2100031921
E.Kowshik
sec-54

Define a symmetric-key cipher. Explain in detail.
Distinguish between a substitution cipher and a transposition cipher.

Symmetric-key Cipher:
A symmetric-key cipher, also known as a secret-key or private-key cipher, is a cryptographic algorithm that uses the same key for both encryption and decryption of data. In this type of encryption, the sender and the recipient share a common secret key, which is used to transform plaintext data into ciphertext and vice versa. Symmetric-key ciphers are generally faster and require less computational resources compared to asymmetric-key (public-key) ciphers, but they require a secure method for key exchange between

parties.

Here's how a basic symmetric-key cipher works:

Key Generation: A secure random key is generated, which both the sender and the recipient agree upon and keep secret.

Encryption: The sender takes the plaintext message and applies the symmetric key using an encryption algorithm. This process converts the plaintext into ciphertext, making it unreadable without the key.

Transmission: The sender transmits the ciphertext to the recipient over a potentially insecure communication channel.

Decryption: The recipient receives the ciphertext and applies the same symmetric key using the decryption

algorithm. This process reverses the encryption, transforming the ciphertext back into the original plaintext.

Advantages of Symmetric-key Ciphers:

Fast and efficient encryption and decryption.
Suitable for encrypting large volumes of data.
Useful for real-time communication and data transfer.

Disadvantages of Symmetric-key Ciphers:

Key distribution can be challenging, as the same key needs to be shared secretly between parties.
In large systems, managing a large number of symmetric keys can become complex.

Substitution Cipher vs. Transposition

Cipher:

Both substitution and transposition ciphers are types of symmetric-key ciphers that operate on the basic principle of rearranging or substituting characters within a message. However, they achieve this in different ways:

Substitution Cipher:
A substitution cipher replaces each character or symbol in the plaintext with another character or symbol according to a predetermined key. The key defines the mapping of each character to its substitute. Substitution ciphers are further categorized into monoalphabetic and polyalphabetic ciphers.

monoalphabetic Substitution: In a monoalphabetic substitution cipher, each character in the plaintext is replaced by a single fixed character from the key. For example, the Caesar cipher shifts

each letter by a fixed number of positions in the alphabet.

Polyalphabetic Substitution: In a polyalphabetic substitution cipher, the mapping of characters to substitutes changes based on their positions in the plaintext. The Vigenère cipher is a common example of a polyalphabetic substitution cipher.

Transposition Cipher:
A transposition cipher involves rearranging the characters or symbols of the plaintext without altering the characters themselves. The key determines the order in which the characters are rearranged.
Transposition ciphers do not change the characters' identities, but they change the sequence of characters.

Columnar Transposition: This type of transposition cipher involves writing the plaintext in a grid and then reading the

ciphertext column by column, following a specific key or pattern.

Rail Fence: In the rail fence cipher, the plaintext characters are written diagonally, like a zigzag, across a number of "rails," and then the ciphertext is read off row by row.