Unit-2

1.Explain the Advanced Encryption Standard (AES) in detail. 10

Ans: Advanced Encryption Standard (AES) is a highly trusted **encryption algorithm** used to secure data by converting it into an unreadable format without the proper key. Developed by the National Institute of Standards and Technology (NIST), **AES encryption** uses various **key lengths** (128, 192, or 256 bits) to provide strong protection against unauthorized access. This **data security** measure is efficient and widely implemented in securing **internet communication**, protecting **sensitive data**, and encrypting files. AES, a cornerstone of modern cryptography, is recognized globally for its ability to keep information safe from cyber threats.

Features:

1.S**ymmetric Key Algorithm**: AES uses the same key for both encryption and decryption, which means both the sender and receiver must keep the key secret.

2.**Block Cipher**: AES operates on fixed-size blocks of data. It processes data in 128-bit blocks.

3. **Key Sizes**: AES supports three key lengths: 128 bits, 192 bits, and 256 bits, with longer keys offering higher security.

Structure and Operations:

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows :

- 128-bit key – 10 rounds
- 192-bit key – 12 rounds
- 256-bit key – 14 rounds

Components of a Round:

- **SubBytes**: Non-linear substitution step where each byte is replaced with another byte using a substitution box (S-Box).
- **ShiftRows**: Rows of the state are shifted to the left by different offsets.
- **MixColumns**: Each column of the state is mixed, providing diffusion.
- **AddRoundKey**: The round key is combined with the state using bitwise XOR.

Initialization and Final Round

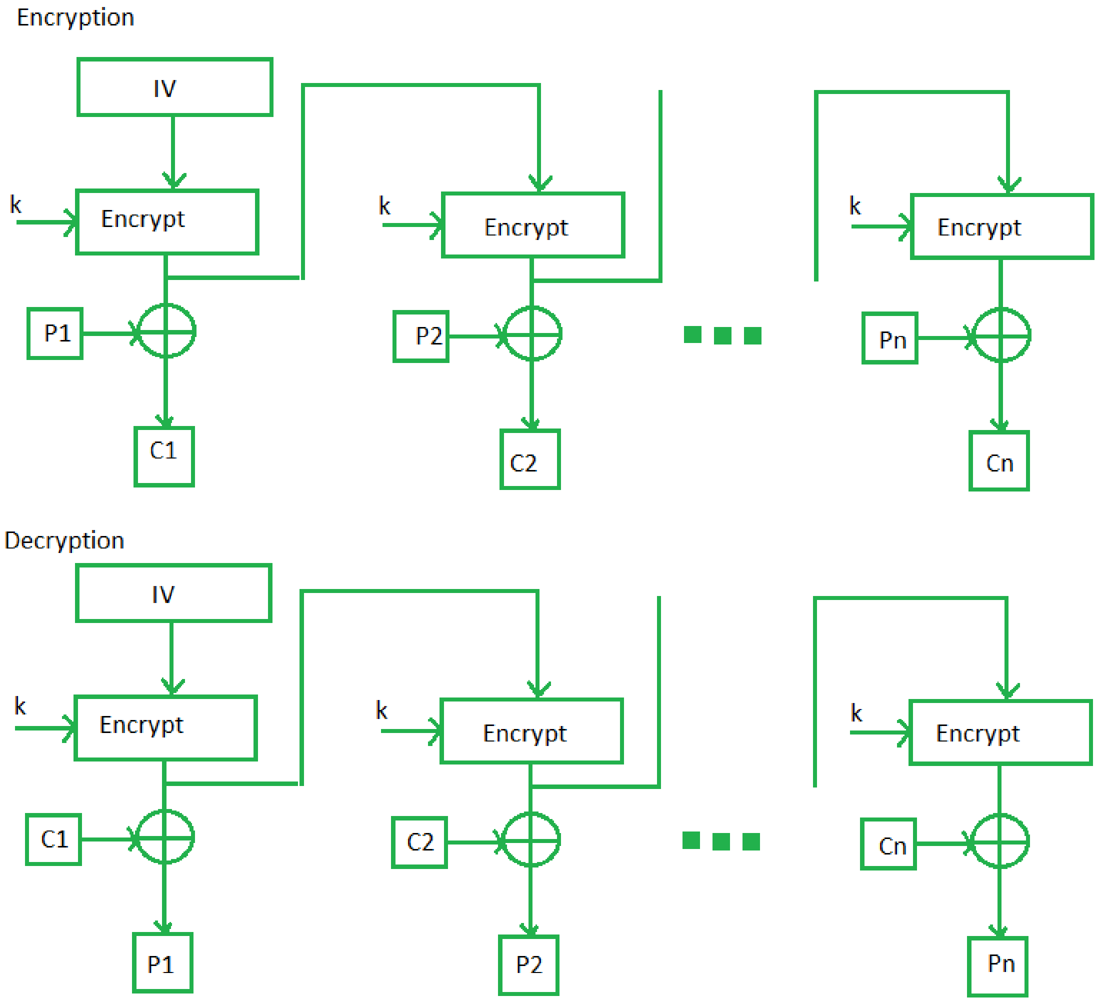
- **Key Expansion**: The original key is expanded into a series of round keys for use in each round.
- **Initial Round**: The process starts with the AddRoundKey step, where the initial round key is combined with the plaintext.
- **Final Round**: The last round omits the MixColumns step and consists only of SubBytes, ShiftRows, and AddRoundKey.

