Bharatiya Vidya Bhavan's
SARDAR PATEL INSTITUTE OF TECHNOLOGY
(Autonomous Institute Affiliated to University of Mumbai)
Munshi Nagar, Andheri (W), Mumbai – 400 058.

Experiment No. 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.

Useful Links – The useful links of all substitution ciphers namely Caesar, Monoalphabetic, Playfiar Hill and Polyalphabetic ciphers are as follows:

1. Caesar Ciphers https://www.youtube.com/watch?v=JtbKh_12ctg
2. Monoalphabetic Cipers https://www.youtube.com/watch?v=J-utjSeUq_c
3. Playfair Cipher https://www.youtube.com/watch?v=UURjVI5cw4g
4. Hill Cipher https://www.youtube.com/watch?v=JK3ur6W4rvw
5. Polyalphabetic Ciphers https://www.youtube.com/watch?v=Ic4BzVggNY8

Note – These videos are not self sufficient. Students need to refer text and reference books for the details.

Input – There are two tasks of the experiment. The first task of this experiment is to implement all substitution techniques. At the time of implementation, you may visit virtual laboratory designed IIIT Hyderbad and use plain-cipher text pair in the simulation section. Each member of a group has to independently implement all algorithms. Each group members have to decide symmetric keys for respective encryption and decryption and these keys have to be kept secret. Each group member has to also create a few pairs of plan-cipher texts and then handover to a member in the same group without sharing secret key. The second task of this experiment is to implement brute-force attack on all substitution techniques. Each member of a group has to independently implement all brute-force attack on all substitution techniques. Each group member has to take plan-cipher pairs from the member in the same group.

Submission and Output –

1) Part 1 – Implementation of all substitution encryption techniques along with plain-cipher text pairs, key etc in text file. All these should be in one folder named substitution-techniques-<your UID>
2) Part 2 – Implementation brute-force attack on all substitution encryption techniques along with plain-cipher text pairs received from group members and key found. All these should be in one folder named substitution-techniques-attack-<your UID>
3) Part 3 – Plot relative frequency of occurrence of letters (Fig. 2.6 Page 69) as given the textbook "Cryptography and Network Security" by William Stallings. Submit all parts in single zipped file on the CSS Moodle page.