Cryptography
- b) Tomography
- c) Chorography
- d) Steganography**

53. Which of the following is not a steganography tool?

- a) Xaio steganography
- b) Image steganography
- c) ReaperExploit**
- d) Steghide

54. The main motive for using steganography is that hackers or other users can hide a secret message behind a \_\_\_\_\_

- a) special file
- b) ordinary file**
- c) program file
- d) encrypted file

55. The Data Encryption Standard (DES) and It's Strength".

1. DES follows
- a) Hash Algorithm
- b) Caesars Cipher
- c) Feistel Cipher Structure**
- d) SP Networks

56. The DES Algorithm Cipher System consists of \_\_\_\_\_ rounds (iterations) each with a round key

- a) 12
- b) 18
- c) 9
- d) 16**

57. The DES algorithm has a key length of

- a) 128 Bits
- b) 32 Bits
- c) 64 Bits**
- d) 16 Bits

58. In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.

- a) True
- b) False**

59. In the DES algorithm the round key is \_\_\_\_\_ bit and the Round Input is \_\_\_\_\_ bits.

- a) 48, 32**
- b) 64,32
- c) 56, 24
- d) 32, 32

60. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via

- 
- a) Scaling of the existing bits**
  - b) Duplication of the existing bits
  - c) Addition of zeros
  - d) Addition of ones

61. The Initial Permutation table/matrix is of size

- a)  $16 \times 8$
- b)  $12 \times 8$
- c)  $8 \times 8$**
- d)  $4 \times 8$

62. The number of unique substitution boxes in DES after the 48 bit XOR operation are

- a) 8**
- b) 4
- c) 6
- d) 12

63. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.

- a) True
- b) False**

64. During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.

- a) True**
- b) False

65. A preferable cryptographic algorithm should have a good avalanche effect.

- a) True**
- b) False

66. The number of tests required to break the DES algorithm are

- a)  $2.8 \times 10^{14}$

- b)  $4.2 \times 10^9$
- c)  $1.84 \times 10^{19}$
- d)  $7.2 \times 10^{16}$**

67. The number of tests required to break the Double DES algorithm are

- a)  $2^{112}$
- b)  $2^{111}$**
- c)  $2^{128}$
- d)  $2^{119}$

68. How many keys does the Triple DES algorithm use?

- a) 2
- b) 3
- c) 2 or 3**
- d) 3 or 4

69. In triple DES, the key size is \_\_\_\_ and meet in the middle attack takes \_\_\_\_ tests to break the key.

- a)  $2^{192}, 2^{112}$
- b)  $2^{184}, 2^{111}$
- c)  $2^{168}, 2^{111}$
- d)  $2^{168}, 2^{112}$**

70. Using Differential Crypt-analysis, the minimum computations required to decipher the DES algorithm is

- a) 256
- b) 243
- c) 255
- d) 247**

71. What is the size of the key in the SDES algorithm?

- a) 24 bits
- b) 16 bits
- c) 20 bits
- d) 10 bits

72. Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K1?

- a) 10100100**
- b) 01011011
- c) 01101000
- d) 10100111

73. Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K2?

- a) 10100111
- b) 01000011**
- c) 00100100
- d) 01011010

74. AES uses a \_\_\_\_\_ bit block size and a key size of \_\_\_\_\_ bits.

- a) 128; 128 or 256
- b) 64; 128 or 192
- c) 256; 128, 192, or 256
- d) 128; 128, 192, or 256**

75. Like DES, AES also uses Feistel Structure.

- a) True
- b) False**

76. Which one of the following is not a cryptographic algorithm- JUPITER, Blowfish, RC6, Rijndael and Serpent?

- a) JUPITER**
- b) Blowfish
- c) Serpent
- d) Rijndael

77. How many rounds does the AES-192 perform?

- a) 10
- b) 12**
- c) 14
- d) 16

78. How many rounds does the AES-256 perform?

- a) 10
- b) 12
- c) 14**
- d) 16

79. What is the expanded key size of AES-192?

- a) 44 words
- b) 60 words
- c) 52 words**
- d) 36 words

80. The 4×4 byte matrices in the AES algorithm are called

- a) States**
- b) Words

- c) Transitions
- d) Permutations

81. In AES the  $4 \times 4$  bytes matrix key is transformed into a keys of size \_\_\_\_\_

- a) 32 words
- b) 64 words
- c) 54 words
- d) 44 words**

82. For the AES-128 algorithm there are \_\_\_\_\_ similar rounds and \_\_\_\_\_ round is different.

- a) 2 pair of 5 similar rounds ; every alternate
- b) 9 ; the last**
- c) 8 ; the first and last
- d) 10 ; no

83. Which of the 4 operations are false for each round in the AES algorithm

- i) Substitute Bytes
  - ii) Shift Columns
  - iii) Mix Rows
  - iv) XOR Round Key
- 
- a) i) only
  - b) ii) iii) and iv)**
  - c) ii) and iii)
  - d) only iv)

84. There is an addition of round key before the start of the AES round algorithms.

- a) True**
- b) False

85. How many computation rounds does the simplified AES consists of?

- a) 5
- b) 2**
- c) 8
- d) 10

86. On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function?

- a) f function
- b) permutation p
- c) swapping of halves**
- d) xor of subkey with

