**Course – Cryptography and System Security (CSS)**

|  |  |
| --- | --- |
| **UID** | 2021300038 |
| **Name** | Atharva Gite |
| **Class and Batch** | BE Computer Engineering - Batch VIII |
| **Date** | 29/08/2024 |
| **Lab #** | 1 |
| **Aim** | Implement different substitution techniques. |
| **Problem Definition** | To implement all substitution encryption techniques namely Caesar Ciphers, Monoalphabetic Cipers, Playfair Cipher, Hill Cipher and Polyalphabetic Ciphers. Then, perform ethical hacking on all substitution encryption techniques. |
| **Theory** | In Network Security Model, encryption and decryption play important role of sending message so that other cannot see them. When encryption and decryption is performed by the same key it is called symmetric cryptosystem, a mathematical model for secure communication. There is a class of symmetric encryption cryptosystem where each letter of plain text is substituted to another letter called as substitution encryption techniques.  *Substitution techniques*– *Caesar Cipher* is one of the simplest and oldest methods of encrypting messages, named after Julius Caesar, who reportedly used it to protect his military communications. This technique involves shifting the letters of the alphabet by a fixed number of places. For example, with a shift of three, the letter ‘A’ becomes ‘D’, ‘B’ becomes ‘E’, and so on. *Monoalphabetic substitution* is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate cipher text. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed. In *playfair cipher* unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet. *Hill cipher* is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26). *Polyalphabetic Cipher* is a cipher where each letter in the plaintext can be encrypted to multiple possible letters in the ciphertext, depending on its position and a more complex algorithm. In this article, we will see the differences between Monoalphabetic Cipher and Polyalphabetic Cipher. |
| **Output** | **Part 1**  **Caesar Cipher:**    **MonoAlphabetic Cipher:**    **PolyAlphabetic Cipher:**    **Hill Cipher:**    **Playfair Cipher:**    **Part 2**  **Caesar:**    **MonoAlphabetic:**      **PolyAlphabetic:**    **Hill:**    **Playfair:**  **Part 3** |