A Study of Different Type of Encryption and Decryption Techniques and Build a Java Application

CSE 4116

By

S M Taslim Uddin Raju

Roll:1407038

Department of Computer Science and Engineering

Khulna University of Engineering& Technology

Khulna 9203,Bangladesh

1. Introduction

We all know that now a day this is the world of information technology and almost everyone have to communicate with each other. Most of the time this communication occurs on the network. During the communication of data it may be possible that the data we are sending or receiving can be hacked or edited by someone. The data we are communicating may be bank a/c number, passwords or some important files etc. To protect the data from this type of unwanted things "Cryptography" is very useful.

This project is all about providing security while communicating any data on the network between two or many user. We are going to discuss about the main ciphers used in Cryptography in this project. There are various techniques of encryption and decryption which are used in this project such as

(1) RSA Cryptography
(2) El Gamal Cryptography
(3) Caesar Cipher

Encryption and Decryption

Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.

A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption.

The sections that follow introduce the use of keys for encryption and decryption.

(1) Symmetric-Key Encryption

(2) Public-Key Encryption

Symmetric-Key Encryption

With symmetric-key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure.

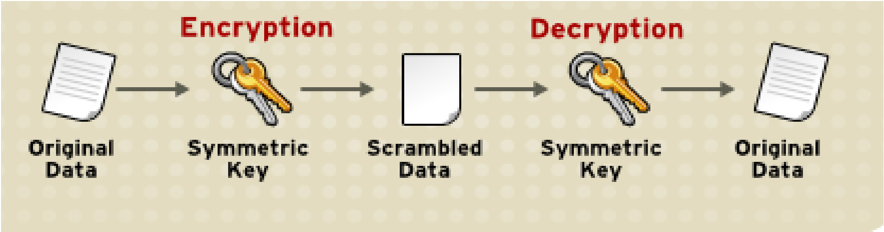


Fig 1: Symmetric-key encryption & decryption

Public-Key Encryption

The most commonly used implementations of public-key encryption are based on algorithms patented by RSA Data Security. Therefore, this section describes the RSA approach to public-key encryption.

Public-key encryption (also called asymmetric encryption) involves a pair of keys-a public key and a private key-associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret. Data encrypted with your public key can be decrypted only with your private key. Figure 2 shows a simplified view of the way public-key encryption works.

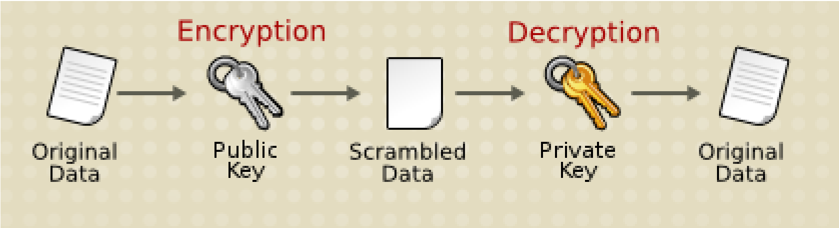


Fig 2 : Public-key encryption and decryption

2. Project-Specific Objectives

1. To familiar with RSA Cryptography and its applications .
2. To know how to use RSA , El Gamal and Caesar Cipher for encrypted and decrypted files.
3. To know about Sqlite and Intellij with their applications and uses .

3. Approach/Methods

For the project we use RSA and Caesar Cipher Crypto-system.

(1) RSA Encryption & Decryption

To encrypt a message M the sender:

Obtains public key of recipient KU={e,N}

Computes: $C=M^e$ mod N, where $0 \leq M < N$

To decrypt the ciphertext C the owner:

Uses their private key KR={d,p,q}

Computes: $M=C^d$ mod N

(2) Caesar cipher cryptography,

Caesar cipher, also known as Caesar's cipher, the 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 left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

For example :

Here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key):

