A Strong Secured Message Transaction System using RSA, Triple-DES and Enveloped Data Systems

Md. Ismail Jabiullah[1*], Jerin Akter[2]
[1,2] Department of Computer Science and Engineering (CSE),
Daffodil International University, Dhaka, Bangladesh.
****Corresponding Author***
E-mail Id:-*drismail.cse@diu.edu.bd*

ABSTRACT

Secured message transactions are considerably demanding issues for any electronic transactions system. A strong secured message communication system has been designed, developed and implemented using JAVA programming languages. For this, RSA is used as public key, Triple-DES is used as private key cryptographic technique and the enveloped data is used ensure better security in the proposed system. First the public-key algorithm RSA and private key cryptography technique Triple-DES jointly employed on the intended message to produce improved cipher text message. Then another cryptographic process enveloped data is applied on the produced cipher text that finally creates strong scramble message that is sent to the destination. This can be applied on any length of secured message transactions in any cryptographic applications where needed.

Keywords:- *Security, Cryptography, Public key, RSA, Envelop Data, DES3, SHA1.*

INTRODUCTION

Now-a-days secured message communication systems are very much demanding in several applications. More and more sensitive information is stored on computers and transmitted over the unsecured web or other communication means. Several methods are employed in this regard for creating secured communication process. So that one can easily transmits sensitive and important data message among the communicants. Public-key cryptographic technique RSA is a process that establishes a very strong communicative systems for message transaction with strong security services. Triple-DES is a private key cryptographic technique that also works for building secure message transaction system proving various secured services. In this paper, both the cryptographic systems are studied and presented for describing how they works on messages.

Public key cryptography systems use a pair of keys: private and public key to encrypt and decrypt the intended message. Encryption is essentially a sign of users' distrust of the safety of the system, the owner or operator of the system, or enforcement authorities. Here, the Rivest-Shamir-Adelman (RSA) algorithm works on the cryptosystem that is applied on the message to several systems for performing encryption and decryption on that plain text message. Once the intended data or message has been encrypted, an individual cannot add up of the data without valid key or figuring it out. With regards to confidentiality, RSA cryptography system is employed to encrypt data residing on storage devices or traveling through communication channels to make sure that any illegal access is not successful [1]. During the communications transacted data are often encoded to stop disclosure of their contents through eavesdropping or message interception, using codes and other methods, in order that only certain people can see the important message [2].

In cryptography, Triple-DES is that the common name for the Triple encoding Algorithm symmetric-key block cipher, which applies the info Encryption Standard (DES) cipher algorithm 3 times to every data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the supply of increasing computational power made brute-force attacks feasible [3]. Triple-DES takes three 64-bit keys, for an overall key length of 192 bits. In this process, encryption is performed within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The triple-DES then breaks the user-provided key into three sub keys, padding the keys if necessary in order that they are each 64 bits ling. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3 times. Triple-DES runs 3 times slower than DES, but is far safer if used properly. The message is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key. Triple-DES private cryptographic technique that works three times on the message with two keys for imposing better security on the system. Envelop data are often applied to supply most secured message transaction system using PKCS #7 standards with RSA algorithm.

Here, a combined embedded system of cryptographic algorithms has been designed and developed to build a more secured process that imposes better security services. Java programming language is used to implement the proposed system. Finally, a comparative study has been analyzed and presented in a table to realize the improved security services.

REVIEW WORK

To realize and apply the encryption algorithms RSA, Triple-DES and enveloped data in this proposed system all are studied and summarized below. Using an encryption key (e,n), the algorithm is as follows[4]:

(a) Working Process of RSA: Following the steps that is working on the message:

- Represent the message as an integer between 0 and (n-1). Large messages are often choppy into variety of blocks. Each block would then be represented by an integer within the same range.
- Encrypt the message by raising it to the eth power modulo n. The result's a cipher text message C.
- To decrypt cipher text message C, raise it to a different power d modulo n. The encryption key (e, n) is formed public. The decryption key (d, n) is kept private by the user.

The working process of RSA cryptographic technique on the message is depicted by the following Figure 1.

