File Encryption Decryption

**Submitted to**

*Dr. Kazi Md. Rokibul Alam*

*Professor*

*Dept. of CSE, KUET*

*Sk. Imran Hossain*

*Assistant Professor  
Dept. of CSE, KUET*

**Submitted by**

Safial Islam Ayon

1407041

Dept. of CSE, KUET

Date: 28 June, 2018

**CSE – 4116**

**Computer and Network Security Laboratory**

**Objective**

* The main objective of this project is to encrypt/decrypt the textual files for personal and professional security.
* Know about different types of encryption and decryption mechanism.
* Knowledge about how the encryption decryption algorithm works.
* Know how we can secure our file using encryption decryption algorithm.

**Introduction**

The increased use of computer and communications system by industry has increased the risk of theft of proprietary information although these threats may require a variety of counter measures. Encryption is a primary method of protecting valuable electronic information. Encryption is the process of encoding a message in such a way as to hide its contents. Modern cryptography includes several secure algorithms for encrypting and decrypting messages. They are all based on the use of secrets called keys. A cryptography key is a parameter used in an encryption algorithm in such a way that the encryption cannot be reversed without the knowledge of the key. Terms used in cryptography are as follows:

* Plain text: original message is known as plain text.
* Cipher text: coded message is known as cipher text.
* Encryption: the process of converting the plain text to cipher text is known as encryption.
* Decryption: the process of restoring the plain text from the cipher text is known as decryption.

There are different methods to encrypt and decrypt files. Among them I use RSA, Elgamal and Caesar Cipher encryption decryption mechanism to decrypt and decrypt files.

**Project Description**

At first the user need to login the system with his user id and password. The user id and password are saved in a file. If user put wrong id or password warning message show. If user successfully put the correct id and password he login the system.

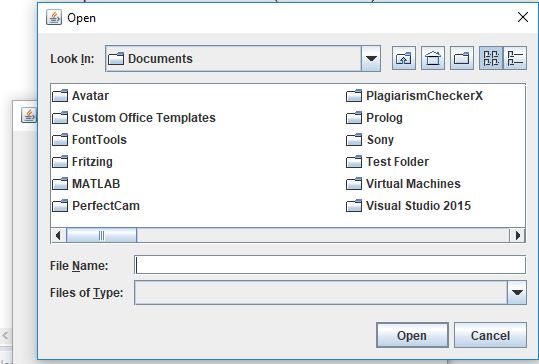
After login he sees three options: 1) RSA, 2) Elgamal, and 3) Caesar Cipher.



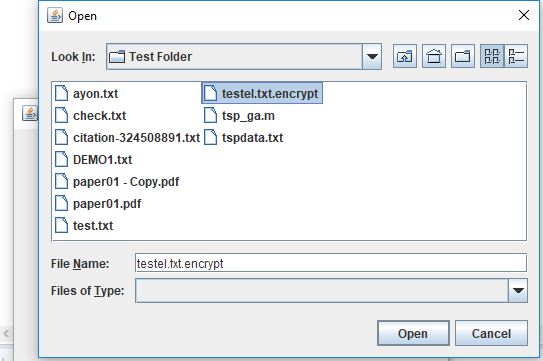
If user click any button he sees two options: 1) Encryption and 2) Decryption.



If he clicks Encryption options then first he selects a file to encrypt. Then the file will encrypt to use RSA or Elgamal or Caesar Cipher algorithm and change the extension into .encrypt. The original file is represented into byte array into the .encrypt file.



Then when he clicks Decryption options then he selects the .encrypt file to decrypt the file. After the decryption process the original file come again in the previous extension and user can see the original file again.



**Discussion**

Using this system user can secure their files from others. They also encrypt their files into 3 ways. Also, the user interface of the system is very user friendly. But there is some limitation in the system. Such as: for big files encryption and decryption are slower. Image files are not encrypt and decrypt all the times.

**Conclusion**

User can easily use this system to encrypt their files and secure those files contain. It will also help the user to encrypt their files in different ways. In future the real time database and other encryption decryption mechanism will add in the system.