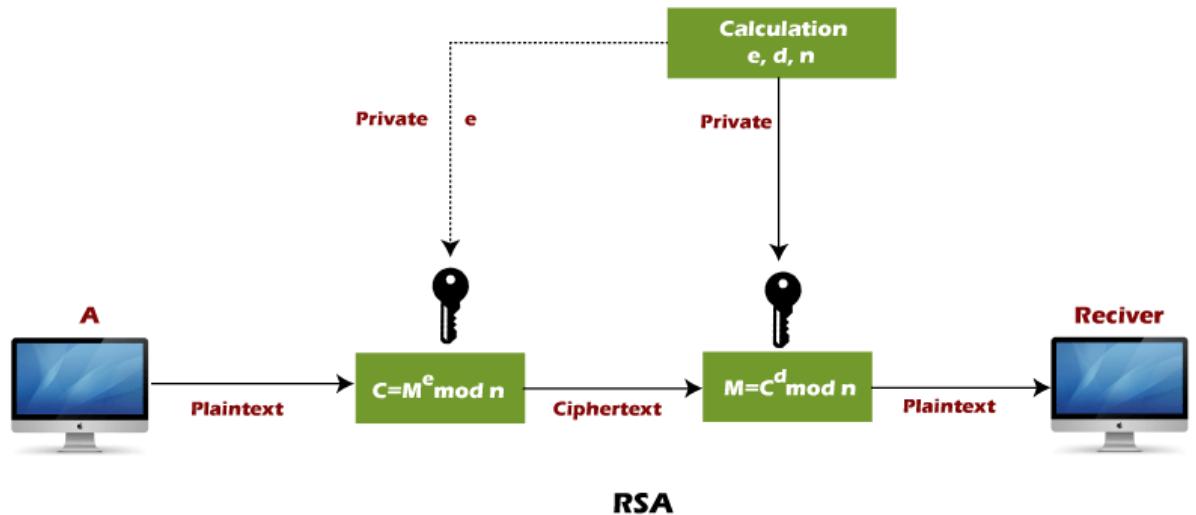


1. Write a program for default passwords, printed passwords and password in plain text form. Draw flowchart, algorithm and attach output results for the same.
2. Explain RSA algorithm in detail with example.

RSA algorithm is a type of public-key encryption algorithm.

Public Key algorithm is also known as asymmetric algorithm. They are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned with a pair of keys: a public key and a private key.

RSA algorithm is named after its inventors Rivest, Shamir and Adelman.



Let's understand the steps of RSA algorithm with an example :

Step 1: Select two large prime numbers, p , and q . $p = 7$, $q = 11$

Step 2: Multiply these numbers to find $n = p \times q$, where n is called the modulus for encryption and decryption.

First, we calculate $n = p \times q = 7 \times 11 \Rightarrow n = 77$

Step 3: Choose a number e less than n , such that n is relatively prime to $(p - 1) \times (q - 1)$. It means that e and $(p - 1) \times (q - 1)$ have no common factor except 1. Choose "e" such that $1 < e < \varphi(n)$, e is prime to $\varphi(n)$, $\gcd(e, \varphi(n)) = 1$.

Second, we calculate

$$\varphi(n) = (p - 1) \times (q - 1)$$

$$\varphi(n) = (7 - 1) \times (11 - 1)$$

$$\varphi(n) = 6 \times 10$$

$$\varphi(n) = 60$$

Let us now choose relative prime e of 60 as 7.

Thus the public key is $\langle e, n \rangle = (7, 77)$

Step 4: A plaintext message m is encrypted using public key $\langle e, n \rangle$. To find ciphertext from the plain text following formula is used to get ciphertext C.

To find ciphertext from the plain text following formula is used to get ciphertext C.

$$C = m^e \bmod n$$

$$C = 9^7 \bmod 77$$

$$C = 37$$

Step 5: The private key is $\langle d, n \rangle$. To determine the private key, we use the following formula d such that:

$$D_e \bmod \{(p - 1) \times (q - 1)\} = 1$$

$$7d \bmod 60 = 1, \text{ which gives } d = 43$$

$$\text{The private key is } \langle d, n \rangle = (43, 77)$$

Step 6: A ciphertext message c is decrypted using private key $\langle d, n \rangle$. To calculate plain text m from the ciphertext c following formula is used to get plain text m.

$$m = c^d \bmod n$$

$$m = 37^{43} \bmod 77$$

$$m = 9$$

In this example, Plain text = 9 and the ciphertext = 37

3. Explain any two of following with example

i. Playfair Cipher

The playfair cipher was the first practical digraph substitution cipher. In playfair cipher, we encrypt a pair of alphabets (called digraphs) instead of a single alphabet.

Procedure:

1] Generate a key square

The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I. The grid is first filled with the unique characters of the key and is then filled with the remaining unique alphabets in order.

2] Splitting input message into diagraphs

PlainText: "instruments".

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sx' Here 'x' is the bogus letter.

3] Encryption based on 3 rules

a) Same Row Rule (RHS Rule): If the letters of the diagraph fall in the same row, each is replaced by the letter to the right, with the first letter of the row circularly following the last.

b) Same Column Rule (Top-Down Rule): If the letters of the diagraph fall in the same col, each is replaced by the letter beneath, with the top letter of the col circularly following the bottom.

c) Form a Rectangle: Otherwise, each letter of the diagraph is replaced by the character in its own row and in the col of the other letter of the diagraph (like taking the adjacent endpoints of the rectangle).

ii. Hill Cipher

The Hill cipher works on multiple letters at the same time. Hence, it is a type of polygraphic substitution cipher.

Procedure:

a) Treat every character of the alphabet as a number like A = 0, B = 1 ... Z = 25.

b) Our plaintext message is organized as a matrix of numbers based on the above conversion.