Applications

- AES is widely used in various applications, including file encryption, VPNs, and secure communications protocols (e.g., TLS, SSL).
- It is also employed in hardware implementations, smart cards, and wireless communications.

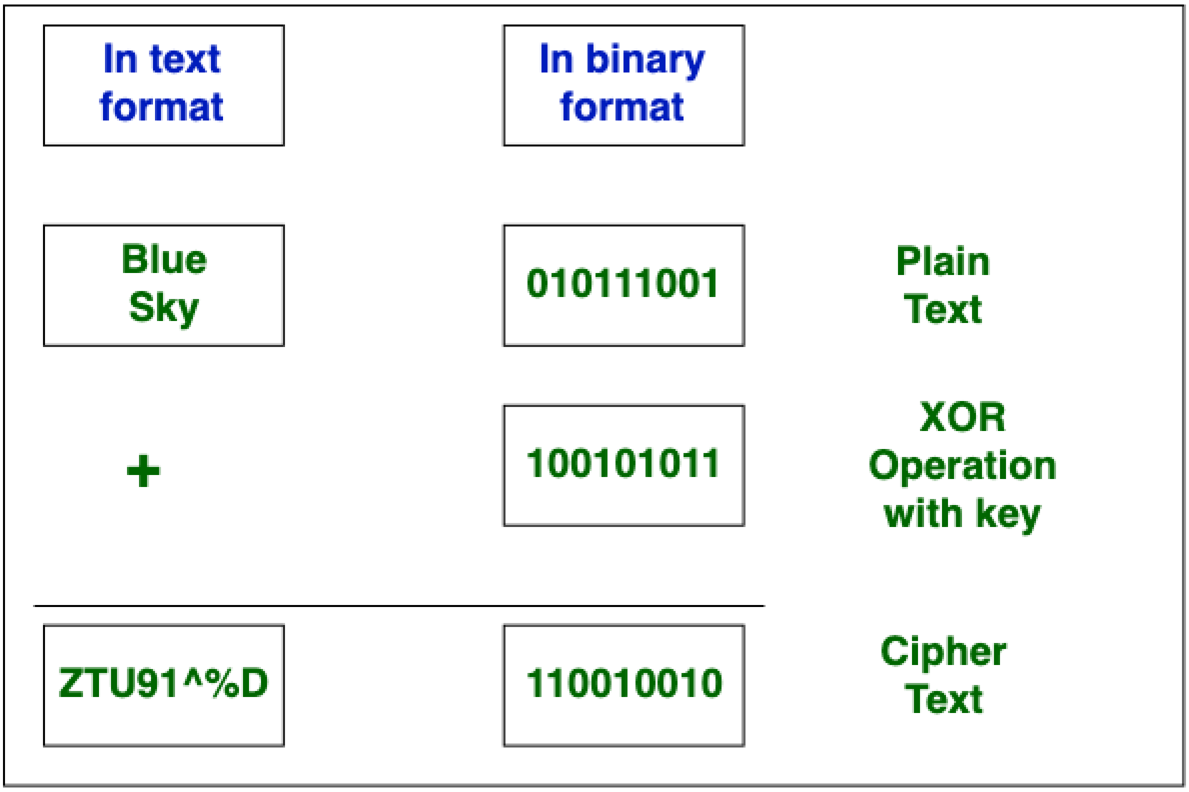
2.Explain the Output Feedback mode with the help of a block diagram.5

Ans: The output feedback mode follows nearly the same process as the Cipher Feedback mode except that it sends the encrypted output as feedback instead of the actual cipher which is XOR output. In this output feedback mode, all bits of the block are sent instead of sending selected *s* bits. The Output Feedback mode of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.