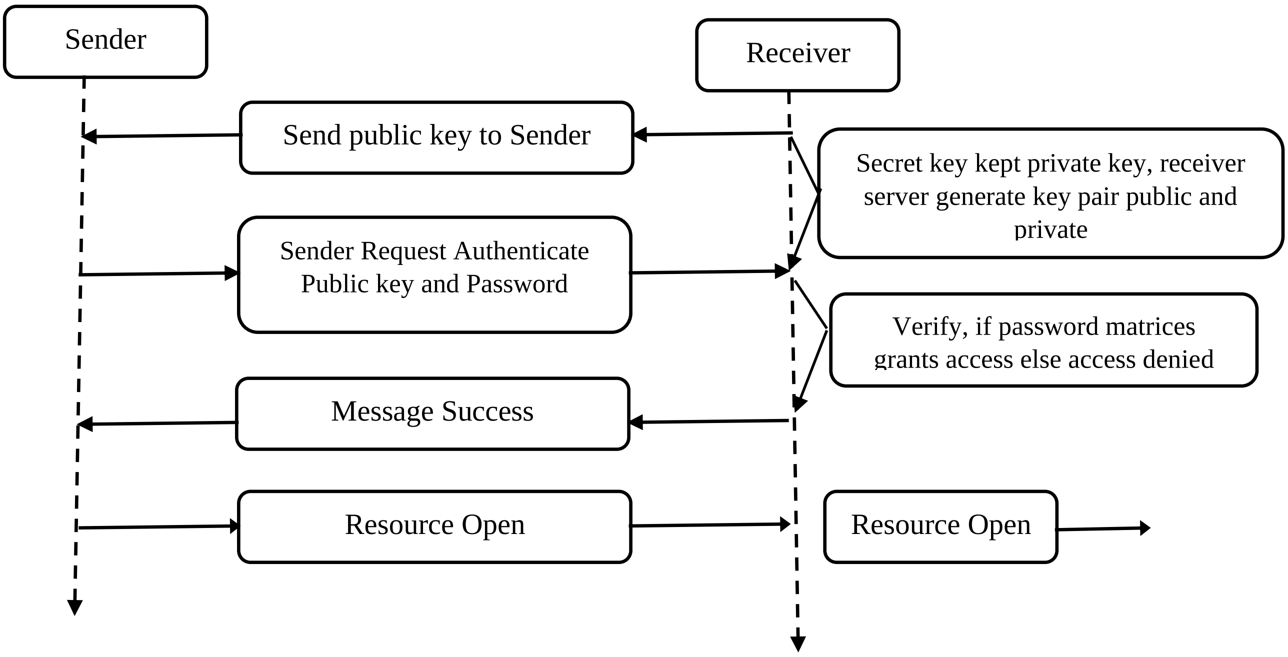

Sender
Receiver
Send public key to Sender
Secret key kept private key, receiver server generate key pair public and private
Sender Request Authenticate Public key and Password
Verify, if password matrices grants access else access denied
Message Success
Resource Open
Resource Open

***Fig.1:**-RSA Working Process*

(b) Working Process of Triple-DES: The procedure for decrypting something is that the same because the procedure for encryption, except it's executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the many bit in in each byte may be a parity, and will be set in order that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most vital bits of each byte are used, leading to a key length of 56 bits. this suggests that the effective key strength for Triple DES is really 168 bits due to the three keys contains 8 parity bits that aren't used during the encryption process [9]. The system produces cipher text (C) from the plaintext message (M) using keys K_1 and K_2 by the encryption method (E) that can be represented as follows:

$$C = E_{K1}(D_{K2}(E_{K1}(M))$$

and the decryption process of Triple-DES using in this system is

$$M = D_{K1}(E_{K2}(D_{K1}(C)))$$

(c) Working Process of Enveloped Data: The enveloped-data content type consists of encrypted content of at all type and encrypted content-encryption keys for one or more recipients. The mixture of encrypted content and encrypted content-encryption key for a recipient may be a "digital envelope" for that recipient [10]. Any sort of content are often enveloped for any number of recipients in parallel. It is expected that the standard applications of the enveloped-data content type are going to be to represent one or more recipients' digital envelopes on content of the info, digested-data, or signed-data content types.

