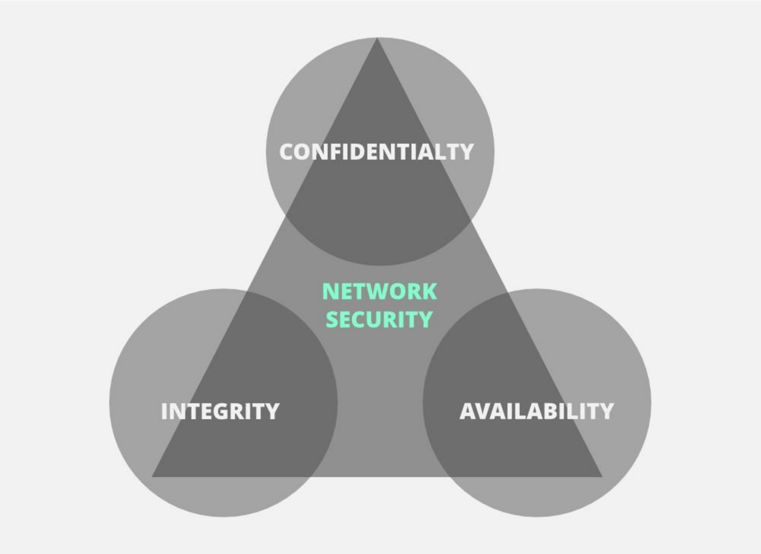
Network Security Question Bank

Chapter 1

▼ Q.1 Explain information security with its merits and demerits.

1. Security is defined as: "*The quality or state of being secure – to be free from danger*".
2. Information security protects sensitive information from unauthorized activities. It is the protection of data saved to a network or hard drive.
3. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

- The 3 principles of Information Security:



1. **Confidentiality**: Its measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private.
2. **Integrity**: The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly.
3. **Availability**: Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a

specified time).

1. Components of Information Security are: i) Software ii) Hardware iii) Data iv) People v) Procedures vi) Network

Merits and Demerits of Information Security:

Advantages	Disadvantages
It protects the data the organization collects and uses.	Since technology is always changing nothing will ever be completely secure.
It is easy to use.	It can be extremely complicated.
Information security protects users valuable information both while in use and while it is being stored.	

▼ Q.2 Compare and contrast the current scenario and the past scenario of information and network security.

Information Security	Network Security
It protects information from unauthorized users, access, and data modification.	It protects the data flowing over the network.
It is a superset of cyber security and network security.	It is a subset of cyber security.
It deals with the protection of data from any form of threat.	It deals with the protection from DOS attacks.
It deals with information assets and integrity, confidentiality, and availability.	It secures the data traveling across the network terminals.

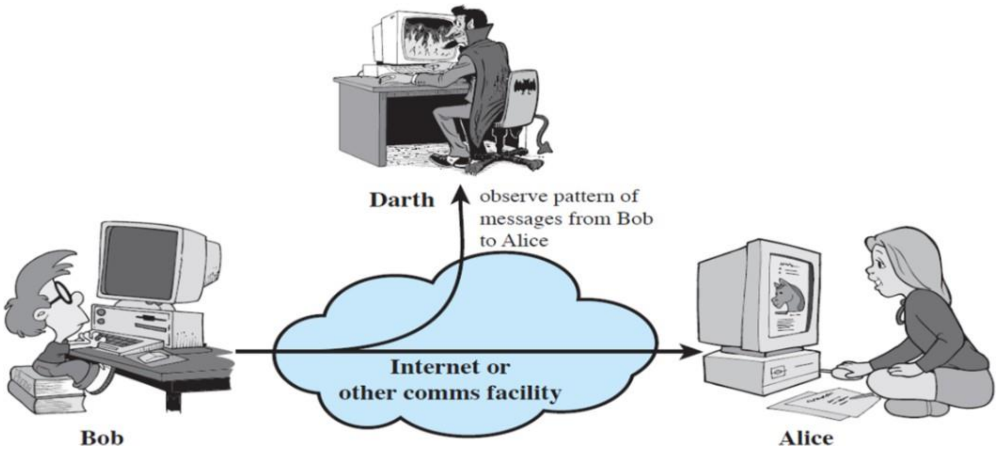
▼ Q.3 What are the different types of attack? Explain any one attack with a case scenario.

There are two types of attack:

Active Attack	Passive Attack
Involves modification of the data stream or creation of a false stream.	The goal is to obtain information that is being transmitted.
In an active attack, the attacker tries to bypass or break into secured systems.	It can only be through the Interception.
Active attacks can be through Interruption, Modification, or Fabrication.	E.g. Release of confidential information, Traffic analysis, etc.

Active Attack	Passive Attack
E.g. message modification, and denial of services.	

Case Scenario: Traffic analysis


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

1. Traffic analysis refers to obtaining information by monitoring online traffic.
2. Done by Packet sniffers (Packet analyzer).
3. For example: enables attackers to see upcoming actions.
4. It is an Attack on Confidentiality.

▼ Q.4 Explain the purpose of information security.

Answer same as Q.1

▼ Q.5 What is e-commerce? What are the types of e-commerce? How are e-commerce security measures?

Ecommerce (electronic commerce) refers to all online activity/transactions that involves the buying and selling of products and services.

Types:

1. **B2C** (Business to Consumer): Refers to selling goods or services to individual customers.
2. **B2B** (Business to Business): Refers to selling products or services to businesses.
3. **D2C** (Direct to Consumer): It is similar to B2C in that the end customer is an individual consumer, but differs in that it gives manufacturers, without involvement of third-party.

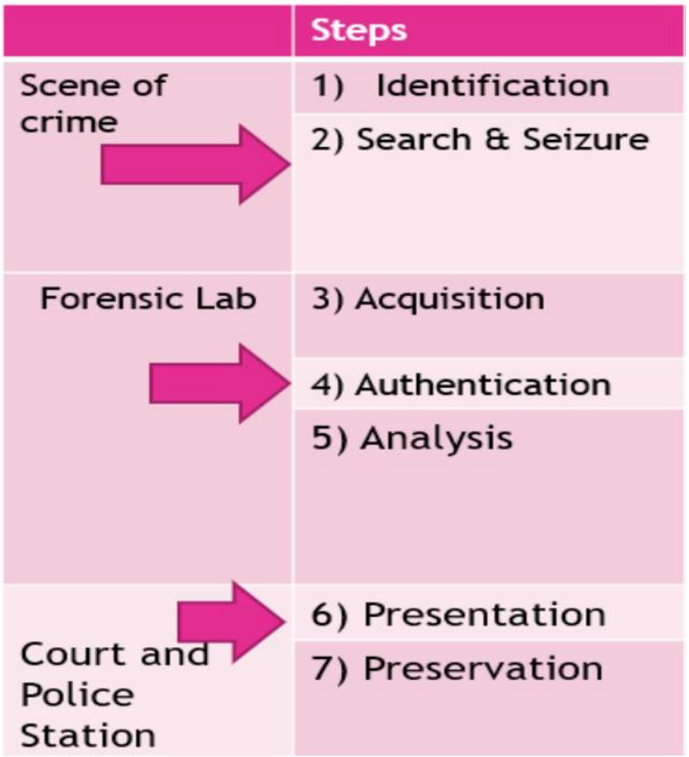
E-Commerce security is the protection of e-commerce assets from unauthorized access, destruction and alteration in the data.

Following characteristics/dimensions must be verified in e-commerce transactions:

1. **Integrity**: prevention against unauthorized data modification.
2. **Non-repudiation**: prevention against any one party from reneging on an agreement after the fact.
3. **Authenticity**: authentication of data source.
4. **Confidentiality**: protection against unauthorized data disclosure.
5. **Privacy**: provision of data control and disclosure.
6. **Availability**: prevention against data delays or removal.

▼ Q.6 Explain computer forensics with the process that the investigation takes place.

1. Computer Forensics is a scientific technique of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body.
2. It is also called digital or cyber forensic.
3. Digital evidence includes computer evidence, laptop, i-pad, hard disc, digital audio recorder, video recorder, CCTV mobile phones, etc.
4. Process involves:
    a. **Identification**: Identifying what evidence is present, where it is stored , and how it is stored(in which format).
    b. **Preservation**: Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.
    c. **Analysis**: Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
    d. **Documentation**: A record of all the visible data is created. All the findings from the investigations are documented.
    e. **Presentation**: All the documented findings are produced in a court of law for further investigations.