E.g. CAT, based on the above step, we know that C=2, A=0, and T=19.

Therefore, our plaintext matrix would look as:

2
0
19

c) Now, our plaintext matrix is multiplied by a randomly chosen keys. The key matrix of size $n \times n$, where n is the number of rows in our plaintext matrix. E.g. 6 24 1

13 16 10
20 17 15

d) Now, multiply the 2 matrices as shown.

e) Compute the mod26 of result matrix.

$[31, 216, 325] \text{ mod } 26 = [5, 8, 13]$

f) Now, translating the numbers to alphabets, 5=F, 8=I, and 13=N.
Therefore, our ciphertext is FIN.

g) For decryption, follow the reverse procedure. Take the cipher matrix and multiply it with the inverse of the key matrix. Take the mod26 of the result which when converted to alphabets gives us our original plaintext back!

iii. Vigenère cipher

iv. One-Time Pad cipher

One-Time Pad is a provably secure cryptosystem was developed by Gilbert Vernam is 1918.

Process:

- a) The message is represented in the form of a binary string of 0's and 1's using a coding mechanism like ASCII coding.
- b) The key is a truly random sequence of 0's and 1's, which has the length, same as that of the message.
- c) The encryption is done by adding key to message modulo 2, bit by bit. This process is also called as performing XOR operation.
- d) XOR table
- e) Example : message = "IF"
ASCII: 1001001 1000110
Key: 1010110 0110001
Cipher: 0011111 1110111

v. Monoalphabetic cipher

4. Compare in Tabular fashion, Confidentiality, Integrity, Authentication and Non repudiation for following security techniques
 - a. Classical Encryption/Decryption
 - b. Symmetric Encryption
 - c. Asymmetric Encryption
 - d. Hashing Technique
 - e. MAC technique
 - f. Digital Signature System

Service	Encryption Classical	Symmetric Encryption Modern	Asymmetric Encryption Modern	Hashing (md5,sha)	MAC (hmac,cmac)	Digital Signature
Confidentiality	Yes	Yes	Yes	No	Yes	Yes
Integrity	No	No	No	Yes	Yes	Yes
Authentication	No	Yes/No	Yes	No	Yes/No	Yes
Non-Repudiation	No	Yes/No	Yes	No	Yes/No	Yes

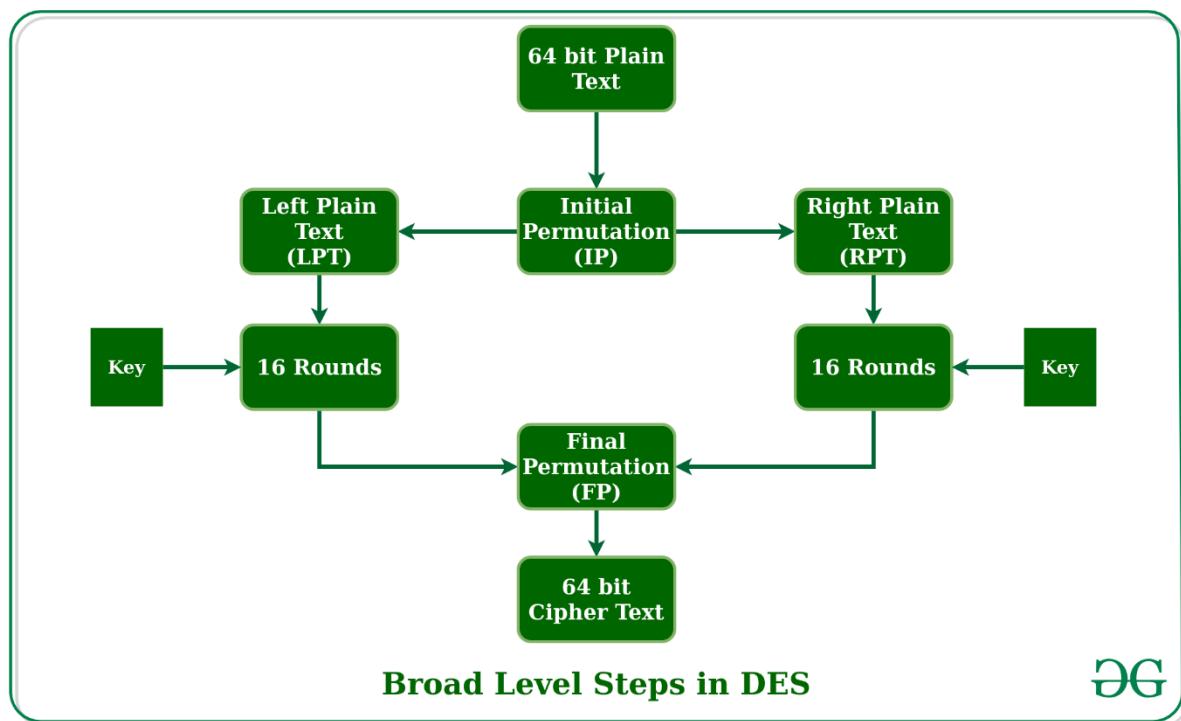
5. Explain DES algorithm in detail.

DES stands for Data Encryption Standard. DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is **56 bits**.

DES is based on the two fundamental attributes of cryptography: substitution and transposition. DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition.

Let us now discuss the broad-level steps in DES.

- In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.
- The initial permutation is performed on plain text.
- Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).
- Now each LPT and RPT go through 16 rounds of the encryption process.
- In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
- The result of this process produces 64-bit ciphertext.



Initial Permutation(IP): It happens only once and it happens before the first round. It suggests how the transposition in IP should proceed.

Key Transformation: Initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available. From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called key transformation.

