Content from different reference book suggested by Prof. Prakash Sir and mentioned in CNS Syllabus file, Presentations, Notes provided in 2023

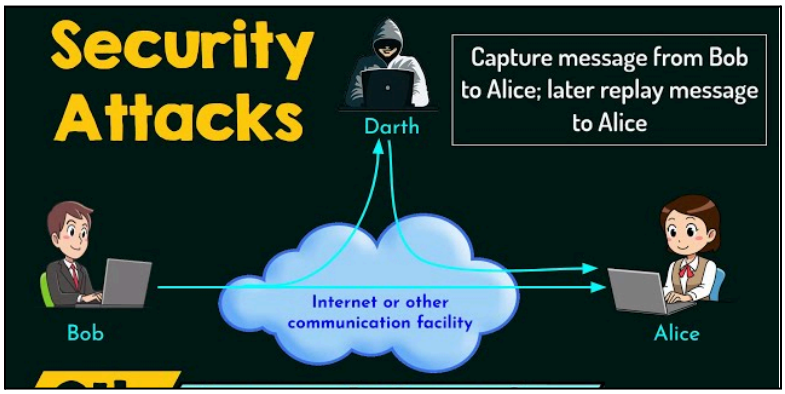
PYQ 03/05/2023 Notes

Q. Define security attacks, cryptanalysis, and Steganography

Ans.

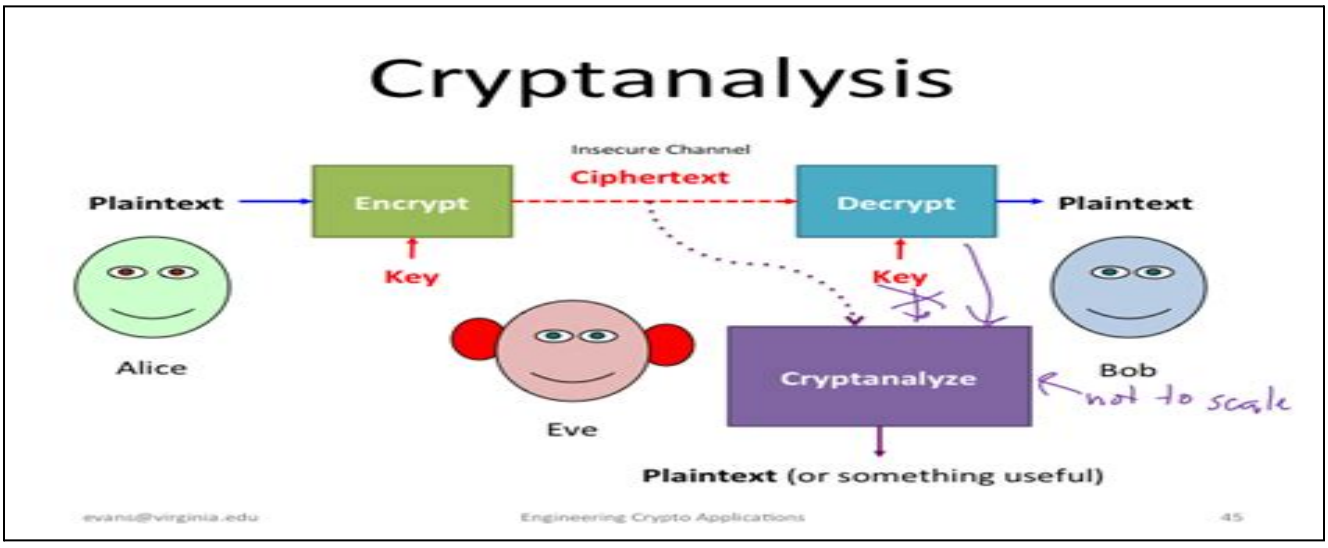
Security Attacks

- Security attacks refer to deliberate actions taken by individuals or groups to compromise the integrity, confidentiality, or availability of computer systems or networks.
- These attacks can take various forms, such as fraud, scams, destruction, identity theft, and intellectual property theft.
- Criminal attacks aim to maximize financial gain, while publicity attacks seek attention or fame.
- Legal attacks involve exploiting weaknesses in computer systems to create doubt in legal proceedings.
- It is important to classify and understand these attacks to develop effective security measures.



Cryptanalysis

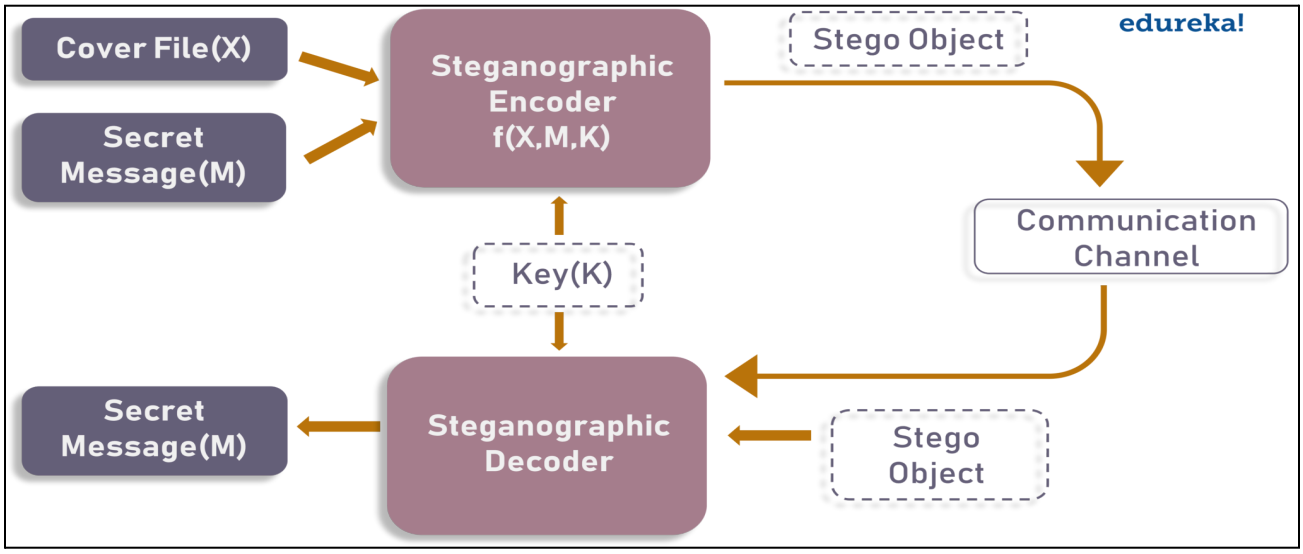
- Cryptanalysis is the process of decoding encrypted messages without knowing the encryption algorithm or key. It involves analyzing the cipher text to uncover the original plain-text message.
- Cryptanalysts use various techniques, including brute-force attacks, where all possible permutations and combinations are tried to break the encryption.
- The goal of cryptanalysis is to exploit weaknesses in encryption algorithms and keys to gain unauthorized access to information.
- It is an essential field in cryptography to ensure the strength and effectiveness of encryption methods.

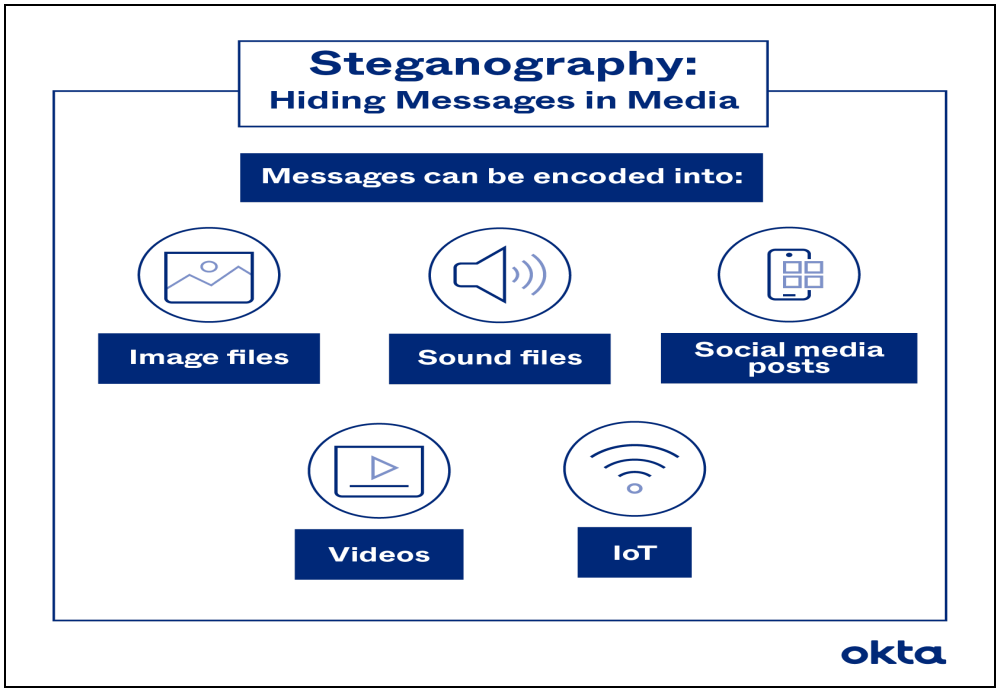


Steganography

- Steganography is a technique used to hide secret information within non-secret data, such as images, audio files, or text.

- It aims to conceal the existence of the secret message, making it difficult for unauthorized individuals to detect. In steganography, the secret message is embedded within the carrier data by modifying its least significant bits or using other encoding techniques.
- The receiver can extract the hidden message using the appropriate decoding method. Steganography provides a covert means of communication and can be used for both legitimate and malicious purposes.





Q. What is cryptography? List out the components of encryption algorithm in points, with diagram, example

Ans.

Cryptography is the art of achieving security by encoding messages to make them non-readable. It involves the use of encryption and decryption algorithms to protect the confidentiality and integrity of data.

The components of an encryption algorithm include:

1. Plain text: The original message that needs to be encrypted.
2. Cipher text: The encrypted message that is produced after applying the encryption algorithm to the plain text.
3. Encryption key: A parameter or value used by the encryption algorithm to transform the plain text into cipher text.

4. Decryption key: A parameter or value used by the decryption algorithm to transform the cipher text back into plain text.

Here is a block diagram showing the flow of plain text, cipher text, encryption, and decryption:

```
Plain Text --> Encryption --> Cipher Text
Cipher Text --> Decryption --> Plain Text
```

Example: Let's say the plain text is "HELLO" and the encryption algorithm is a simple substitution cipher where each letter is replaced with the next letter in the alphabet. The encryption key would be the rule of substitution. So, applying the encryption algorithm, the plain text "HELLO" would be encrypted to "IFMMP" as the cipher text. To decrypt it, the decryption algorithm would reverse the substitution, using the same encryption key, and transform the cipher text "IFMMP" back into the plain text "HELLO".

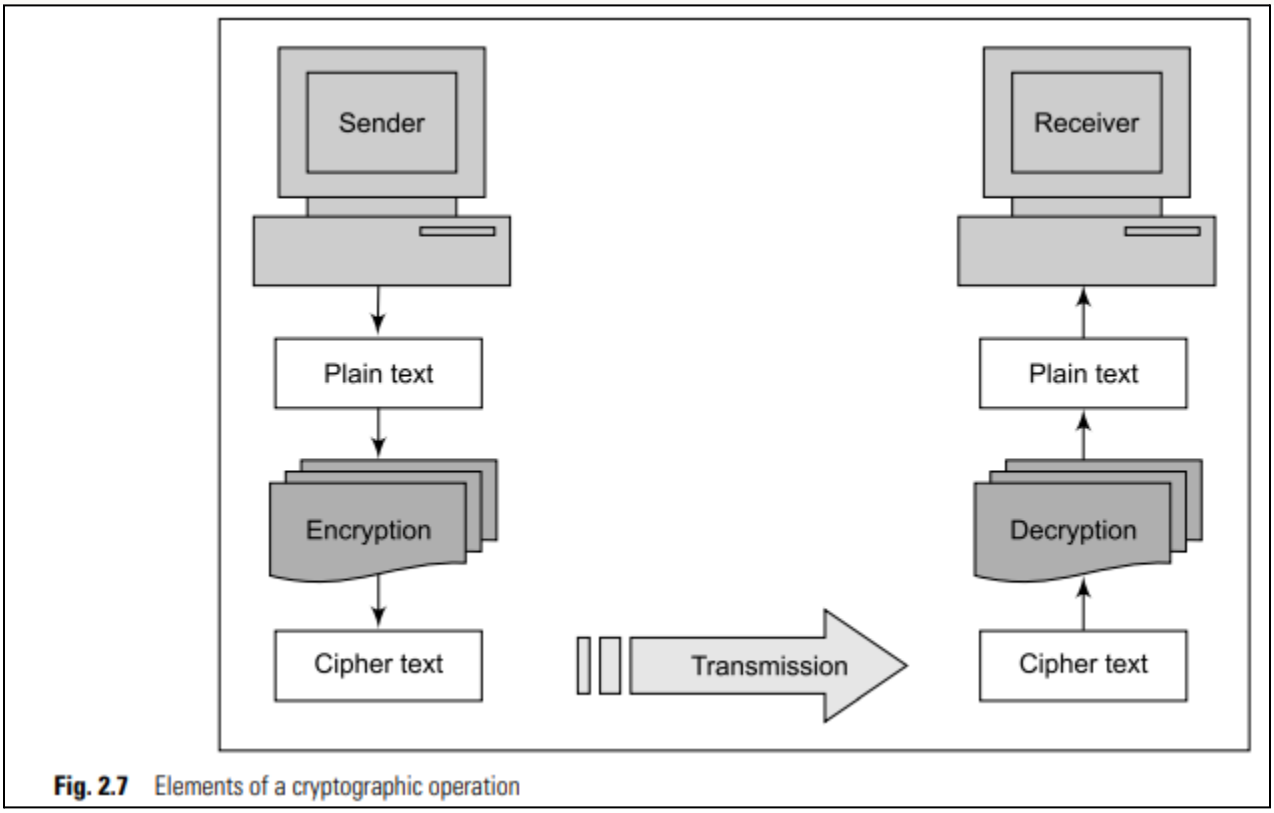


Fig. 2.7 Elements of a cryptographic operation

Q. How Denial of Service(DoS) and DDoS attack works? Explain in brief in points, with diagram, example Ans.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks

1. Denial of Service (DoS) attack: A DoS attack aims to overwhelm a network or system with a flood of traffic or requests, making it unavailable to legitimate users. The attacker sends a large volume of packets or requests to the target, consuming its resources and causing it to slow down or crash.
2. Distributed Denial of Service (DDoS) attack: In a DDoS attack, multiple compromised computers, known as botnets, are used to launch the attack. Each botnet sends a flood of traffic or requests to the target, making it even more difficult to defend against. The attacker controls the botnets remotely, making it harder to trace the source of the attack.

