UNIT 4

Q1) What is the importance and need for security and explain network attack ?  
**Importance of Security:**

* **Protection of Assets:** Security, in its modern form, utilizes sophisticated systems like alarms and cameras to protect secure locations such as banks. Asset protection systems are designed to recover stolen goods and high-value assets, deter criminals, and track and manage critical assets in real-time.
* **Ensuring Privacy and Confidentiality:** Techniques like criminal investigation methods using genetic material, voice, retinal patterns, and fingerprints highlight the importance of securing personal information. Data security specifically focuses on protecting data from unauthorized disclosure and modification.
* **Maintaining Data Integrity and Availability:** Data and information security aim to balance the availability of information with its confidentiality, ensuring that data is accurate and accessible only to authorized individuals.
* **Protection Against Threats:** Security is crucial due to the increasing threat of attacks. Computer security provides tools to protect data and systems from hackers, while network and internet security focus on protecting data during transmission over networks.

**Need for Security:**

* **Increasing Threat Landscape:** The rising number of attacks necessitates robust security measures to protect systems and data.
* **Growth of Networking:** The rapid growth of computer networking for information sharing increases the attack surface and the need for securing data in transit and at rest.
* **Availability of Malicious Tools:** The internet provides numerous tools and resources, which can be exploited for malicious purposes, thus increasing the need for protective security measures.
* **Lack of Specialized Resources:** A shortage of specialized resources for securing systems contributes to the vulnerability of systems and highlights the need for dedicated security efforts and expertise.
* **Protecting Data During Transmission:** With increased reliance on networks and communication links, there is a critical need to protect data from interception or modification during transmission.

**Network Attack**  
In a network attack, attackers focus on penetrating the corporate network perimeter and gaining access to internal systems. Once inside, attackers will very often combine other types of attacks. This can include compromising an endpoint, spreading malware, or exploiting a vulnerability in a system within the network.  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
**Q2)Distributed Denial of Service (DDoS) Attacks**A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

The key characteristic of a DDoS attack is that the attack traffic originates from multiple compromised computer systems (often referred to as a "botnet" or "zombie network") that are distributed across different geographical locations. This distribution makes it significantly harder to stop the attack compared to a single-source DoS attack.

**How it Works:  
1. Botnet Creation:** Attackers infect a large number of computers with malware, turning them into "bots" or "zombies" that can be controlled remotely. **2. Command and Control:** The attacker communicates with the botnet through a command and control (C&C) server, instructing the bots on when and how to launch the attack. **3. Attack Launch:** On command, all the bots in the botnet simultaneously send a massive volume of traffic (e.g., requests, packets) towards the target.

**Impact of a DDoS Attack:  
1. Resource Exhaustion:** The sheer volume of traffic overwhelms the target's resources, such as server bandwidth, processing power, or network capacity. **2. Service Disruption:** As a result, legitimate users are unable to access the targeted service or website, leading to service outages.  
**3. Financial Loss:** Businesses can suffer significant financial losses due to lost revenue, damage to reputation, and the cost of mitigating the attack.

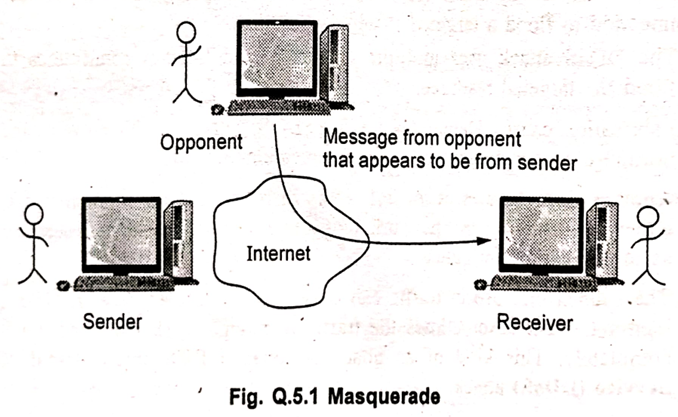
**Types of DDoS Attacks:**DDoS attacks can target different layers of the network and can be categorized based on the type of traffic used:  
**Volume-based Attacks:** Aim to flood the target with a massive amount of traffic, consuming bandwidth (e.g., UDP floods, ICMP floods).  
**Protocol Attacks:** Exploit weaknesses in network protocols to consume server resources (e.g., SYN floods, fragmented packet attacks).     
**Application-layer Attacks:** Target specific vulnerabilities in applications to crash or overwhelm the server (e.g., HTTP floods, DNS query floods).