87. What is the key size in the S-AES algorithm?

- a) 16 bits**
- b) 32 bits
- c) 24 bits
- d) None of the mentioned

88. S-AES and S-DES were both developed by the same person as an educational cryptography system to teach students

- a) True**
- b) False

89. Which of the following is a faulty S-AES step function?

- a) Add round key
- b) Byte substitution**
- c) Shift rows
- d) Mix Columns

90. How many step function do Round 1 and 2 each have in S-AES?

- a) 4 and 3**
- b) Both 4
- c) 1 and 4
- d) 3 and 4

91. For a key 25D5 and PT input A479 what is the output we obtain after the “add round key” function?

- a) F34D
- b) 81AC**
- c) 79DF
- d) 327D

92. The output of the previous question, on passing through “nibble substitution” gets us the output

- a) 3267
- b) 1344
- c) 64C0**
- d) CA37

93. The output of the previous question on passing through the “shift row” step function gives us the output

- a) C046
- b) 0C64**
- c) 64C0

d) 640C

94. The output of the previous question on passing through the “mix columns” step function gives us the output

- a) 3252
- b) 3743
- c) 3425
- d) 3473**

95. How many round keys are generated in the AES algorithm?

- a) 11**
- b) 10
- c) 8
- d) 12

96. How many modes of operation are there in DES and AES?

- a) 4
- b) 3
- c) 2
- d) 5**

96. Which one of the following modes of operation in DES is used for operating short data?

- a) Cipher Feedback Mode (CFB)
- b) Cipher Block chaining (CBC)
- c) Electronic code book (ECB)**
- d) Output Feedback Modes (OFB)

97. Which of the following statements are true

- i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption
  - ii) The CTR mode does not require an Initialization Vector
  - iii) The last block in the CBC mode uses an Initialization Vector
  - iv) In CBC mode repetitions in plaintext do not show up in ciphertext
- a) iii)
  - b) ii) and iv)
  - c) All the Statements are true
  - d) i) ii) and iv)**

98. There is a dependency on the previous ‘s’ bits in every stage in CFB mode. Here ‘s’ can range from \_\_\_\_

- a) 8-16 bits
- b) 8-32 bits**

- c) 4-16 bits
- d) 8-48 bits

99. Which of the following can be classified under advantages and disadvantages of OFB mode?

- i) Transmission errors
  - ii) A bit error in a ciphertext segment
  - iii) Cannot recover from lost ciphertext segments
  - iv) Ciphertext or segment loss
- a) Advantages: None; Disadvantages: All
  - b) Advantages: All; Disadvantages: None
  - c) Advantages: i); Disadvantages: ii) iii) iv)
  - d) Advantages: i); ii) Disadvantages: iii) iv)**

100. In OFB Transmission errors do not propagate: only the current ciphertext is affected, since keys are generated “locally”.

- a) True**
- b) False

101. Which mode of operation has the worst “error propagation” among the following?

- a) OFB
- b) CFB
- c) CBC
- d) ECB**

102. Which block mode limits the maximum throughput of the algorithm to the reciprocal of the time for one execution?

- a) OFB
- b) CTR**
- c) CBC
- d) ECB

103. Which of the following is a natural candidates for stream ciphers?

- a) OFB**
- b) CFB
- c) CBC
- d) ECB

104. Use Caesar’s Cipher to decipher the following

HQFUBSWHG WHAW

- a) ABANDONED LOCK
- b) ENCRYPTED TEXT**
- c) ABANDONED TEXT
- d) ENCRYPTED LOCK

105. Caesar Cipher is an example of

- a) Poly-alphabetic Cipher
- b) Mono-alphabetic Cipher**
- c) Multi-alphabetic Cipher
- d) Bi-alphabetic Cipher

106. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.

- a) True
- b) False**

107. Confusion hides the relationship between the ciphertext and the plaintext.

- a) True
- b) False**

108. Which of the following ciphered text would have used transposition cipher for encryption of the plain text “SANFOUNDRY”?

- a) SSCMBNUMERY
- b) TBMGPVOESZ
- c) UCNHQWPFTA
- d) SNONRAFUDY**

109. What will be the encrypted text corresponding to plain text “SANFOUNDRY” using rail fence cipher with key value given to be 2?

- a) SNONRAFUDY**
- b) SORAFUDYNN
- c) SNAUDNORFY
- d) SANFOUNDRY

110. What will be the encrypted text corresponding to plain text “SANFOUNDRY” using columnar transposition cipher with the keyword as “GAMES”?

- a) SNONRAFUDY
- b) SORAFUDYNN
- c) SNAUDNORFY
- d) ANFRSUNDOY**

111.

## Unit 3

**1. In public key cryptosystem \_\_\_\_\_ keys are used for encryption and decryption.**

- a) Same
- b) Different**
- c) Encryption Keys
- d) None of the mentioned

**2. In public key cryptosystem which is kept as public?**

- a) Encryption keys**
- b) Decryption keys
- c) Encryption & Decryption keys
- d) None of the mentioned

**3.Which one of the following algorithm is not used in asymmetric-key cryptography?**

- a) rsa algorithm
- b) diffie-hellman algorithm
- c) electronic code book algorithm**
- d) dsa algorithm

**4.What is the objective of Diffie-Hellman key exchange?**

- A. To protect encrypted data from man-in-the-middle attack
- B. To perform mutual authentication on both sides
- C. To prove to another party that one holds a secret key without revealing it
- D. To establish a shared secret key on both sides**
- E. None of the above

**5.The security of RSA encryption relies on which assumption?**

- A. It is computationally infeasible to compute a GCD of two large numbers.
- B. It is computationally infeasible to factor a large number.**
- C. It is computationally infeasible to test whether a large number is prime.