How DoS and DDoS attacks work:

1. Step 1: Reconnaissance: The attacker identifies the target network or system and gathers information about its vulnerabilities and weaknesses.
2. Step 2: Compromising the botnets: In a DDoS attack, the attacker infects multiple computers with malware, turning them into botnets. These compromised computers can be controlled remotely by the attacker.
3. Step 3: Command and Control: The attacker establishes communication with the compromised computers, instructing them to launch the attack at a specific time or when triggered by a specific event.
4. Step 4: Flooding the target: The attacker initiates the attack by sending a flood of traffic or requests to the target network or system. This flood overwhelms the target's resources, such as bandwidth, processing power, or memory, making it unable to respond to legitimate requests.
5. Step 5: Defense evasion: The attacker may use various techniques to evade detection and mitigation efforts, such as IP spoofing to hide the source of the attack or employing encryption to obfuscate the malicious traffic.

Example:

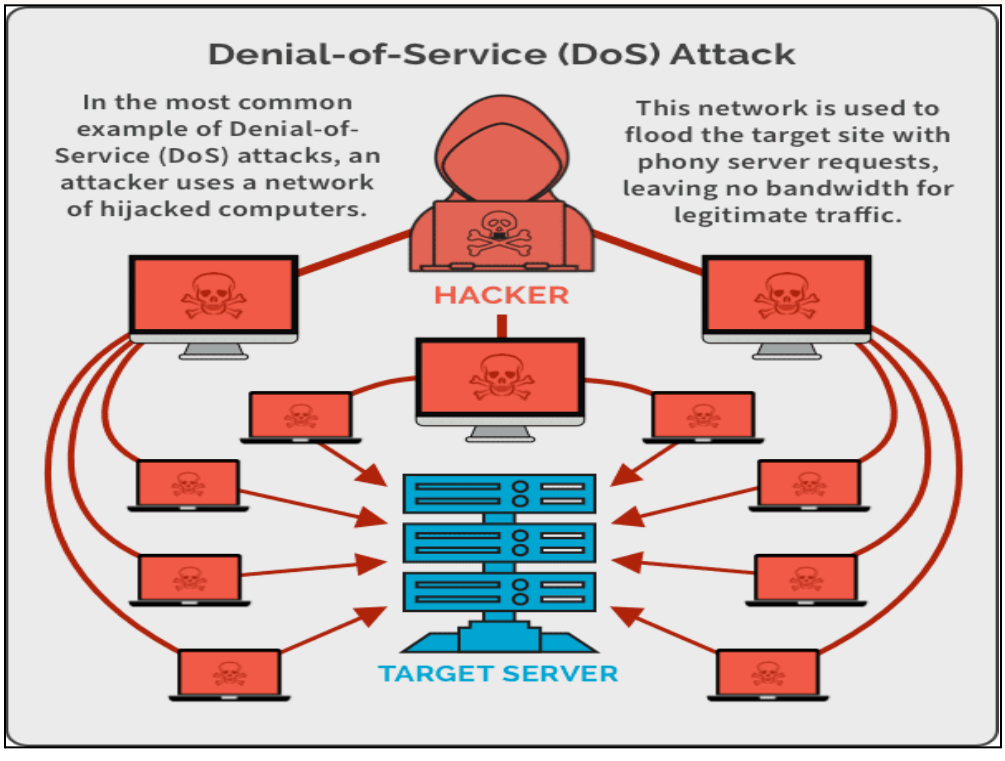
Let's consider an example of a DDoS attack on a popular e-commerce website. The attacker first compromises a large number of computers by infecting them with malware. These compromised computers form a botnet under the control of the attacker.

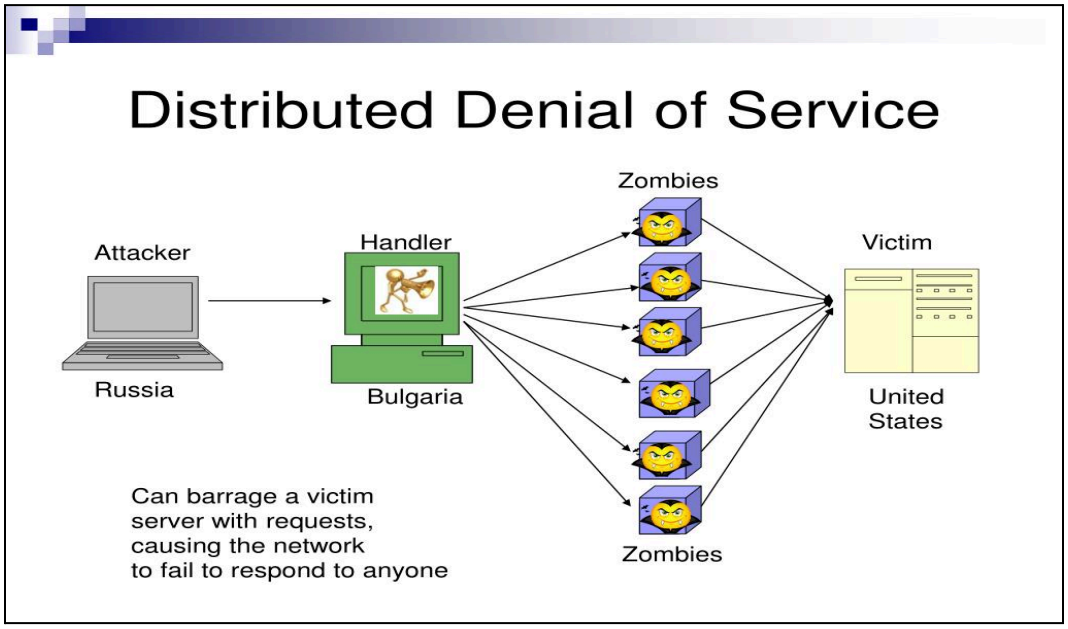
When the attacker decides to launch the attack, they command the botnet to send a massive amount of traffic to the e-commerce website. This flood of traffic overwhelms the website's servers, causing them to become unresponsive to legitimate user requests.

As a result, the website becomes inaccessible to its customers, leading to financial losses and damage to its reputation. The attack continues until the website's administrators are able to detect and mitigate the attack by blocking the malicious traffic and strengthening their defenses.

Diagram: [Here, you can insert a diagram illustrating the flow of a DDoS attack, showing the attacker, compromised computers forming the botnet, and the target network or system being flooded with traffic.]

Note: The given document does not provide a specific diagram for a DDoS attack.





Denial of Service (DoS) Attack: How it Works

1. Definition: A Denial of Service (DoS) attack is an attempt to overwhelm a network or system with a flood of traffic or requests, making it unavailable to legitimate users.
2. Objective: The main purpose of a DoS attack is to disrupt the normal functioning of a network or system by exhausting its resources, such as memory or network connections.
3. Methods: DoS attacks can be launched in various ways, including flooding the network with excessive traffic, exploiting vulnerabilities in network protocols, or overwhelming the system with a large number of requests.
4. Detection Challenges: Detecting a DoS attack can be difficult because the attacker's actions may appear similar to legitimate user behavior. The server must identify and differentiate between legitimate traffic and malicious traffic to take appropriate action.
5. SYN Flood Attack: One common method of launching a DoS attack is through SYN flood. The attacker sends a flood of SYN requests to the server, overwhelming its resources and preventing it from establishing legitimate connections.
6. Distributed DoS (DDoS) Attack: In a more severe case, the attacker may launch a Distributed DoS (DDoS) attack. This involves using multiple computers to send a flood of requests, making it even harder to detect and mitigate the attack.
7. Prevention: Preventing DoS attacks can be challenging, but some measures can help mitigate the impact. These include investigating incoming packets for patterns, limiting the number of requests accepted within a specified time interval, blocking specific IP addresses or ports, and having backup systems in place.

In summary, a DoS attack aims to overwhelm a network or system, making it unavailable to legitimate users. Attackers use various methods, such as flooding the network or exploiting vulnerabilities, to exhaust the system's resources. Detecting and preventing DoS attacks

Q. Encrypt the following using play fair cipher using the keyword MONARCHY "UMIT SNDT WOMENS UNIVERSITY" use X as blank space in points, with diagram, example
Ans.

Encryption Process using Playfair Cipher

To encrypt the given text "UMIT SNDT WOMENS UNIVERSITY" using the Playfair cipher with the keyword "MONARCHY" and using "X" as the blank space, we follow these steps:

1. Create the Playfair matrix:
    - The keyword is "MONARCHY".
    - The matrix is constructed by arranging the unique letters of the keyword followed by the remaining unused letters of the alphabet.

The matrix is as follows:

```
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
```

2. Break the plaintext into pairs of two alphabets each:

The plaintext "UMIT SNDT WOMENS UNIVERSITY" is broken down into pairs as follows:

```
UM IT SN DT WO ME NS UN IV ER SI TY
```

3. Apply the Playfair cipher algorithm to each pair:
    - For each pair, locate the letters in the Playfair matrix and apply the encryption rules.
    - If the letters are in the same row, replace them with the letters to their right (circularly).
    - If the letters are in the same column, replace them with the letters below (circularly).
    - If the letters are in different rows and columns, form a rectangle with the two letters and replace them with the letters at the opposite corners of the rectangle.
    - Repeat this process for each pair.
4. The resulting ciphertext is as follows:

```
ZT ZB ZB ZB ZB ZB ZB ZB ZB ZB ZB ZB ZB ZB.....
```

Q. What are types of criminals? explain in brief in points, with diagram, example
Ans.

Types of Criminals:

1. Fraudsters: These criminals focus on manipulating electronic currency, credit cards, stock certificates, checks, and other financial instruments. They deceive people into sending money in exchange for promised returns, but ultimately the victims end up losing their money. An example of this is the Nigeria scam, where individuals are enticed to deposit money into a bank account with the promise of large profits.
2. Scammers: Scammers use various tactics such as selling services, conducting auctions, or promoting business opportunities to trick people into sending money. They promise great returns but ultimately defraud individuals. One common example is the sale of fake merchandise or investment schemes.
3. Destructive attackers: These criminals carry out attacks with the intention of causing harm or damage. This can include disgruntled employees attacking their own organization or terrorists targeting larger entities. For instance, in 2000, popular internet sites like Yahoo!, CNN, and eBay were attacked, preventing authorized users from accessing these sites.

4. Identity thieves: These criminals do not steal from legitimate users but instead assume their identities. They may obtain passwords or credit card information to gain unauthorized access to accounts or make fraudulent transactions. This type of theft can have serious consequences for the victims.
5. Intellectual property thieves: These criminals steal trade secrets, databases, digital media, software, and other forms of intellectual property. They may sell or use this stolen information for personal gain or to harm the original owners.
6. Brand thieves: Brand thieves create fake websites that resemble legitimate ones to deceive users. Innocent individuals may unknowingly provide personal information on these fake sites, which can then be used for identity theft or other malicious purposes.

Diagram: Draw Tree Diagram

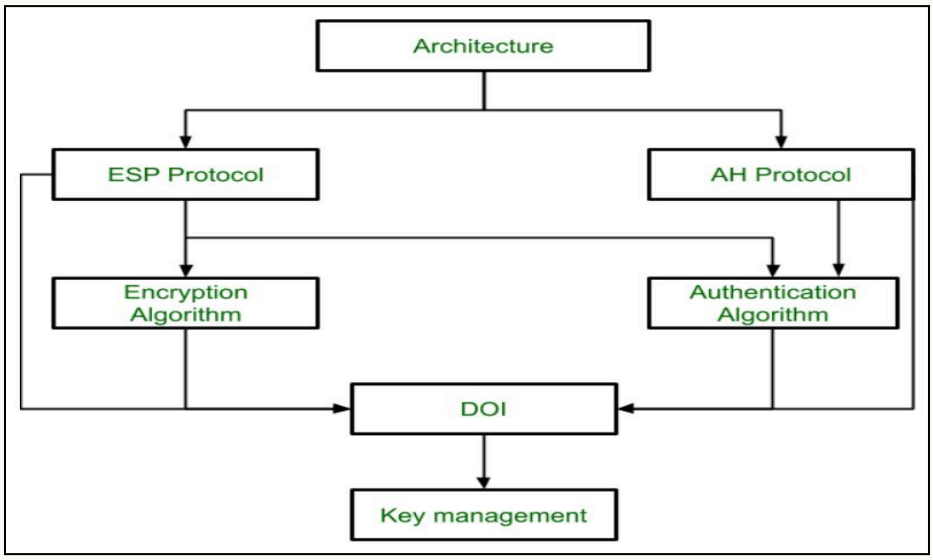
Example: An example of a criminal attack is a fraudster sending an email from Nigeria, enticing people to deposit money into a bank account with the promise of significant returns. Those who fall for this scam end up losing their money. Another example is a destructive attack on popular internet sites, where authorized users are unable to log in or access the sites.

