**File Encryption & Decryption using RSA**

CSE 4116: Computer and Network Security Laboratory

**Submitted to-**

Dr. Kazi Md. Rokibul Alam

Professor   
Department of CSE, KUET

Sheikh Imran Hossain

Assistant Professor   
Department of CSE, KUET

**Submitted by-**

Shahriar Parvej

Roll-1507109   
Department of CSE, KUET

**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 used RSA encryption decryption mechanism to encrypt and decrypt files.

**Project Description**

In this case we will have two options. Encryption and Decryption. First of all to encrypt a file we will enter two initial numbers to calculate the value of our n and private key with the help of RSA algorithm. Then we will select a file & encrypt that file.

In case of decryption, we need to provide the value of n and our private key and open that encrypted file. We also need to provide the file type. Then pressing the button for decryption we are done with the encryption process.

**Discussion**

Using this system, user can secure their files from others. 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 not possible. Image files are not encrypted and decrypted 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.