Expansion Permutation: After the initial permutation, we had two 32-bit plain text areas called Left Plain Text(LPT) and Right Plain Text(RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called expansion permutation.

6. Compare classical Vs Modern Cryptography.

Aspect	Classical Cryptography	Modern Cryptography
Time Period	Before the 20th century	20th century onwards
Key Management	Manual key exchange and distribution	Automated key exchange and distribution
Encryption Algorithms	Substitution and transposition ciphers	Symmetric and asymmetric encryption algorithms
Security Strength	Typically weaker security	Stronger security
Security Assumptions	Often relies on the secrecy of the algorithm	Relies on computational complexity assumptions
Complexity	Simpler algorithms	Complex mathematical algorithms
Cryptanalysis Techniques	Relatively basic and limited techniques	Advanced mathematical and computational methods
Dependence on Computers	Not dependent on computers	Heavily dependent on computers
Use of Cryptographic Protocols	Rarely used	Widely used

7. What is DoS attack? What is DDoS attack? How to Mitigate it?

The attacker attempts to overwhelm the target system's resources, such as network bandwidth, processing power, memory, or disk space. By sending a large volume of requests or flooding the target with excessive traffic, the attacker consumes the available resources, making them unavailable for legitimate users.

DDOS :

A Distributed Denial-of-Service (DDoS) attack is a more advanced form of a Denial-of-Service attack in which multiple compromised systems, often referred to as a botnet, are used to overwhelm a target system or network with a flood of illegitimate requests or excessive traffic.

Traffic Filtering: Implementing network filtering mechanisms, such as firewalls or intrusion prevention systems (IPS), can identify and block traffic that matches known DDoS attack patterns.

Rate Limiting: Setting up rate-limiting mechanisms, such as request or connection limits, can restrict the number of requests from individual sources.

Incident Response Plan: Having a well-defined incident response plan in place enables organizations to respond swiftly to a DDoS attack. It includes procedures for detecting, analyzing, and mitigating the attack

8. Write a program of encryption and decryption for transposition cipher. Draw flowchart, algorithm and attach output results for the same.

Use key

- a. MEGABUCK, or
- b. PICTENTG, or
- c. NBAISOKR

for message: please transfer one million dollars to my swiss bank account six two two four

9. Explain C, I, A, Authentication and Non-Repudiation.

Confidentiality: The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.

Integrity: Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

Availability: Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

Authentication: Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password.

Non-Repudiation: Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender

sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

10. Explain the Interruption, Interception, Modification and Fabrication attack. Corelate the said attacks with C,I,A, Authentication and Non-Repudiation.

i. Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file management system.

ii. Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network, and the unauthorized copying of files or programs, packet sniffing and keylogging.

iii. Modification: An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network

iv. Fabrication: An authorized party inserts counterfeit objects into the system.

This is an attack on authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file, SQLi, Email Spoofing

11. Write a program of encryption and decryption for Substitution Cipher-Caesar Cipher. Draw flowchart, algorithm and attach output results for the same. Use key

- a. 3, or
- b. 5, or
- c. 7

for message: please transfer one million dollars to my swiss bank account six two two four

12. Demonstrate installation and configuration of mobile Security app. Explain the different features and record the different working snapshots for the same.

13. What is WEP and WAP security techniques? Explain the details.

WEP (Wired Equivalent Privacy)

WEP is a security protocol used to secure wireless networks. It was introduced as the first security standard for Wi-Fi networks. WEP employs the RC4 encryption algorithm to provide confidentiality and the CRC-32 algorithm for data integrity. However, WEP has several security flaws and is considered weak and vulnerable to various attacks.

Key Management: WEP uses a shared key approach, where all devices on the network share the same encryption key.

Due to its vulnerabilities, WEP is no longer considered secure, and it is strongly recommended to use more robust security protocols such as WPA or WPA2.

WPA (Wi-Fi Protected Access)

WPA is a security protocol designed to overcome the weaknesses of WEP. It provides improved security for Wi-Fi networks. WPA introduced two versions: WPA and WPA2, with WPA2 being the more secure and widely adopted option.

WPA/WPA2 uses a more robust key management system called 802.1X authentication, which allows for dynamic key generation and distribution.

WPA2 is currently the recommended security protocol for securing Wi-Fi networks. It provides a higher level of security compared to WPA, and it is compatible with most modern Wi-Fi devices.

14. What are the different wireless components used for Wi-Fi, Bluetooth Communications?

1. Wi-Fi Components:

- Wireless Access Point (WAP): Acts as a central hub for Wi-Fi connections, allowing devices to connect to a network and access the internet.
- Wireless Router: Routes network traffic between devices and manages the connection between the WAP and the internet service provider.
- Wi-Fi Network Interface Card (NIC): Enables a device to connect to a Wi-Fi network and communicate wirelessly.

2. Bluetooth Components:

- Bluetooth Transmitter: Converts data into a Bluetooth signal and transmits it wirelessly.
- Bluetooth Receiver: Receives the Bluetooth signal and converts it back into data for the receiving device.
- Bluetooth Antenna: Enhances the wireless signal strength and range for reliable communication between devices.
- Bluetooth Chipset: Contains the necessary circuitry and protocols for enabling Bluetooth connectivity in devices.