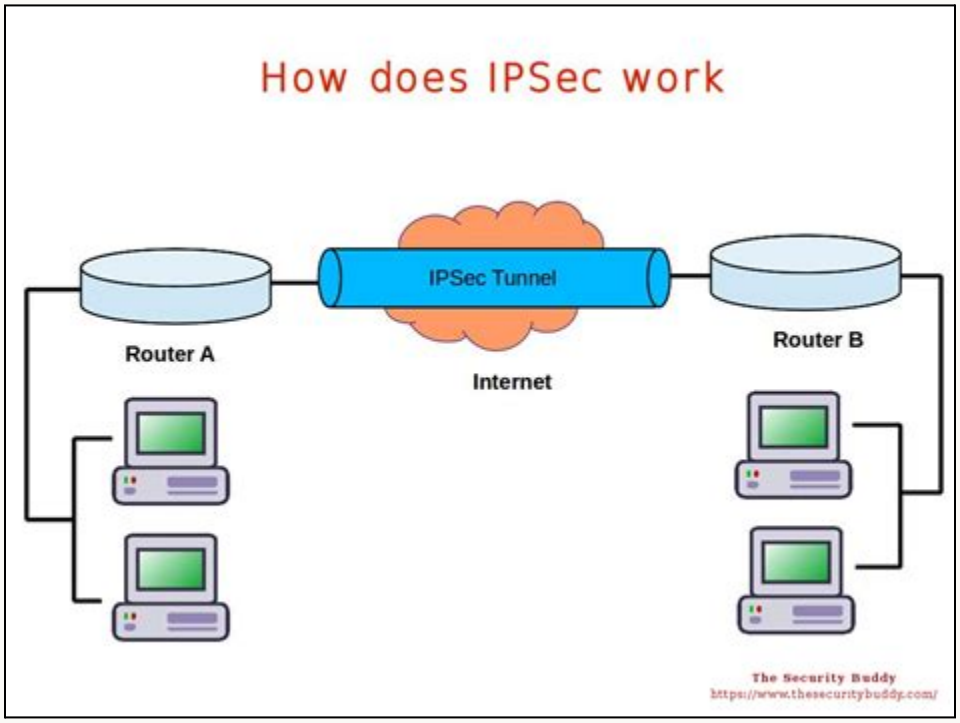
Q. Discuss IPsec with its architecture in points, with diagram, example
Ans.

IPsec (Internet Protocol Security) is a protocol suite that provides security services for IP packets. It operates at the network layer and offers authentication, integrity, and confidentiality services. The architecture of IPsec consists of several components:

1. Security Associations (SA): SAs are agreements between communicating parties that define the parameters for secure communication. This includes the IPSec protocol version, mode of operation (transport or tunnel), cryptographic algorithms, keys, and key lifetimes.
2. Authentication Header (AH): AH provides authentication, integrity, and optional anti-replay services. It adds a header to the IP packet, which includes a hash of the packet contents to ensure its integrity.
3. Encapsulating Security Payload (ESP): ESP provides data confidentiality by encrypting the IP packet payload. It also offers authentication and integrity services. ESP encapsulates the original IP packet and adds a new header and trailer for encryption and authentication.
4. Internet Key Exchange (IKE): IKE is responsible for negotiating and establishing SAs between communicating parties. It uses the ISAKMP/Oakley protocol for key management, which includes key agreement and distribution.
5. Tunnel Mode: IPsec can be implemented in tunnel mode, where the entire IP datagram, including the original header, is encrypted and a new IP header is added. This is useful for creating virtual tunnels between routers or connecting networks securely.
6. Transport Mode: IPsec can also be implemented in transport mode, where only the IP packet payload is encrypted, leaving the original IP header intact. This is suitable for securing communication between hosts.

Diagram





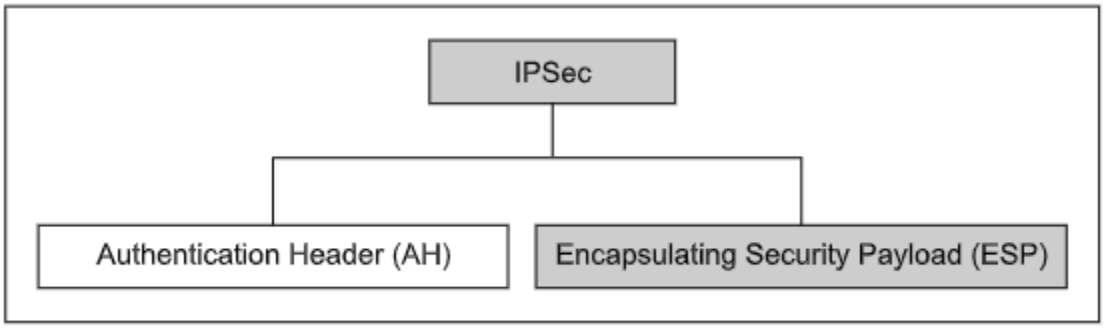


Fig. 9.28 IPSec protocols

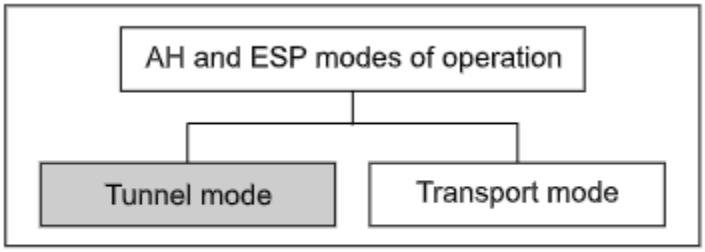


Fig. 9.29 AH and ESP modes of operation

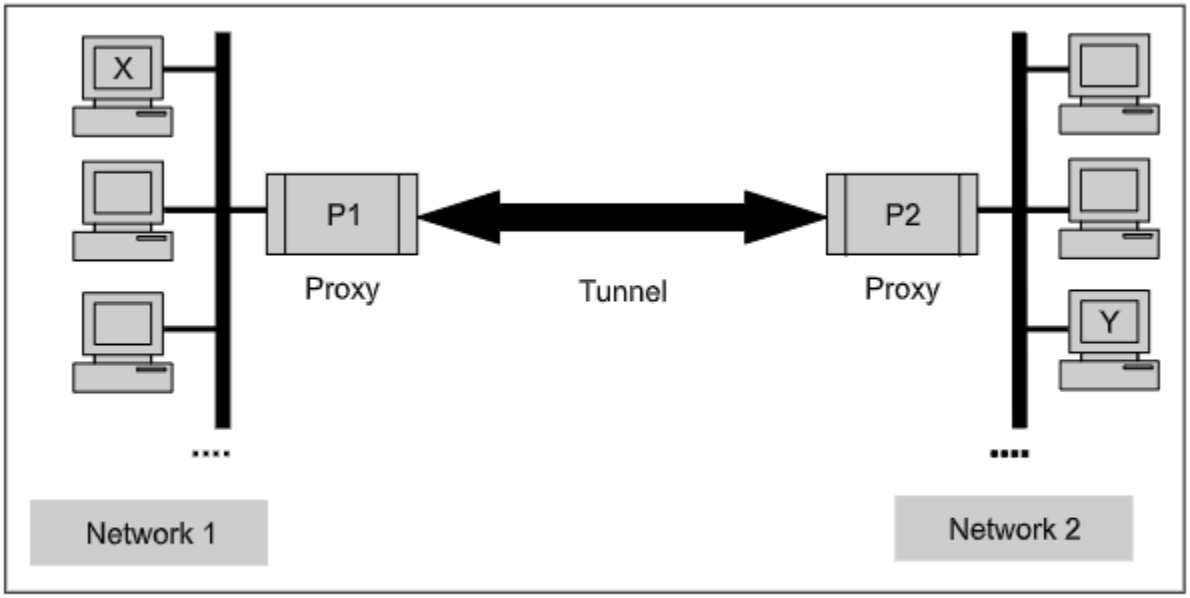


Fig. 9.30 Concept of tunnel mode

Example

For example, let's consider a scenario where two branch offices of an organization need to securely communicate over the internet. They can set up an IPsec-enabled network using SAs, AH, and ESP. The IP packets between the branch offices will be encrypted and authenticated, ensuring the confidentiality and integrity of the data. This secure communication can be established using tunnel mode, where the original IP packets are encapsulated and encrypted with a new IP header added.

Overall, IPsec provides a robust security solution for protecting network communication, allowing organizations to securely connect their branches, establish communication with other organizations, and provide secure remote internet access.

Q. Explain Diffie-Hellman Key Exchange algorithm with its merits and demerits in points, with diagram, example
Ans.
Diffie-Hellman Key Exchange Algorithm

The Diffie-Hellman key exchange algorithm is a method for two parties, Alice and Bob, to agree upon a shared symmetric key for secure communication. It works by utilizing the difficulty of calculating discrete logarithms in a finite field.

Working of the Algorithm

1. Alice and Bob agree on a public number, known as 'g', which is shared between them.
2. Alice selects a random number 'x' and calculates A = g^x mod n.
3. Bob selects a random number 'y' and calculates B = g^y mod n.
4. Alice and Bob exchange A and B.
5. Alice computes the shared key K1 = B^x mod n.
6. Bob computes the shared key K2 = A^y mod n.
7. Both Alice and Bob now have the same shared key K.

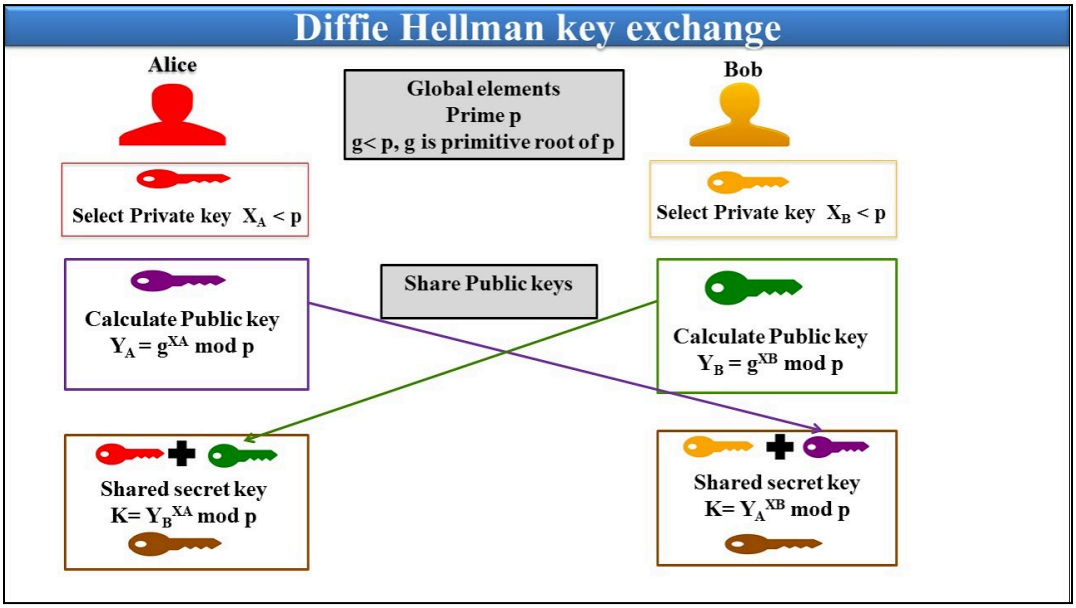
Merits of Diffie-Hellman Key Exchange Algorithm

1. Secure Key Exchange: The algorithm allows two parties to securely agree upon a shared key without transmitting it directly.
2. Public/Private Key Pair: The algorithm uses a public/private key pair, ensuring that the shared key remains confidential.
3. Simplicity: The algorithm is relatively simple to understand and implement.

Demerits of Diffie-Hellman Key Exchange Algorithm

1. Vulnerable to Man-in-the-Middle Attack: The algorithm is susceptible to a man-in-the-middle attack, where an attacker intercepts the communication and impersonates both parties.
2. Lack of Authentication: The algorithm does not provide authentication of the communicating parties, making it important to combine it with other security measures.
3. Limited to Key Agreement: The Diffie-Hellman algorithm is only used for key agreement and not for encryption or decryption of messages.

Diagram



Example

Let's consider a simple example with small values for ease of understanding.

Suppose Alice and Bob agree on n = 11 and g = 7.

Alice selects x = 3 and calculates A = 7^3 mod 11 = 3.

Bob selects y = 4 and calculates B = 7^4 mod 11 = 4.

They exchange A and B. Alice computes K1 = 4^3 mod 11 = 9.

Bob computes K2 = 3^4 mod 11 = 9. Both Alice and Bob now have the shared key K = 9.

Q. Describe the process of working of Virus? List out various kind of viruses based on working style in points, with diagram, example
Ans.
Working of Virus

A virus is a computer program that attaches itself to another legitimate program and causes damage to the computer system or network. It goes through four phases during its lifetime: dormant phase, propagation phase, triggering phase, and execution phase. In the dormant phase, the virus is idle until a certain action or event activates it. In the propagation phase, the virus copies itself and creates more copies to spread. The triggering phase occurs when the virus is activated by a specific action or event. Finally, in the execution phase, the virus performs its intended actions, which can be harmless or destructive.