D. It is computationally infeasible to compute a square modulo n.

E. All of the above

**7. The security of Diffie-Hellman key exchange relies on which assumption?**

A. It is computationally infeasible to compute a GCD of two large numbers.

B. It is computationally infeasible to compute an inverse modulo prime p.

C. It is computationally infeasible to test whether a large number is prime.

**D. It is computationally infeasible to solve the discrete log problem.**

E. All of the above

**8. RSA\_\_\_\_\_ be used for digital signature.**

a) Must no

b) Cannot

**c) Can**

d) Should not

**9. “Elliptic curve cryptography follows the associative property.”**

**a) True**

b) False

**10. “In ECC, the inverse of point P = $(x_1, y_1)$  is Q =  $(-x_1, y_1)$ . “**

a) True

**b) False**

2. If P = (1,4) in the elliptic curve E13(1, 1) , then 4P is

a) (4, 2)

b) (7, 0)

- c) (5, 1)
- d) (8, 1)

**11. Public key encryption/decryption is not preferred because**

- a) it is slow
- b) it is hardware/software intensive
- c) it has a high computational load
- d) all of the mentioned

**12. Message authentication is a service beyond**

- a. Message Confidentiality
- b. **Message Integrity**
- c. Message Splashing
- d. Message Sending

**13. In Message Confidentiality, the transmitted message must make sense to only intended**

- a. Receiver
- b. Sender
- c. Modulator
- d. Translator

**14. A hash function guarantees the integrity of a message. It guarantees that the message has not been**

- a. Replaced
- b. Overwritten
- c. **Changed**
- d. Violated

**15. To check the integrity of a message, or document, the receiver creates the**

a. Hash-Table

**b. Hash Tag**

c. Hyper Text

d. Finger Print

**16. A digital signature needs a**

a. Private-key system

b. Shared-key system

**c. Public-key system**

d. All of them

17. MAC stands for

**a. Message authentication code**

b. Message arbitrary connection

c. Message authentication control

d. Message authentication cipher

**18. The digest created by a hash function is normally called a**

**a. Modification detection code (MDC)**

b. Modify authentication connection

c. Message authentication control

d. Message authentication cipher

**19. Encryption and decryption provide secrecy, or confidentiality, but not**

a. Authentication

b. Integrity

c. Privacy

d. All of the above

**20. The subject unique identifier of the X.509 certificates was added in which version?**

a) 1

**b) 2**

c) 3

d) 4

**21. Which of the following is not an element/field of the X.509 certificates?**

a) Issuer Name

**b) Serial Modifier**

c) Issuer unique Identifier

d) Signature

**22. Suppose that A has obtained a certificate from certification authority X1 and B has obtained certificate authority from CA X2. A can use a chain of certificates to obtain B's public key. In notation of X.509, this chain is represented in the correct order as –**

a) X2 X1 X1 B

b) X1 X1 X2 A

**c) X1 X2 X2 B**

d) X1 X2 X2 A

**23. "Conveys any desired X.500 directory attribute values for the subject of this certificate."**

**Which Extension among the following does this refer to?**

a) Subject alternative name

b) Issuer Alternative name

**c) Subject directory attributes**

d) None of the mentioned

**24. SHA-1 has a message digest of**

**a. 160 bits**

- b. 512 bits
- c. 628 bits
- d. 820 bits

**25.The DSS signature uses which hash algorithm?**

- a. MD5
- b. SHA-2
- c. SHA-1**
- d. Does not use hash algorithm

**26.The RSA signature uses which hash algorithm?**

- a. MD5
- b. SHA-1
- c. MD5 and SHA-1**
- d. None of the mentioned.

**27.What is the size of the RSA signature hash after the MD5 and SHA-1 processing?**

- a. 42 bytes
- b. 32 bytes
- c. 36 bytes**
- d. 48 bytes

28) To authenticate the data origin, one needs a(n) \_\_\_\_\_.

- A) MDC
- B) MAC**
- C) either (a) or (b)
- D) neither (a) nor (b)

29) A(n) \_\_\_\_\_ can be used to preserve the integrity of a document or a message.

- A) message digest**
- B) message summary
- C) encrypted message
- D) none of the above.

30) A digital signature needs a(n) \_\_\_\_\_ system.

- A) symmetric-key
- B) asymmetric-key**
- C) either (a) or (b)
- D) neither (a) nor (b)

## Unit 4

**1. IPSec is designed to provide security at the \_\_\_\_\_**

- a) Transport layer
- b) Network layer**
- c) Application layer
- d) Session layer

**2. In tunnel mode, IPSec protects the \_\_\_\_\_**

- a) Entire IP packet**
- b) IP header
- c) IP payload
- d) IP trailer

**3. Which component is included in IP security?**

- a) Authentication Header (AH)
- b) Encapsulating Security Payload (ESP)
- c) Internet key Exchange (IKE)
- d) All of the mentioned**

**4. Which of the following is not applicable for IP?**

- a) Error reporting**
- b) Handle addressing conventions
- c) Datagram format
- d) Packet handling

**5. Which of the following field in IPv4 datagram is not related to fragmentation?**

- a) Flags
- b) Offset
- c) TOS**
- d) Identifier

**6. The size of an IP address in IPv6 is \_\_\_\_\_**

- a) 4bytes
- b) 128bits**
- c) 8bytes
- d) 100bits

**7. The header length of an IPv6 datagram is \_\_\_\_\_**

- a) 10bytes
- b) 25bytes
- c) 30bytes
- d) 40bytes**

**8.In an IPv6 header, the traffic class field is similar to which field in the IPv4 header?**

- a) Fragmentation field
- b) Fast switching
- c) TOS field**
- d) Option field

**9.I Pv6 does not use \_\_\_\_\_ type of address.**

- a) Broadcast**
- b) Multicast
- c) Any cast
- d) Unicast

**10.Which are the features present in IPv4 but not in IPv6?**

- a) Fragmentation
- b) Header checksum
- c) Options
- d) Anycast address**

**11.Teredo is an automatic tunneling technique. In each client the obfuscated IPv4 address is represented by bits \_\_\_\_\_**

- a) 96 to 127**
- b) 0 to 63
- c) 80 to 95
- d) 64 to 79

**12.Suppose two IPv6 nodes want to interoperate using IPv6 datagrams, but they are connected to each other by intervening IPv4 routers. The best solution here is \_\_\_\_\_**

- a) Use dual-stack approach
- b) Tunneling**
- c) No solution
- d) Replace the system