	Steps
Scene of crime	1) Identification
	2) Search & Seizure
Forensic Lab	3) Acquisition
	4) Authentication
	5) Analysis
Court and Police Station	6) Presentation
	7) Preservation

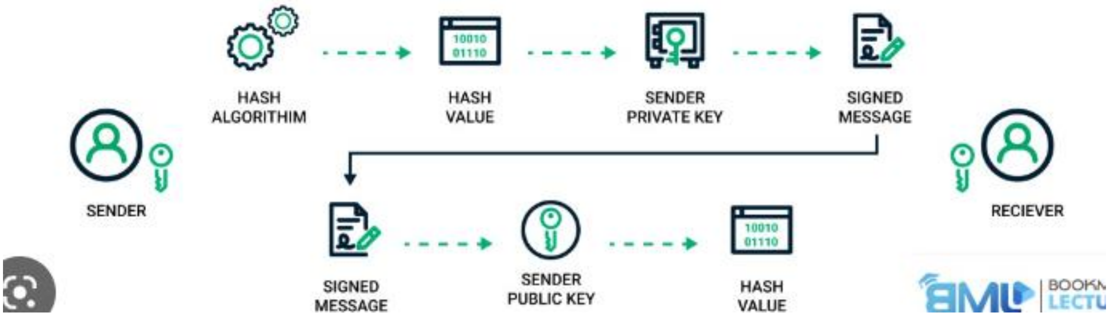
▼ Q.7 Write notes on steganography and digital signature.

Steganography:

1. Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination.
2. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.
3. E.g. Hidden messages on a paper written in secret inks

Digital Signature:

1. A digital signature is a cryptographic output used to verify the authenticity of data.
2. A digital signature algorithm allows for two distinct operations: a signing operation, which uses a signing key to produce a signature over raw data.
3. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.
4. The digital signature must have the following properties:
    a. It must verify the author and the date and time of the signature.
    b. It must authenticate the contents at the time of the signature.
    c. It must be verifiable by third parties, to resolve disputes.



Chapter 2

▼ Q.1 Explain cryptography with different terminologies used in cryptography systems.

Cryptography is derived from a Greek word called “crypto’s” which means “Hidden Secrets”.

‘Crypto’ means secret or hidden. Cryptography is the science of secret writing with the intention of keeping the data secret.

Terminologies used in Cryptography:

1. **Cryptanalysis**: It a technique of decoding of messages from a non-readable format back to readable format without knowing how they were initially knowing converted from readable format to non-readable format.

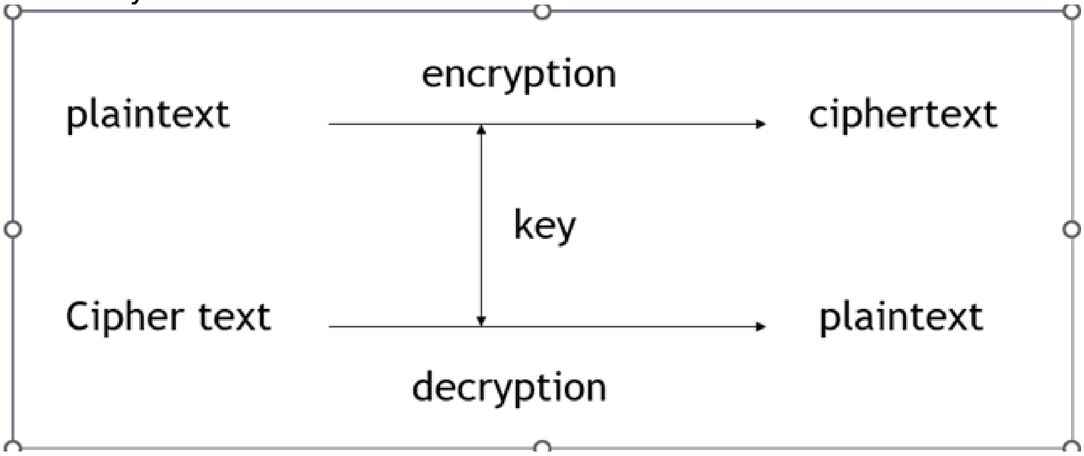
2. **Cryptology**: Is a combination of cryptography and cryptanalysis.
3. **Plain Text**: It is the data to be protected during transmission.
4. **Encryption**: It is a mathematical process that produces a ciphertext for any given plaintext and encryption key.
5. **Cipher Text**: It is the result of encryption performed on plaintext using an algorithm, called a cipher.
6. **Decryption**: It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key.
7. **Encryption Key**: It is a value that is known to the sender.
8. **Decryption Key**: It is a value that is known to the receiver.
9. **Key** is the secret piece of information which is used for encryption and decryption in cryptography.

▼ Q.2 What are the advantages of a cryptographic system?

1. **Confidentiality**: Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private.
2. **Integrity**: The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly.
3. **Availability**: Availability is the protection of a system’s ability to make software systems and data fully available when a user needs it (or at a specified time).

▼ Q.3 What are the different functions of the cryptographic system?

1. Secret key functions:



   a. Uses a single key for encryption/decryption.

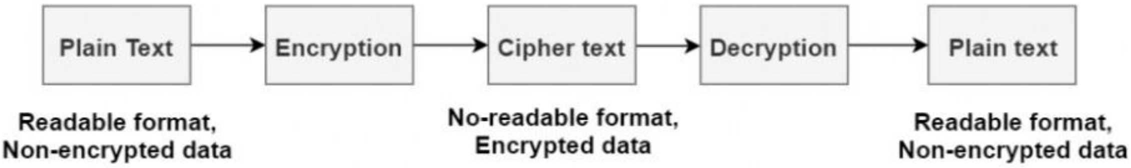
b. It is an encryption system where the sender and receiver of message uses a single common key to encrypt and decrypt messages.

2. Public key functions:
    a. There is no usage of any key in this algorithm.

    b. Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption.

3. Hash functions:
    a. Under this system a pair of keys is used to encrypt and decrypt information.
    b. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different.
    c. There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text.
    d. Many operating systems use hash functions to encrypt passwords.

Q.4 ▼ Explain architecture of cryptography?



▼ Q.5 Explain applications of cryptography?

1. Message Authentication: Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay).
2. Digital Signature: In the case of the digital signature, the hash value of a message is encrypted with a user's private key. Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature.
3. Integrity of the message.
4. Encryption of the messages.
5. Secure web browsing.

Q.5 What are the different techniques used in encryption?

1. Asymmetric Encryption:
    a. Asymmetric cryptography is used when increased security is the priority over speed and when identity verification is required.
    b. This type of encryption is used for digital signatures when signing an online document and in blockchain to authorize transactions for cryptocurrency.
    c. Types of asymmetric encryption include RSA and PKI.
        i. RSA is a popular algorithm used to encrypt data with a public key and decrypt it with a private key for secure data transmission.
        ii. Public key infrastructure (PKI) governs encryption keys through the issuance and management of digital certificates.
2. Symmetric Encryption:

a. Symmetric encryption is used when speed is the priority over increased security and uses one secret symmetric key to both encrypt the plaintext and decrypt the ciphertext.

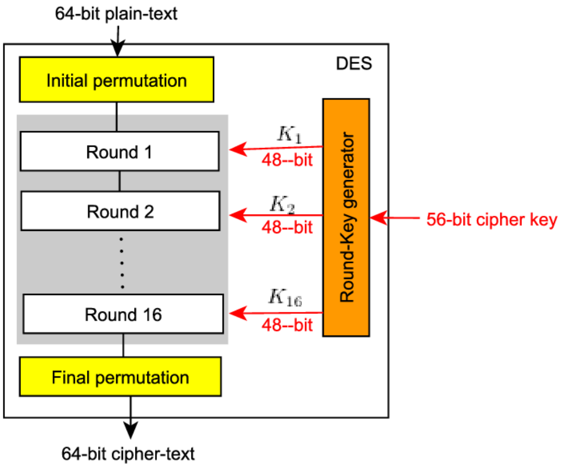
b. This encryption is commonly used in credit card transactions.

c. Types of symmetric encryption includes:

i. Data Encryption Standards (DES)

ii. Advanced Encryption Standard (AES)

Q.6 Explain Data Encryption Standard (DES) algorithm with its rounds.