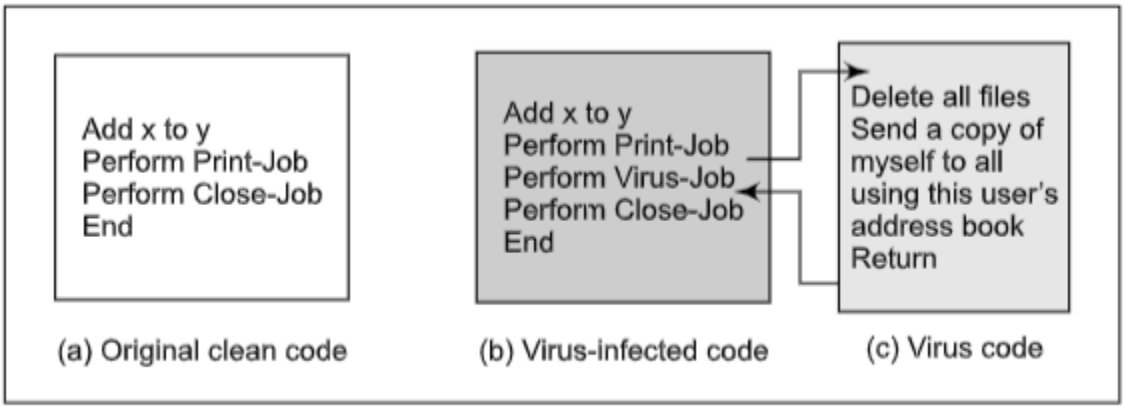
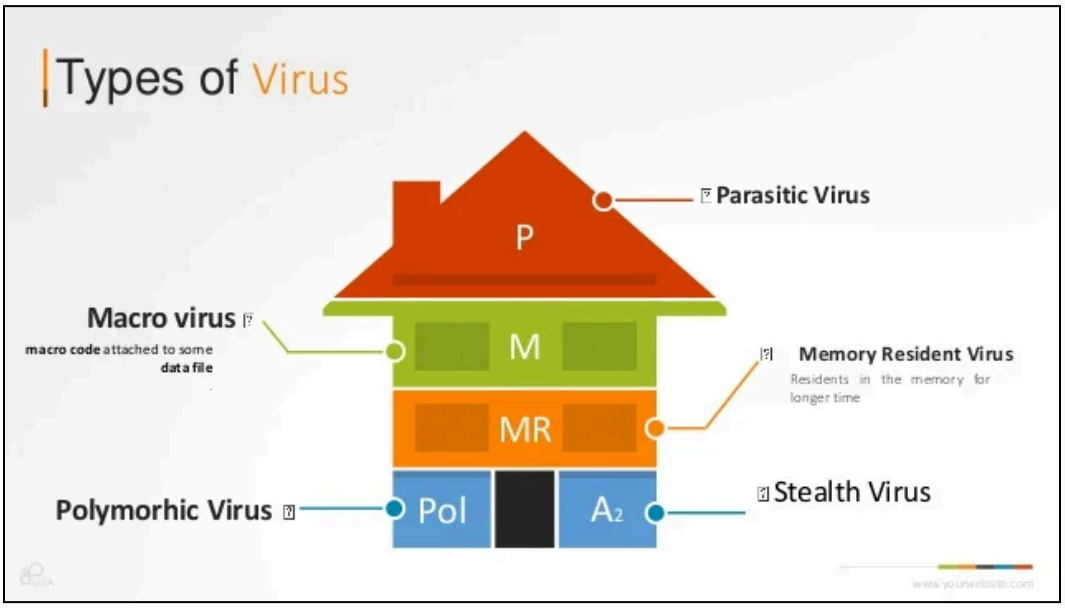


Fig. 1.14 Virus

Types of Viruses

1. Parasitic Virus: This is the most common type of virus that attaches itself to executable files and keeps replicating. It spreads when the infected file is executed.
2. Memory-resident Virus: This virus attaches itself to an area of the main memory and infects every executable program that is executed.
3. Boot sector Virus: This virus infects the master boot record of the disk and spreads when the operating system starts booting the computer.
4. Stealth Virus: This virus has intelligence built-in, making it difficult for anti-virus software to detect.
5. Polymorphic Virus: This virus changes its signature on every execution, making it challenging to detect.
6. Metamorphic Virus: This virus not only changes its signature but also rewrites itself every time, making its detection even harder.
7. Macro Virus: This virus affects specific application software, such as Microsoft Word or Excel, by attacking the macros within the documents.

Each type of virus has its own characteristics and methods of spreading, causing damage, or evading detection.



Q. Explain the working of secure electronic transaction(SET) in points, with diagram, example
Ans.

Working of Secure Electronic Transaction (SET)

SET is a protocol designed for secure e-commerce transactions. It involves three parties: the cardholder, the merchant, and the payment gateway. Here is a brief explanation of how SET works:

1. Authentication and Digital Certificates: All parties involved in SET must have a valid digital certificate from an approved certification authority. This ensures the identification and verification of the cardholder, merchant, and payment gateway.
2. Purchase Request: The transaction begins when the merchant sends a completed order form to the customer. SET is used for the Purchase Request exchange, which consists of four messages: Initiate Request, Initiate Response, Purchase Request, and Purchase Response.

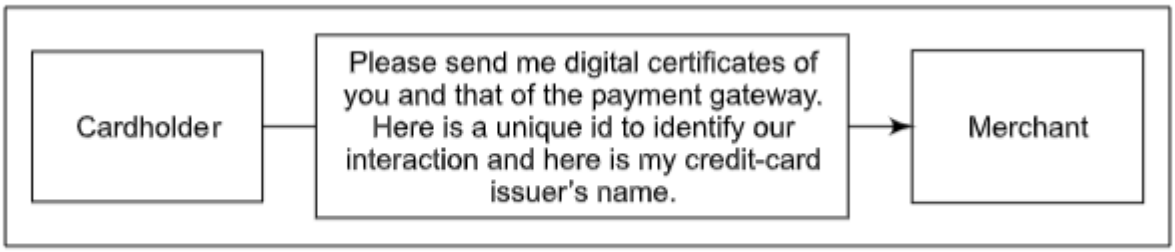


Fig. 6.28 Initiate request

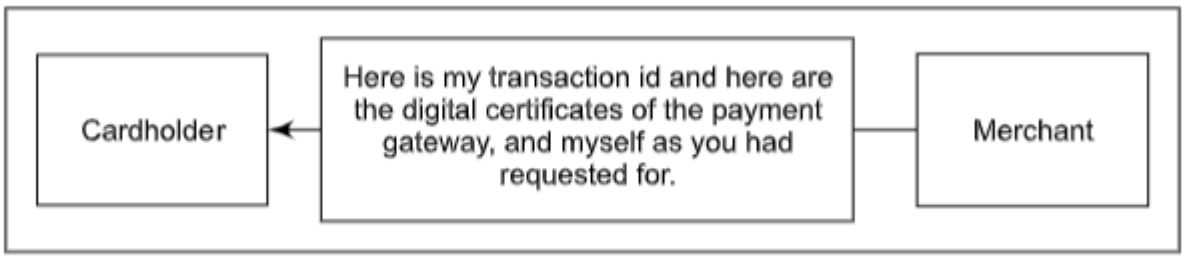


Fig. 6.29 Initiate response

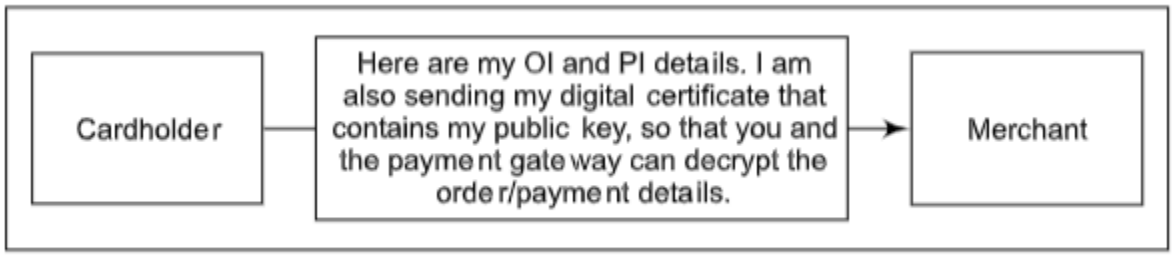


Fig. 6.30 Purchase request

3. Payment Authorization: The payment gateway receives a request from the merchant for making the payment. It interacts with financial institutions such as the issuer, acquirer, and clearing house to effect the payment from the customer's account to the merchant's account.

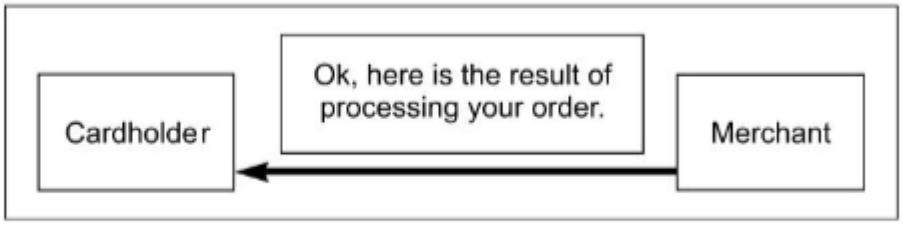


Fig. 6.34 Purchase Response

4. Payment Capture: Once the payment authorization is successful, the payment gateway captures the payment from the customer's account and transfers it to the merchant's account.

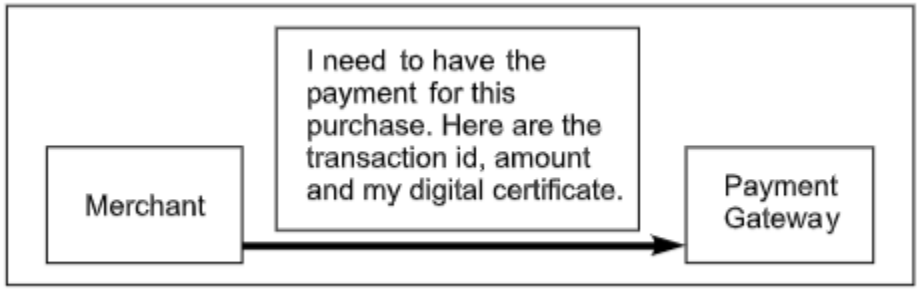


Fig. 6.37 Capture request

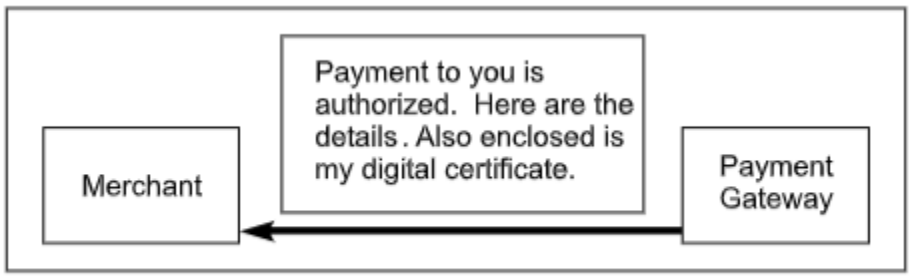


Fig. 6.38 Capture response

5. Hiding Credit Card Details: SET addresses the concern of protecting the credit card number from the merchant. It uses the concept of a digital envelope to hide the cardholder's credit card details. The SET software prepares the Payment Information (PI) on the cardholder's computer, and a one-time session key is created to encrypt the PI.
6. 3-D Secure Protocol: SET has a limitation in preventing a user from using someone else's credit card number. To address this, a new protocol called 3-D Secure has emerged. It requires cardholders to enroll

on the issuer bank's Enrollment Server before participating in a payment transaction. This adds an extra layer of security.

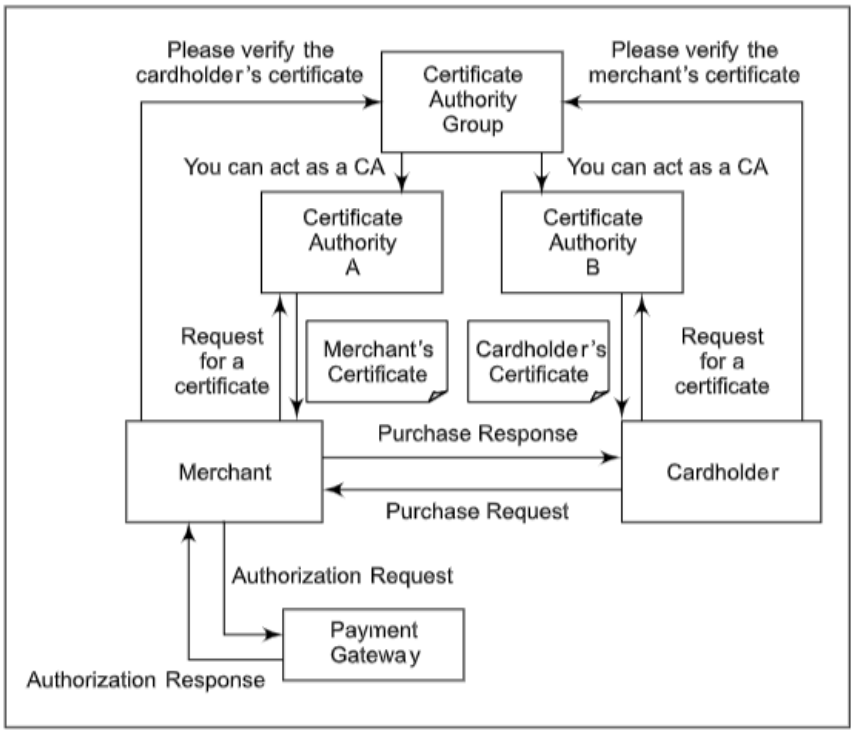


Fig. 6.39 The SET model

Example: A customer wants to make a purchase from an online merchant using SET. The customer opens a credit card account with a bank that supports SET. The merchant sends a completed order form to the customer, and the customer initiates the SET process by sending an Initiate Request message. The payment gateway receives the request, interacts with financial institutions for payment authorization, and captures the payment from the customer's account to the merchant's account. The credit card details are protected using encryption and digital envelopes.

Q. Explain the need for a firewall and intrusion detection system? Also give types of the same in points, with diagram, example
Ans.
The Need for Firewall and Intrusion Detection Systems

Firewalls and intrusion detection systems (IDS) are crucial components of network security.

Firewalls act as sentries, standing between a corporate network and the outside world. They control the flow of traffic between the network and the internet, allowing authorized traffic to pass through while blocking unauthorized access. Firewalls are essential for preventing external attacks and protecting sensitive data.

Intrusion detection systems are designed to detect and respond to unauthorized activities within a network. They help identify potential intrusions, collect information about them, and strengthen intrusion prevention methods. IDS can act as deterrents to intruders and provide valuable insights for improving network security.