3. Explain Stream cipher and block cipher with the help of an example.5

Ans: **Block Cipher** and **Stream Cipher** belong to the symmetric key cipher. These two block ciphers and stream cipher are the methods used for converting the plain text into ciphertext. The main difference between a **Block cipher** and a **Stream cipher** is that a block cipher converts the plain text into cipher text by taking the plain text's block at a time. While stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.



In text format	In binary format	
Blue Sky	010111001	Plain Text
+	100101011	XOR Operation with key
ZTU91^%D	110010010	Cipher Text

Stream Cipher

4. What is a key distribution center? Explain a decentralized key distribution scenario.(2+5)

Ans: A key distribution center (KDC) in cryptography is a system that is responsible for providing keys to the users in a network that shares sensitive or private data. Each time a connection is established between two computers in a network, they both request the KDC to generate a unique password which can be used by the end system users for verification.

A decentralized key distribution scenario allows multiple parties to securely exchange encryption keys without relying on a central authority. Here’s a concise explanation:

1. Peer-to-Peer Exchange

- In a decentralized model, each participant (or node) generates its own key pair (public and private keys). For instance, Alice and Bob both create their own key pairs.

2. Public Key Sharing

- Each participant shares their public key with others directly, often using a secure communication channel. For example, Alice sends her public key to Bob, and Bob sends his public key to Alice.

3. Key Agreement

- Using their private keys and the received public keys, both parties can derive a shared secret key. This can be achieved through protocols like Diffie-Hellman, enabling secure communication without needing a central key server.

5. Explain Blowfish algorithm.What are the properties of the Blowfish algorithm? 8+3

Ans: Blowfish is an encryption technique designed by Bruce Schneier in 1993 as an alternative to DES Encryption Technique. It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is symmetric block cipher algorithm.

1. blockSize: 64-bits
2. keySize: 32-bits to 448-bits variable size
3. number of subkeys: 18 [P-array]
4. number of rounds: 16
5. number of substitution boxes: 4 [each having 512 entries of 32-bits each]

Blowfish features a 64-bit block size with keys that can be 32 bits long or 448 bits long. It features 16 iterations that resemble Feistel and each one operates on a 64-bit block that is partitioned into two 32-bit words. Blowfish uses a single encryption key to encode and decode data.

The two primary parts of the blowfish algorithm are as follows:

Data Encryption: A 16-round Feistel network is used to encrypt data, with each round including a key-dependent permutation and a key- and data-dependent replacement. The replacement approach is used in conjunction with large, key-dependent S-boxes to encrypt data in Blowfish. All encryption processes include add on 32-bit words and XORs, a sort of logic gate.

Key expansion and Sub keys: Maximum size 448-bit keys are expanded into several sub key arrays totaling 4,168 bytes throughout the key expansion procedure. The Blowfish algorithm, which makes extensive use of sub keys, depends on them. Before any encryption or decryption can occur, these sub keys are pre-calculated.

The P-array in Blowfish is made up of four 32-bit S-boxes with 256 entries each, along with 18 32-bit sub keys. Following is the calculation for the sub keys:

1. A predetermined string of pi's hexadecimal digits is used as the initialization value for the P-array and S-boxes.
2. Now, the first P-array element (P1) is XORed with the first 32 bits of the key, followed by P2 with the second 32 bits, and so on, until all P-array elements have been XORed with the key bits.
3. The procedure is applied on all-zero strings in the manner shown in the preceding phases.
4. Replace the P1 and P2 arrays with the results of step 3 above.
5. Blowfish is used to encrypt this output while using changed sub keys.
6. The P-array's P3 and P4 are modified by the output of step 5.
7. The four S-boxes and all the P-arrays are updated when this operation is completed.

To produce all the sub keys and processes, Blowfish executes 521 times in total, using around 4 kilobytes (KB) of data.

PROPERTIES:

1. Block Size and Key Length: Blowfish operates on 64-bit blocks and supports variable key lengths from 32 bits to 448 bits, allowing flexibility in security.

2.Feistel Structure: It uses a Feistel network with 16 rounds, enabling efficient encryption and decryption using the same process.

3.Speed and Efficiency: Blowfish is designed for high-speed performance, particularly on 32-bit processors, making it suitable for applications requiring rapid encryption and low memory usage.