Mitigating DDoS attacks is challenging due to the distributed nature of the sources and the difficulty in distinguishing malicious traffic from legitimate traffic. Defense strategies often involve traffic filtering, rate limiting, anomaly detection, and using specialized DDoS mitigation services.  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
Q3) **Explain with suitable examples what do you mean by active attacks & passive attacks.**

Active attacks: Active attacks involve some modification of the data stream or the creation of a false stream. These attacks can not be prevented easily.

Active attacks can be subdivided into four types:   
1. Masquerade 2. Replay   
3 . Modification of message 4.Denial of service

Active attacks can be subdivided into four types:

1. **Masquerade:** This occurs when one entity pretends to be a different entity. An example given is when authentication sequences are captured and replayed after a valid authentication, allowing an unauthorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. Interruption attacks are also called masquerade attacks.     
   
2. **Replay:** This involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. The diagram shows an opponent capturing a message from the sender and later replaying it to the receiver.     
   A diagram of a computer system

   AI-generated content may be incorrect.
3. **Modification of Message:** This involves some change to the original message, which produces an unauthorized effect. An example provided is a message meaning "Allow Rupali Dhotre to read confidential file accounts" being modified to mean "Allow Mahesh Awati to read confidential file accounts".  
   A diagram of a computer system

   AI-generated content may be incorrect.
4. **Denial of Service (DoS):** Fabrication can cause DoS attacks. DoS prevents the normal use or management of communications facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

**Passive Attacks:**  
Passive attacks are those wherein the attacker indulges in eavesdropping on, or monitoring of data transmission. A passive attack attempts to learn or make use of information from the system but does not affect system resources. The attacker's aim is to obtain information that is in transit. The term "passive" indicates that the attacker does not attempt to perform any modifications to the data.

Passive attacks are of two types:

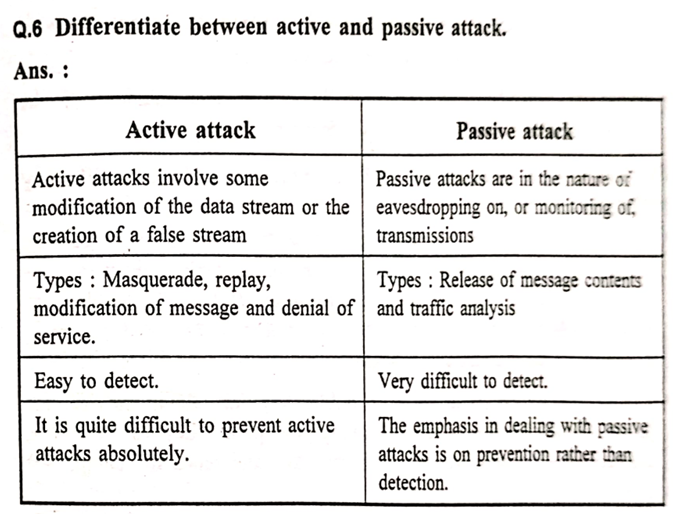
1. **Release of Message Contents:** This involves an opponent listening in on communications to learn the content of the transmissions. Examples include a telephone conversation, an electronic mail message, or a transferred file, which may contain sensitive or confidential information.     
   A diagram of a computer system

   AI-generated content may be incorrect.
2. **Traffic Analysis:** This involves masking the contents of messages so that opponents could not extract information from the message (e.g., using encryption). However, even if the contents are masked, an opponent might still be able to gain information by observing the patterns of communication, such as the frequency, length, and source/destination of messages. This is known as traffic analysis.  
   A diagram of a computer

   AI-generated content may be incorrect.

Passive attacks are very difficult to detect because they do not involve any alteration of data. Preventing the success of a passive attack is usually attempted by means of encryption.