**13.The \_\_\_\_\_ field determines the lifetime of IPv6 datagram**

- a) Hop limit
- b) TTL**
- c) Next header
- d) Type of traffic

**14.This set of Computer Networks test focuses on “IPv6 Addressing”.**

**1. Dual-stack approach refers to \_\_\_\_\_**

- a) Implementing Ipv4 with 2 stacks
- b) Implementing Ipv6 with 2 stacks
- c) Node has both IPv4 and IPv6 support**
- d) Implementing a MAC address with 2 stacks

**15. Which mode of IPsec should you use to assure the security and confidentiality of data within the same LAN?**

- a) AH transport mode
- b) ESP transport mode**
- c) ESP tunnel mode
- d) AH tunnel mode

**16. Which two types of encryption protocols can be used to secure the authentication of computers using IPsec?**

- a) Kerberos V5
- b) SHA
- c) MD5
- d) Both SHA and MD5**

**17. \_\_\_\_\_ provides authentication at the IP level.**

- a) AH**
- b) ESP
- c) PGP
- d) SSL

**18. -----operates in the transport mode or the tunnel mode.**

- A) IPSec**
- B) SSL
- C) PGP
- D) none of the above.

**19. IKE creates SAs for \_\_\_\_\_.**

- A) SSL
- B) PGP
- C) IPSec**
- D) VP

**20.**provides either authentication or encryption, or both, for packets at the IP level.

A) AH

**B) ESP**

C) PGP

D) SSL

**21.**One security protocol for the e-mail system is \_\_\_\_\_.

A) IPSec

B) SSL

**C) PGP**

D) none of the above.

**22.** Typically, \_\_\_\_\_ can receive application data from any application layer protocol, but the protocol is normally HTTP.

A) SSL

B) TLS

C) either (a) or (b)

**D) both (a) and (b)**

**23.** IKE is a complex protocol based on \_\_\_\_\_ other protocols.

A) two

**B) three**

C) four

D) five

**24.**IPSec defines two protocols: \_\_\_\_\_ and \_\_\_\_\_.

- A) AH; SSL
- B) PGP; ESP
- C) AH; ESP**
- D) all of the above

**25. In the \_\_\_\_\_ mode, IPSec protects information delivered from the transport layer to the network layer.**

- A) transport**
- B) tunnel
- C) either (a) or (b)
- D) neither (a) nor (b)

**26. SSL provides \_\_\_\_\_.**

- A) message integrity
- B) confidentiality
- C) compression
- D) all of the above**

**27. \_\_\_\_\_ is a collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level.**

- A) IPSec**
- B) SSL
- C) PGP
- D) none of the above

**28. IKE uses \_\_\_\_\_.**

- A) Oakley**

- B) SKEME
- C) ISAKMP
- D) all of the above**

**29.** IPSec uses a set of SAs called the \_\_\_\_\_.

- A) SAD
- B) SAB
- C) SADB**
- D) none of the above

**30.** In \_\_\_\_\_, there is a single path from the fully trusted authority to any certificate.

- A) X509**
- B) PGP
- C) KDC
- D) none of the above

**31.** The combination of key exchange, hash, and encryption algorithms defines a \_\_\_\_\_ for each SSL session.

- A) list of protocols
- B) cipher suite**
- C) list of keys
- D) none of the above.

**32.** uses the idea of certificate trust levels.

- A) X509
- B) PGP**

- C) KDC
- D) none of the above

**33.---- is designed to provide security and compression services to data generated from the application layer.**

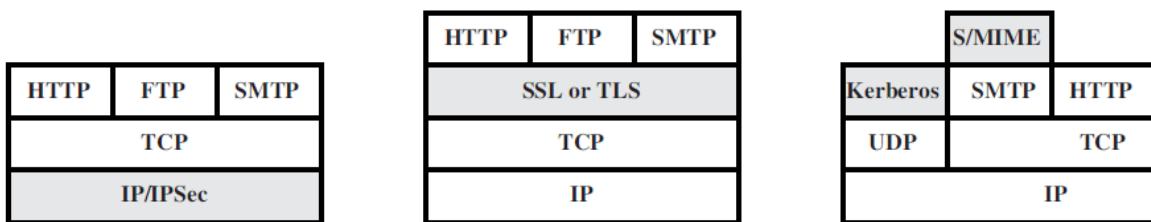
- A) SSL
- B) TLS
- C) either (a) or (b)
- D) both (a) and (b)**

**34.----was invented by Phil Zimmerman.**

- A) IPSec
- B) SSL
- C) PGP**
- D) none of the above

**35.In PGP, to exchange e-mail messages, a user needs a ring of \_\_\_\_\_ keys.**

- A) secret
- B) public**
- C) either (a) or (b)
- D) both (a) and (b)



In the above figure from left to right, the correct order of the shaded levels are

- a) Network level, Application level, Transport level
- b) Application level, Network level, Transport level
- c) Transport level, Application level, Network level
- d) Network level, Transport level, Application level**

**36. In the above figure, which of the above shaded block is transparent to end users and applications?**

- a) IP/IPSec
- b) SSL
- c) Kerberos
- d) S/MIME**

**37. In terms of Web Security Threats, “Impersonation of another user” is a Passive Attack.**

- a) True
- b) False**

**38. Which one of the following is not a higher –layer SSL protocol?**

- a) Alert Protocol
- b) Handshake Protocol
- c) Alarm Protocol**
- d) Change Cipher Spec Protocol.

**39. In the SSL Protocol, each upper layer message is fragmented into a maximum of \_\_\_\_\_ bytes.**

- a)  $2^{16}$
- b)  $2^{32}$
- c)  $2^{14}$**
- d)  $2^{12}$

**40. The difference between HMAC algorithm and SSLv3 is that pad1 and pad2 are \_\_\_\_\_ in SSLv3 whereas \_\_\_\_\_ in HMAC.**

- a) NANDed, XORed
- b) Concatenated, XORed**
- c) XORed, NANDed
- d) XORed, Concatenated.

