ST. FRANCIS INSTITUTE OF TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY

SECURITY LAB (SL)

Experiment – 1: Implementation of Shift (Caesar/Additive) Cipher

Aim: To implement Shift Cipher Technique and understand cryptanalysis of the same.

Objective: After performing the experiment, the students will be able to –

- To understand the encryption and decryption fundamentals.
- To understand that secure encryption is not possible with small key space.

Lab objective mapped: L502.1: Students should be able to apply the knowledge of symmetric cryptography to implement simple ciphers.

Prerequisite: Basic knowledge of cryptography.

Requirements: C/C++/JAVA/PYTHON

Pre-Experiment Theory:

1. **Caesar Cipher**: In cryptography, a Caesar cipher, also known as a shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals.

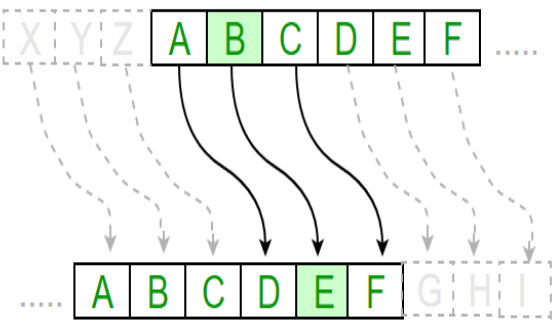
2. **Mathematical Description**

   First we translate all of our characters to numbers, 'a'=0, 'b'=1, 'c'=2, ..., 'z'=25. We can now represent the caesar cipher encryption function, e(x), where x is the character we are encrypting, as:

$$e(x) = (x + k) \pmod{26}$$

   Where, k is the key (the shift) applied to each letter. After applying this function, the result is a number which must then be translated back into a letter.
   The decryption function is:

$$e(x) = (x - k) \pmod{26}$$



- **Breaking of Caesar cipher:**

  With a Caesar cipher, there are only 26 possible keys, of which only 25 are of any use since mapping A to A etc doesn't really crypt the message. The hacker can try each of the keys (shifts) in turn, until he recognizes the original message.
  Note: The hacker need to be able to recognize when he get an original message (ie is in english or other language). This is usually easy for humans, but hard for computers. Cryptanalysis using shift cipher is much harder with compressed data.

  Example "GCUA VQ DTGCM" when broken gives "easy to break", with a shift of 2

  Ref: https://www.youtube.com/watch?v=1Ri7t7VIQJA

Post Experimental Exercise- *(to be handwritten on ruled journal sheets)*

1. Explain substitution cipher technique (Ceasar) with an example ***[theoretical result and code attached should match]***.

Solve the following manually as well as using TOOL (in the references) given (attach screenshots)

2. Encrypt the following plain text using key k = 7.
   Plain Text : Lord Rama was a good king.
3. Given a cipher text, find out the corresponding plain text using brute force attack.
   Cipher text : HAAHJR HA KHDU

Output:

1. Attach complete program performing encryption and decryption of shift cipher.
2. Attach screenshots of program output (for encryption & decryption) and its validation using a virtual lab tool.

Conclusion:

In this experiment we learned the basic features of Shift Cipher by implementing a code for encryption and decryption. We also observed the decryption when the key is known and understood, breaking the cipher when key space is very small by performing cryptanalysis of ciphertext.

References:

Mention your other references here.

1. http://cse29-iiith.vlabs.ac.in/
2.