15. Compare symmetric and asymmetric key cryptography.

Symmetric	Assymmetric
One key used to encrypt and decrypt the message	Different keys for encryption and decryption
Single key is shared among all participants decreasing security	Public key is shared only to message senders. Recipient stores private key secretly
Ciphertext size don't differ much from the original plaintext	Ciphertext is bigger than the plaintext
Very fast	Complex and slower
Usually uses 128 or 256 bits keys	Uses key which are at least 1000 bits long
Isn't used in digital signatures	It's used in digital signatures
Scalability is an issue	Easily scalable
Lack of non-repudiation	Allows non-repudiation and authenticity

16. Write details about ISM band frequencies, BT standards & Wi-Fi standards.

A] ISM Band Frequencies:

Industrial, Scientific, and Medical (ISM) bands: A set of radio frequencies designated for unlicensed use worldwide, typically used for wireless communication technologies such as Wi-Fi and Bluetooth. The most commonly used ISM band frequencies are:

- 1) 2.4 GHz ISM Band
- 2) 5.8 GHz ISM Band

B] Bluetooth Standards:

1. Bluetooth 1.x: Introduced in 1999, it provided basic data transfer capabilities.
2. Bluetooth 2.x: Released in 2004, it added enhanced data rate (EDR) for faster transmission.
3. Bluetooth 3.x: Introduced in 2009, it included high-speed data transfer with the introduction of Bluetooth High-Speed (HS).
4. Bluetooth 4.x: Released in 2010, it brought low-energy technology (Bluetooth Low Energy or BLE) for energy-efficient connections.
5. Bluetooth 5.x: Introduced in 2016, it offered longer range, higher data transfer rates, and improved functionality.

C] Wi-Fi Standards:

1. Wi-Fi 802.11b: Released in 1999, it provided a maximum data rate of 11 Mbps in the 2.4 GHz frequency band.

2. Wi-Fi 802.11a: Also released in 1999, it offered a maximum data rate of 54 Mbps but operated in the less crowded 5 GHz frequency band.
3. Wi-Fi 802.11g: Introduced in 2003, it combined the speed of 802.11a and the compatibility of 802.11b, providing a maximum data rate of 54 Mbps in the 2.4 GHz band.
4. Wi-Fi 802.11n: Released in 2009, it brought significant improvements in speed and range, supporting data rates up to 600 Mbps.
5. Wi-Fi 802.11ac: Introduced in 2013, it offered faster speeds, wider channel bandwidth, and improved performance in crowded environments, reaching up to 6.9 Gbps.
6. Wi-Fi 802.11ax (Wi-Fi 6): Released in 2019, it provided higher capacity, improved efficiency, and reduced latency, supporting data rates up to 9.6 Gbps.

17. Explain Transport and tunnel mode in IPSec.

IPSec (Internet Protocol Security) is a protocol suite used to provide secure communication over IP networks. It includes various components, including authentication, encryption, and key management. IPSec can operate in two modes: transport mode and tunnel mode.

Transport Mode:

In transport mode, IPSec secures the payload (the actual data being transmitted) while leaving the original IP header intact. This mode is typically used for securing communication between two endpoints, such as between two hosts or between a host and a router.

In transport mode, IPSec provides the following security services:

Authentication: Ensures the identity of the communicating parties through mechanisms like digital certificates or pre-shared keys.

Encryption: Protects the payload by encrypting its contents to prevent unauthorized access.

Integrity: Verifies that the transmitted data has not been tampered with during transit.

Transport mode is useful when end-to-end security is required within a network, such as for securing voice or video communication between two hosts.

Tunnel Mode:

In tunnel mode, IPSec encapsulates the entire IP packet within a new IP packet. This means that the original IP packet becomes the payload of the new IP packet, which is then encrypted and authenticated. The new IP packet contains a new IP header, which is used for routing between IPSec gateways or endpoints.

Tunnel mode is typically used for securing communication between networks, such as between two routers or between a remote user and a corporate network. It allows for secure communication between networks that may not trust each other.

In tunnel mode, IPSec provides the following security services:

Authentication: Authenticates the IPSec gateways or endpoints participating in the communication.

Encryption: Encrypts the entire original IP packet, including the original IP header and payload, to ensure confidentiality.

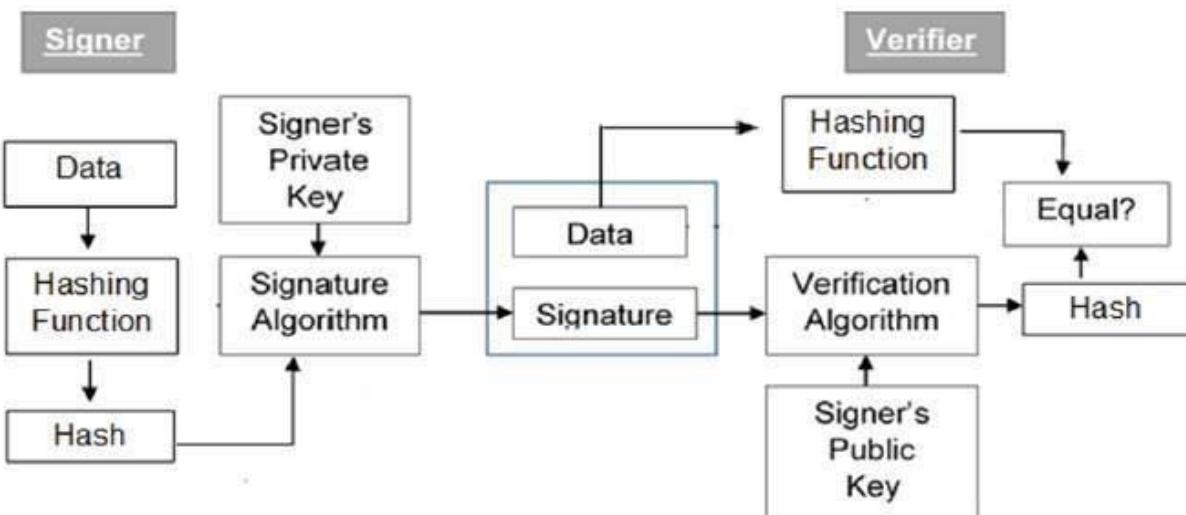
Integrity: Ensures the integrity of the encapsulated IP packet, verifying that it has not been modified during transit.