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   XYZABCDEFGHIJKLMNOPQRSTUVW
```

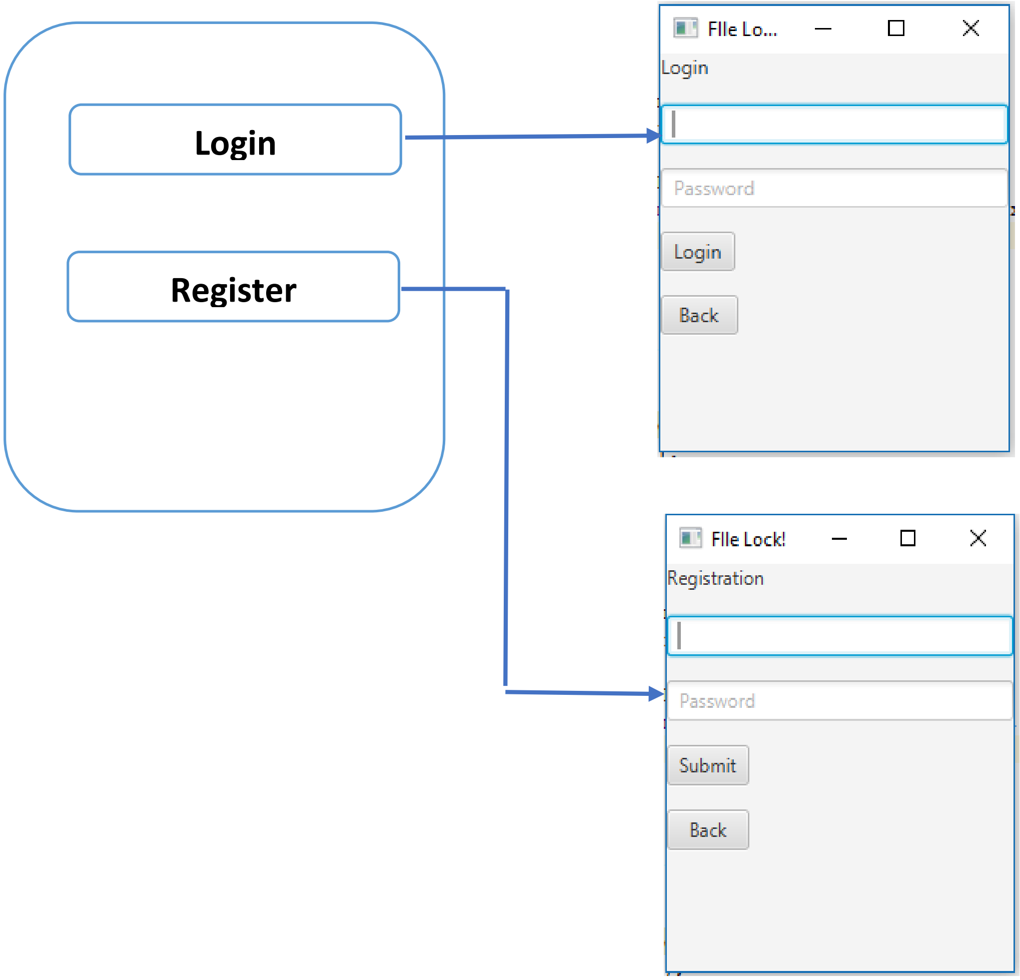
Encryption of a letter x by a shift n can be described mathematically as,

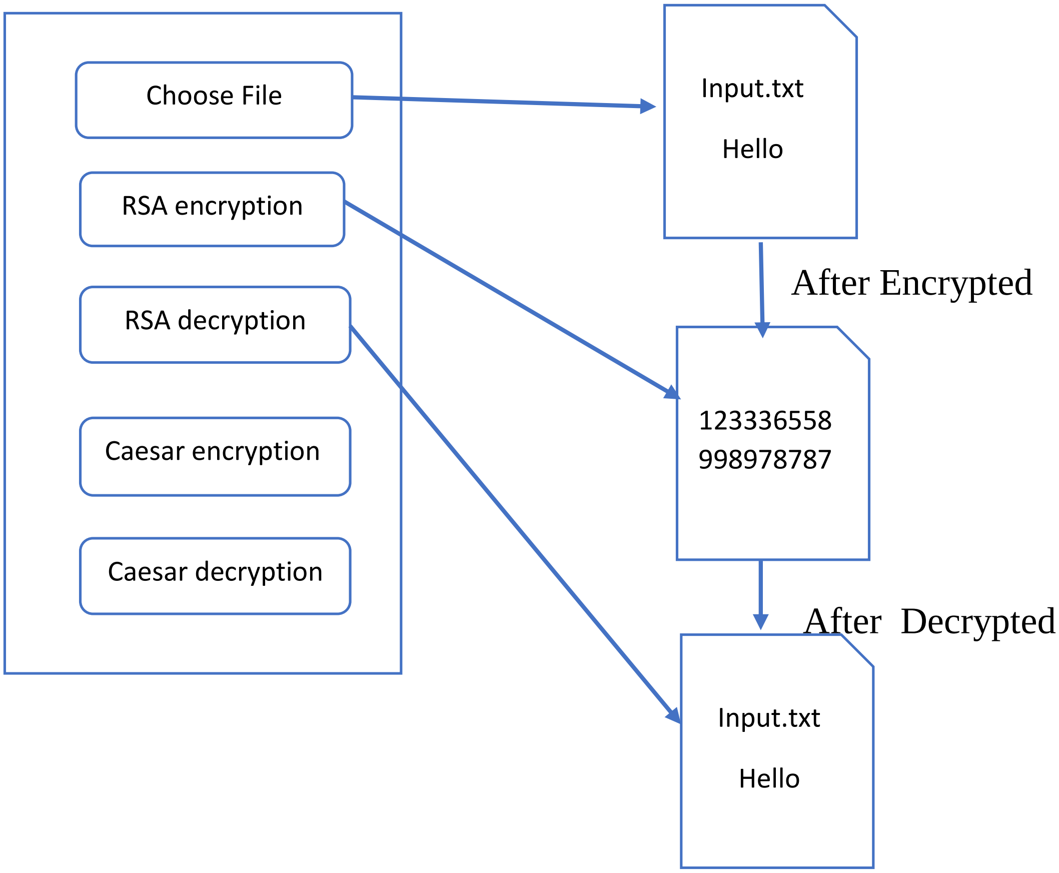
$$E_n\ (x) = (x + n)\ \ \text{mod}\ 26$$

Decryption is performed similarly,

$$E_n\ (x) = (x - n)\ \ \text{mod}\ 26$$

4. Blog Diagram





4. Conclusion

Encryption and decryption are critical security measures that are designed to ensure that communication is received and processed correctly. They are effectively a form of secondary and complex language which excludes those that are not directly concerned with the transaction .We can ensure that the fine will be secured because of RSA or Caesar Cipher.