Don Bosco Institute of Technology, Kurla (W), Mumbai – 400070
Department of Information Technology
Secure Application Development Lab

Roll no.: 52 **Date**: 2 / 10 / 2024

Name: Afzal Siddiquie

Experiment No. 10

Aim: Demonstrate Symmetric, Asymmetric and Hashing Cryptographic Techniques using Cryptool

Objectives: The objective of this experiment is to

- Understand how to apply to secure coding for cryptography.

Outcomes: After study of this experiment, the student will be able to

- Use cryptool to apply cryptography for secure coding

Prerequisite: Knowledge of Cryptography.

Requirements: PC and Internet

Brief Theory: **Cryptography**

Cryptography is the technique of securing information and communications through use of codes so that only those persons for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix "graphy" means "writing". In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at a later stage.
4. **Authentication:** The identities of sender and receiver are confirmed. As well as the destination/origin of information is confirmed.

Types Of Cryptography: In general there are three types Of cryptography:

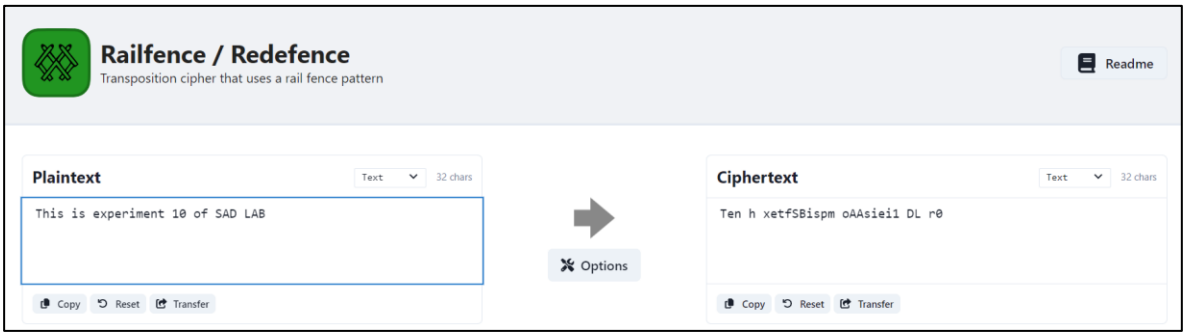
1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange keys in a secure manner. The most popular symmetric key cryptography systems are Data Encryption System(DES) and Advanced Encryption System(AES).

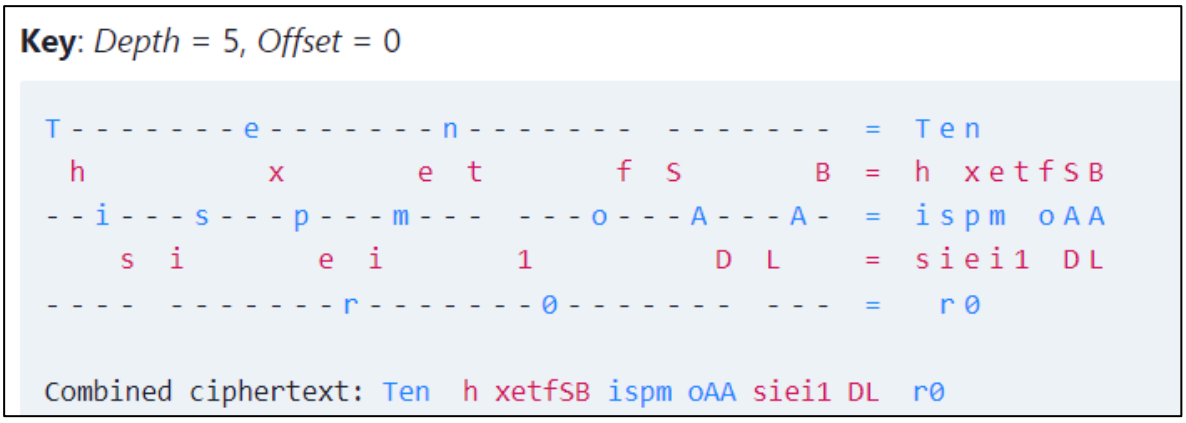
2. **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public keys and Private keys are different. Even if the public key is known by everyone, the intended receiver can only decode it because he alone knows his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

Laboratory Exercise

1. Watch out the following YouTube videos URL:
   a. The Simplified Advanced Encryption Standard (S-AES) Explained
   https://www.youtube.com/watch?v=cl7nGF0iuo0
   OR
   Block Ciphers – Feistel Ciphers & SDES
   https://www.youtube.com/watch?v=wVm7mANbdgw&list=PLMuvAbyIl0PT6zaRVpK0FCSNMgwAOckTt&index=10
   b. Asymmetric Ciphers – RSA
   https://www.youtube.com/watch?v=lqeT5UVzPhI&list=PLMuvAbyIl0PT6zaRVpK0FCSNMgwAOckTt&index=12
   c. Cryptographic Hash Functions
   https://www.youtube.com/watch?v=Rwvpngxp438&list=PLMuvAbyIl0PT6zaRVpK0FCSNMgwAOckTt&index=14

2. Add the screenshot of the step-by-step process of using cryptool for cryptography with detailed explanation.





The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded. In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus, the alphabets of the message are written in a zig-zag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

The number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.

- Hence, rail matrix can be constructed accordingly. Once we have got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).
- Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.

Conclusion: In this experiment, we used Cryptool to apply and understand various cryptographic techniques, including symmetric encryption (AES), asymmetric encryption (RSA), and hashing, and implemented the Rail Fence cipher for secure coding.

Mention your References:

1. https://www.youtube.com/playlist?list=PLMuvAbyIl0PT6zaRVpK0FCSNMgwAOckTt
2. https://www.cryptool.org/en/cto/railfence/
3. https://www.geeksforgeeks.org/rail-fence-cipher-encryption-decryption/