6. Explain the Data Encryption Standard (DES) algorithm in detail.10

Ans: Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security. Data encryption standard (DES) has been found vulnerable to very powerful attacks therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.

Key Features

- **Symmetric Key Algorithm**: DES uses the same key for both encryption and decryption, requiring both the sender and receiver to keep the key confidential.
- **Block Cipher**: It operates on fixed-size blocks of 64 bits, processing data in chunks of this size.

Key Length

- DES uses a 56-bit key for encryption, which is derived from a 64-bit key (the remaining 8 bits are used for parity checks).

Algorithm Structure

- DES follows a Feistel structure and consists of 16 rounds of processing, which includes several operations to enhance security.

Rounds and Operations

- **Initial Permutation (IP)**: The 64-bit plaintext undergoes an initial permutation that rearranges the bits.
- **Round Function (F)**: Each round consists of the following steps:
    - **Expansion**: The 32-bit right half of the data is expanded to 48 bits by duplicating some bits.
    - **Key Mixing**: The expanded data is XORed with a round key derived from the original 56-bit key.
    - **Substitution**: The result is divided into eight 6-bit segments, each passed through a substitution box (S-box) that transforms them into 4-bit segments.
    - **Permutation**: The output is permuted to produce a 32-bit output.
- **Combining Halves**: The left and right halves are combined in each round to form a new left half and a new right half.

Final Permutation

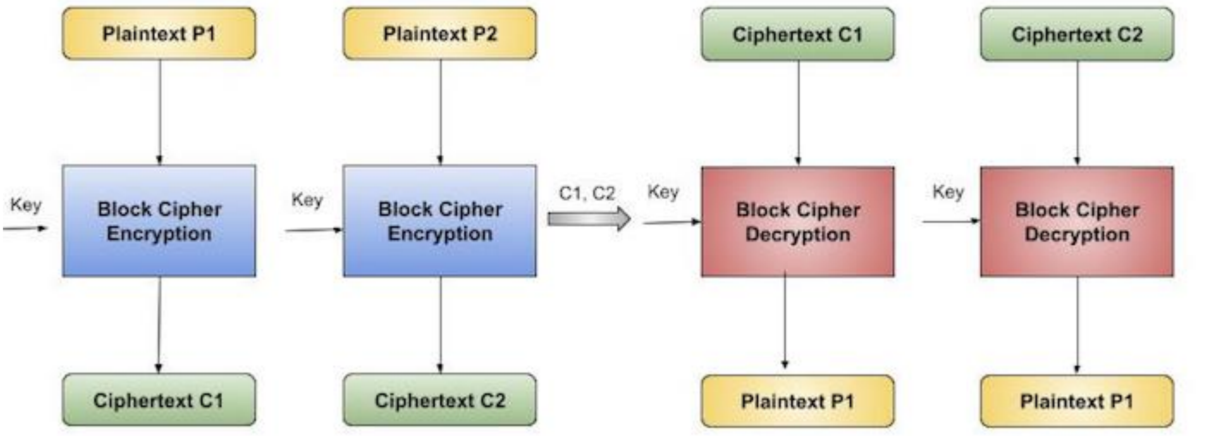
- After completing all 16 rounds, the final output undergoes an inverse of the initial permutation, resulting in the 64-bit ciphertext.

Key Scheduling

- The original 56-bit key is processed to generate 16 subkeys (one for each round). This involves permutation and left shifts to create the round keys.

7. Explain the Electronic Code Book mode with the help of a diagram.5

Ans: The most basic mode is electronic codebook mode, where the plain text is processed block by block and each block is encrypted using a single key. The term codebook is in itself self-explaining. If we are given a particular key, then we have a unique ciphertext for every b-bit block of plaintext. Thus, one can visualize a large codebook with entries for all conceivable b-bit plaintext patterns showing its corresponding ciphertext. This is because it is important to understand how the ECB Mode works and in what context this method is better than the others.



