KHULNA UNIVERSITY OF ENGINEERING & TECHNOLOGY (KUET)

Final Project Report On

File Encryption and Decryption using RSA Algorithm

Course No.

CSE 4116

Course Name

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

Indronil Bhattacharjee
Roll : 1507105
Section : B
Department of Computer Science and Engineering
Khulna University of Engineering & Technology

Project Title:

File encryption and decryption using RSA algorithm.

Introduction:

Cryptography serves a purpose to keep sensitive data secure from unauthorized users. It requires two basic elements for encryption and decryption i.e. encryption/decryption algorithm and key. Based on keys, two types of encryption is done. If the single key is used for both encryption and decryption purpose then it is symmetric cipher (private key cryptography). On the other hand, if different keys (pair of keys) i.e. private keys and public keys are used for encryption and decryption purpose then it is asymmetric cipher (public key cryptography).

Algorithms used:

RSA algorithm (asymmetric key algorithm) is used here for both encryption and decryption.

RSA algorithm:

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public key and Private Key. As the word describes that the Public key is given to everyone and Private Key is kept private.

An example of asymmetric cryptography:

1. A client sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives the data and decrypts it.

Working Procedure:

Here two procedures are performed. First is encryption and the later is decryption.

Encryption:

At first, Key Pair is generated using ‘Generate Key Pair’ and known to the encryptor. Then the file which has to be encrypted is selected and then imported the Public Key to encrypt the file. After encryption, the original file is generated as output.txt”.

As for example –

Original file = “input.txt”

Encrypted file = “output.txt”

Encrypted file will be generated after encryption.

Decryption:

For the decryption process, the encrypted file is selected. Then Private Key is imported and also the manifest file. The decrypted file will be in “.Decrypted” format.

As for example –

Original file =“input.txt”

Encrypted file = “output.txt”

Decrypted file = “decrypt.txt”

The decrypted file will be generated after the decryption process.

Conclusion:

RSA algorithm was used to create an application for the file encryption and decryption purpose. This can encrypt and decrypt text files. It will also be able to encrypt any large sized file comparatively faster and more secure by using asymmetric algorithm.

References:

i. https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

ii. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

iii. https://en.wikipedia.org/wiki/RSA_(cryptosystem)