1. The DES Algorithm is a block cipher.

2. It uses symmetric keys to convert 64-bit plaintext blocks into 48-bit ciphertext blocks.

3. The DES encryption algorithm uses symmetric keys, which means that the same key is used for encrypting and decrypting the data.

4. Rounds in DES:

a. Electronic Codebook (ECB): In this mode, each block of 64-bits is independently encrypted and decrypted.

b. Cipher Block Chaining (CBC): In this mode, each block of 64-bits is dependent on the one before it. It uses an initialization vector (IV).

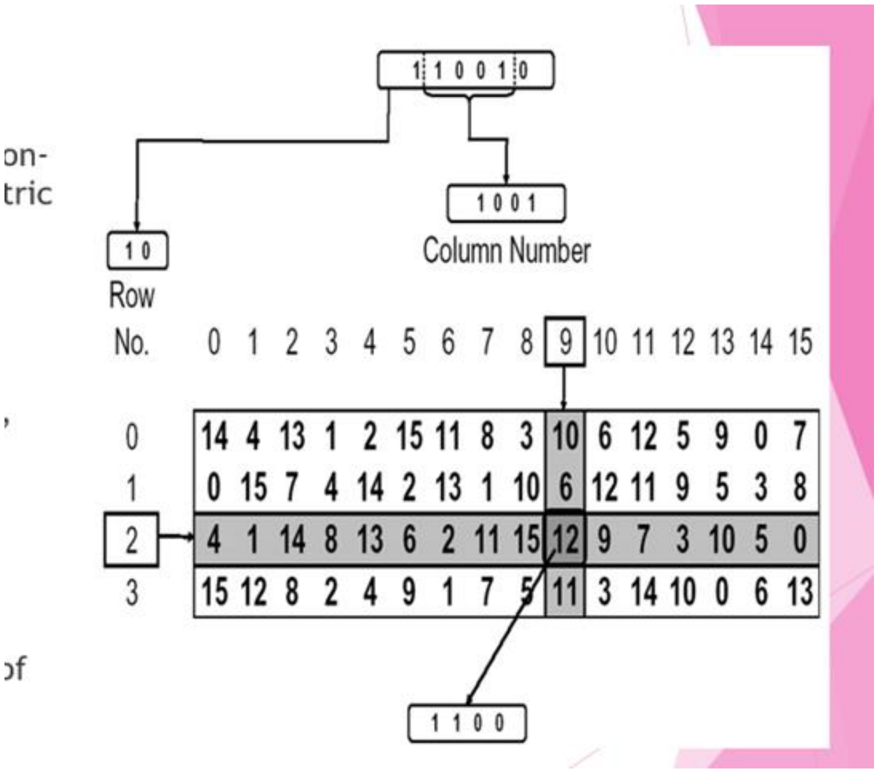
c. Cipher Feedback (CFB): In this mode, the previous ciphertext is used as the input for the encryption algorithm.

d. Output Feedback (OFB): This mode is like CFB, except for the fact that the input for the encryption algorithm is the output of the previous DES.

e. Counter (CTR): In this mode, every block of plaintext gets XORed with a counter that has been encrypted. The counter is incremented for every next block.

- Q.7 Explain S-box technique with its working.

1. In cryptography, an S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution.
2. In general, an S-box takes some number of input bits, m, and transforms them into some number of output bits, n, where n is not necessarily equal to m.

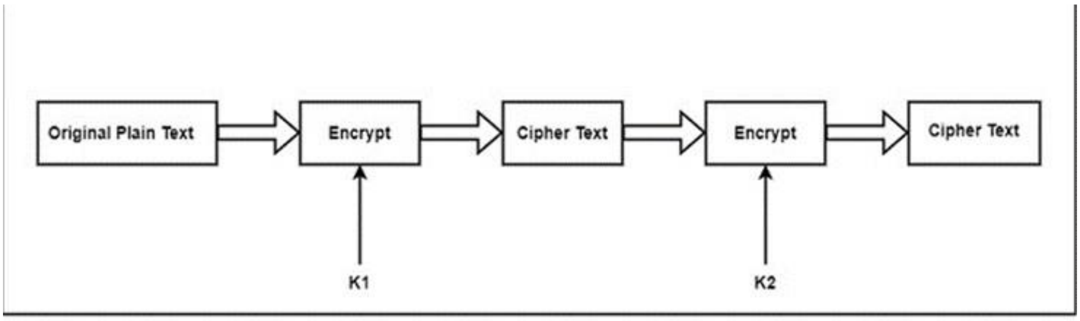


Row No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

3. An S-Box is the only non-linear component in a block cipher system.
4. It plays an important role in symmetric block cipher cryptosystems.
5. It transforms any input plaintext block into a ciphertext block, which can confuse the relationship between ciphertext and plaintext.
6. For example, an input "011011" has outer bits "01" and inner bits "1101"; the corresponding output would be "1001".
7. The S-boxes carry out the real mixing (confusion).
8. DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.

▼ Q.8 What are the different DES encryptions?

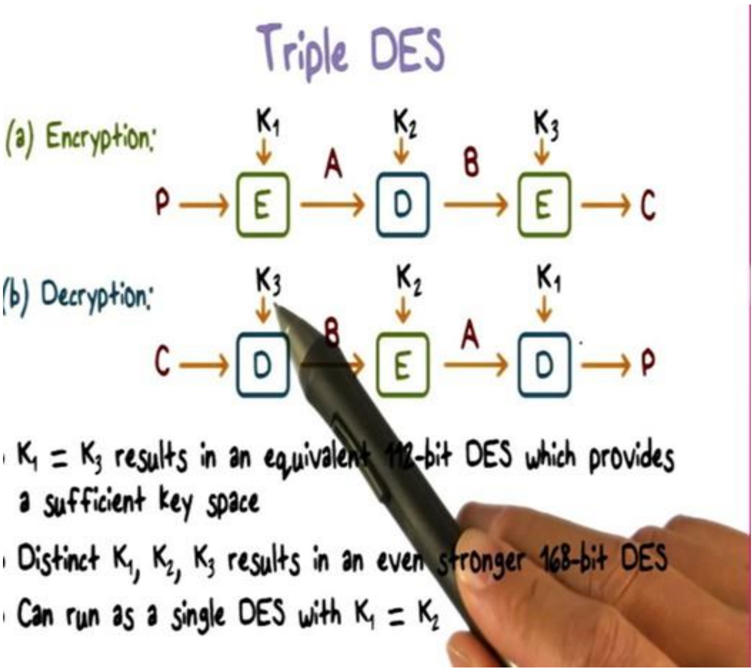
1. Double DES:



Double DES Encryption

   1. Double DES is an encryption approach which need two instance of DES on same plain text.
   2. In both instances it uses multiple keys to encrypt the plain text.
   3. Both keys are needed at the time of decryption.
   4. The 64 bit plain text goes into first DES instance which than transformed into a 64 bit middle text utilizing the first key and thus it goes to second DES instance which provides 64 bit cipher text by utilizing second key.
   5. The final output is the encryption of encrypted text with the original plain text encrypted twice with two different keys.

2. Triple DES:



- $K_1 = K_3$ results in an equivalent 112-bit DES which provides a sufficient key space
- Distinct K_1, K_2, K_3 results in an even stronger 168-bit DES
- Can run as a single DES with $K_1 = K_2$

1. Triple DES is a symmetric key-block cipher which applies the DES cipher in triplicate. It encrypts with the first key (k1), decrypts using the second key (k2), then encrypts with the third key (k3).
2. There is also a two-key variant, where k1 and k3 are the same keys.

Chapter 3

▼ Q.1 Explain modular arithmetic with an example?

1. In modular arithmetic, the numbers we are dealing with are integers and the operations used are addition, subtraction, multiplication and division.
2. The only difference between modular arithmetic is that all operations are performed regarding a positive integer, i.e. the modulus.

3. The Modulus: If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. The integer n is called the modulus. 11 mod 7 = 4.
4. Modular Arithmetic Operations: the (mod n) operator maps all integers into the set of integers {0, 1, 2, (n - 1)}.
5. Modular arithmetic exhibits the following properties:
    a. [(a mod n) + (b mod n)] mod n = (a + b) mod n
    b. [(a mod n) - (b mod n)] mod n = (a - b) mod n
    c. [(a mod n) * (b mod n)] mod n = (a * b) mod n
6. E.g.