8. Differentiate between link encryption and end-to-end encryption.4

Ans:

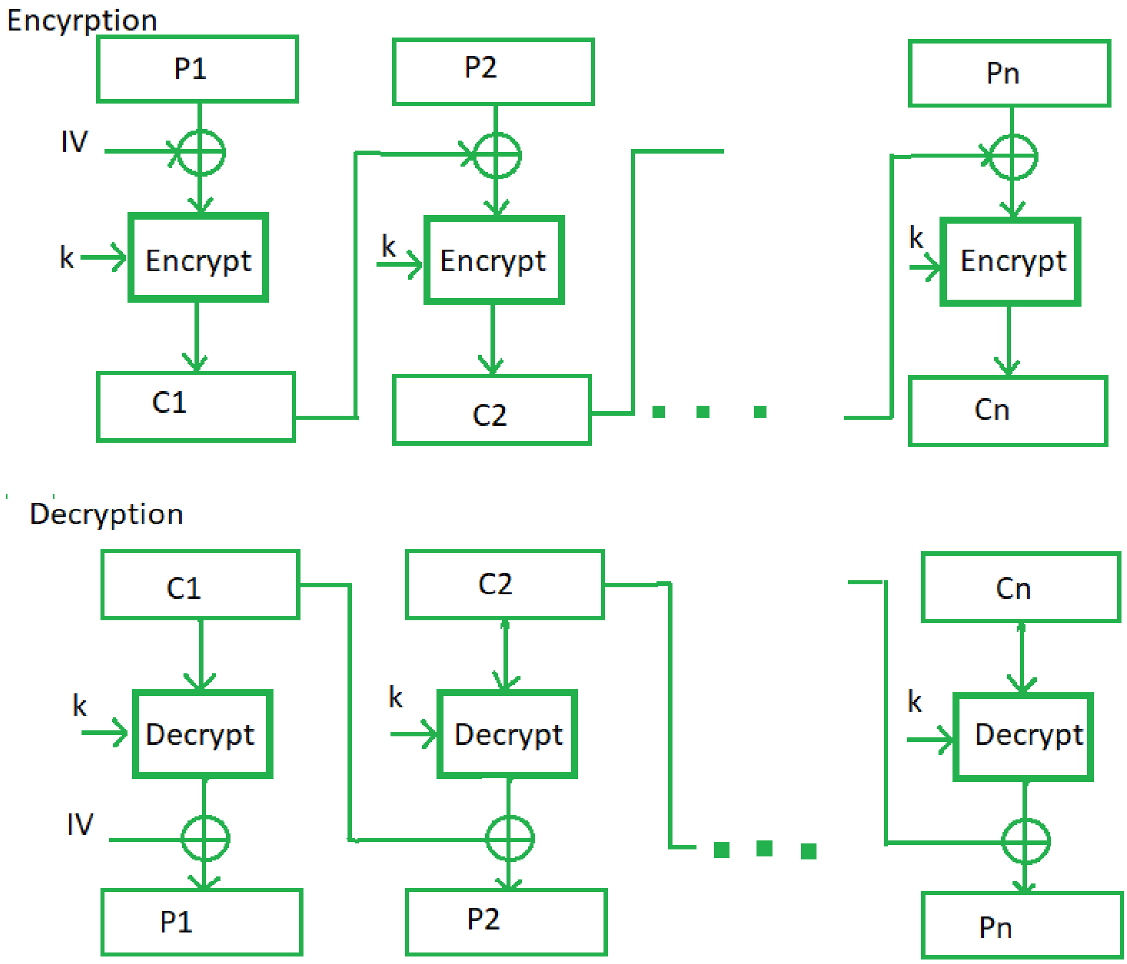
Link Encryption	**End-to-End Encryption**
Encrypts data at each link in the communication path.	Encrypts data from the sender to the receiver.
Requires multiple keys for each segment of the path.	Typically uses a single key or key pair for both endpoints.
Data may be exposed at intermediate nodes, as it is decrypted at each link.	Data remains encrypted at all points except the endpoints, enhancing privacy.
Commonly used in network-level security (e.g., VPNs, secure tunnels).	Often used in messaging applications and secure communications (e.g., WhatsApp, Signal).

9. What is avalanche effect?1

Ans: The avalanche effect means that a small change in the input of a cryptographic system causes a big and unpredictable change in the output.

10. Explain the Cipher Block Chaining mode with the help of a diagram.5

ANS: Cipher block chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, the previous cipher block is given as input to the next encryption algorithm after XOR with the original plaintext block. In a nutshell here, a cipher block is produced by encrypting an XOR output of the previous cipher block and present plaintext block.



11. What are the two levels of keys that are used in Key Distribution Centre?2

ANS:

Session Keys

Session keys are temporary encryption keys generated for a specific communication session between two parties. They enhance security by ensuring that even if a session key is compromised, it only affects that particular session, minimizing the risk of long-term exposure.

Master Keys

Master keys are long-term keys associated with users or devices within a Key Distribution Centre (KDC). They are used to derive session keys and are securely stored, playing a crucial role in authentication and establishing trust between the KDC and its users.