The process by which enveloped data is made involves the subsequent steps:

- A content-encryption key for a specific content-encryption algorithm is generated randomly.
- For every recipient, the content-encryption key's encrypted with the recipient's public key.
- For each recipient, the encrypted content- encryption key and other

recipient-specific information are collected into a Recipient Info value.
- The content is encrypted with the content-encryption key.
- The Recipient Info values for all the recipients are collected along with the encrypted content into an Enveloped Data value.

PROPOSED SYSTEM METHODOLOGY

The user encrypted the formatted message using RSA algorithm then that file is stored in our database with unique private key and public key. Then the authorized party download user only to look at that non-public key after to access that file using the private key. As we are using PKCS #7 [7] standards with RSA algorithm so actually our process is split into four parts. The primary part describes the top-level type Enveloped Data, the second part describes the per-recipient information type Recipient Info, and the third and fourth parts describe the content-encryption and key-encryption processes. The sequence of the three steps: RSA encryption, Triple-DES encryption and applying Enveloped Data that are used in the proposed system and are presented in Figure 2.

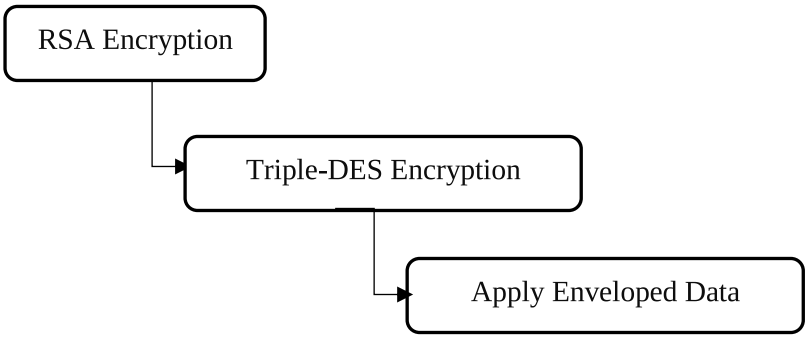


Fig.2:-Steps of the Proposed System

The process of creating secured data message using the RSA public-key and Triple-DES private key and finally enveloped data is presented in the following Figure 3. The output encrypted message is sent to the destination.

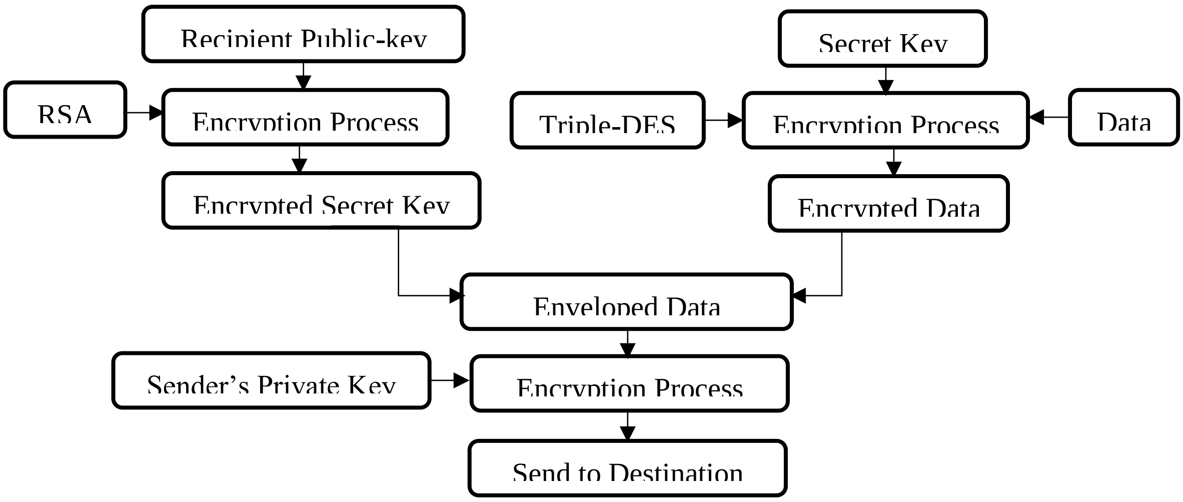


Fig.3:-Prepare Secure Data Message and Share

Messages are encrypted with the keys. The various secret key's generated for each individual message. Triple-Data Encryption Standard algorithm is employed to encrypt a message. An encrypted message decrypt with an equivalent secret key and algorithm. Within the message sharing process, secret key that is employed to encrypt messages) encrypt with recipient public key generated by RSA. An envelope data, prepare with encrypted secret key, encrypted message and recipient information. A digital signature which is generated by using SHA1 adds to the enveloped data and share it to the precise recipient. Enveloped data share via Server Message Block (SMB).