18. Demonstrate installation and configuration of Steganography technique in view of network security. Explain the different features and record the different working snapshots for the same.
19. Draw and explain the block diagram of Steganography for Image as data. (in file)
20. Compare Steganography versus Cryptography.

	Steganography	Cryptography
Definition	Depend on hiding the message existence	Depend on hiding the message meaning
Purpose	Keep communication secure.	Provide protection for data
Visibility	Never	Always
Failure	When discover the presence of a hidden message	When able to decrypt and read the message
Concern	Embedding capacity and detectability of cover object	Robustness against deciphering.
Carrier	Any type of digital media	Depend on text as a carrier
Key	Optional, but provide more security	Necessary

21. Draw and explain the following block diagrams

a. Digital Signature system.

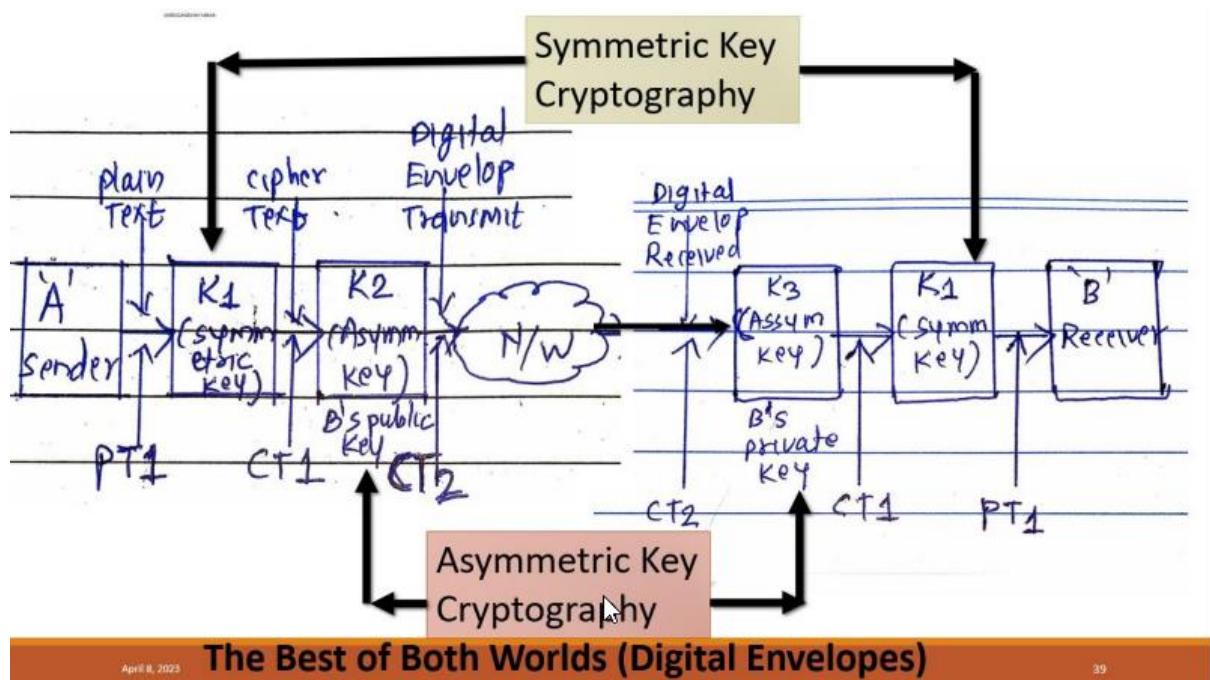


Digital signature is based on public key cryptography. It is the technique that binds a person/entity to the digital data.

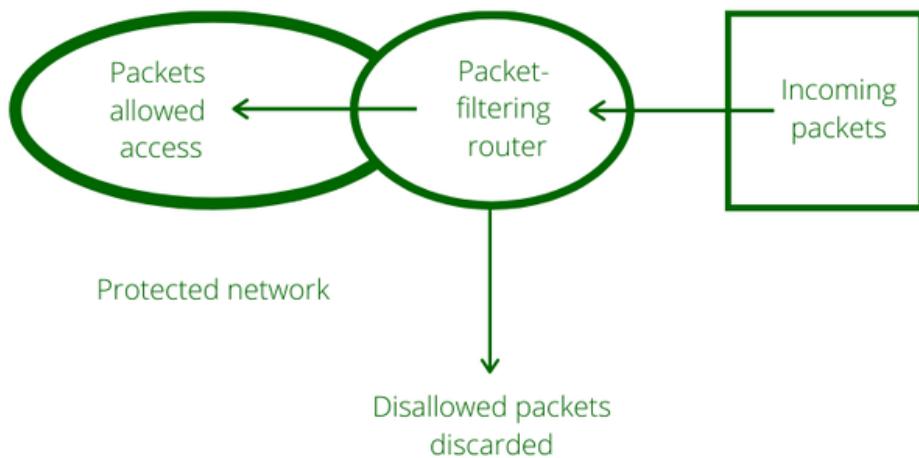
Procedure:

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

- b. End to End Email Communication system with Hashing, Digital signature and Digital Envelope processing blocks.