Types of Firewalls

1. Packet Filters: These firewalls apply a set of rules to each packet and decide whether to forward or discard it based on criteria such as source/destination IP addresses, protocol, and port numbers. Packet filters are implemented using routers and are effective for basic network security.

2. Circuit-Level Gateways: These firewalls operate at the transport layer and establish a connection between the internal and external networks. They verify the legitimacy of the connection and monitor the state of the connection to ensure it remains secure.
3. Application-Level Gateways: Also known as proxy firewalls, these firewalls provide a higher level of security by examining the content of packets at the application layer. They act as intermediaries between clients and servers, filtering and validating traffic based on application-specific rules.

Types of Intrusion Detection Systems

1. Statistical Anomaly Detection: This type of IDS captures and analyzes user behavior over time, comparing it to predefined statistical data. It can detect deviations from normal behavior and raise alerts for potential intrusions.
2. Rule-Based Detection: Rule-based IDS apply a set of predefined rules to determine if a behavior is suspicious. These rules are designed to identify known attack patterns and trigger alerts when such patterns are detected.

Diagram Example

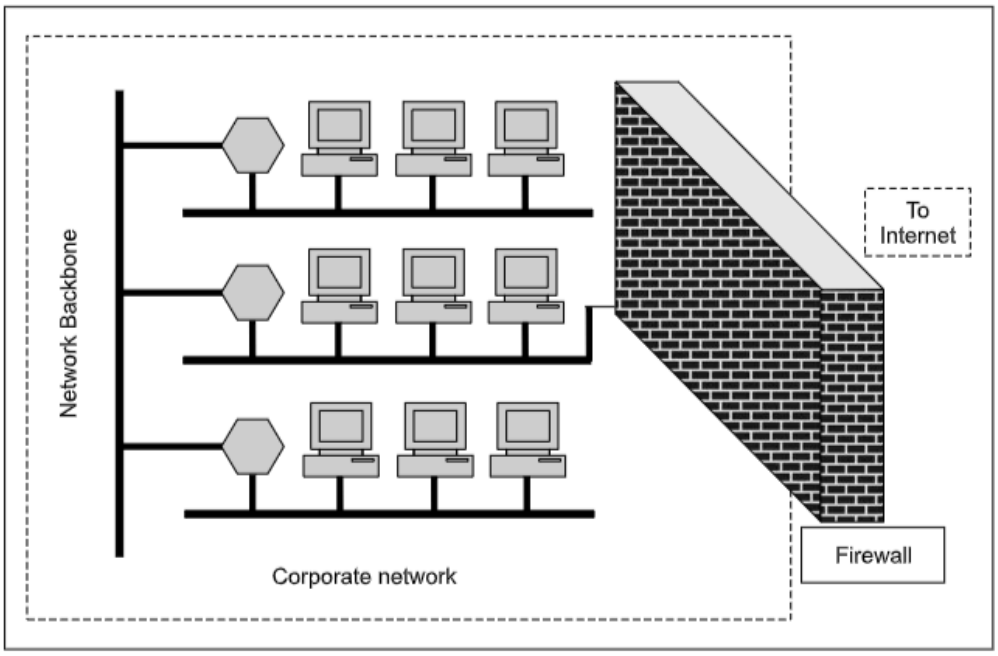


Fig. 9.6 Firewall

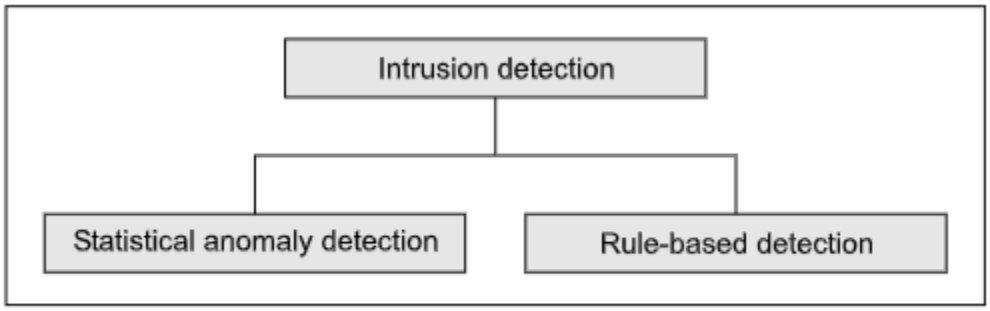


Fig. 9.50 Classification of intrusion detection

This diagram illustrates the classification of intrusion detection systems into statistical anomaly detection and rule-based detection. Statistical anomaly detection analyzes user behavior over time, while rule-based detection applies predefined rules to identify suspicious behavior.

Q. Explain rsa algorithm with p=7,q=11,e=17,M=8. Discuss its merit in points, with diagram, example
Ans.

RSA Algorithm with p=7, q=11, e=17, M=8

The RSA algorithm is an asymmetric-key cryptography algorithm that involves the use of two prime numbers, p and q, to generate a public key and a private key. In this case, let's consider p=7 and q=11.

1. Key Generation:
    - Calculate N = p x q = 7 x 11 = 77.
    - Calculate φ(N) = (p-1) x (q-1) = 6 x 10 = 60.
    - Choose a value for e such that 1 < e < φ(N) and gcd(e, φ(N)) = 1. In this case, e=17 satisfies these conditions.
    - Calculate d, the modular multiplicative inverse of e modulo φ(N). In other words, d is the value such that (d x e) mod φ(N) = 1. In this case, d=53.
2. Encryption:
    - To encrypt a message M, raise M to the power of e and take the remainder when divided by N. In this case, M=8.
    - CT = (M^e) mod N = (8^17) mod 77 = 64.
3. Decryption:
    - To decrypt the ciphertext CT, raise CT to the power of d and take the remainder when divided by N.
    - PT = (CT^d) mod N = (64^53) mod 77 = 8.

Merits of RSA Algorithm:

1. Security: RSA provides a high level of security due to the difficulty of factoring large numbers, making it resistant to attacks.
2. Asymmetric Key: RSA uses different keys for encryption and decryption, providing a secure method for communication.
3. Digital Signatures: RSA can be used for digital signatures, ensuring the authenticity and integrity of messages.
4. Key Exchange: RSA can be used for secure key exchange, allowing two parties to establish a shared secret key without transmitting it directly.
5. Versatility: RSA can be used for encryption, decryption, digital signatures, and key exchange, making it a versatile algorithm for various cryptographic applications.

Example: Let's consider an example with p=7, q=11, e=17, and M=8.

- The public key is (N=77, e=17).
- The private key is (N=77, d=53).
- Encryption: CT = (M^e) mod N = (8^17) mod 77 = 64.
- Decryption: PT = (CT^d) mod N = (64^53) mod 77 = 8.

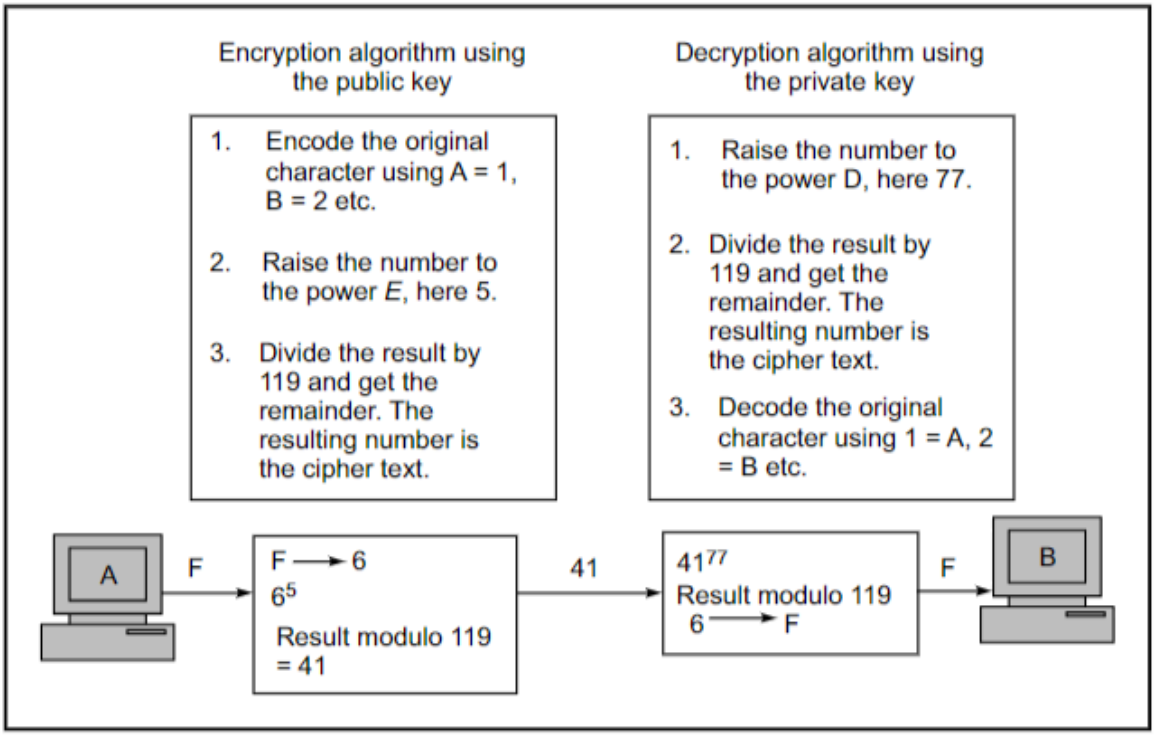
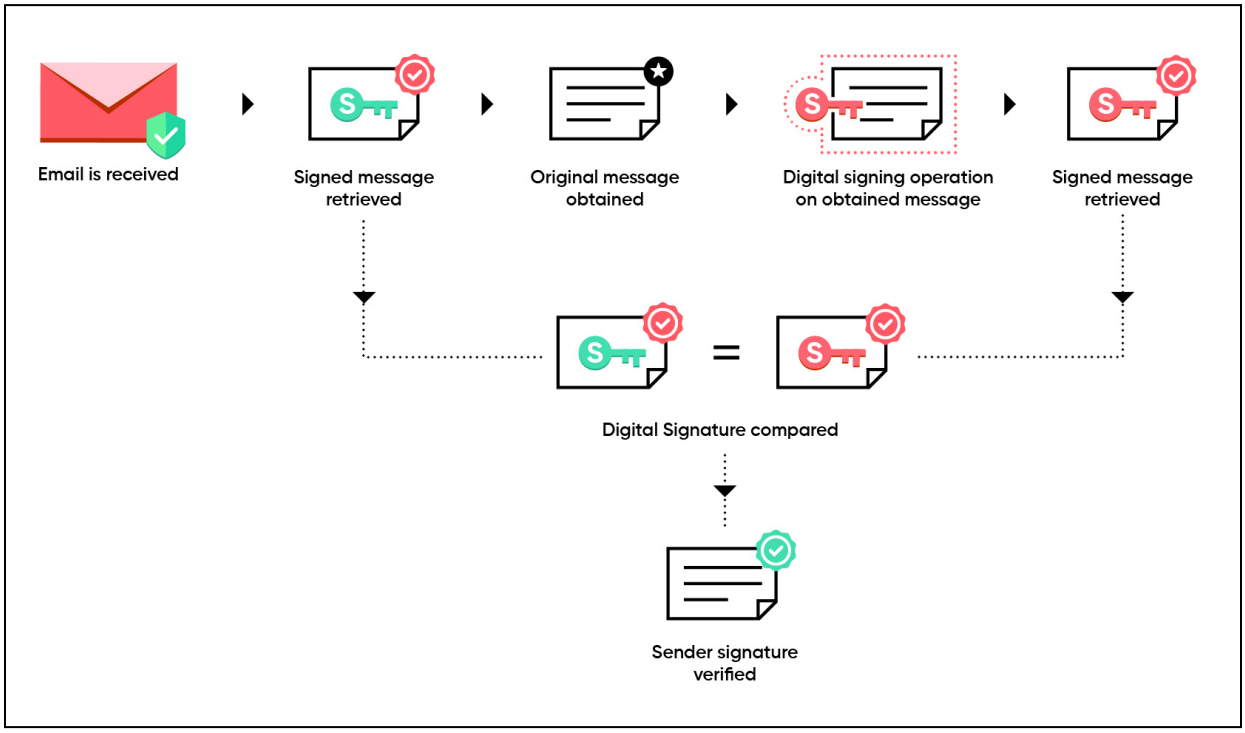


Fig. 4.6 Example of the RSA algorithm

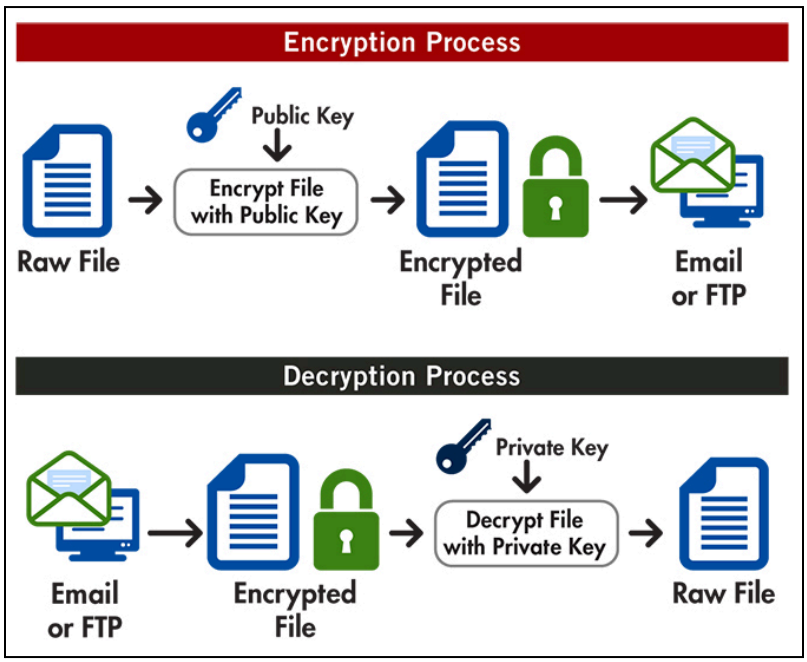
Q. Explain in detail about security services (PGP or S/MIME) for email in points, with diagram, example Ans.

