Assignment Number: 2

Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115 24/08/2023

**Aim:** Cryptanalysis or decoding of polyalphabetic ciphers: Playfair, Vigenère cipher.

**LO mapped:** LO1

**Theory:**

Polyalphabetic ciphers:

Polyalphabetic ciphers have a rich history in the field of cryptography. They offer enhanced security compared to simple substitution ciphers by employing multiple sets of substitutions. This assignment focuses on cryptanalysis, the process of breaking codes, to understand the inner workings of the Playfair and Vigenère ciphers and the methods to crack them.

* Playfair Cipher

The Playfair cipher involves setting up a key table, typically a 5x5 matrix, using a keyword. The key table is used for encryption. To encrypt a message, each pair of letters in the plaintext is substituted based on their positions in the key table. The decryption process follows a similar approach using the inverse of the key table setup.

*Playfair Cipher Example:*

Plaintext: CRYPTOLOGY

Keyword: KEYWORD

Key Table Setup:

Encryption:

1. Divide the plaintext into pairs: CR YP TO LO GY
2. Find each pair in the key table and apply the encryption rule.
3. Resulting Ciphertext: GA CI XN HP IQ

Decryption:

1. Reverse the process using the decryption formula.
2. Original Plaintext: CR YP TO LO GY

|  |
| --- |
|  |
|  |

* Vigenère Cipher

The Vigenère cipher employs a keyword that is repeated to match the length of the plaintext. The key letters are then used to shift the plaintext letters to generate the ciphertext. Decryption involves reversing the process using the same keyword and shifting in the opposite direction.

*Vigenère Cipher Example:*

Plaintext: CRYPTOLOGY

Keyword: CODE

Encryption:

1. Repeat the keyword to match the plaintext length: CODECODECO
2. Shift each letter in the plaintext by the corresponding keyword letter.
3. Resulting Ciphertext: GIDAKWFTQW

Decryption:

1. Reverse the process using the decryption formula.
2. Original Plaintext: CRYPTOLOGY

|  |
| --- |
|  |
|  |

**Conclusion:** This assignment has provided a hands-on opportunity to explore and dissect the Playfair and Vigenère ciphers. Through the examples and decryption exercises, you have gained insights into the strengths and vulnerabilities of these historical encryption techniques. As cryptography continues to evolve, understanding these foundational ciphers becomes essential to appreciating the advancements in modern encryption methods.