12. What is traffic confidentiality? Explain the Link Encryption approach.(3+4)

Ans: Traffic confidentiality refers to the protection of data transmitted over a network from unauthorized access or interception. It ensures that the content of communications is kept private, preventing eavesdropping or tampering by malicious actors. This is critical in maintaining the integrity and privacy of sensitive information as it travels across potentially insecure channels. Achieving traffic confidentiality often involves the use of encryption techniques that secure the data before it is transmitted, ensuring that only authorized parties can access and understand the content.

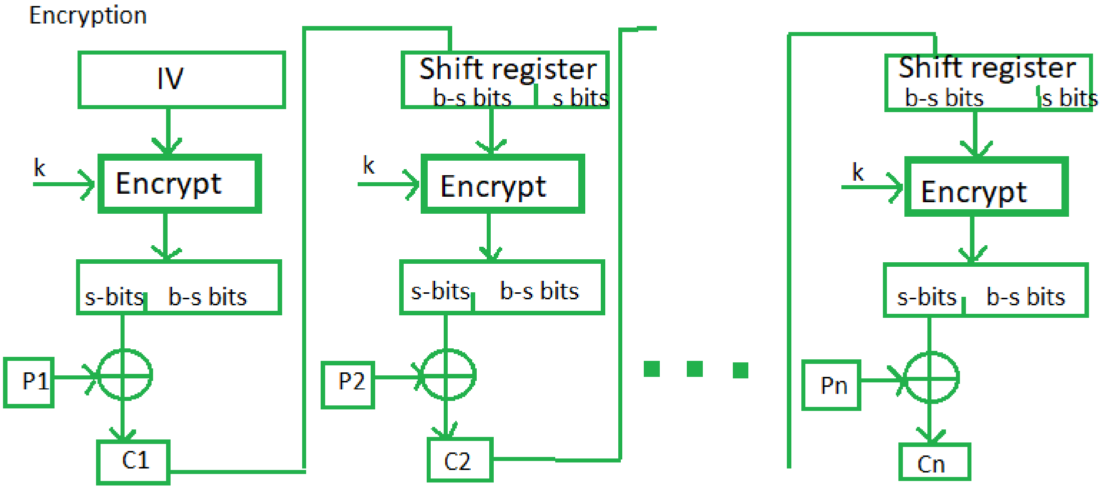
Link encryption is a method of securing data as it travels through each segment (or link) of a communication path. In this approach:

1. **Encryption at Each Link**: Data is encrypted and decrypted at each node (router, switch, etc.) along the communication path. Each segment of the transmission is treated independently, meaning that the data is encrypted before leaving one node and decrypted when it arrives at the next.
2. **Use of Multiple Keys**: Different encryption keys can be used at each link, requiring a robust key management system. This may complicate key distribution and synchronization.
3. **Intermediate Nodes**: Since data is decrypted at each intermediate node, these nodes can access the plaintext. This poses a potential risk if any of these nodes are compromised, as attackers could gain access to sensitive information while it is in transit.
4. **Applications**: Link encryption is commonly used in network-level security protocols, such as Virtual Private Networks (VPNs), where secure tunnels are established between nodes to protect data during transmission.

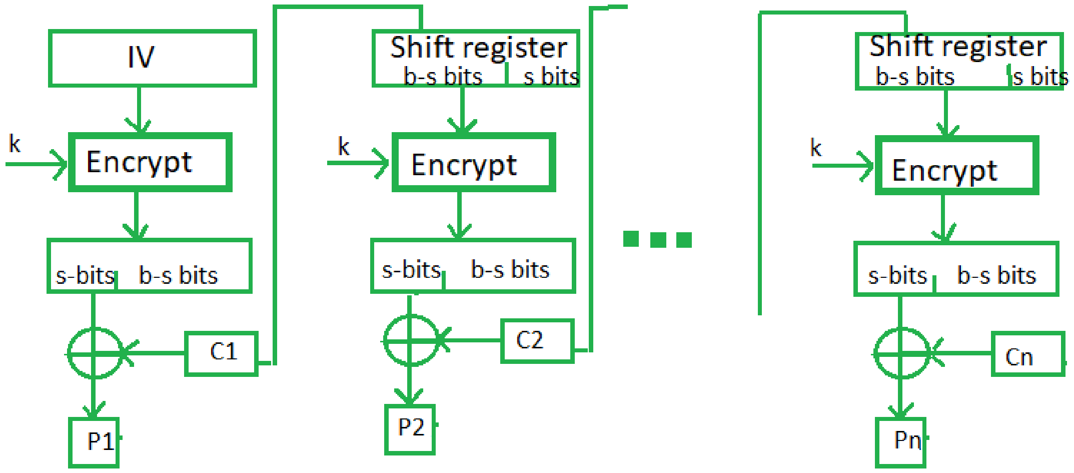
13. Explain the Cipher Feedback Mode (CFB) with the help of a diagram.5