Security Services for Email: PGP and S/MIME

1. Introduction: Pretty Good Privacy (PGP) and Secure MIME (S/MIME) are two popular email security protocols that provide security services for email communication.
2. PGP Security Services: PGP offers encryption, message digest, and digital signatures as its security services. It uses algorithms like RSA, DSS, MD5, SHA-1, IDEA, DES-3, and AES. PGP allows for four security options when sending an email message: signature only, signature and Base-64 encoding, signature, encryption, enveloping, and Base-64 encoding.
3. S/MIME Security Services: S/MIME adds security to the Multipurpose Internet Mail Extension (MIME) protocol. It secures MIME contents through encryption, message digests, and digital signatures. S/MIME supports various cryptographic algorithms like RSA, DSS, MD5, SHA-1, and DES-3. S/MIME messages can be signed, encrypted, or both.
4. Working of PGP: PGP follows a series of steps to secure an email message. These steps include digital signature, compression, encryption, digital enveloping, and Base-64 encoding. The receiver performs these steps in reverse to retrieve the original plain text email message.
5. Working of S/MIME: S/MIME prepares a MIME entity along with security-related data like algorithm identifiers and digital certificates. This entity is then processed by S/MIME to create a Public Key



S/MIME Diagram



PGP Diagram

Q. Assume that you are a cyber security advisor in a leading IT company -How will you do a Security Audit? -Suggest Some preventive measures to prevent attacks? -what will be the course of action in case an attack occurs? in points, with diagram, example

Ans.

As a cybersecurity advisor in a leading IT company, conducting a security audit is a crucial step to assess the security posture of the organization, identify vulnerabilities, and develop preventive measures and an incident response plan. Here's a step-by-step plan with some preventive measures and an incident response diagram:

~ Security Audit Process:

1. Scoping the Audit:

- Define the scope and objectives of the audit, including specific systems, networks, and data to be assessed.

2. Gather Information:
- Collect relevant information, including network architecture, asset inventory, policies, and procedures.

3. Vulnerability Assessment:
- Perform a vulnerability scan to identify weaknesses in systems and applications.
- Use tools like Nessus, Qualys, or OpenVAS.

4. Penetration Testing:
- Conduct penetration testing to simulate real-world attacks and assess the effectiveness of security controls.
- Engage certified ethical hackers or use tools like Metasploit.

5. Compliance Assessment:
- Ensure that the organization complies with relevant regulations and industry standards (e.g., GDPR, HIPAA, ISO 27001).

6. Security Policy and Procedure Review:
- Evaluate the existing security policies and procedures to ensure they align with best practices.

7. User Awareness Training:
- Assess the security awareness of employees and provide training as needed.

8. Log and Incident Analysis:
- Review logs and incidents from the past to identify patterns and trends.

9. Risk Assessment:
- Perform a risk assessment to prioritize vulnerabilities based on their potential impact.

10. Documentation:
- Document all findings, including vulnerabilities, compliance issues, and recommendations.

~ Preventive Measures:

- Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS): Implement these to monitor and block malicious network traffic.

- Antivirus and Anti-Malware Software: Regularly update and scan systems for threats.

- Patch Management: Keep all software and systems up to date with the latest security patches.

- Strong Authentication: Implement two-factor authentication (2FA) and password policies.

- Data Encryption: Encrypt sensitive data at rest and in transit.

- Employee Training: Conduct regular security awareness training to educate employees on best practices.

- Access Control: Limit access to sensitive data and systems on a need-to-know basis.

- Regular Audits: Schedule periodic security audits and assessments.

- Incident Response Plan: Develop and maintain an incident response plan to address security breaches.

~ Incident Response Plan:

1. Detection:
   - Detect the security incident through monitoring tools and anomaly detection.

2. Containment:
   - Isolate affected systems or networks to prevent further damage.

3. Eradication:
   - Identify and remove the root cause of the incident.

4. Recovery:
   - Restore affected systems to normal operation.

5. Communication:
   - Notify stakeholders, including management, legal, and affected parties, as required by law.

6. Investigation:
   - Conduct a detailed investigation to understand the scope and impact of the incident.

7. Documentation:
   - Document all actions taken during the incident response.

8. Lessons Learned:
   - Analyze the incident to improve security measures and policies.

9. Legal and Regulatory Reporting:
   - Comply with legal and regulatory requirements regarding data breach reporting.

10. Public Relations:
    - Manage public relations and communications with customers and the media.

Remember, an incident response plan should be well-documented and regularly tested through tabletop exercises to ensure the organization is prepared to respond effectively to security incidents.

Q. What is difference between public key and private key cryptosystem in points, with diagram, example Ans.

Public Key Cryptosystem:

- Public key cryptosystem uses two different keys for encryption and decryption: a public key and a private key.
- The public key is freely available to anyone and is used for encryption.
- The private key is kept secret and is used for decryption.

- The sender uses the recipient's public key to encrypt the message, ensuring confidentiality.
- The recipient uses their private key to decrypt the message and retrieve the original content.
- This system provides secure communication between parties without the need to share a secret key.

Private Key Cryptosystem:

- Private key cryptosystem, also known as symmetric key cryptosystem, uses the same key for both encryption and decryption.
- The same secret key is shared between the sender and the recipient.
- The sender uses the secret key to encrypt the message, ensuring confidentiality.
- The recipient uses the same secret key to decrypt the message and retrieve the original content.
- This system is faster than public key cryptosystem but requires a secure method to share the secret key between parties.

Diagram:

```
Public Key Cryptosystem:
Sender (A)                                  Receiver (B)
   |                                                |
   |   Encrypt with B's public key    ----
```

Key details	*A* should know	*B* should know
A's private key	Yes	No
A's public key	Yes	Yes
B's private key	No	Yes
B's public key	Yes	Yes

Fig. 4.1 Matrix of private and public Keys

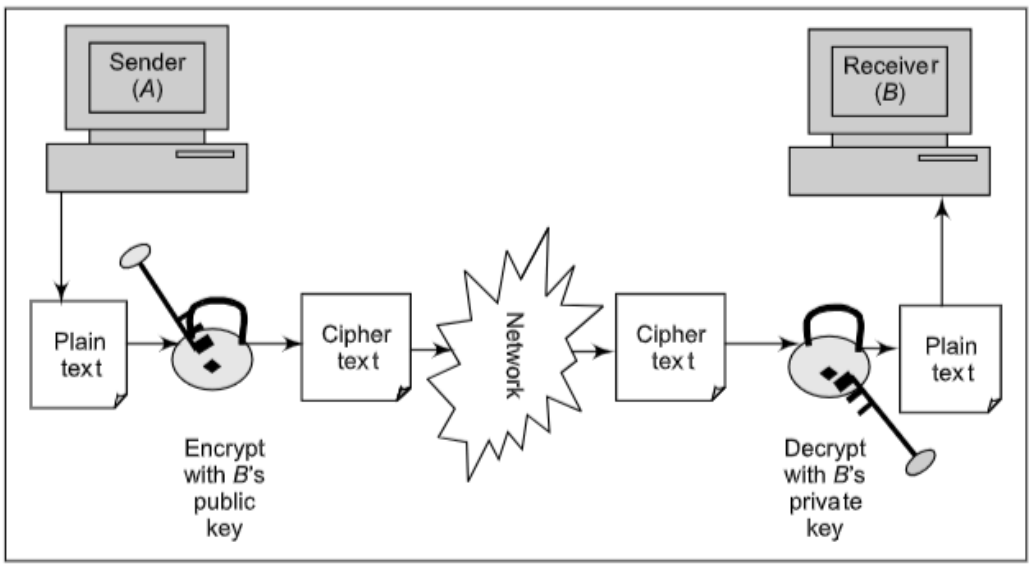
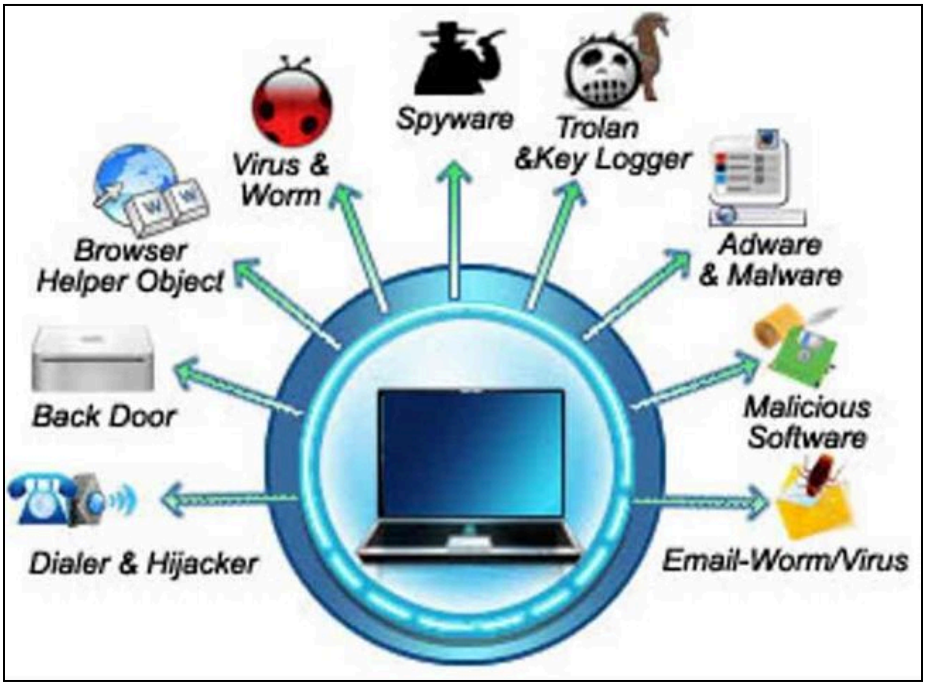


Fig. 4.2 Asymmetric-key cryptography

Q. Give brief information about program threats and system threats in points, with diagram, example Ans.

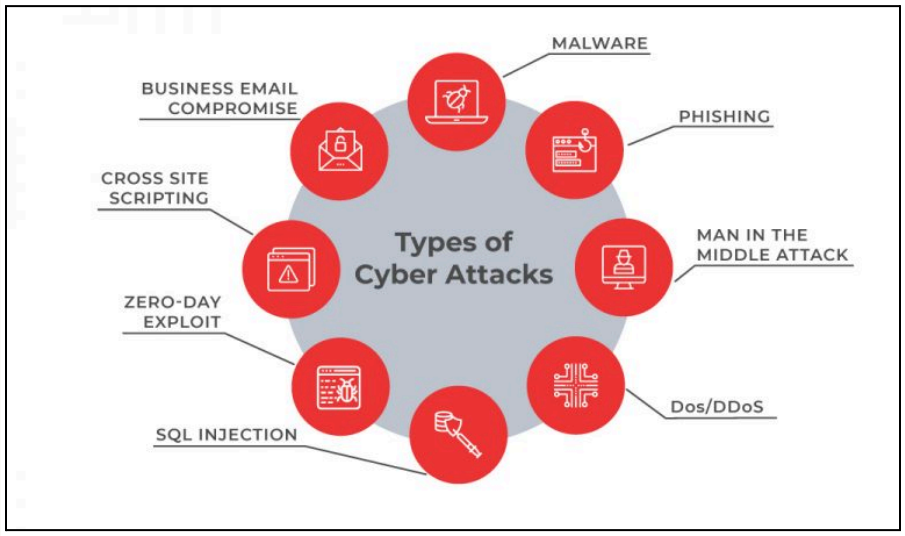
Program Threats:

- Program threats refer to attacks or malicious activities that target computer programs or software. These threats can cause damage to the program itself or compromise the security of the system it is running on.
- Examples of program threats include viruses, worms, Trojan horses, and spyware. These threats can be introduced into a system through infected files, email attachments, or malicious websites.
- Program threats can disrupt the normal functioning of a program, steal sensitive information, or allow unauthorized access to the system. They can also spread to other programs or systems, causing widespread damage.
    - Program threats can be prevented or mitigated through the use of antivirus software, firewalls, and regular software updates to patch vulnerabilities.



System Threats:

- System threats refer to attacks or malicious activities that target the overall security and integrity of a computer system. These threats can compromise the availability, confidentiality, and integrity of the system and its data.
- Examples of system threats include denial-of-service (DoS) attacks, unauthorized access, data breaches, and network attacks. These threats can be carried out by hackers, insiders, or automated bots.
- System threats can result in system downtime, loss of data, unauthorized access to sensitive information, and financial losses. They can also lead to reputational damage and legal consequences.
- System threats can be prevented or mitigated through the use of strong access controls, encryption, intrusion detection systems, and regular security audits. It is also important to educate users about safe computing practices and to implement security best practices at the organizational level.



Example: An example of a program threat is a virus that infects a computer system by attaching itself to a legitimate program. Once the infected program is executed, the virus can replicate itself and spread to other programs or systems. This can result in the loss of data, system crashes, and unauthorized access to sensitive information.

An example of a system threat is a denial-of-service (DoS) attack, where an attacker floods a system with a large volume of traffic or requests, overwhelming its resources and causing it to become unavailable to legitimate users. This can disrupt business operations, lead to financial losses, and damage the reputation of the organization.

Q. Write an overview of symmetric key cryptography with its merits and demerits in points, with diagram, example
Ans.

Overview

Symmetric-key cryptography is a method of encryption where the same key is used for both encryption and decryption. It is fast and efficient, but it has some drawbacks. Key distribution is a problem, as parties need to agree on a key. Also, if multiple parties are involved, each pair of parties needs a separate key. However, these drawbacks can be overcome with intelligent solutions.