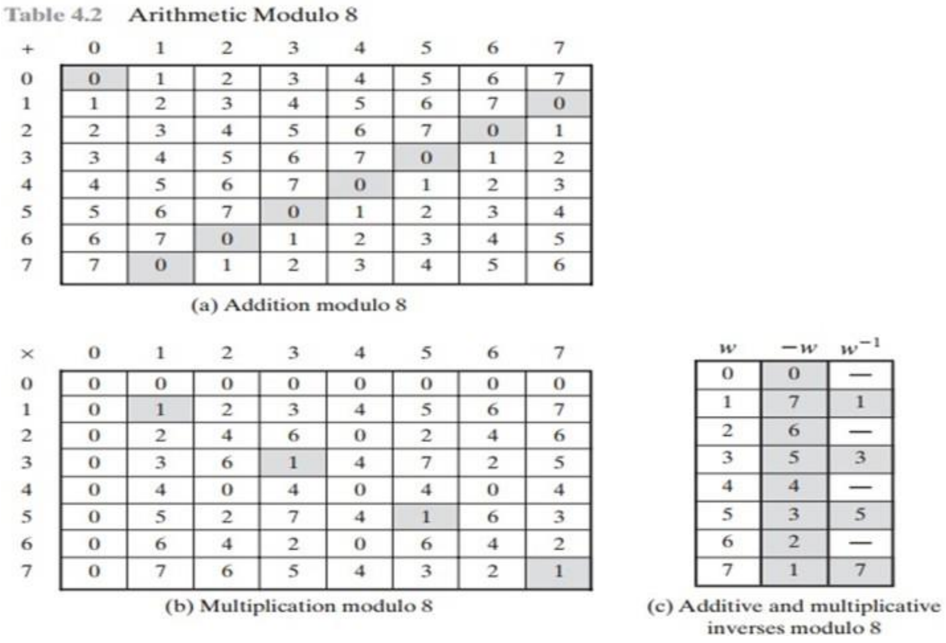


Table 4.2 Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

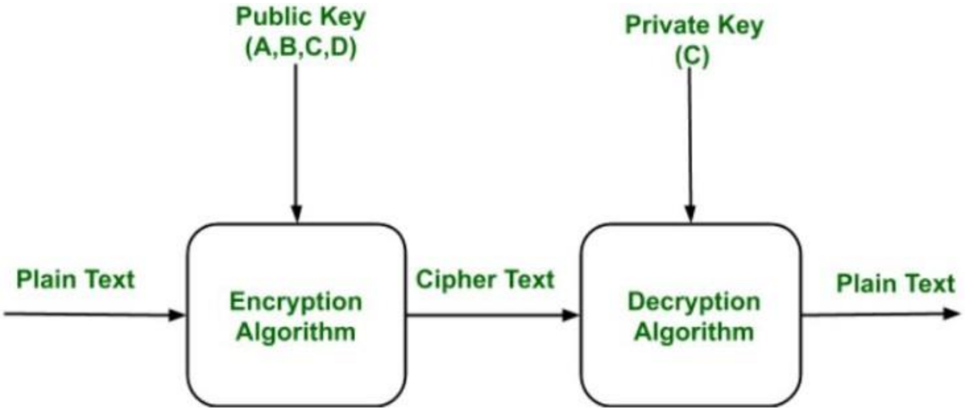
w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

▼ Q.2 What is a public key cryptographic system?

1. Public key cryptography is a method of encrypting or signing data with two different keys and making one of the keys, the public key, available for anyone to use.
2. The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key.
3. PKCS were first developed by RSA Laboratories.
4. The primary goal of developing PKCS was to make different applications from different vendors interoperable.

5. PKCS specifications are defined for both binary and American Standard Code for Information Interchange (ASCII) data types.
6. It is widely used, especially for TLS/SSL, which makes HTTPS possible.



▼ Q.3 Write the steps of the RSA Algorithm?

1) Choose two large prime numbers (p and q)
2) Calculate n = p*q and z = (p-1)(q-1)
3) Choose a number e where 1 < e < z
4) Calculate d = e-1mod(p-1)(q-1)
5) You can bundle private key pair as (n,d)
6) You can bundle public key pair as (n,e)
7) Encryption: C = M (mod n)
8) Decryption: CM = C(mod n)

▼ Q.4 What are the components of a public key encryption scheme?

1. **Plain Text**: It is the data to be protected during transmission.

2. **Encryption**: It is a mathematical process that produces a ciphertext for any given plaintext and encryption key.
2. **Cipher Text**: It is the result of encryption performed on plaintext using an algorithm, called a cipher.
3. **Decryption**: It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key.
4. **Encryption Key**: It is a value that is known to the sender.
5. **Decryption Key**: It is a value that is known to the receiver.
6. **Key** is the secret piece of information which is used for encryption and decryption in cryptography.

▼ Q.5 Explain how to generate keys in RSA Algorithm?

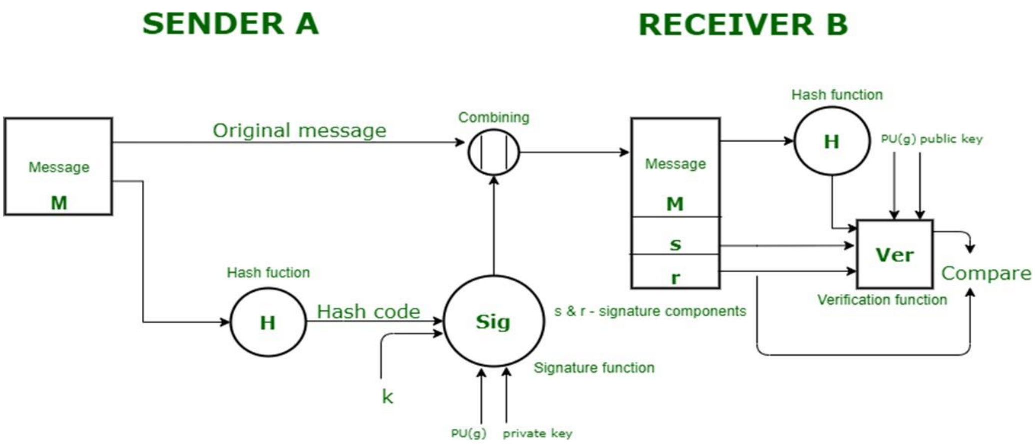
Keys are generated as follows:

1. Select two prime numbers, p = 17 and q = 11.
2. Calculate n = pq = 17 * 11 = 187.
3. Calculate f(n) = (p - 1)(q - 1) = 16 * 10 = 160.
4. Select e such that e is relatively prime to f(n) = 160 and less than f(n); we choose e = 7.
5. Determine d such that de = 1 (mod 160) and d < 160.

   The correct value is d = 23, because 23 * 7 = 161 = (1 * 160) + 1;

▼ Q.6 Write notes on: I) Public key cryptographic system II) DSS III) Diffie Hellman

1. PKCS: Same as Q2
2. DSS:
   a. Digital signature is a way of authenticating digital data coming from a trusted source.
   b. The Digital Signature Standard (DSS) is a digital signature algorithm developed by the U.S. National Security Agency as a means of authentication for electronic documents.
   c. A digital signature is equivalent to a written signature used to sign documents and provide physical authentication.
   d. DSS only provides us with the digital signature function and not with any encryption or key exchanging strategies.



e. Sender Side: In DSS Approach, a hash code is generated out of the message.

f. Receiver Side: At the receiver end, verification of the sender is done.

3. Diffie Hellman:

a. The Diffie-Hellman algorithm is being used to establish a mutual secret that can be used for secret communications while exchanging data over a public network and get the secret key using the parameters.

b. The Diffie-Hellman algorithm will be used to establish a secure communication channel.

c. This channel is used by the systems to exchange a private key.

d. This private key is then used to do symmetric encryption between the two systems.

e. Steps:

i. Sender have public keys

ii. Use private key a

iii. Key generation x= G^a mod P

iv. Exchange of generated key takes place

v. Key received = y

vi. Generated secret key = k_a = y^a mod P

vii. $K_a = K_b$

f. Limitations:

i. Lack of authentication procedure.

ii. Algorithm can be used only for symmetric key exchange.

iii. Expensive.

Chapter 4

▼ Q.1 Explain the concept of Authorization and authentication with examples.