Ans: In this mode the cipher is given as feedback to the next block of encryption with some new specifications: first, an initial vector IV is used for first encryption and output bits are divided as a set of *s* and *b-s* bits.The left-hand side *s* bits are selected along with plaintext bits to which an XOR operation is applied. The result is given as input to a shift register having b-s bits to lhs,s bits to rhs and the process continues.

Encryption



Decryption



14. Explain the triple DES. Why is the middle portion of triple DES a decryption rather than an encryption?6+2

Ans: Triple DES is an encryption algorithm based on the original Data Encryption Standard (DES). It is a symmetric encryption algorithm that uses multiple rounds of the Data Encryption Standard (DES) to improve security. It is also known as Triple DES because it uses the Data Encryption Standard (DES) cypher which takes three times to encrypt its data. It is essentially a block cypher used to encrypt data in 64-bit blocks.

Encryption Process

The Encryption process of Triple DES involves the following steps:-

Key Generation

This is the first step of the Encryption process of Triple DES. In this step, three unique keys are generated using a key derivation algorithm.

Initial Permutation

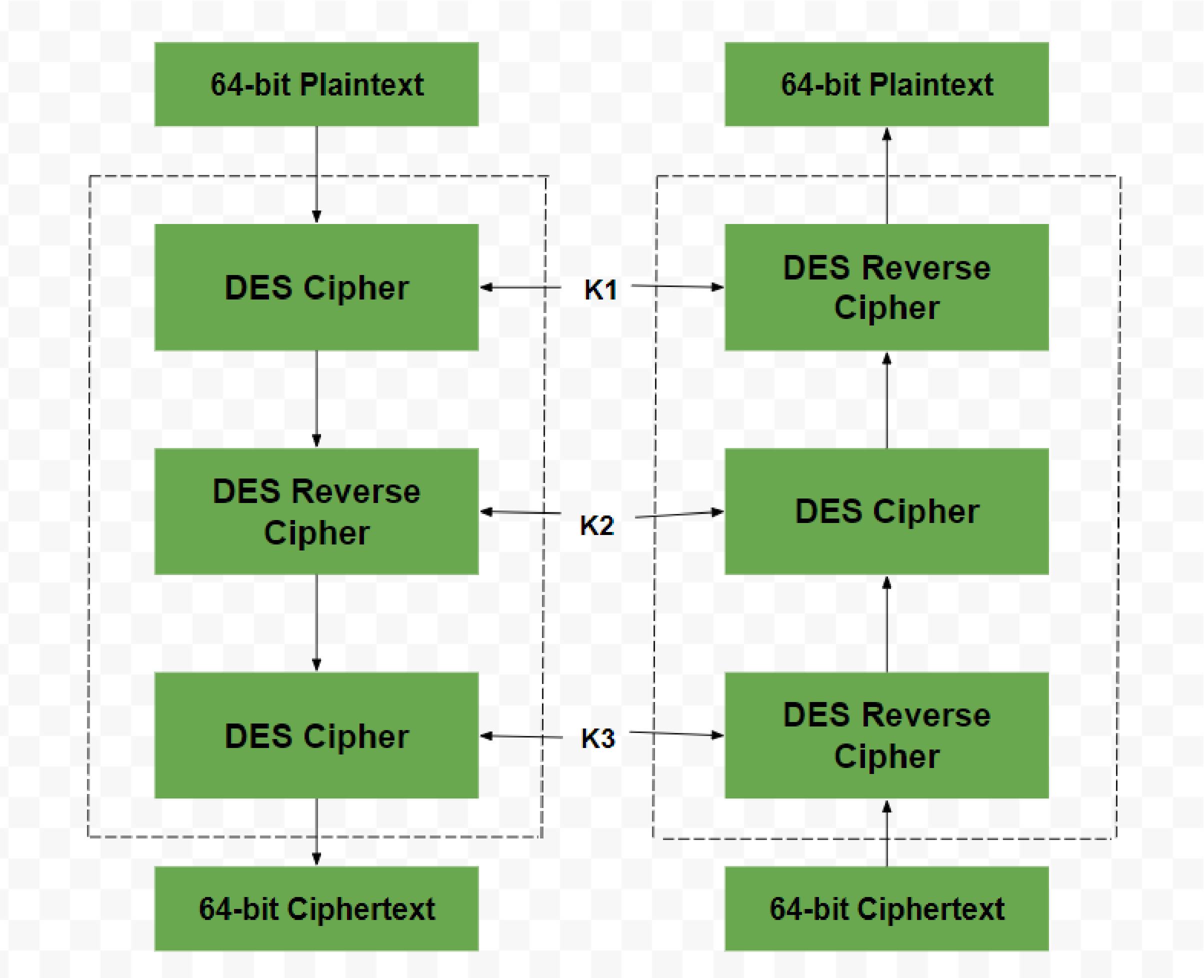
This step comes after the process of Key Generation. It involves the rearrangement of the bits of the plaintext according to a predefined permutation table.