-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

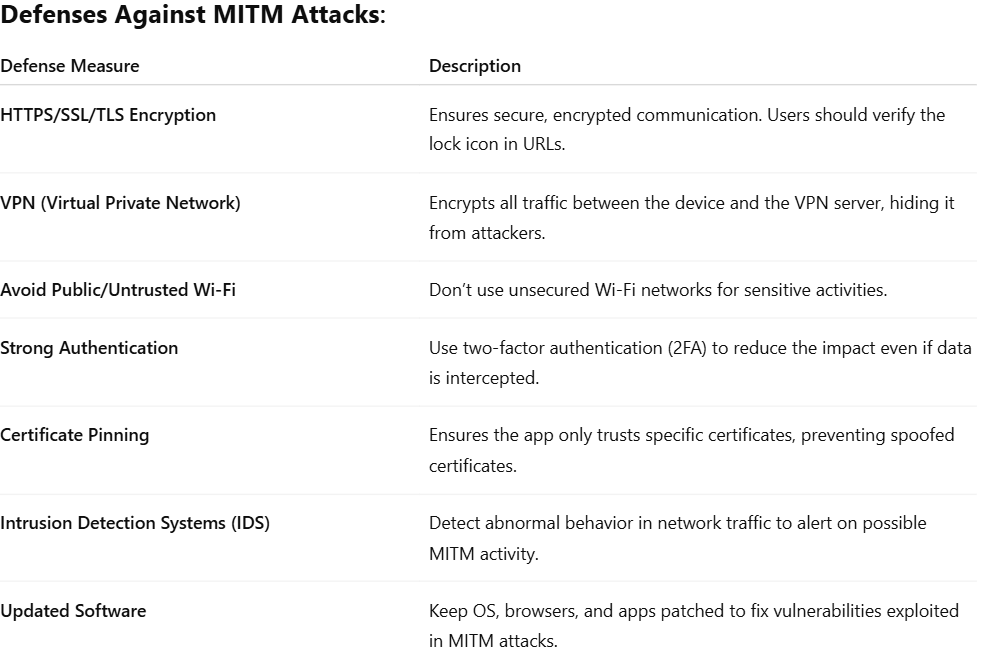
Q4)  
  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
Q5) **Explain Man in the middle attacks. How to defenses against the attack?**In cryptography, a Man-In-The-Middle (MITM) attack is a security attack where an attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attacker can read, insert, and modify messages between the two parties without either party knowing that the link between them has been compromised. MITM is typically used to refer to active manipulation of messages, rather than passively eavesdropping.

During a MITM attack, the attacker is able to observe and intercept messages going between the two victims. MITM attacks can work against public-key cryptography and are particularly applicable to the original Diffie-Hellman key exchange protocol when used without authentication.

**Types of MITM Attacks:**  
The MITM attack may include one or more of the following:  
1. **Eavesdropping:** Including traffic analysis and possibly a known-plaintext attack.  
2. **Chosen ciphertext attack:** Depending on what the receiver does with a message that it decrypts.  
3. **Substitution attack.**  
4. **Replay attacks.**  
5. **Denial of service attack:** The attacker may, for instance, jam all communications before attacking one of the parties.

**How It Works:  
1.** Interception: The attacker places themselves between the sender and receiver. **2.** Data Access: The attacker can eavesdrop, steal sensitive data (passwords, credit card numbers), or inject malicious content. **3.** Common Methods:  
Wi-Fi Eavesdropping: Attacker sets up a rogue Wi-Fi hotspot.ARP Spoofing: Attacker sends false ARP messages to associate their MAC address with the IP of another device.DNS Spoofing: Redirects user to malicious websites by altering DNS responses.HTTPS Spoofing: Attacker uses fake SSL certificates to impersonate trusted sites.

**Real-life Example:** User connects to a fake public Wi-Fi named "Free\_Cafe\_WiFi". All traffic goes through the attacker's laptop, allowing them to read or manipulate data like login credentials.