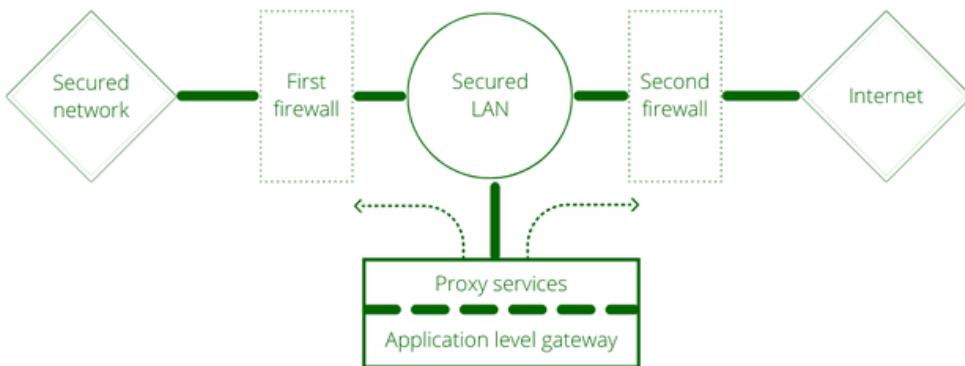
22. Install and configure firewall for Host security. Explain the different features and record the different working snapshots for the same.
23. Draw and explain following.
- A) Packet filtering firewall



- It works in the network layer of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.

- Packet filter firewall controls access to packets on the basis of packet source and destination address or specific transport protocol type. It is done at the OSI (Open Systems Interconnection) data link, network, and transport layers. Packet filter firewall works on the network layer of the OSI model.
- Packet filters consider only the most basic attributes of each packet, and they don't need to remember anything about the traffic since each packet is examined in isolation. For this reason, they can decide packet flow very quickly.
- Example: Filter can be set to block all UDP segments and all Telnet connections. This type of configuration prevents outsiders from logging onto internal hosts using Telnet and insider from logging onto external hosts using Telnet connections.

B) Application and Circuit Layer Gateway Firewall



- Application-level gateway is also called a bastion host. It operates at the application level. Multiple application gateways can run on the same host but each gateway is a separate server with its own processes.
- These firewalls, also known as application proxies, provide the most secure type of data connection because they can examine every layer of the communication, including the application data.
- Example: Consider FTP service. The FTP commands like getting the file, putting the file, listing files, and positioning the process at a particular point in a directory tree. Some system admin blocks put command but permits get command, list only certain files, or prohibit changing out of a particular directory. The proxy server would simulate both sides of this protocol exchange. For example, the proxy might accept get commands and reject put commands.

24. Compare Firewall Versus Antivirus.

S.NO	Firewall	Antivirus
1.	Firewall is implemented in both hardware and software.	Antivirus is implemented in software only.
2.	Firewall deals with external threats only.	Antivirus deals with both external threats and internal threats.
3.	In firewall counter attacks are possible such as IP Spoofing and routing attacks.	In antivirus no counter attacks are possible after removing the malware.>
4.	Firewall works on monitoring and filtering.	Antivirus works on Scanning of infected files and software.
5.	Firewall checks the threat from incoming packets.	Antivirus checks the threat from malicious software.
6.	Firewall saves the system from all kinds of threats to the system.	Antivirus saves the system only from viruses.
7.	Firewall's programming is complex than antivirus.	Antivirus's programming is simpler as comparison to firewall.

25. Compare IDS and IPS in detail.

PARAMETER	IPS	IDS
Abbreviation for	Intrusion Prevention System	Intrusion Detection System
System Type	Active (monitor & automatically defend) and/ or passive	Passive (monitor and Notify)
Detection mechanism	Statistical anomaly based detection Signature detection: * Exploit-facing signatures * Vulnerability-facing signatures	Signature detection: * Exploit-facing signatures
Placement	Inline to data communication	Out of band from data communication
Anomaly response	Drop, alert or clean malicious traffic	Sends alarm/alert of detecting malicious traffic
Network performance impact	Slow down network performance due to delay caused by inline IPS processing	Does not impact network performance due to non-line deployment of IDS.
Benefits	Preferred by most organization since detection and prevention are automatically performed	Does not block legitimate traffic which might be blocked by IPS at times.

26. Demonstrate process to ensure Security of web browser (Google Chrome) with respect to A) Cookies settings B) Website Blocking C) Phrase/Word blocking. Explain the different features and record the different working snapshots for the same.

27. What are different types of cookies?

A] Cookies Based on Source

- **First-party cookies** – The user's browser sets first-party cookies when they visit a website. The information gathered by first-party cookies is used to calculate page views, sessions, and the number of users. Ad agencies and advertisers primarily utilize it to locate potential ad targets.
- **Third-party cookies** – These are set by domains that the user does not visit directly. This occurs when publishers include third-party elements on their website (such as a chatbot, social plugins, or advertisements).

B] Cookies Based on Duration

- **Session cookie** – A session cookie is a file that a website server delivers to a browser with an identification (a string of letters and numbers) for temporary use during a set period. By default, session cookies are enabled. Their goal is to make individual webpages load faster and improve website navigation.
- **Persistent cookies** – Persistent cookies are those that remain in the browser for an extended length of time. They will only be erased when the cookies expire or the users clear them from the browser after being installed.

C] Cookies Based on Purpose

- **Necessary cookies** – These are cookies that have to be present for a website to work.
- **Non-Necessary cookies** – These cookies help keep track of the behavior on a browser.

28. What are advantages and drawback of cookies?

Advantages:

- a) User Friendly: Cookies are extremely user friendly. The client can choose what they need to do with cookies.
- b) Availability: Once the cookies are stored on the user's hard drive, it will be available as long as the user deletes them manually.
- c) Convenience: Besides websites, cookies can also remember information related to forms. So, it becomes very convenient to fill a new form with Autofill.
- d) Marketing: Most companies, especially, e-commerce sites tends to use cookies to target products to their customers.