**41. The full form of SSL is**

- a) Serial Session Layer

- b) Secure Socket Layer**
- c) Session Secure Layer
- d) Series Socket Layer

**42.After the encryption stage in SSL, the maximum length of each fragment is**

- a)  $2^{14}+1028$
- b)  $2^{14}+2048$**
- c)  $2^{16}+1028$
- d)  $2^{16}+2048$

**43.Which protocol is used to convey SSL related alerts to the peer entity?**

- a) Alert Protocol**
- b) Handshake Protocol
- c) Upper-Layer Protocol
- d) Change Cipher Spec Protocol.

**44.Which of the following are possible sizes of MACs?**

- i) 12 Bytes**
- ii) 16 Bytes**
- iii) 20 Bytes**
- iv) 24 Bytes**

- a) i and iii
- b) ii only
- c) ii and iii**
- d) ii iii and iv

**45.Pretty good privacy (PGP) security system uses**

- a) Public key cryptosystem
- b) Private key cryptosystem
- c) Public & Private key cryptosystem**
- d) None of the mentioned

**46.Public key cryptosystem is used for the encryption of**

- a) Messages
- b) Session key**

- c) Session key & Messages
- d) None of the mentioned,

**47. PGP offers \_\_\_\_\_ block ciphers for message encryption.**

- a) Triple-DES
- b) CAST
- c) IDEA
- d) All of the mentioned**

**48. Which operation is used in encryption using IDEA?**

- a) Addition modulo 2<sup>16</sup>
- b) Bit wise XOR
- c) Addition modulo 2<sup>16</sup> & Bit wise XOR**
- d) None of the mentioned

**49.DSA protocol is based on**

- a) Discrete logarithm problem**
- b) Continuous logarithm problem
- c) Discrete & Continuous logarithm problem
- d) None of the mentioned

**50.Digest created by a hash function is normally called a**

- A.modification detection code (MDC).**
- B.message authentication connection.
- C.message authentication control.
- D.message authentication cipher.

**51.Message digest needs to be**

- A.public.
- B.private.
- C.kept secret.**
- D.None.

**52.In Message Integrity, SHA-I hash algorithms create an N-bit message digest out of a message of**

- A.512 Bit Blocks.**
- B.1001 Bit Blocks.
- C.1510 Bit Blocks.
- D.2020 Bit Blocks.

**53.One of protocols to provide security at application layer is**

- A.Pretty Good Privacy.**
- B.Handshake Protocol.
- C.Alert Protocol.
- D.Record Protocol.

- 54.S/MIME is abbreviated as \_\_\_\_\_**
- a) Secure/Multimedia Internet Mailing Extensions
  - b) Secure/Multipurpose Internet Mailing Extensions
  - c) Secure/Multimedia Internet Mail Extensions
  - d) Secure/Multipurpose Internet Mail Extensions**

**55.Users are able to see a pad-lock icon in the address bar of the browser when there is \_\_\_\_\_ connection.**

- a) HTTP
- b) HTTPS**
- c) SMTP
- d) SFTP

**56.Why did SSL certificate require in HTTP?**

- a) For making security weak
- b) For making information move faster
- c) For encrypted data sent over HTTP protocol**
- d) For sending and receiving emails unencrypted.

**57.In SSL, what is used for authenticating a message?**

- a) MAC (Message Access Code)
- b) MAC (Message Authentication Code)**
- c) MAC (Machine Authentication Code)
- d) MAC (Machine Access Code)

**58.in the SSL record protocol operation pad\_1 is –**

- a) is the byte 0x36 repeated 40 times for MD5
- b) is the byte 0x5C repeated 40 times for MD5
- c) is the byte 0x5C repeated 48 times for SHA-1
- d) is the byte 0x36 repeated 48 times for MD5**

**59.In the Handshake protocol action, which is the last step of the Phase 2 : Server Authentication and Key Exchange?**

- a) server\_done**
- b) server\_key\_exchange
- c) certificate\_request
- d) crtificate\_verify

**60.A digital signature is**

- a. a bit string giving identity of a correspondent
- b. a unique identification of a sender
- c. an authentication of an electronic record by tying it uniquely to a key only**

a sender knows

- d. an encrypted signature of a sender

**61.A digital signature is required**

- (i) to tie an electronic message to the sender's identity
  - (ii) for non repudiation of communication by a sender
  - (iii) to prove that a message was sent by the sender in a court of law
  - (iv) in all e-mail transactions
- a. i and ii
  - b. i, ii, iii
  - c. i, ii, iii, iv
  - d. ii, iii, iv

**62.The certificate message is required for any agreed-on key exchange method except**

- a) Ephemeral Diffie-Hellman
- b) Anonymous Diffie-Hellman**
- c) Fixed Diffie-Hellman
- d) RSA

**63.Hashed message is signed by a sender using**

- a. his public key
- b. his private key**
- c. receiver's public key
- d. receiver's private key

**64.The responsibility of a certification authority for digital signature is to  
authenticate the**

- a. hash function used
- b. private keys of subscribers
- c. public keys of subscribers**

d. key used in DES

**65.The Secure Electronic Transaction protocol is used for**

- a. credit card payment
- b. cheque payment
- c. electronic cash payments
- d. payment of small amounts for internet services

**66.In SET protocol a customer encrypts credit card number using**

- a. his private key
- b. bank's public key**
- c. bank's private key
- d. merchant's public key

**67.In SET protocol a customer sends a purchase order**

- a. encrypted with his public key
- b. in plain text form
- c. encrypted using Bank's public key
- d. using digital Signature system**

**68.One of the problems with using SET protocol is**

- a. the merchant's risk is high as he accepts encrypted credit card
- b. the credit card company should check digital signature
- c. the bank has to keep a database of the public keys of all customers**
- d. the bank has to keep a database of digital signatures of all customers