  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
Q6)**What is a Stream Cipher?**  
Stream cipher algorithms are designed to accept a crypto key and a stream of plaintext to produce a stream of ciphertext. A stream cipher is similar to a one-time pad.     
A diagram of a stream cipher

AI-generated content may be incorrect.  
**How it Works:**  
A stream cipher encrypts smaller blocks of data, typically bits or bytes.  
A key stream generator outputs a stream of bits K1​,K2​,K3​,…,Ki​.  
This key stream is XORed with a stream of plaintext bits P1​,P2​,P3​,…,Pi​ to produce the stream of ciphertext bits Ci​=Pi​⊕Ki​.  
At the decryption end, the ciphertext bits are XORed with an identical key stream to recover the plaintext bits Pi​=Ci​⊕Ki​.     
The security system depends entirely on the insides of the keystream generator.

**Advantages of Stream Ciphers:**  
1. Speed of transformation.  
2. Low error propagation.

**Disadvantages of Stream Ciphers:**  
1. Low diffusion.  
2. Susceptibility to malicious insertion and modifications.  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
Q7)   
A paper with text on it

AI-generated content may be incorrect.  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
Q8) **Block Cipher Modes of Operation/ Block Cipher muscles of Operation**  
The modes of operation of block ciphers are configuration methods that allow these ciphers to work with large data streams without compromising the provided security. A block cipher itself allows encryption of only a single data block of the cipher's block length under a single key. Modes of operation enable the repeated and secure use of a block cipher under a single key.

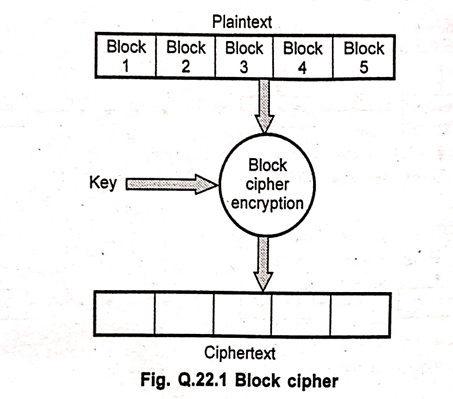
When targeting a variable-length message, the data must first be partitioned into separate cipher blocks. Typically, the last block must also be extended to match the cipher's block length using a suitable padding scheme.

Modes of operation have primarily been defined for encryption and authentication. While modes of operation are commonly associated with symmetric encryption, they may also be applied to public-key encryption primitives such as RSA in principle.

There are five types of operations in block cipher modes:  
1. **ECB (Electronic Code Book) mode:**  
Used for transmitting a single value in a secure manner.  
Works on block ciphers.  
2. **CBC (Cipher Block Chaining) mode:**  
Used for encrypting blocks of text authentication.  
Works on block ciphers.  
3. **CFB (Cipher Feedback) mode:**  
Used for transmitting encrypted stream of data.  
Works on block ciphers acting as stream ciphers.  
4. **OFB (Output Feedback) mode:**  
Used for transmitting encrypted stream of data.  
Works on block ciphers acting as stream ciphers.  
5. **CTR (Counter) mode:**  
Used for transmitting block-oriented applications.

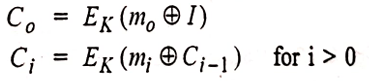
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
Q9)**What is block cipher? Explain counter mode of block cipher.**

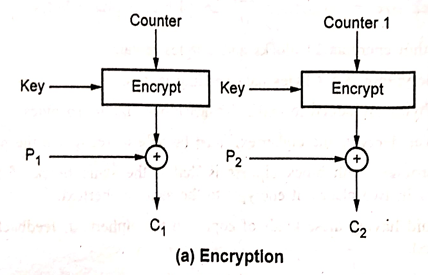
Block Cipher : A block cipher operates on blocks of data.

Fig. Q.22.1 shows block cipher method.   


Algorithm breaks the plaintext into blocks and operates on each block independently.   
Usually blocks are 8 or 16 bytes long.   
Security of block ciphers depends on the design of the encryption function.   
Software implementations of block ciphers run faster than software implementation of the stream ciphers.   
Errors in transmitting one block generally do not affect other blocks.   
Each block is enciphered independently, using the same key, identical plaintext blocks produce identical ciphertext blocks.   
Suppose that plaintext is 227 bytes long and the cipher you are using operates on 16-byte blocks.   
Algorithm grabs the first 16-bytes of data, encrypts them using the key table.