Authentication	**Authorization**
Determines whether users are who they claim to be.	Determines what users can and cannot access.
Challenges the user to validate credentials (for example, through passwords, answers to security questions, or facial recognition).	Verifies whether access is allowed through policies and rules.
Usually done before authorization.	Usually done after successful authentication.
Generally, transmits info through an ID Token.	Generally, transmits info through an *Access Token.*
Generally governed by the *OpenID Connect (OIDC) protocol.*	Generally governed by the OAuth 2.0 framework.
Example: Employees in a company are required to authenticate through the network before accessing their company email	Example: After an employee successfully authenticates, the system determines what information the employees are allowed to access

▼ Q.2 Explain why Authentication is required?

1. "Who are you". This ensures an individual users.
2. This also ensures authenticated user only perform transactions or use of device.
3. There is no use of encryption without authentication.
4. Determines whether users are who they claim to be.
5. Challenges the user to validate credentials(for example, through passwords, answers to security questions, or facial recognition).

▼ Q.3 Explain password authentication mechanism with the authentication steps?

Authentication mechanism works as follows:

Step 1: Prompt for user id and password – during authentication the application sends a screen to the user, prompting for the user id and password.

Step 2: User enters user name and passwords – once user name and password entered by user it goes to in clear text to the server.

Step 3: User id and password validation – server consult the user database to verify the received data (user id and password).

Step 4: Authentication Result – Depending upon success or failure of the validation of the user id and password, the user authenticator program return an appropriate result back to the server.

Step 5: Inform user accordingly – Depending upon result server sends message and act accordingly.

▼ Q.4 What are the problems with password mechanisms?

1. **DB contain passwords in clear text** – user database contain user ids and passwords in clear text. If the attacker succeeds in obtaining an access to the DB. The whole list of user ids and passwords are available to the attacker. It is advised that passwords should not be stored in clear text.
2. **Password travels in clear text from user's computer to the server** – if the attacker breaks in the communication link between the user's computer and the server, attacker easily obtain the clear text passwords.

▼ Q.5 Explain Authentication token with its working?

Authentication token is an extremely useful alternative to a password. It is a small device that generates a new random value every time it is used.

Each authentication token is pre-programmed with a unique number, called a random seed or just seed.

How authentication token works:

Step 1: Creation of token – when authentication token is created, the corresponding random seed is generated for the token by the authentication server.

Step 2: Use of token – authentication token automatically generates numbers, called one time password. This is generated randomly by authentication token based on the seed value. OTP is one time because it is one time and used once. Then both user id and OTP sends to the server for authentication.

Step 3: server returns appropriate message to the user.

▼ Q.6 What are the types of authentication tokens?

There are two types of authentication tokens:

1. Challenge/Response tokens:
   a. **Step 1**: User sends a login request – user sends the login request only with his/her user id.
   b. **Step 2**: Server creates random challenge – Server first check the user id is valid. If not then server sends appropriate error message back to the user.
   c. **Step 3**: User signs the random challenge with the message digest of the password
   d. **Step 4**: Server verifies the encrypted random challenge received from the user.
   e. **Step 5**: Server sends appropriate message back to the user.
2. Time-based tokens:
   a. **Step 1**: Password generation and login request. The token is preprogrammed with seed, copy of the seed is available to the authentication server and password is generated.
   b. **Step 2**: server side verification. Server receives password, it performs and independent cryptographic function on user's seed value and current system time.
   c. **Step 3**: Server returns appropriate message to the user.

▼ Q.7 Explain certificate based authentication with steps?

Steps for certificate based authentication:

Step 1: create, storage and distribution of digital certificates.

- Certificates are created by the certificate authority for each user and it is sent to the respective user.
- The copy of certificate is also available on server.

Step 2: Login request.

- During login, user sends user id to the server.

Step 3: Server creates a random challenge.

- Server creates a random challenge (i.e. random number generated using pseudo-random number generation technique)

Step 4: user signs the random challenge.

- User has to signs the random challenge using private key. It means user’s public key.
  Private key’s are not directly to anybody, passwords are used to protect.
- Only correct password can open a private key file.
- Server creates random challenge and sends the random challenge to the user.

Step 5: Server returns appropriate message back to the user.

- Depending upon validation server used to send appropriate message.

▼ Q.8 How do smart cards work?

Working of smart cards:

1. The server’s user authentication program obtains the public key for the user from the user DB.
2. The server decrypt’s the signed random challenge from the user, using the user’s public key.
3. The server compares two encrypted random challenges.
4. Server sends and appropriate message to the user.

▼ Q.9 What are different biometric authentication? Explain working in detail.

Biometric authentication device works on the basis of human characteristics such as fingerprints, voice or patterns of lines in the iris of the eye’s. User database contain a sample of the user’s biometric characteristics.

During authentication, the user is required to provide another sample of the user’s biometric characteristics. This is matched with DB, if both are same then it is consider as a valid.

Working:

1. Creation of user’s sample.
2. During authentication, user has to provide biometric.
3. This sent to the server in encrypted form

4. On server side, it is decrypted if both are matches at certain degree on the basis of FAR (False Accept Ratio) and FRR(False Reject Ratio) values then it’s valid.

▼ Q.10 Write a note on 0Auth 2.0 or 0Auth?

OAuth 2.0 enables the safe retrieval of secure resources while protecting user credentials.
Some apps may need to authenticate during the configuration phase and others may need OAuth only when a user invokes a service.

OAuth authentication follows a six step pattern:

1. An application requests authorization on a user's behalf.
2. The application obtains a Grant Token.
3. The client requests an access token by using the Grant Token.
4. The authorization server validates the Grant Token and issues an Access Token and a Refresh Token.
5. The client requests the protected resource, authenticating using the Access Token.
6. The resource server verifies the Access Token and serves the request.

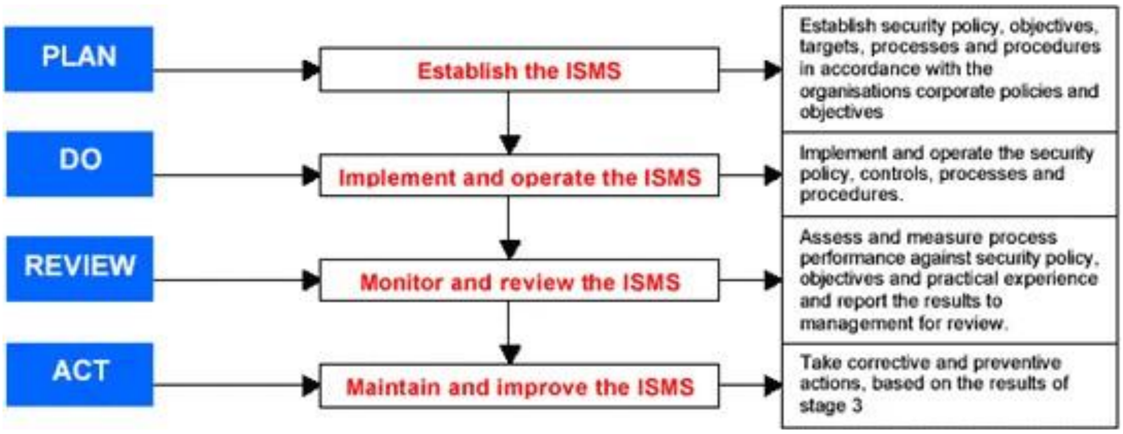
Chapter 5

▼Q.1 Explain the concept of security policy with the design and standards?

- Concept of security policy:
    - A security policy is a document that enhance the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data.
    - A network security policy defines guidelines for computer network access, lays out the architecture of the organization’s network security environment and defines how the security policies are implemented throughout the network architecture.
    - Network security policies describes an organization’s security controls. It aims to keep malicious users out. It also observe and keep watch on the malicious practices within organization.

    - 8 The initial stage to generate a policy is to understand what information and services are available, and to whom, what the potential is for damage, and what protections are already in place.
    - ○ Physical security policies protect all physical assets in an organization, including buildings, vehicles, inventory and machines.
- Policy design: Basic rules
    1. Modify the policy to specific business needs.
    2. Keep the policy easy to understand and follow.
    3. Update the policy regularly.
    4. Enforce the policy consistently.
    5. Train employees on how to apply the policy.
- Policy design: Network security protocols
    1. Assess the Current State of the Network: This stage identifies any security gaps and conduct assessment to identify it.
    2. Develop a Plan
    3. Make Changes
    4. Test the Changes
    5. Monitor the Network
- Standards:
    1. BS7799
    2. ISO17799
    3. ISO27001

▼ Q.2 Explain the BS7799 standard with the different steps to be followed to implement these standards?
A2)
1) BS7799 is a standard to guide the development and implementation of an Information Security Management System, commonly known as an ISMS.
2)It identifies the security threats and risks for an organization.