## Unit V Firewall And Intrusion

1. Network layer firewall works as a \_\_\_\_\_

- a) Frame filter
- b) Packet filter**
- c) Content filter
- d) Virus filter

2. Network layer firewall has two sub-categories as \_\_\_\_\_

- a) State full firewall and stateless firewall**
- b) Bit oriented firewall and byte oriented firewall
- c) Frame firewall and packet firewall
- d) Network layer firewall and session layer firewall

3. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as \_\_\_\_\_

- a) Chock point**
- b) Meeting point
- c) Firewall point
- d) Secure point

4. Which of the following is / are the types of firewall?

- a) Packet Filtering Firewall**
- b) Dual Homed Gateway Firewall
- c) Screen Host Firewall
- d) Dual Host Firewall

5. A proxy firewall filters at \_\_\_\_\_

- a) Physical layer
- b) Data link layer
- c) Network layer
- d) Application layer**

6. A packet filter firewall filters at \_\_\_\_\_

- a) Physical layer
- b) Data link layer
- c) Network layer or Transport layer**
- d) Application layer

7. What is one advantage of setting up a DMZ with two firewalls?

- a) You can control where traffic goes in three networks
- b) You can do stateful packet filtering
- c) You can do load balancing**
- d) Improved network performance

8. What tells a firewall how to reassemble a data stream that has been divided into packets?

- a) The source routing feature**
- b) The number in the header's identification field
- c) The destination IP address
- d) The header checksum field in the packet header

9. A stateful firewall maintains a \_\_\_\_\_ which is a list of active connections.

\*\* Verify Correct Answer\*\*

- a) Routing table**
- b) Bridging table
- c) State table
- d) Connection table

10. A firewall needs to be \_\_\_\_\_ so that it can grow proportionally with the network that it protects.

- a) Robust
- b) Expansive**
- c) Fast
- d) Scalable

11 A firewall needs to be \_\_\_ so that it can grow with the network it protects.

- A. Robust
- B. Expensive
- C. Fast
- D. Scalable**

12. A(n) \_\_\_ is a fancy term for a computer that has two network interfaces.

- A. Proxy gateway
- B. Dual-homed host**
- C. Routing workstation
- D. NAT server

13. A(n) \_\_\_\_ host is sometimes called a dual-homed gateway or bastion host.

- A. Proxy
- B. Stub
- C. Screened**
- D. Blocked

14. The \_\_\_\_ server in the DMZ needs only list a limited number of public IP addresses.

- A. DNS**
- B. NAT
- C. Proxy
- D. Firewall

15. A(n) \_\_\_\_ server is a server that creates a secure tunnel connection.

- A. RADIUS
- B. VPN**
- C. Tunnel
- D. Authentication

16. What is one advantage of setting up a DMZ with two firewalls?

Discuss

- A. You can control where traffic goes in the three networks**

- B. You can do stateful packet filtering
- C. You can do load balancing
- D. Improved network performance

**17.** A system that monitors traffic into and out of a network and automatically alerts personnel when suspicious traffic patterns occur, indicating a possible unauthorized intrusion attempt is called a(n) \_\_\_\_\_.

- A. IDS**
- B. Firewall
- C. Router
- D. Anti-virus software

**18.** In an IP packet header, the \_\_\_ is the address of the computer or device that is to receive the packet.

- A. Source address
- B. Flag
- C. Destination address**
- D. Total length

**19.** In an IP packet header, the \_\_\_ describes the length of the header in 32-bit words and is a 4-bit value.

- A. Internet header length**
- B. Fragment offset
- C. Total length
- D. Header checksum

**20.** What tells a firewall how to reassemble a data stream that has been divided into packets?

- A. The source routing feature
- B. The number in the header's identification field
- C. The destination IP address
- D. The header checksum field in the packet header**

**21.** What is the most effective security approach for a stateless packet filter?

- A. Deny all except specified hosts**
- B. Allow all except specified hosts
- C. Allow access to only specified destination servers
- D. Deny access to all destinations except specified servers

**22.** What TCP port is used by Telnet?

- A. 80
- B. 110
- C. 23**
- D. 72

**23.** What TCP port is used to filter out Web traffic?

- A. 25
- B. 21
- C. 23
- D. 80**

**24.** Some \_\_\_ firewalls are able to examine the contents of packets as well as the headers for signs that they are legitimate.

A. Boundary

**B. Stateful**

C. Stateless

D. Personal

**25.** What is the most common command to use ICMP?

**A. Ping**

B. Trace

C. Netstat

D. NBTstat

**26.** What port does secure HTTP use?

A. 8080

B. 224

C. 442

**D. 443**

**27.** What port does DNS use for connection attempts?

A. 68

B. 21

**C. 53**

D. 56

**28.** FTP uses port \_\_\_\_ for the control port.

A. 20

**B. 21**

C. 22

D. 23

**29.**

A datagram is called \_\_\_\_\_ at the network layer of OSI.

A. Bits

B. Segments

C. Frames

**D. Packets**

**30.** A \_\_\_\_\_-level proxy provides protection at the session layer of OSI.

A. Application

**B. Circuit**

C. Proxy

D. Server

**31.** \_\_\_\_\_ is an error-checking procedure performed in the trailer section of an IP packet.

**A. CRC**

B. ACK

C. FQDN

D. FIN

**32.** This 8-bit value identifies the maximum time the packet can remain in the system before it is dropped.

A. Fragment

**B. Time to live**

C. Protocol

D. Checksum

**33.** Zone Alarm is an example of a \_\_\_\_\_ firewall.

**A. Personal**

B. Corporate

C. IDS

D. None of the above

**34.** \_\_\_\_\_ is another term for a packet of digital information.

A. Footer

B. Header

C. Data

**D. Datagram**

**35** The practice of designing operational aspects of a system to work with a minimal amount of system privilege is called \_\_\_\_\_.