Key points

- Symmetric-key cryptography uses the same key for encryption and decryption.
- It is fast and efficient.
- Key distribution is a challenge in symmetric-key cryptography.
- Multiple parties require separate keys for secure communication.
- Intelligent solutions can overcome the challenges of symmetric-key cryptography.

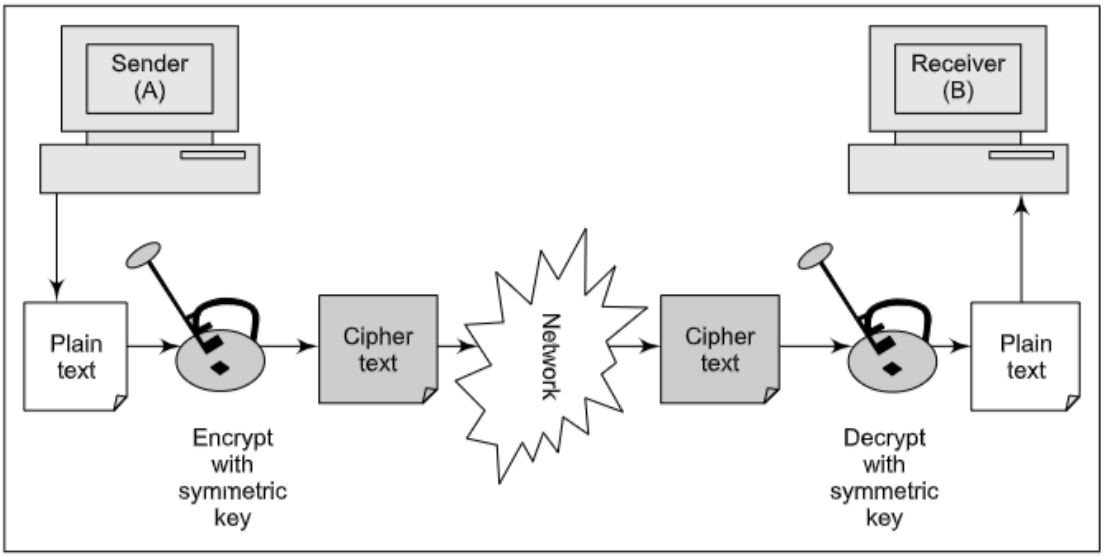


Fig. 3.17 Symmetric-key cryptography

Q. What is meant by message authentication? list out attacks during the Communication across the network in points, with diagram, example

Ans.

Message Authentication

Message authentication refers to the process of verifying the integrity and authenticity of a message. It ensures that the message has not been altered during transmission and that it has been sent by the claimed sender. This is achieved through the use of cryptographic techniques such as digital signatures.

Attacks during Communication across the Network

1. Interception: This attack involves an unauthorized party gaining access to a message during transmission. It can lead to the loss of message confidentiality.
2. Fabrication: In this attack, an attacker creates and sends a false message, pretending to be a legitimate sender. This can lead to the compromise of message authenticity.
3. Modification: This attack involves altering the contents of a message while it is in transit. It can result in the loss of message integrity.
4. Denial of Service (DoS): In a DoS attack, the attacker attempts to disrupt the normal functioning of a network or system, making it unavailable to legitimate users.

These attacks can be classified into two categories: passive attacks and active attacks.

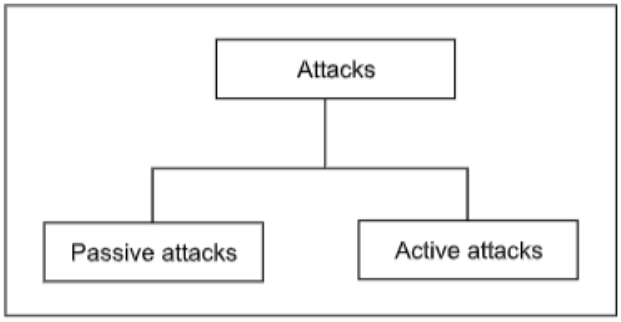


Fig. 1.10 Types of attacks

Passive Attacks

Passive attacks do not modify the contents of a message but focus on observing and gathering information. Examples include interception and traffic analysis.

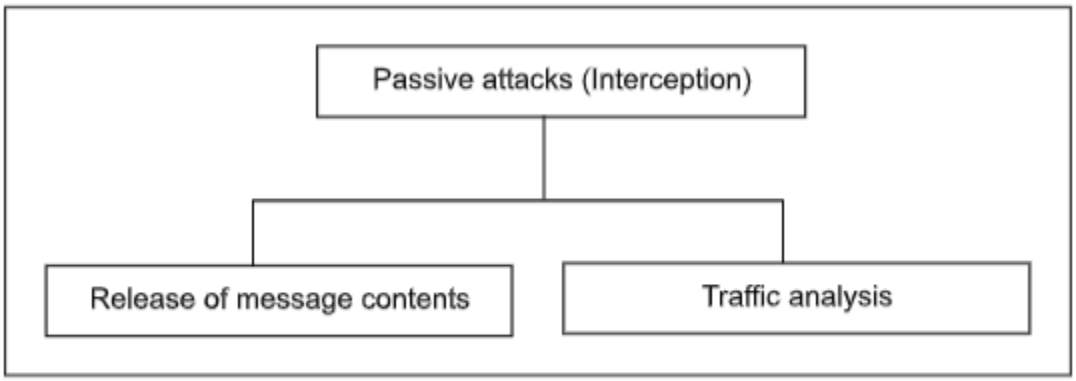


Fig. 1.11 Passive attacks

Active Attacks

Active attacks involve modifying the contents of a message or performing actions that can cause harm. Examples include fabrication, modification, and interruption. Masquerade, replay attacks, alteration of messages, and DoS attacks are types of active attacks.

Here is a diagram illustrating the different types of attacks during communication across the network:

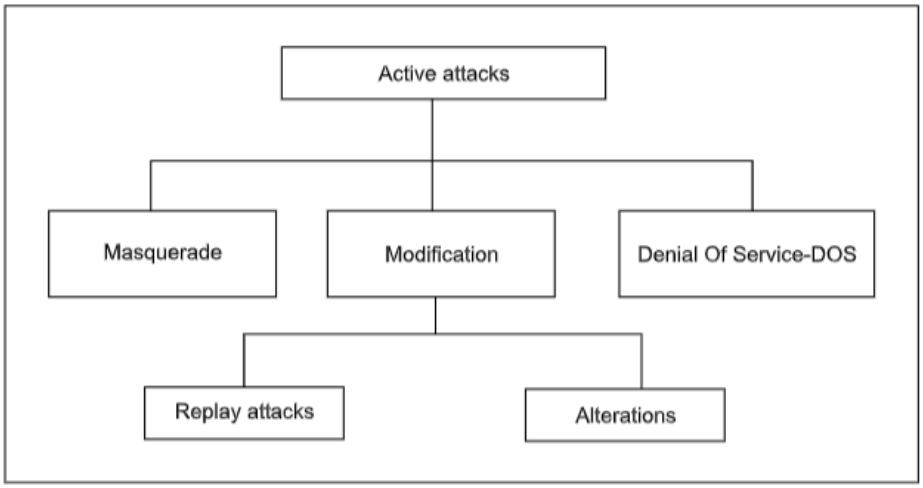


Fig. 1.12 Active attacks

For example, consider a scenario where User A sends a confidential email message to User B. If an unauthorized User C intercepts and accesses this message, it would be an interception attack. If User C modifies the contents of the message before it reaches User B, it would be a modification attack. If User C fabricates a false message and sends it to User B, pretending to be User A, it would be a fabrication attack.

It is important to implement security measures such as authentication mechanisms, encryption, and access control to protect against these attacks and ensure secure communication across the network.

Q. Classify attacks with respect to two views: the common person's view and Technologist View in points, with diagram, example
Ans.

Attacks Classification: Common Person's View vs Technologist's View

Common Person's View:

- Attacks from a common person's point of view can be classified into three categories: criminal attacks, publicity attacks, and legal attacks.
- Criminal attacks aim to maximize financial gain by attacking computer systems. Examples include fraud, scams, destruction, identity theft, and intellectual property theft.
- Publicity attacks occur when attackers want to see their names appear on television news channels and newspapers. These attackers are usually not hardcore criminals and may include students or employees seeking publicity by attacking computer systems.
- Legal attacks are novel and unique. Attackers try to make the judge or jury doubtful about the security of a computer system. They exploit the weakness of the judge and jury in technological matters to defend their actions.

Technologist's View:

- Attacks on computers and network systems can be classified into two categories: theoretical concepts and practical approaches.
- Theoretical concepts include interception, fabrication, alteration of messages, and denial of service (DOS) attacks.
- Interception refers to unauthorized access to a resource, such as copying data or listening to network traffic.
- Fabrication involves creating illegal objects on a computer system, like adding fake records to a database.
- Alteration of messages involves changing the contents of a message, which can lead to unauthorized transfers or modifications.
- DOS attacks aim to prevent legitimate users from accessing services by flooding the network with excessive login requests.
- Practical approaches to attacks can be categorized as application-level attacks and network-level attacks.
- Application-level attacks target specific applications to access, modify, or prevent access to information. Examples include obtaining credit card information or changing transaction amounts.
- Network-level attacks aim to reduce the capabilities of a network, potentially leading to application-level attacks. These attacks can slow down or halt a computer network.

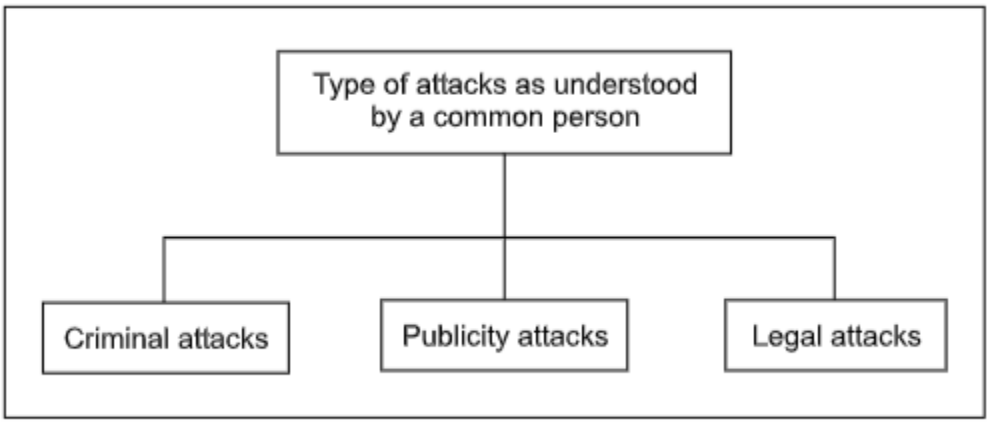


Fig. 1.9 Classification of attacks as understood in general terms

Example:

- An example of a common person's view attack is a criminal attack where an attacker uses a phishing scam to trick innocent users into providing their confidential information on fake websites.
- An example of a technologist's view attack is an alteration of messages attack, where an attacker intercepts and modifies a message to change the beneficiary and amount in a transaction.

Note: The diagram provided is a representation of the attacks classification, but the actual diagram is not available in the given document.

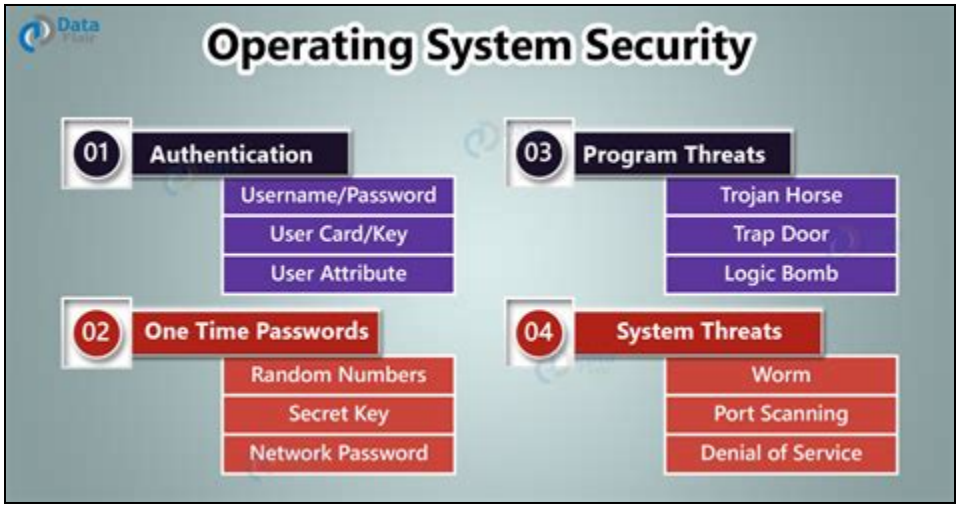
Q. Design your own the architecture of Operating system security mechanism where you are protecting objects, protecting memory address, and giving limited privileges to subjects(users, programmers) in points, with diagram, example

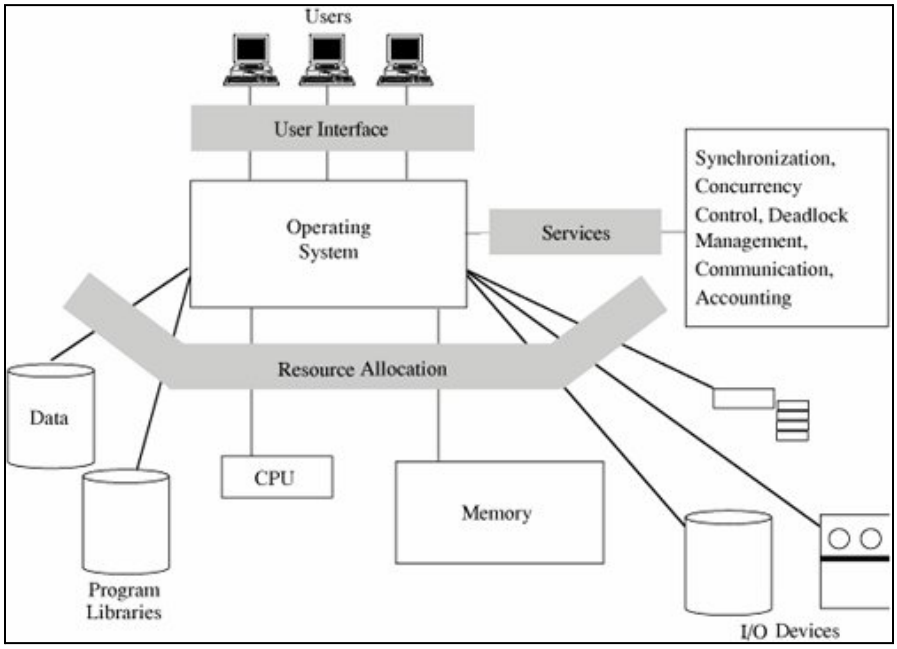
Ans.