Drawbacks:

- a) Browser Impacts: Whenever a user surfs the web, more and more cookies will be accumulated. Unless the user deletes them, these cookies will be a part of the hard drive space. This eventually slows down or lags the browser.
- b) Security Risks: Not all the sites that collect information from cookies are legitimate. Some of them can be malicious that uses cookies for the purpose of hacking.
- c) Size Limitation: Size limitations also exist on cookies. They cannot store large amount of information. Most cookies are able to store information only up to 4kb
- d) Privacy Concern: Whenever the user browses the internet, the cookie enabled sites will be recording all the online activities. Most users are unaware that such information are stored on their hard drive.

29. Explain “Session Hijacking” by misusing cookies information.

Session hijacking, also known as session sidejacking, is a security attack where an attacker intercepts and misuses the session information contained within cookies to gain unauthorized access to a user's session on a website or web application.

Intercepting Cookies: The attacker intercepts the cookies transmitted between the user's browser and the website. This can be achieved through various means, such as sniffing network traffic, exploiting vulnerabilities in the network infrastructure, or using malicious software on the user's device.

Obtaining Session Information: Cookies often contain session identifiers or tokens that are used to authenticate and authorize user sessions. By obtaining these session details from the intercepted cookies, the attacker gains access to the victim's session information.

Impersonating the User: With the hijacked session information, the attacker can assume the user's identity and access their account or session on the targeted website. This gives the attacker the same privileges and access rights as the victim, potentially allowing them to perform unauthorized actions, access sensitive information, or manipulate the victim's account.

30. Explain TLS and S/MIME used in Email Security. Compare PGP Vs S/MIME.

a] TLS is a cryptographic protocol that ensures secure communication between email servers. It establishes an encrypted connection, commonly known as SSL/TLS handshake, between the sending and receiving mail servers. TLS protects the confidentiality and integrity of email messages during transit, preventing eavesdropping and tampering.

b] S/MIME is a standard for securing email messages using digital certificates and encryption. It provides end-to-end security by encrypting the content of the email and digitally signing it to ensure message integrity and authenticity.

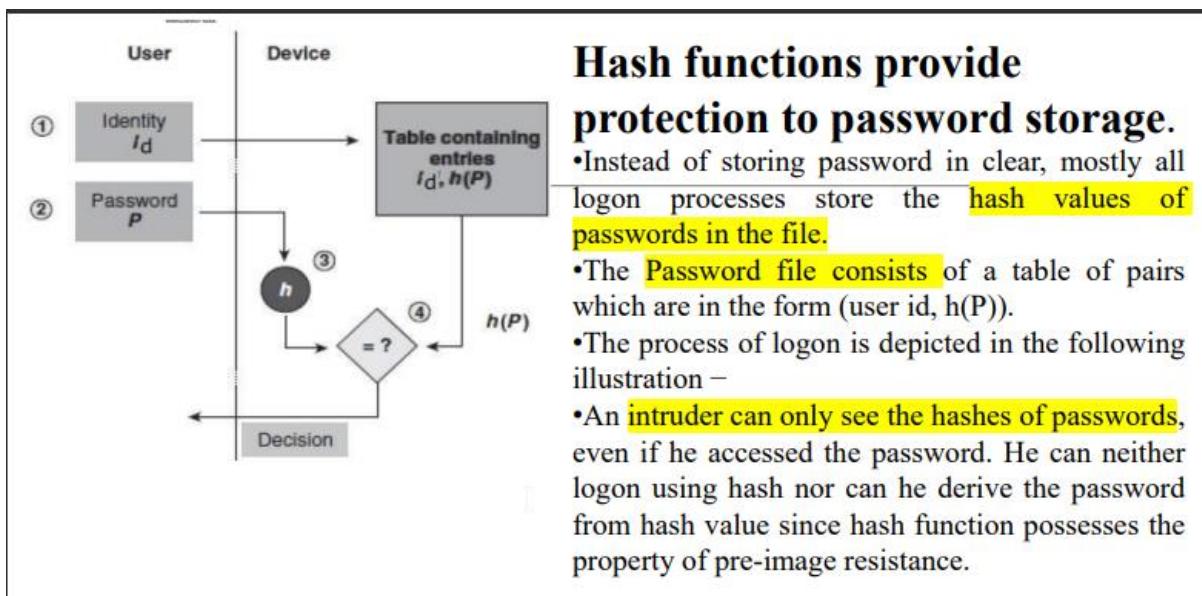
Comparison between PGP and S/MIME

S.NO	PGP	S/MIME
1.	It is designed for processing the plain texts	While it is designed to process email as well as many multimedia files.
2.	PGP is less costly as compared to S/MIME.	While S/MIME is comparatively expensive.
3.	PGP is good for personal as well as office use.	While it is good for industrial use.
4.	PGP is less efficient than S/MIME.	While it is more efficient than PGP.
5.	It depends on user key exchange.	Whereas it relies on a hierarchically valid certificate for key exchange.
6.	PGP is comparatively less convenient.	While it is more convenient than PGP due to the secure transformation of all the applications.
7.	PGP contains 4096 public keys.	While it contains only 1024 public keys.
8.	PGP is the standard for strong encryption.	While it is also the standard for strong encryption but has some drawbacks.
9.	PGP is also be used in VPNs.	While it is not used in VPNs, it is only used in email services.
10.	PGP uses Diffie hellman digital signature.	While it uses Elgamal digital signature.

31. Implement Hash function technique for secured network using Suitable Hashing tool and Validate using available online tools/Website tools. Explain the different features and record the different working snapshots for the same.