**A. Least privilege**

B. Failover firewall

C. IP forwarding

D. Access denied

**35 Firewall is ?**

a hardware

a software

can be a hardware as well as software

can neither be a hardware nor a software

**Answer:** Option C

**36 When configuring a firewall to deny port 3389 to a RDP server that is to receive the SYN packet, what is the address?**

- A. Flag
- B. Destination
- C. Source
- D. Connected

Ans: B

**37 Which of the following firewalls keeps track of the state of network connections ?**

- A. Static filtering
- B. Stateless inspection
- C. Stateful inspection
- D. Dynamic Filtering

Ans: C

**38 What is the primary purpose of a firewall?**

- A. Enables fast forwarding
- B. Route frames
- C. Route hot packets
- D. Inspect packets

Ans: D

**39 Your customer asks you to allow ALL hosts from the Internet to company's secure webserver (Secure HTTP), what port do you open on the firewall?**

- A. 23
- B. 22
- C. 443

D. 43

Ans: C

40 Which of the following is not a recognized generation of Firewall?

A. First Generation

B. Third Generation

C. DMZ

D. Second generation

Ans: C

41 What device logically filters traffic at the edge of a computer network and the Internet?

A. Switch

B. Firewall

C. Router

D. Hub

Ans: B

42 Which of the following is TRUE?

A. The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices

B. All of the given options are correct

C. Firewalls can be categorized by processing mode, development era, or structure

D. Firewalls categorized by which level of technology they employ are identified by generation, with the later generations being more complex and more recently developed

Ans: B

43 You want to filter all traffic going to an internal web server from the Internet side of the firewall, what port will you filter on the firewall?

A. 8080

B. 80

C. 21

D. 25

Ans: B

44 Which of the following firewalls works at the application level?

A. Packet filtering firewall

B. application-level firewalls

C. circuit firewall

D. MAC layer firewalls

Ans: B

45 What application controls what information is transmitted or received from an external source destined to a server, workstation, or computer that is based on a preset of rules and/or user preferences?

A. Server

B. Repeater

C. Router

D. Firewall

Ans: D

46 What is a host based firewall?

A. Software firewall installed on a server/workstation/desktop

B. A proxy server configured to handle http requests

C. A device that is installed by your Internet Service Provider

D. A Firewall connected directly to the Network Interface Card of a Computer

Ans: A

47 When referring to firewall concepts, what are application level gateways?

A. HTTP servers

B. Proxy servers

C. IP Servers

D. HTTP servers

Ans: B

48 Which of the following is not a VALID basic criteria for rule in the firewall policy?

A. Destination

- B. User
- C. Service
- D. Source

Ans: B

49 When referring to firewalls, what does SPI Stand for?

- A. Stateless Packet Inspection
- B. Shared Packet Interconnection
- C. Stateful Packet Inspection
- D. Source Packet Information

Ans: C

50 Which particular firewall usually consists of two separate firewall devices?

- A. Application –level firewall
- B. MAC layer firewalls
- C. Hybrid Firewall
- D. Dynamic Filtering

Ans: C

51 What main attributes are used at layer 4 of the OSI model to filter traffic on a firewall?

- A. Frames and packets

- B. Source and/or destination IP Addresses
- C. Source and/or destination TCP/UDP ports
- D. ICMP and IP

Ans: C

52 When packets are being processed by a hardware firewall, one of the several steps in processing the packets is an error-checking procedure that is performed in the trailer section of an IP Packet, this is called what?

- A. IFG
- B. IPC (IP Check)
- C. CRC
- D. FQDN

Ans: C

53 The basic concept of a SYN flooding attack lies in the design of what handshake that begins a TCP connection?

- A. 4-way
- B. 2-way
- C. TCP
- D. 3-way

Ans: D

54What it is called when a packet arrives at a firewall, gets analyzed and determines that no connection exists and the packet is dropped?

- A. Stateful Packet Inspection
- B. Connection Oriented Inspection
- C. Stateless Packet Inspection
- D. Stateful Frame Inspection

Ans: A

55What technology is used on firewalls that process stateful packet inspections at the hardware level and as close to the line rate as possible?

- A. ACL
- B. ASIC
- C. Intel
- D. SPI

Ans: B

56 True/False: Application proxy firewalls are faster than Stateful Packet Inspection firewalls.

- A. False
- B. True

Ans: A

57What device should be the front line defense in your network?

- A. Network Layer Firewalls
- B. Application Based Firewalls
- C. Packet Filtering Firewalls
- D. Stateful Packet Inspection firewall

Ans: D

58What kind of firewall is the integrated Microsoft Windows firewall application?

- A. Stateful
- B. Stateless
- C. Zone Based
- D. Connection oriented firewall

Ans: A

59 What is a Cisco Access Control List (ACL) considered as?

- A. Controlled
- B. Stateful
- C. Stateless
- D. NAT

Ans: C

60 Which generation firewalls are stateful inspection firewalls?

A. Second generation

B. First Generation

C. Fourth Generation

D. Third Generation

Ans: D

61 What layer of the OSI model do Circuit Layer Firewalls operate at?

A. Application Layer

B. Session Layer

C. Transport Layer

D. Network Layer

Ans: B

62 Which of the following is an INVALID common architectural implementation of firewall?

A. packet filtering routers

B. Dynamic Filtering

C. dual-homed firewalls

D. screened host firewalls

Ans: B

63 A \_\_\_\_\_ is a device that forwards packets between networks by processing the routing information included in the packet. a) bridge b) firewall c) router d) all of the mentioned View Answer Answer:c

## IDS

1. What are the different ways to intrude?

- a) Buffer overflows
- b) Unexpected combinations and unhandled input
- c) Race conditions
- d) All of the mentioned**

2. What are the major components of the intrusion detection system?

- a) Analysis Engine
- b) Event provider
- c) Alert Database
- d) All of the mentioned**