Algorithms produce 16-bytes of ciphertext.   
After first block, algorithm takes next block.   
The key table does not change from block to block.   
Plaintext 227 bytes   
Block size 16 bytes = 227/16 = 14 blocks plus 3 bytes

Algorithm encrypts 14 blocks and 3 bytes remain.   
For encrypting last 3 bytes data padding is used.   
Extra bytes are added to make the last block size to 16 bytes.   
Whoever decrypts the ciphertext must be able to recognize the padding.   
One problem with block ciphers is that if the same block of plaintext appears in two places, it encrypts to the same ciphertext.   
To avoid having these kinds of copies in the ciphertext, feedback modes are used.   
Cipher block chaining does not require the extra information to occupy bit spaces, so every bit in the block is part of the message.   
Before a plaintext block is enciphered, that block is XOR'ed with preceding ciphertext block.   
In addition to the key, this technique requires an initialization vector to XOR the initial plaintext block.   
For decrypting the data, copy a block of ciphertext, decrypt it and XOR the result with the preceding block of ciphertext.   
Taking Ex to be the encipherment algorithm with key K and I to be the initialization vector, the cipher block chaining technique is  
   
**Counter (CTR) Mode of Block Cipher**  
In Counter (CTR) mode, block ciphers use sequence numbers as the input to the algorithm. This mode effectively turns a block cipher into a stream cipher.

**How it Works:**  
Instead of encrypting the plaintext blocks directly or chaining them, CTR mode encrypts a sequence of counter values.  
A unique counter value is used for each plaintext block. This counter is typically incremented for each subsequent block.  
The output of the encryption of the counter is then XORed with the corresponding plaintext block to produce the ciphertext block (Ci​=Pi​⊕EK​(Counter i​)).  
For decryption, the same counter sequence is generated and encrypted with the same key. The resulting output is XORed with the ciphertext block to recover the plaintext block (Pi​=Ci​⊕EK​(Counteri​)).  
More than one message can be encrypted with the same key, provided that a different initialisation vector (which can be used to derive the initial counter value) is used.  
 A diagram of a computer system

AI-generated content may be incorrect.

**Characteristics of CTR Mode:**  
Plaintext is very easy to manipulate; any change in ciphertext directly affects the plaintext.  
A ciphertext error affects only the corresponding bit of plaintext.  
Synchronization error is unrecoverable.

**Advantages of Counter Mode:**  
1. Simple to implement.  
2. It provides confidentiality.  
3. Random access of blocks is possible.  
4. Efficiency is the same as a block cipher.  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
Q10) **Explain Electronic Code block (ECB) mode.**   
A block of plaintext encrypts into a block of ciphertext. Block size is 64-bits. Each block is encrypted independently.

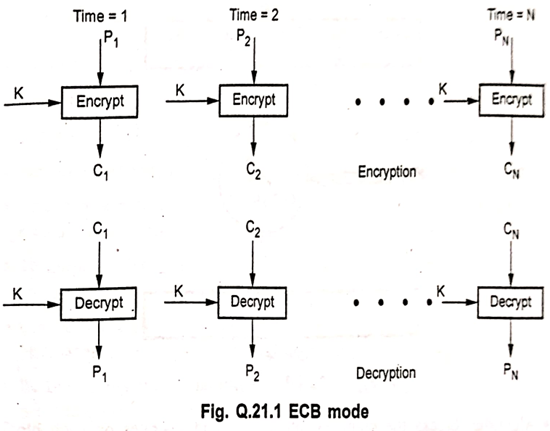
Plaintext patterns are not concealed since identical blocks of plaintext give identical blocks of ciphertext. It is not necessary to encrypt the file linearly.

User can encrypt the 10 blocks in the middle first, then the blocks at the end, and finally the blocks in the beginning. Because of this, encrypted files are accessed randomly like a data base.

It is very easy to parallelize the process. Pad the last block with some regular pattern i.e. zeros, ones to make it a complete block.

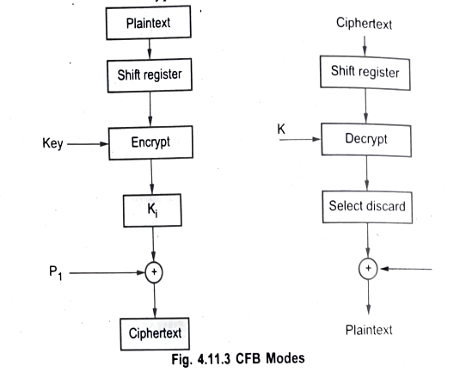
End of file character is used to denote the final plaintext byte before padding.