32. Explain following applications of Hash functions in detail

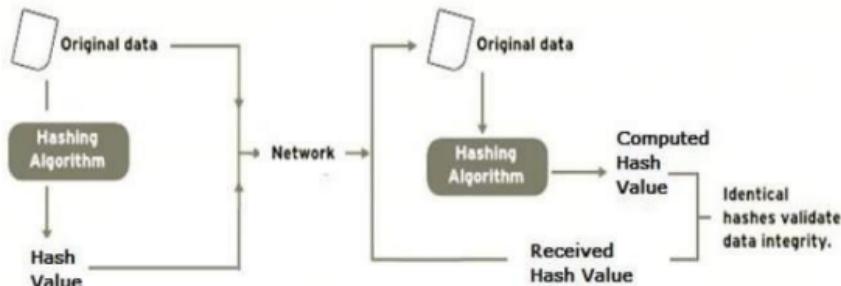
a. Protection to password storage



b. Data Integrity check

Data Integrity Check

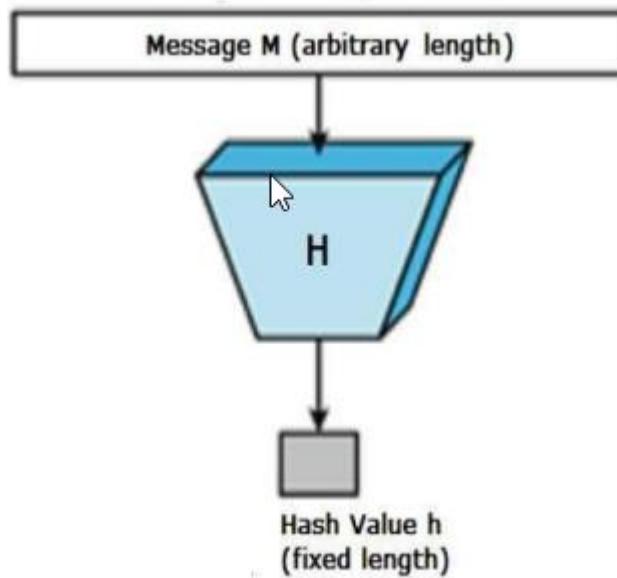
Data integrity check is a most common application of the hash functions. It is used to generate the checksums on data files. This application provides assurance to the user about correctness of the data. The process is depicted in the following illustration –



The integrity check helps the user to detect any changes made to original file. It however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver. This integrity check application is useful only if the user is sure about the originality of file.

33. What is Hash function? Explain How it works briefly? List the different applications of SHA2.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. Values returned by a hash function are called message digest or simply hash values.

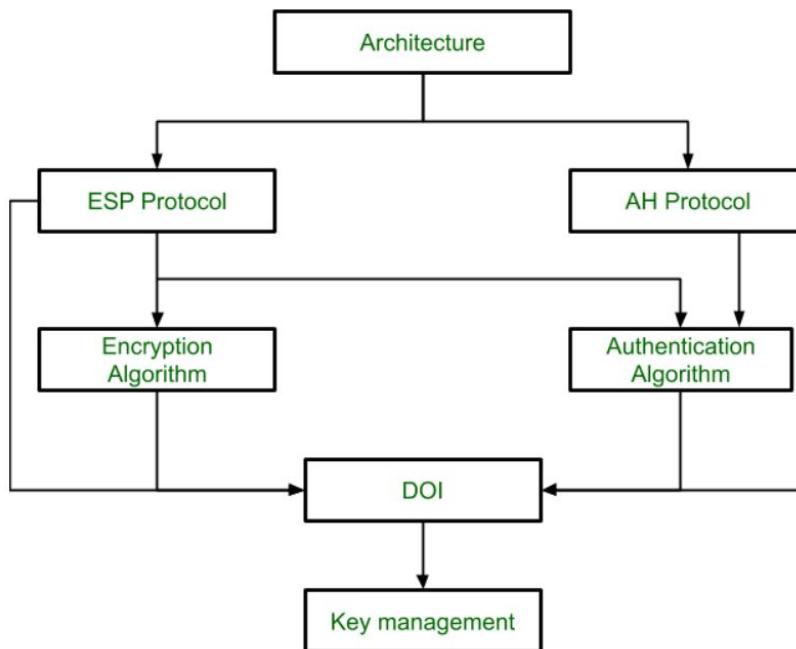


- Hash function converts data of arbitrary length to a fixed length. This process is often referred to as **hashing the data**.
- In general, the hash is much smaller than the input data, hence hash functions are sometimes called **compression functions**.
- Since a hash is a smaller representation of a larger data, it is also referred to as a **digest**.
- Hash function with n bit output is referred to as an **n -bit hash function**. Popular hash functions generate values between 160 and 512 bits.
- Generally for any hash function h with input x , computation of $h(x)$ is a fast operation.
- Computationally hash functions are much faster than a symmetric encryption.

34. Simulate Diffie-Hellman secure key exchange protocol using Vlabs simulation tool. Explain the different features of above protocol and record the different working snapshots for the same.
35. Simulate Vernam Cipher for encryption and decryption using Vlabs simulation tool. Explain the different features of above technique with suitable example and record the different working snapshots for the same.

36. Explain AH and ESP working in IPSec.

IPSec Architecture:



IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authentication
- Integrity

Difference Basis	Authentication Header	Encapsulating Security Payload
Function	It provides a mechanism for Sender Data Origin Authentication. So it cannot provide data Confidentiality/Encryption.	Provides Data Authentication and Data Privacy/Encryption and So it ensures both Confidentiality and Integrity for Packet Payload.
Difference in Authentication Process Coverage	It authenticates the entire IP packet, including the outer IP header.	It authenticates only the IP datagram portion of the IP packet.
Working through NATed network	It will not work through a NATed network as it hashes both the payload and header of a packet while NAT changes the IP header of a packet during translation.	It uses a hash algorithm for data integrity which does not include the IP header of the packet, thus ESP will work normally through a NATed device.