PLAN
DO
REVIEW
ACT
Establish the ISMS
Implement and operate the ISMS
Monitor and review the ISMS
Maintain and improve the ISMS

Establish security policy, objectives, targets, processes and procedures in accordance with the organisations corporate policies and objectives

Implement and operate the security policy, controls, processes and procedures.

Assess and measure process performance against security policy, objectives and practical experience and report the results to management for review.

Take corrective and preventive actions, based on the results of stage 3

▼ Q.3 What are the contents of ISO27001 standard?

ISO 27001 is the international standard for information security.

It sets out the specification for an information security management system (ISMS).

It helps organizations manage their information security by addressing people, processes, and technology.

ISO 27001 is a framework that helps organizations establish, implement, operate, monitor, review, maintain and continually improve an ISMS.

Controls in ISO 27001:

1. **Technical controls**: These are primarily implemented in information systems, using software, hardware, and firmware components added to the system. E.g. backup, antivirus software, etc.
2. **Organizational controls**: These are implemented by defining rules to be followed, and expected behavior from users, equipment, software, and systems. E.g. Access Control Policy, BYOD Policy, etc.
3. **Legal controls**: These are implemented by ensuring that rules and expected behaviors follow and enforce the laws, regulations, contracts, and other similar legal instruments that the organization must comply with. E.g. NDA (non-disclosure agreement), SLA (service level agreement), etc.
4. **Physical controls**: These are primarily implemented by using equipment or devices that have a physical interaction with people and objects. E.g. CCTV cameras, alarm systems, locks, etc.

5. **Human resource controls**: These are implemented by providing knowledge, education, skills, or experience to persons to enable them to perform their activities in a secure way. E.g. security awareness training, ISO 27001 internal auditor training, etc.

   Advantages:-

   1) Secure information in all forms
   2) Helps organizations to identify the security threats and risks .
   3) Protect CIA of data
   4) Reduce cost

▼ Q.4 Why different standards are required in Security?

1. Security standards enhance the physical security of an organization and contribute to the overall risk management in several ways.
2. Security standards also allow the sharing of knowledge and best practices by helping to ensure common understanding of conditions, terms, and definitions, which can prevent costly errors.
3. It avoids third party interference and keeps the data secured.
4. Standards help establish common security requirements and the capabilities needed for secure solutions.

▼ Q.5 Explain ISO17799 standard with its contents?

It is known as the Code of Practice for information security management, was developed by an IT Security Subcommittee of the International Organization for Standardization and was published in June 2005.

ISO 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

ISO 17799 refers to a set of general practice guidelines that aid in implementation of security standards for information systems.

ISO 17799 helps companies build safe and secure inter-organizational computer systems.
The objective is to provide common guidelines for accepted goals of information security.

ISO17799 focused on following areas:

1. Security policy
2. Organization of information security

3. Asset management
4. Human resources security, etc.

▼ Q.6 Write notes on incident handling and escalation procedures?

- Incident handling is based on type of severity:

1. **Severe 1** - A critical problem affecting a significant number of users in a production environment. The issue impacts essential services, or the service is inaccessible, degrading the customer experience. These incident requires thoughtful staff intervention early in the process to determine when stakeholders should be notified.
2. **Severe 2** - A severe problem affecting a limited number of users in a production environment, degrading the customer experience. You may have an escalation policy for website outages affecting some users in isolated geographic areas.
3. **Severe 3** - A not-so-major incident that causes errors, excessive load, or minor problems for customers in a production environment.

- Following process is used in escalation process:

1. Provide clear criteria for when an incident should be escalated to the next level. You should also specify if the steps vary depending on if the incident occurs within regular business hours.
2. During an incident, IT team members may need to contact staff outside their department for support.
3. Define a comprehensive list of resolvers for your incident management solution to notify.
4. Some incidents may be minor enough that on-call systems built within your incident management tool are comprehensive enough to handle the chain of communications.
5. Outline every step in detail. If your organization uses automated incident response management tools, make sure team members understand the workflows.

▼ Q.7 Explain firmware implementation process?

1) Firmware is a software program on the hardware device, which perform functions like basic input/output tasks and communicate with other software running on a device.

2) Firmware provides low-level control for a device's hardware.

1. **Design**: It is important to catch design issues that will lead to security issues, and correct them during design. Threat modelling should be performed on all components.
2. **Input Validation**: “User input” is used to describe any commands or data that are directly or indirectly supplied by any entity not controlled by the firmware itself. External input, including configuration data, must always be sanitized or validated before use.
3. **Memory Safety**: Probably the most common source of exploitable vulnerabilities is bugs that allow an attacker to corrupt memory and use that to execute arbitrary code. Use memory safe practices.
4. **Security Code Reviews**: Firmware must be routinely reviewed for security issues for various websites.
5. **Third party libraries**: Use of 3rd-party libraries, including open source, is often required as part of the firmware being developed.
6. **Testing**: An important part of secure development includes testing for security issues.
   Use appropriate testing to ensure security.
7. **Capture Security Exceptions**: Document all security exceptions and consider them in the next versions development cycle. Institute processes to audit security progress across versions.
8. **Build & Compilation**: The code that actually runs in production is the compiled code. It is important to ensure integrity of builds, and optimize compilation for security.
9. **Source Code Access**: Granting firmware users access to the source code helps raise the security level of that code, and increases trust in the firmware security.
10. **Verification/Compliance**: In order to be able to prove that the firmware development followed the right security best practices, it is often required to produce evidence of the following artifacts for the firmware builds that were publicly released:

    a. An independent (not firmware development team) security review / pentest.

b. Reports of testing & reviews.

c. Build logs, test logs, etc.

▼ Q.8 Write a note on the Internet protocol(IP) chain?

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.

Data traversing the Internet is divided into smaller pieces, called packets.

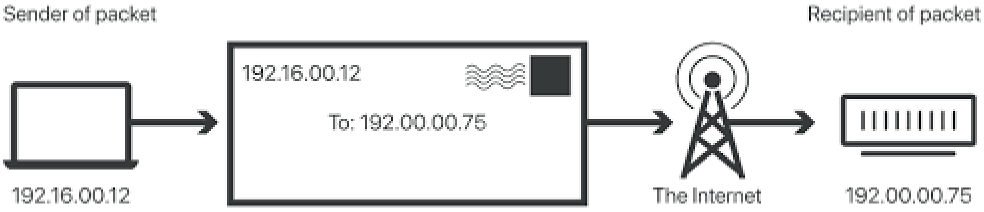
IP information is attached to each packet, and this information helps routers to send packets to the right place.

Every device or domain that connects to the Internet is assigned an IP address

The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers.

Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP.

The most common transport protocols are TCP and UDP.



▼ Q.9 Explain how the incident handling and escalation process is related to each other?

An escalation process is a written procedure that guides team members on how to escalate the incident management process.

It outlines the upward flow of alerts and responsibility within your organization and ensures the necessary parties are brought on board at the appropriate time in an incident’s lifecycle.

Chapter 6

Q1) Explain email security in detail ?

A1)

1) Email security is a term for describing different procedures and techniques for protecting email accounts.
2) Email is often used to spread malware, spam mails, etc.

3) Email is also a common entry point for attackers looking to gain information in an enterprise network and obtain valuable company data.

4) Following are the email security techniques:-

    a. Privacy Enhanced Mail (PEM) :-

        1) It is an email security standard adopted by the Internet Architecture Board (IAB) to provide secure email communication over the internet.

        2) Working of PEM:-

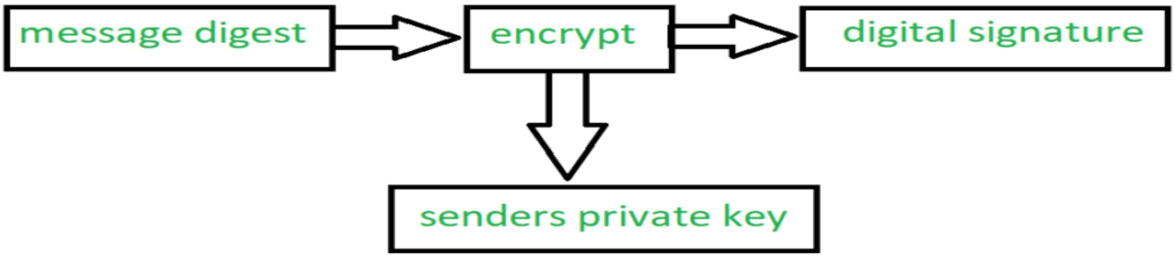
            a. Canonical conversion :-
                i. This step involves the conversion of the message into a standard format that is independent of the computer architecture and the operating system of the sender and the receiver.
                ii. If the sender and receiver has different computer architecture or operating system. It may lead to generation of different message.