ECB method is ideal for a short amount of data, such as an encryption key.

* Fig. Q.21.1 shows ECB mode.  
  

In ECB mode, plaintext is divided into 64-bit blocks, with each block encrypted independently using the same key. The result of this encryption is the ciphertext.

* At the receiver's end, the ciphertext is also divided into 64-bit blocks. Using the same key, each ciphertext block is decrypted back into plaintext.
* ECB mode is not secure for lengthy messages.
* It is suitable for secure transmission of single values, such as encryption keys.
* ECB has security limitations, including:
  + Patterns in the plaintext can be visible in the ciphertext.
  + Ciphertext can easily be modified by adding, removing, or switching encrypted blocks.
  + Synchronization errors are unrecoverable.

-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
q11) Cipher Feedback (CFB) Mode:  
**Data Encryption:** Data is encrypted in units that are smaller than a defined block size.  
**Stream Cipher Conversion:** It is possible to convert the DES into a stream cipher using the cipher feedback mode.  
**Unit Size:** In this mode, the data is encrypted in the form of units, where each unit is often 8 bits.  
**Initialization Vector (IV):** Like cipher block chaining mode, the IV is initialized and kept in the shift register. It is encrypted using the key to form the ciphertext.  
 ****  
**Encryption Process (as shown in the diagram):**   
An initial shift register value (often the IV) is encrypted with the key.  
The output of the encryption is combined with the plaintext (P1) using an XOR operation to produce the ciphertext (C1).  
The ciphertext (C1) is then shifted into the shift register for the next step.  
**Decryption Process (as shown in the diagram):**   
The ciphertext (C1) is used as the input for the shift register.  
The value in the shift register is encrypted with the key.  
The output of the encryption is combined with the ciphertext (C1) using an XOR operation to produce the plaintext (P1).  
The ciphertext (C1) is shifted into the shift register for the next step. A "Select discard" step is shown, indicating that only a portion of the encrypted output is used in the XOR operation, corresponding to the unit size.

**Multiple Messages:** More than one message can be encrypted with the same key, provided that a different initialization vector is used for each message.  
**Speed:** CFB speed is the same as the block cipher speed.  
**Parallelizability:** Encryption is not parallelizable, but decryption is parallelizable and has a random access property.  
CFB is self recovering with respect to synchronization errors as well.  
**Advantages**:   
1. Simplicity   
2. Need not be used on a byte boundary.   
3. Input to the block cipher is randomized   
4. Ciphertext size is the same size as the plaintext size. .

**Disadvantages:**1. Encryption is not parallelizable. 2. Plaintext is somewhat difficult to manipulate.

-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Q12**) Cipher Block Chaining (CBC) Mode**

Cipher block mode at the sender side, the plain text is divided into blocks. In this mode IV(Initialization Vector) is used which can be a random block of text. IV is used to make the ciphertext of each block unique.   
The first block of plain text and IV is combined using the XOR operation and then encrypted the resultant message using the key and form the first block of ciphertext. the first block of ciphertext is used as IV for the second block of plain text. The same procedure will be followed for all blocks of plain text.   
At the receiver side, the ciphertext is divided into blocks. The first block ciphertext is decrypted using the same key which is used for encryption. The decrypted result will be XOR with the IV and form the first block of plain text. The second decryption will be XOR with the first block of ciphertext and form the second block of plain text. The same procedure is used for all the blocks. is XORed with the previous ciphertext block before it is encrypted.   
The plaintext The CBC mode is iterative mode.   
After a plaintext block is encrypted, the resulting ciphertext is also stored in a feedback register.   
Before the next plaintext block is encrypted, it is XORed with the feedback register to became the next input to the encrypting routine   
The encryption of each block depends on all the previous blocks.   
A ciphertext block is decrypted normally and also saved in a feedback register.   
After the next block is decrypted, it is XORed with the results of the feedback register  
Mathematically, it is represented as:

* + Ci = Ek(Pi ⊕ Ci-1)
  + Pi = Ci-1 ⊕ Dk(Ci)

It hides patterns in the plaintext.  
In order to guarantee that there is always some random looking ciphertext to apply to the actual plaintext, the process is started with a block of random bits called the Initialization Vector (IV).

