Name – Krishnaprasad Awala

Enrollment no – MITU21BTITD006

Roll no – D2215004

Q. What are the classical encryption techniques and how do they work?

The Caesar cipher, polyalphabetic cipher, and monoalphabetic cipher are all classical encryption techniques used to conceal the content of a message.

**Caesar Cipher**

The Caesar cipher involves shifting each letter in the plaintext by a fixed number of positions in the alphabet. For example, a shift of 3 would encode the letter "A" as "D", "B" as "E", and so on. The weakness of this cipher lies in the fact that there are only 25 possible keys, making it vulnerable to brute-force attacks.

Example: Plaintext: HELLO WORLD Key: 3 Ciphertext: KHOOR ZRUOG

**Advantages:**

Simple and easy to understand and implement

Fast encryption and decryption process

**Disadvantages:**

Vulnerable to brute force attacks and frequency analysis

Key is easily guessable for small shift amounts

**Polyalphabetic Cipher**

The polyalphabetic cipher, on the other hand, uses multiple alphabets to encode the plaintext. It involves shifting each letter by a variable number of positions, based on a key that is repeated throughout the message. This makes the cipher more secure than the Caesar cipher, as there are many more possible keys.

Example: Plaintext: ATTACK AT DAWN Key: LEMON Ciphertext: LXFOPVEFRNHR

**Advantages:**

More secure than monoalphabetic cipher

Same plaintext letter can be encrypted to different ciphertext letters

**Disadvantages:**

Key management can be difficult

Still vulnerable to frequency analysis

**Monoalphabetic Cipher:**

The monoalphabetic cipher uses a fixed substitution table to encode each letter in the plaintext. For example, the letter "A" could be substituted with "Q", and so on. While this cipher is more secure than the Caesar cipher, it is still vulnerable to frequency analysis attacks, where the most commonly used letters in the ciphertext are mapped back to the most commonly used letters in the plaintext.

Example: Plaintext: HELLO WORLD Ciphertext: FOLLE UNEJB

**Advantages:**

Simple to understand and implement

Fast encryption and decryption process

**Disadvantages:**

Vulnerable to frequency analysis

Same plaintext letter will always be encrypted to the same ciphertext letter

Overall, classical encryption techniques are considered less secure than modern encryption methods, which use complex mathematical algorithms and keys to ensure the confidentiality and integrity of messages.