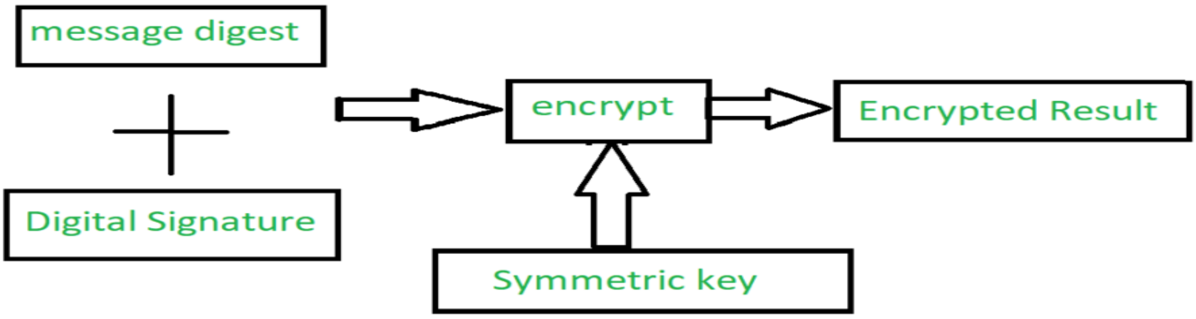
            b. Digital Signature:-
                i. In this step, the digital signature is generated by encrypting the message of an email message with the sender's private key.

            c. Encryption:-
                i. The encrypted message is generated by encrypting the original message and digital signature together along with the symmetric key.
                ii. This step is very important to obtain the confidentiality.

            d. Base 64 encoding:-

                i. This is the last step where the binary output is transformed into character output.





b. PGP (Pretty Good Privacy):-

1)It is a popular program that is used to provide confidentiality and authentication services for electronic mail and file storage.
2)It was designed in 1991.
3)The following are the services offered by PGP:-
1)Authentication
2)Confidentiality

4) Working of PGP:-

a. Digital Signature:-
   i. In this step, the digital signature is generated by encrypting the message of an email message with the sender's private key.

b. Compression:-
   i. Input message and digital signature are compressed together to reduce size of the final message that will be transferred.

c. Encryption:-
   i. The encrypted message is generated by encrypting the original message and digital signature together along with the symmetric key.
   ii. This step is very important to obtain the confidentiality.

d. Digital Enveloping:-
   i. Output of encryption and enveloping combines into digital enveloping.

e. Base 64 encoding:-

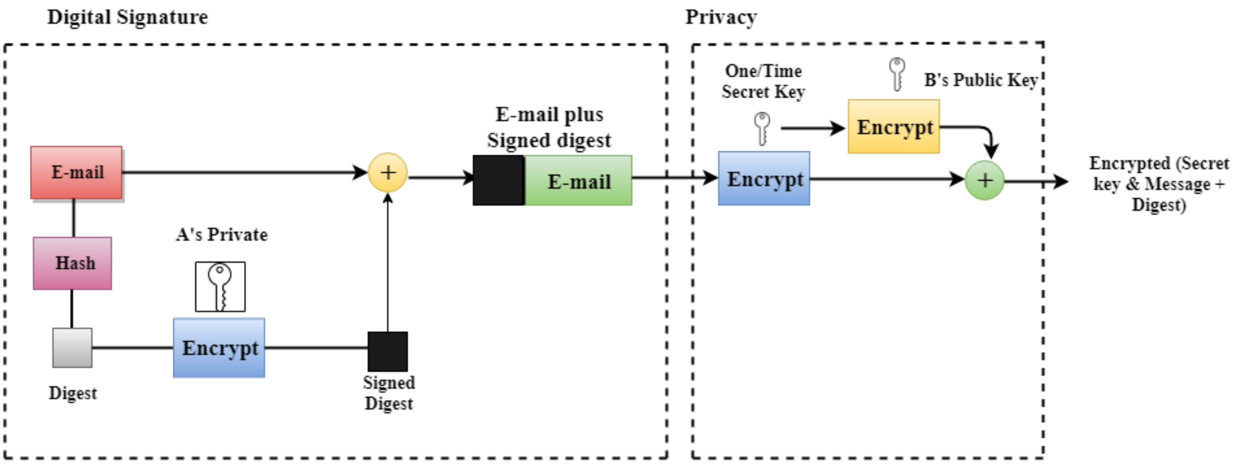
   i. This is the last step where the binary output is transformed into character output.

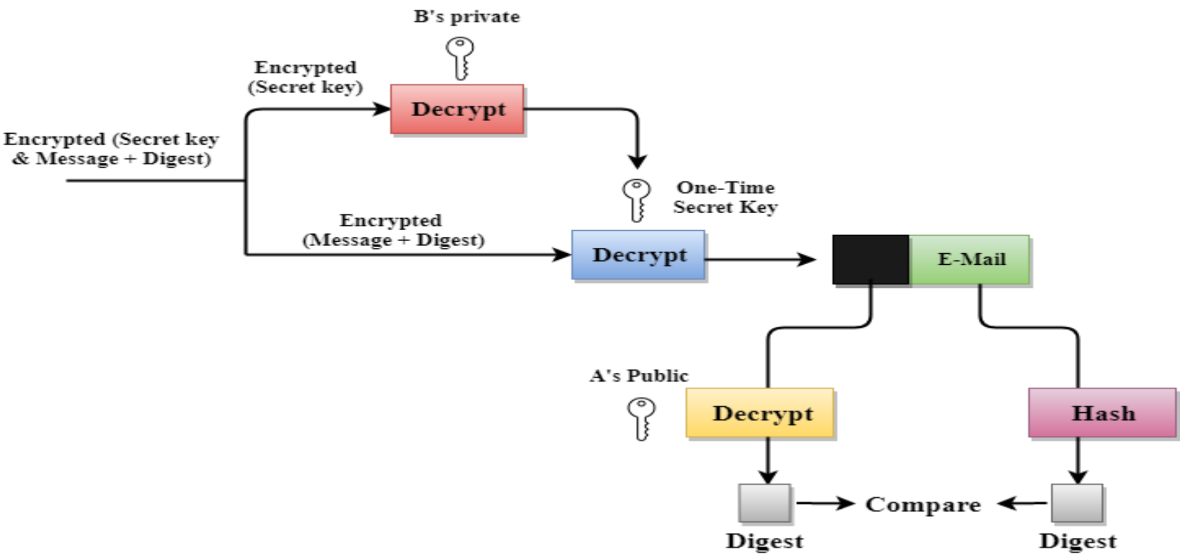
5) Drawbacks:-
1) The administration is difficult

2) It has complex structure

3) No Recovery

4) Compatibility issue





Q2)What is IP Security ? Working of IP Security ?Components of IP Security ?
A2)
1)The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality.
2) It also defines the encrypted, decrypted and authenticated packets.
3) The protocols needed for secure key exchange and key management are defined in it.

4)Components :-

1) Encapsulating Security Payload (ESP) -
   a. It provides data integrity, encryption, authentication and anti replay.
   b. It also provides authentication for payload.

2) Authentication Header (AH) -
   a. It also provides data integrity, authentication and anti replay and it does not provide encryption.
   b. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data’s confidentiality.

3) Internet Key Exchange (IKE) -
    a. It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.
    b. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication

5)Working:-

1) The host checks if the packet should be transmitted using IPsec or not.

2) Then the IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes,
The Main mode which provides the greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly

3)The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.

4)Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.

5)Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.

6)When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

Q3)What are different task in network security management ?
A3)
1)Secure local network resources
2)Enforce least privilege
3)Secure access to corporate devices
4)Secure mobile devices infrastructure
5)Ensure computer images are current
6)Ensure new policies are applied immediately
7)Incident response
8)Email detection/Spam detection

Q4)Explain SSl(Secure Socket Layers) ?
A4)

1) The Secure Sockets Layer (SSL) protocol was developed by Netscape Communications Corporation.