Operating System Security Mechanism

1. Object Protection: In the operating system security mechanism, object protection is implemented to ensure that only authorized subjects can access and modify objects. Objects can include files, directories, devices, and other system resources. Access control lists (ACLs) or capabilities can be used to specify the permissions and privileges associated with each object. For example, a file may have read, write, and execute permissions assigned to different subjects.
2. Memory Address Protection: To protect memory addresses, the operating system uses techniques such as memory segmentation and memory protection keys. Memory segmentation divides the memory into logical segments, and each segment is assigned specific access permissions. Memory protection keys are used to restrict access to specific memory regions, preventing unauthorized access or modification.
3. Limited Privileges to Subjects: Subjects, such as users and programmers, are assigned limited privileges to ensure that they can only perform authorized actions. This is achieved through user account management and privilege levels. User accounts are created with specific privileges, and subjects must authenticate themselves to access the system. Privilege levels, such as administrator or standard user, determine the scope of actions that a subject can perform.

Example Architecture:





In this example architecture, the operating system security mechanism consists of several components:

1. Access Control Module: This module handles object protection by enforcing access control policies based on ACLs or capabilities. It checks the permissions associated with each object and grants or denies access accordingly.
2. Memory Protection Module: The memory protection module ensures that memory addresses are protected from unauthorized access or modification. It uses techniques like memory segmentation and memory protection keys to restrict access to specific memory regions.
3. User Management Module: The user management module is responsible for managing user accounts and assigning limited privileges to subjects. It handles user authentication, password management, and privilege level assignment.
4. Security Policy Module: The security policy module defines the overall security policy of the operating system. It specifies the rules and guidelines for object protection, memory address protection, and privilege assignment. It also ensures compliance with legal requirements.

By implementing this architecture, the operating system can provide robust security mechanisms to protect objects, memory addresses, and provide limited privileges to subjects.

Q. MD5(message digest 5) algorithm in points, with diagram, example
Ans.

Overview

MD5 (Message Digest Algorithm 5) is a cryptographic hash function developed by Ron Rivest. It is designed to produce a 128-bit message digest, which is a fixed-size representation of the input message. MD5 is fast and widely used for integrity checking and fingerprinting purposes. However, it has been found to have potential weaknesses and is no longer considered secure for cryptographic applications.

Key points

- MD5 is a message-digest algorithm developed by Ron Rivest.
- It is a fast algorithm that produces a 128-bit message digest.
- MD5 has its roots in a series of message-digest algorithms, with MD5 being the final version.
- Over the years, researchers have identified potential weaknesses in MD5.
- MD5 is no longer considered secure for cryptographic purposes.

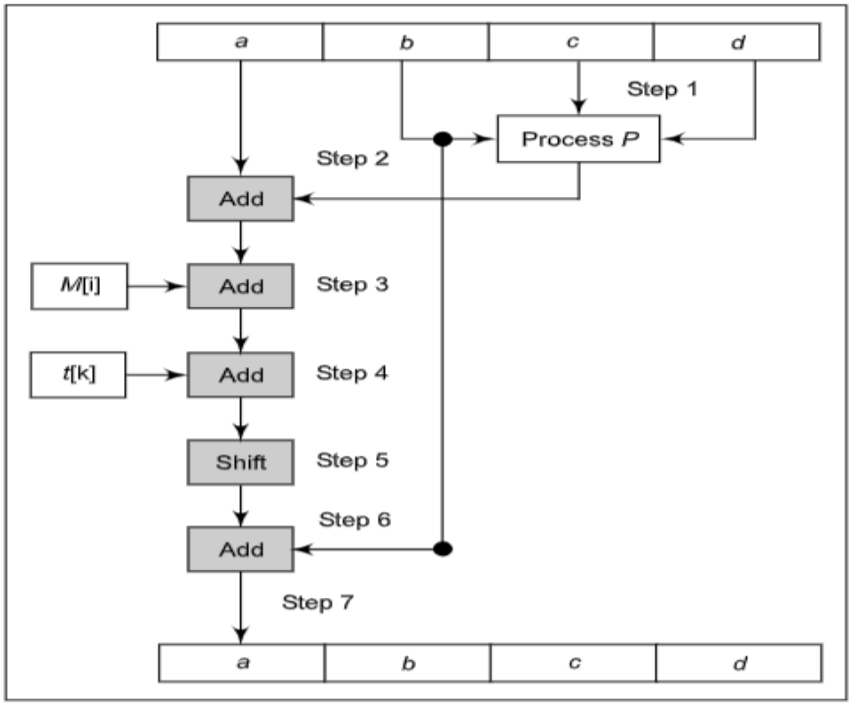


Fig. 4.33 One MD5 operation

Q. Wireless application protocol(WAP) security in points, with diagram, example

Ans.

Wireless Application Protocol (WAP) Security

WAP security is designed to provide secure communication between wireless mobile devices and the Internet. It includes several features such as authentication, privacy, and secure connections.

Authentication in WAP

Authentication in WAP involves the process of verifying the identity of the client and the server. This is done through the use of protocols like Wireless Transport Layer Security (WTLS) and the exchange of challenge-response messages.

Privacy in WAP

Privacy in WAP ensures that the messages exchanged between the client and the server are encrypted and cannot be

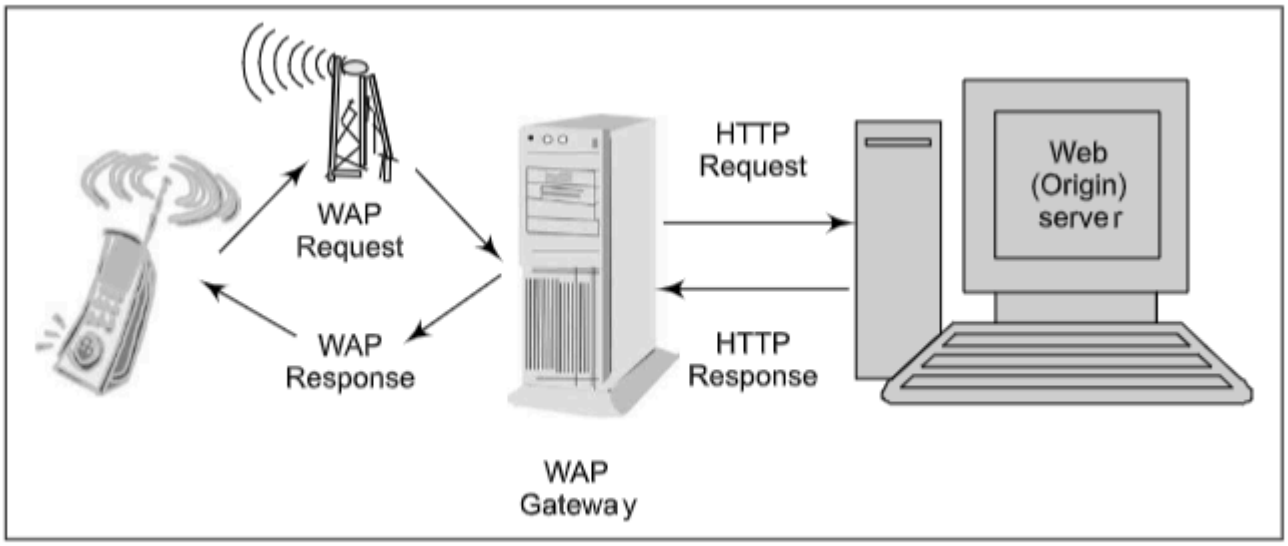


Fig. 6.74 Interaction of a mobile phone with the Internet

Q. Netiquettes in points, with diagram, example

Ans.

Netiquettes

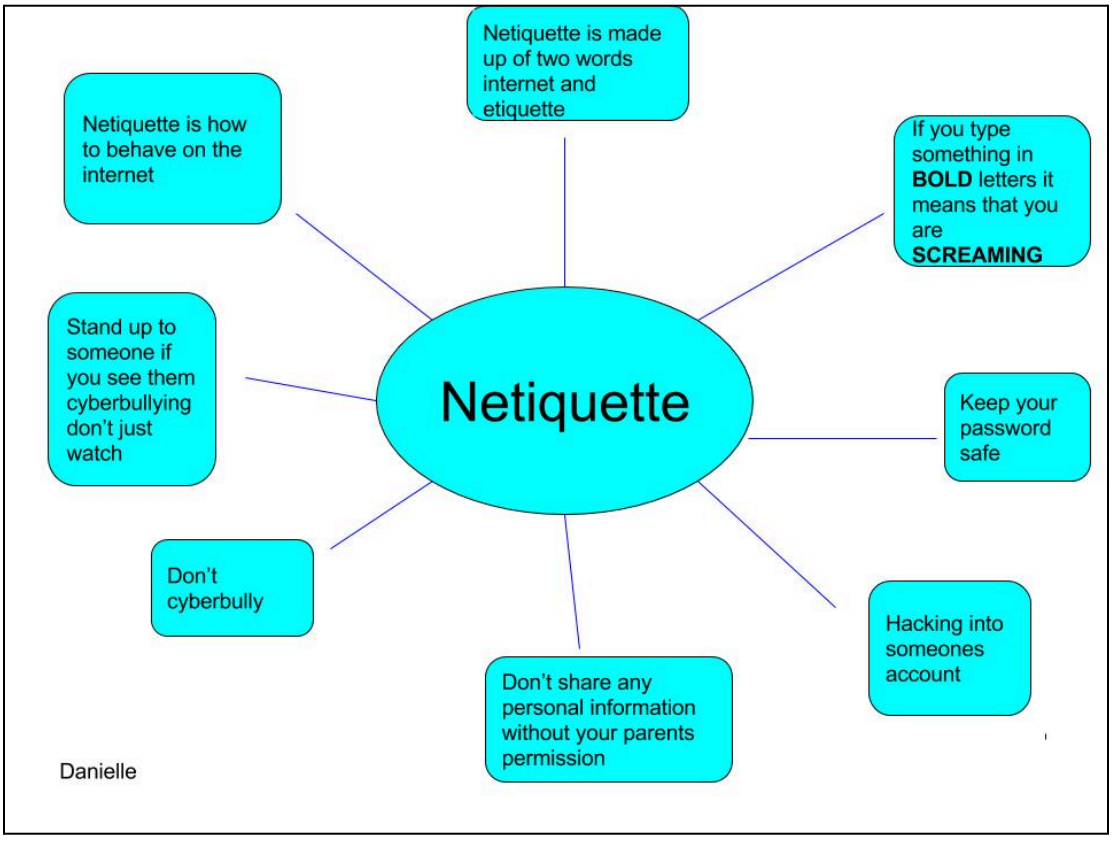
Netiquettes are a set of guidelines for proper online behavior. Here are some key points to remember:

1. Be respectful: Treat others with respect and courtesy in all online interactions. Avoid offensive language, personal attacks, and cyberbullying.
2. Use appropriate language: Avoid using excessive capitalization, which is considered shouting, and refrain from using offensive or inappropriate language.
3. Be mindful of others' privacy: Respect others' privacy by not sharing personal information without their consent. Be cautious when sharing sensitive information online.
4. Use proper grammar and punctuation: Use correct grammar, spelling, and punctuation to ensure clear communication. Avoid using excessive abbreviations or acronyms that may be confusing to others.
5. Be mindful of your tone: Tone can be easily misinterpreted online, so choose your words carefully to convey your message accurately and avoid misunderstandings.
6. Avoid spamming and excessive self-promotion: Do not send unsolicited messages or spam others with unnecessary information. Avoid excessive self-promotion or advertising.
7. Use appropriate emojis and emoticons: Emojis and emoticons can add context and emotion to your messages, but use them sparingly and appropriately.

Example of Netiquette in Action

Imagine you are participating in an online discussion forum. Instead of posting a comment that says, "Your idea is stupid," which is disrespectful and offensive, you could rephrase it as, "I have a different perspective on this topic." This shows respect for others' opinions and encourages constructive dialogue.

Diagram of Netiquettes



Q. Development control for security in points, with diagram, example
Ans.

Development Control for Security

Development control for security involves implementing measures and practices to ensure the security of software and systems during the development process. Here are some key points to consider:

1. Security Models: Organizations can choose different approaches to implement their security models, such as no security, security through obscurity, host security, or network security. Each approach has its advantages and limitations.
2. Security-Management Practices: Good security-management practices include having a security policy in place. This policy should address aspects like affordability, functionality, cultural issues, and legality. It is important to communicate the policy to all stakeholders, outline responsibilities, use simple language, establish accountability, and provide for exceptions and periodic reviews.
3. Basic Concepts: The need for security in computer applications has grown significantly with the realization of the importance of data. User authentication and password mechanisms, as well as data encryption, are examples of basic security measures employed by organizations.
4. Communication Infrastructure: As technology and the Internet have advanced, basic security measures have proven insufficient. The communication infrastructure has become more mature, and the development of applications for various user demands and needs requires stronger security measures.
5. Example: An example of the importance of security in development control is the transmission of sensitive information, such as credit card details, over the Internet. Insufficient security measures can lead to unauthorized access and potential data breaches.