Fig. 4.11.2 shows cipher block chaining mode  
A diagram of a circuit

AI-generated content may be incorrect.  
When used in networking messages, most CBC implementations add the IV to the beginning of the message in plaintext.

A single bit error in a plaintext block will affect that ciphertext block and all subsequent ciphertext blocks.   
CBC mode is self recovering.   
Two blocks are affected by an error, but the system recovers and continues to work correctly for all subsequent blocks. Synchronization error is unrecoverable.   
Encryption is not parallelizable.   
Decryption is parallelizable and has a random access property.  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
q13) **Security Services**   
security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or X.800 defines a of data transfers.   
X.800 divides security services into five different categories.   
1. Authentication 2. Access control   
3. Data confidentiality 4. Data integrity   
5. Nonrepudiation

**1. Authentication**Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In public and private computer network, authentication is commonly done through the use of login passwords.

Two specific authentication services are defined in X.800:   
a. Peer entity authentication   
b. Data origin authentication

**Peer entity authentication** used in association with a logical connection to provide confidence in the identity of the entities connected.

Data origin outhentication enables the recepient to verify that the message have not been tempered in transit (data integrity) and they originally from expected sender (authenticity).

**Data origin authentication** does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.

**2. Access Control**Access control is an important tool of security to protect data and other resources. The access control mechanism refers to prevention of unauthorized use of a resource. Access control includes: 1. Authentication of users 2. Authorization of their privileges 3. Auditing to monitor and record user actions

Three types of access controls system are:   
1. Discretionary access control   
2. Mandatory access control   
3. Role-based access control

A password scheme used to allow access to a user's computer account may be viewed as the simplest instance of an access control matrix: each resource has a list of identities associated with it (e.g. a computer account which authorized entities may access), and successful corroboration of an identity allows access to the authorized resources as listed for that entity.  
The simplest framework for describing a protection system is the access control matrix model. Two fundamental concepts in field authorization are:   
1. Access Control Lists (ACLS)   
2. Capabilities (C-lists)

**3. Data confidentiality**Confidentiality is the concealment of information or resources. It is the protection of transmitted data from passive attacks. Confidentiality is classified into 1. Connection confidentiality: The protection of all user data on a connection. 2. Connectionless confidentiality: The protection of all user data in a single data block. 3. Selective field confidentiality: The confidentiality of selected fields within the user data on a connection or in a single data block. 4. Traffic flow confidentiality: The protection of the information that might be derived from observation of traffic flows.

**4. Data integrity**Integrity can apply to a stream of messages a within a message. single message or selected fields Modification causes loss of message integrity. Data integrity can be classified as 1. Connection integrity with recovery 2. Connection integrity without recovery 3. Selective field connection integrity 4. Connectionless integrity 5. Selective field connectionless integrity

Connection integrity with recovery provides for the integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence with recovery attempted.   
Connection integrity without recovery provides only detection without recovery.   
Selective field connection integrity provides for the integrity of selected fields within the user data of a data block transferred over a connection.

Connectionless integrity provides for the integrity of a single connectionless data block and may take the form of detection of data modification.  
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------  
q14) **i) Unauthorized Access  
Definition**: Unauthorized access refers to the act of gaining access to a computer system, network, or data **without permission**. It is a major security threat where attackers bypass authentication mechanisms to reach restricted resources. **Causes:**Weak or stolen passwordsLack of proper access control mechanismsExploiting software vulnerabilities (e.g., unpatched systems)Phishing and social engineering attacks

**Types of Unauthorized Access:  
External Unauthorized Access** – Performed by outsiders (e.g., hackers) attempting to break into the network. **Internal Unauthorized Access** – Carried out by employees or insiders accessing data they’re not permitted to view.

**Consequences:**Data theft or leakageLoss of privacy and intellectual propertyFinancial lossDamage to organization’s reputation

**Prevention Techniques:**Strong authentication (e.g., MFA)Access control lists (ACLs) and role-based access control (RBAC)Regular auditing and monitoringKeeping systems and software updatedUser education and awareness