2) SSL ensures the data that is transferred between a client and a server remains private.

3) Secure Sockets Layer (SSL) is a standard technique for transmitting documents securely across a network.

4) When your server has a digital certificate, SSL-enabled browsers can communicate securely with your server, using SSL.

5) With SSL, you can easily establish a security-enabled Web site on the Internet
6) HTTPS represents a unique protocol that combines SSL and HTTP.
7) SSL communicates using the Transport Control Protocol (TCP).
8) SSL is based on an asymmetric cryptographic process in which a Web browser

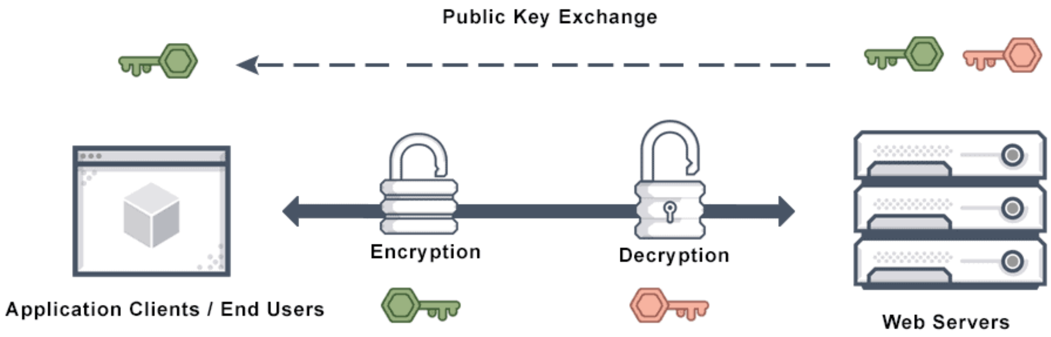
generates both a public and a private (secret) key.

9) Goals of SSl:-

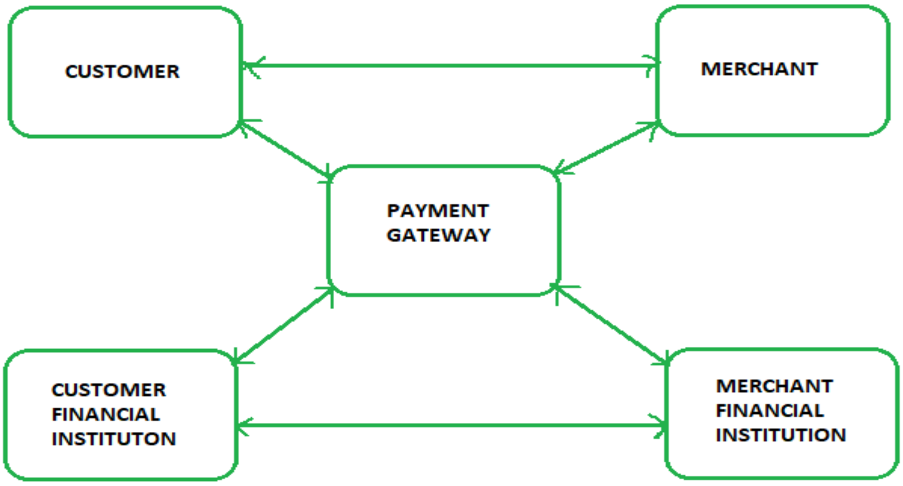
a. Data Integrity:- The principle of data integrity is to provide reliable and accurate data without being modified incorrectly.

b. Client-server authentication:- The SSL protocol authenticates the client and server using standard cryptographic procedures.

c. Transport Layer Security (TLS):- A cryptographic technology for secure data transfer over the Internet.



Q5)Explain SET (Secure Electronic Transaction) ?
A5)



1) The Secure Electronic Transaction (SET) is a protocol designed for protecting credit card transactions over the Internet.

2) It is an industry-backed standard that was formed by MasterCard and Visa in February 1996.

3)SET relies on cryptography

4) SET is the only Internet transaction protocol to provide security through authentication.

5)It uses digital certificates to verify the identity of those accessing payment details.

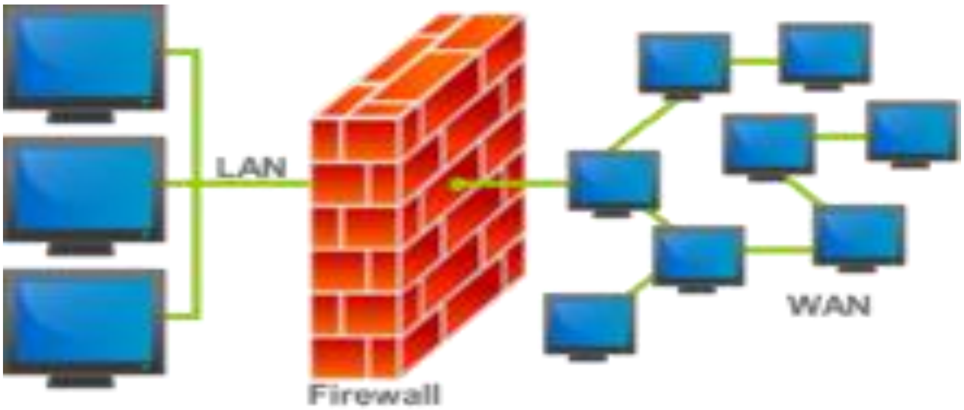
6)The purpose of the SET protocol is to establish payment transactions that:-

a. Provide confidentiality of information
b. Ensure the integrity of payment instructions for goods and services order data
c. Authenticate both the cardholder and the merchant.

7)Participants invovled in SET:-

a. Cardholder
b. Merchant
c. Issuer
d. Acquirer
e. Payment Gateway
f. Certification Authority

Q6)Write a note on FireWall ?
A6)



1) A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
2) Firewalls have been a first line of defense in network security for over 25 years.
3) They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
4) The 4 general techniques in Firewall are:-

    a. Service Control:-
        a. Determines the types of Internet services that can be accessed, inbound or outbound.

    b. Direction Control:-
        a. Determines the direction in which particular service requests may flow through the firewall.

    c. User Control:-
        a. Controls access to a service according to which user is attempting to access it.

    d. Behaviour Control:-
        a. Controls how particular services are used.

5) Limitations:-
    a. The firewall cannot protect against attacks that bypass the firewall
    b. The firewall may not protect fully against internal threats

c. An improperly secured wireless LAN may be accessed from outside the organization
d. Complex Structure

Q7)What are Intruders and Viruses ?
A7)
1)Intruders:-

a. Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security.
b. They have immense knowledge and an in-depth understanding of technology and security.
c.They are divided into 3 categories:-
1)Masquerader
2)Misfeasor
3)Clandestine User

2)Viruses:-

a. A computer program that can copy itself and infect a computer without permission or knowledge of the user is known as a virus.
b. Viruses are self-replicating and are designed to infect other programs.
c.Types of Viruses are:-
1)File Virus
2)Boot sector Virus
3)Macro Virus
4)Source code Virus
5)Polymorphic Virus
6)Stealth Virus

Q8)How intrusion is detected ?
A8)
1)An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
2)It is a software application that scans a network or a system for the harmful activity or policy breaching.
3)Two methods used are:-

a. Signature-based Method:
Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1’s or number of 0’s in the network traffic

b. Anomaly-based Method:
Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly.
In anomaly-based IDS there is use of machine learning to create a trustful activity model

Chapter 8

Q1)Explain web security with its requirement ?

A1)

1)Web Security also known as Cyber Security relates to the securing of websites and servers from online risks.

2)It is aimed to protect sensitive data by restricting, discovering and responding to attacks.

3)Web security is important to keeping hackers and cyber-thieves from accessing sensitive information.

4)Without providing security to website , the attackers can easily breach into critical information such as user details, account details, etc.

5)Web Security Requirements:-

1)Keep Software and Plugins Up-To Date:-

2)Add Https and SSL Certificate

3)Choose a smart password

4)Use a secure web host

5)Backup your website

6)Record User access

7)Use biometrics

6)Web Security Threats :-

1)Data Confidentiality:-

a. If website is not secured the user details which had to be kept private may be get accessed by the attackers

2)Data Integrity:-

a. User details can be modified and misused

3)Data Availability:-

a. Storage damage or system crash may occur

4)Denial Of Services :-

a. Killing of user threads