3. What are the different ways to classify an IDS?

- a) anomaly detection
- b) signature based misuse
- c) stack based
- d) all of the mentioned**

4. What are the different ways to classify an IDS?

- a) Zone based**
- b) Host & Network based**
- c) Network & Zone based
- d) Level based

**5. What are the characteristics of anomaly based IDS?**

- a) It models the normal usage of network as a noise characterization
- b) It doesn't detect novel attacks
- c) Anything distinct from the noise is not assumed to be intrusion activity
- d) It detects based on signature

**6. What is the major drawback of anomaly detection IDS?**

- a) These are very slow at detection
- b) It generates many false alarms
- c) It doesn't detect novel attacks
- d) None of the mentioned

**7. What are the characteristics of signature based IDS?**

- a) Most are based on simple pattern matching algorithms
- b) It is programmed to interpret a certain series of packets
- c) It models the normal usage of network as a noise characterization
- d) Anything distinct from the noise is assumed to be intrusion activity

**8. What are the drawbacks of signature based IDS? \* Verify\***

- a) They are unable to detect novel attacks
- b) They suffer from false alarms
- c) They have to be programmed again for every new pattern to be detected
- d) All of the mentioned

**9. What are the characteristics of Host based IDS?**

- a) The host operating system logs in the audit information
- b) Logs includes logins,file opens and program executions
- c) Logs are analysed to detect tails of intrusion
- d) All of the mentioned

**10. What are the drawbacks of the host based IDS?**

- a) Unselective logging of messages may increase the audit burdens
- b) Selective logging runs the risk of missed attacks
- c) They are very fast to detect
- d) They have to be programmed for new patterns

**11. What are the strengths of the host based IDS?**

- a) Attack verification
- b) System specific activity
- c) No additional hardware required
- d) All of the mentioned

**12. What are characteristics of stack based IDS?**

- a) They are integrated closely with the TCP/IP stack and watch packets**
- b) The host operating system logs in the audit information
- c) It is programmed to interpret a certain series of packets
- d) It models the normal usage of network as a noise characterization

13. What are characteristics of Network based IDS?

- a) They look for attack signatures in network traffic**
- b) Filter decides which traffic will not be discarded or passed
- c) It is programmed to interpret a certain series of packet
- d) It models the normal usage of network as a noise characterization

14. What are strengths of Network based IDS?

- a) Cost of ownership reduced
- b) Malicious intent detection
- c) Real time detection and response
- d) All of the mentioned**

15 Which of the following is an advantage of anomaly detection?

- a. Rules are easy to define.**
- b. Custom protocols can be easily analyzed.
- c. The engine can scale as the rule set grows.
- d. Malicious activity that falls within normal usage patterns is detected.

16 A method used by an IDS that involves checking for a pattern to identify unauthorized activity

- A. CORRECT: Pattern Matching**
- B. Session Splicing
- C. Protocol Decoding
- D. State Table

17 A list or table of stored by a router (or switch) that controls access to and from a network.

- 1. State Table
- 2. CORRECT: Access Control List (ACL)**
- 3. Session Splicing

#### 4. Packet Filter

18 An analysis method used by some IDS that looks for instances that are not considered normal behavior.

1. Stateful Inspection
2. **CORRECT: Anomaly Detection**
3. Evasion
4. Pattern Matching

19 Bypassing a device, or performing another action, to attack or place malware on a target network without being detected.

- a. Packet Filter
- b. State Table
- c. **CORRECT: Evasion**
- d. Honeypot

20 A type of firewall closely related to a packet filter that can track the status of a connection through use of a state table that keeps track of connection activities.

1. Anomaly Detection
2. Protocol Decoding
3. **CORRECT: Stateful Inspection**
4. State Table

**21** A tool that uses the monitoring of network traffic, detection of unauthorized access attempts, and notification of unauthorized access attempts to network administrator.

1. Anomaly Detection
2. Access Control List (ACL)
3. **CORRECT: Intrusion Detection System (IDS)**
4. Session Splicing

**22** A type of stateless inspection used in some routers and firewalls to limit flow of traffic to what is on the ACL.

1. **CORRECT: Packet Filter**
2. Proxy Server
3. Evasion
4. State Table

**23** A way of looking at raw packet data.

1. Proxy Server
2. Session Splicing
3. **CORRECT: Protocol Decoding**
4. Pattern Matching

**24** A server (or application) that intercepts the requests clients make of another server, fills the requests that it can, and then forwards the requests it can't handle on to the other server thus helping to improve performance and security.

1. Honeypot
2. **CORRECT: Proxy Server**
3. Packet Filter

#### 4. State Table

25 A table in which data about connection activity is kept by a stateful firewall.

1. Evasion
2. **CORRECT: State Table**
3. Honeypot
4. Proxy Server

26 Something set up on a separate network (or in DMZ) to attract hackers and lure them away from the real network; it logs keystrokes, provides other information about an attacker, and also provides warning that someone is trying to attack your network.

1. Proxy Server
2. State Table
3. Evasion
4. **CORRECT: Honeypot**

27 A way to change network address information in IP packet headers with a router by connecting multiple computers using one IP address connected to the Internet (or IP network) to convert many private addresses into one public address.

1. Access Control List (ACL)
2. **CORRECT: Network Address Translation (NAT)**
3. Anomaly Detection
4. Intrusion Detection System (IDS)

**28 A method of avoiding detection by an IDS by sending portions of a request in different packets.**

1. **CORRECT: Session Splicing**
2. Protocol Decoding
3. Pattern Matching
4. Evasion

**What are characteristics of signature based IDS ?**

- a. Most are based on simple pattern matching algorithms
- b. It is programmed to interpret a certain series of packets
- c. It models the normal usage of network as a noise characterization
- d. Anything distinct from the noise is assumed to be intrusion activity