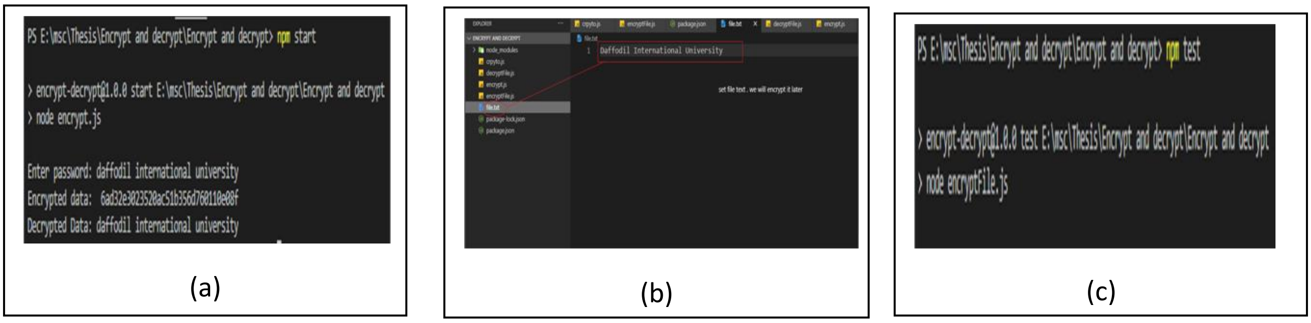
IMPLEMENTATION

To implement the proposed system Swing Java has been used for design interface (UI). Swing is employed to create a Java program with a graphical interface (GUI). Swing is a component of Java Foundation Class (JFC). Swing isn't a replacement for Abstract Window Toolkit (AWT), actually it's built on top of the core AWT libraries to supply a more sophisticated set of GUI components. The following are a number of the Graphical Interface of the proposed Secured Message Transactions:

The skeleton of the Swing Java program code is given below:

```
{
“name”: “encrypt-decrypt”,
“version”: “1.0.0”,
“description”: “”,
“main”: “index.js”,
“script”: {
“start”: “node encrypt.js”, ---npm start command for process encryption
“test”: “node encryptFyle.js”, ---npm start command for process encryptfile
},
“author”: “jerin”,
“license”: “ISC”,
“dependencies”: {
“concurrently”: “^5.5.0”,
“crypto”: “^1.0.1”,
“prompt-sync”: “^4.2.0”,
}
}
```

The password encryption-decryption is processed in Swing Java and the output screen is depicted in Figure 4. The implemented outputs of the proposed system are given in Figure 4.



```
PS E:\msc\Thesis\Encrypt and decrypt\Encrypt and decrypt> npm start

> encrypt-decrypt@1.0.0 start E:\msc\Thesis\Encrypt and decrypt\Encrypt and decrypt
> node encrypt.js

Enter password: daffodil international university
Encrypted data:  6ad32e3023520ac51b356d760110e08f
Decrypted Data: daffodil international university
```

