MINOR PROJECT

Report on different types Of Ciphers

Submitted By: Shashank Rai

Ciphers are cryptographic algorithms used to encrypt and decrypt messages. The main goal of ciphers is to transform plaintext into ciphertext that can be securely transmitted over insecure communication channels

1.Substitution Ciphers: The most well-known example of a substitution cipher is the Caesar Cipher. In the Caesar Cipher, each letter in the plaintext is shifted a certain number of places down the alphabet.

For example, with a shift of 3, A would be replaced by D, B would become E, and so on.

2. **Transposition Ciphers**: A simple example of a transposition cipher is the Rail Fence Cipher. In the Rail Fence Cipher, the plaintext is written out diagonally on a grid, and then read off row by row to create the ciphertext.

For example, if the plaintext was "HELLO WORLD", and we used a rail fence with 3 rails, the ciphertext would be "HOLELWRDLO".

3**.** **Caesar Cipher:** As mentioned above, the Caesar Cipher is a type of substitution cipher where each letter in the plaintext is shifted a certain number of places down the alphabet.

For example, with a shift of 3, the plaintext "HELLO" would become "KHOOR".

4. **Vigenère Cipher:** The Vigenère Cipher is a polyalphabetic substitution cipher. This means that instead of using a fixed substitution pattern, the cipher uses a different substitution pattern for each letter in the plaintext. The substitution pattern is determined by a keyword.

For example, if the keyword was "LEMON", and the plaintext was "ATTACKATDAWN", the ciphertext would be "LXFOPVEFRNHR".

5. **One-Time Pad:** The One-Time Pad is a type of substitution cipher that uses a random key that is at least as long as the plaintext, and the key is never reused.

For example, if the plaintext was "HELLO" and the key was "XZFSL", the ciphertext would be "WJMMR".

6. **Playfair Cipher:** The Playfair Cipher uses a 5x5 grid of letters to encrypt and decrypt messages. Each letter in the plaintext is replaced by a corresponding letter in the grid, based on a specific rule.

For example, if the plaintext was "HELLO WORLD" and the key was "PLAYFIREXMOTZNBCDGHKQSU", the ciphertext would be "DLDHDVZKKTJL".

7. **Hill Cipher:** The Hill Cipher uses linear algebra to transform plaintext into ciphertext.

For example, if the plaintext was "HELLO" and the key matrix was:

| 1 2 | | 3 4 |

the ciphertext would be "XQASU".

8. **Enigma Machine:** The Enigma Machine was used by the Germans in World War II to encrypt messages. It used multiple rotors to substitute letters in the plaintext.

For example, if the plaintext was "HELLO" and the Enigma settings were "AAA", the ciphertext might be "BQXPC".

9. **RSA Cipher**: The RSA Cipher is a type of public key encryption algorithm that uses two keys, one for encryption and one for decryption.

For example, if the plaintext was "HELLO" and the encryption key was 17, the ciphertext would be 244.

10. **Blowfish Cipher:** The Blowfish Cipher is a symmetric key block cipher that can be used for encryption and decryption of electronic data.

For example, if the plaintext was "HELLO" and the encryption key was "PASSWORD", the ciphertext would be "8f8e7aa03c".