Three Rounds of Encryption

This is regarded as the most important round of the encryption process of Triple DES. It consists of multiple rounds typically 48 rounds in total. In this step, the plaintext is processed three times and get encrypted, each time we take use of a different key, to create three layers of encryption.

Final Permutation

It completes the Triple DES encryption process. In this step, the resulting ciphertext block undergoes a final permutation (FP) operation, which is the inverse of the initial permutation. It returns the bits of the ciphertext block to their original order.



In Triple DES (3DES), the middle portion is a decryption step to enhance security through the "encrypt-decrypt-encrypt" (EDE) approach. This design helps to increase resistance against certain cryptanalytic attacks by complicating the patterns that can be exploited. Additionally, using decryption allows for effective key management, especially when two keys are employed, ensuring that even if one key is compromised, the data remains secure.

15. Describe briefly about differential and linear cryptanalysis.3+3

Ans:

Differential cryptanalysis is a sort of cryptanalysis that may be used to decrypt both block and stream ciphers, as well as cryptographic hash functions. In the widest sense, it is the study of how alterations in information intake might impact the following difference at the output. In the context of a block cipher, it refers to a collection of strategies for tracking differences across a network of transformations, finding where the cipher displays non-random behavior, and using such attributes to recover the secret key (cryptography key).

Linear cryptanalysis is a general type of cryptanalysis based on discovering affine approximations to a cipher's action in cryptography. Block and stream ciphers have both been subjected to attacks. Linear cryptanalysis is one of the two most common attacks against block ciphers, with differential cryptanalysis being the other.

16.Explain the Logical Placement of end-to-end encryption function with the help of a Diagram.3+3

Ans:

E2EE or **End to End Encryption** refers to the process in which encryption of data are being done at the end host. It is an implementation of Asymmetric encryption and hence ensures a secure way of data communication. It is the most secure way to communicate privately and securely as data can be read-only by the sender and the receiver.

Sender Side:

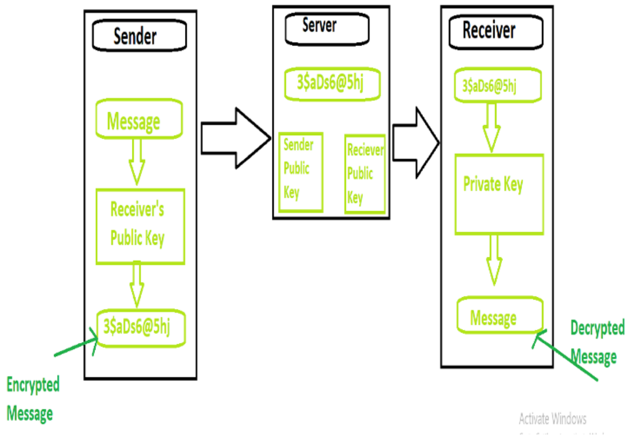
- The sender encrypts the message using the recipient's public key. This ensures that only the recipient, who has the corresponding private key, can decrypt the message.

Transmission:

- The encrypted message travels across the network, passing through various intermediaries (servers, routers, etc.). These intermediaries can see only the encrypted data and cannot decrypt it.

Recipient Side:

- Upon receiving the encrypted message, the recipient uses their private key to decrypt it, accessing the original plaintext message.


Sender
Message
Receiver's Public Key
3$aDs6@5hj
Encrypted Message
Server
3$aDs6@5hj
Sender Public Key
Reciever Public Key
Receiver
3$aDs6@5hj
Private Key
Message
Decrypted Message
Activate Windows