(a)

```
1  Daffodil International University
```

set file text . we will encrypt it later

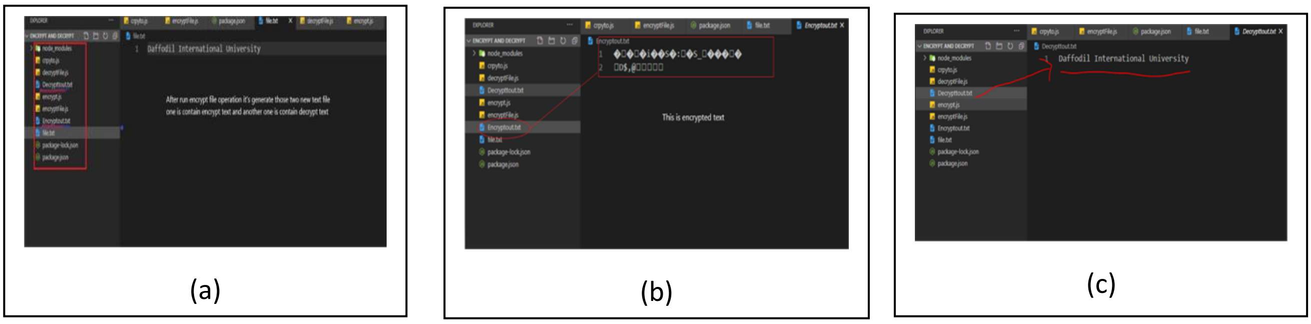
(b)

```
PS E:\msc\Thesis\Encrypt and decrypt\Encrypt and decrypt> npm test

> encrypt-decrypt@1.0.0 test E:\msc\Thesis\Encrypt and decrypt\Encrypt and decrypt
> node encryptFile.js
```

(c)

***Fig.4:**-Password Encryption-decryption*



Daffodil International University

After run encrypt file operation it's generate those two new text file one is contain encrypt text and another one is contain decrypt text

(a)

This is encrypted text

(b)

Daffodil International University

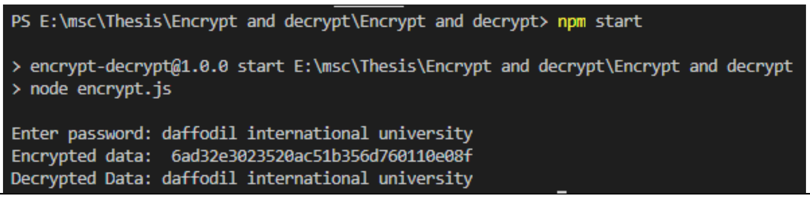
(c)

Fig.5:*-File Encryption-decryption*

The input-output screenshots of the implemented proposed system in Swing Java are observed and analyzed. A sample input-output screenshot with its description is presented in Table 1.

Table 1:*-Description of Proposed System*

Properties	Description

Input Output Screenshot	
	`PS E:\msc\Thesis\Encrypt and decrypt\Encrypt and decrypt> npm start`
	
	`> encrypt-decrypt@1.0.0 start E:\msc\Thesis\Encrypt and decrypt\Encrypt and decrypt`
	`> node encrypt.js`
	
	`Enter password: daffodil international university`
	`Encrypted data:  6ad32e3023520ac51b356d760110e08f`
	`Decrypted Data: daffodil international university`

Pattern of inputs	Single line

COMPARATIVE ANALYSIS

All the fundamental security services are studied on the existing system and the proposed system. A comparative study on the proposed system and the existing systems are analyzed and presented in Table 2.

Table 2:*- Comparative Study*

Security Services	**Existing Systems**			**Proposed System**
	RSA	3-DES	Enveloped Data	
Authentication	Yes	No	No	Yes
Confidentialty	Yes	Yes	Yes	Yes
Secrecy	Yes	Yes	No	Yes
Non-repudiation	No	No	Yes	Yes

CONCLUSION

Secured Message Transactions are considerably desirable for several reasons. A secured message communication system has been designed, developed and implemented using JAVA programming languages. Here, RSA is used as public key, Triple-DES is used as private key cryptographic technique and the enveloped data is used ensure better security in the proposed developed system. For this, the public-key algorithm RSA and private key cryptography technique Triple-DES jointly employed on the intended message to produce improved cipher text message. Then another cryptographic process enveloped data is applied on the produced cipher text that finally creates strong scramble message that is sent to the destination. The proposed system can be applied in any cryptographic applications where strong security services are needed.

REFERENCES

1. Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.
2. ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, January 2003.
3. Jonsson, J., & Kaliski, B. (2003). *Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1* (pp. 1-68). RFC 3447, February..
4. Kaliski, B. and M. Robshaw (1995). The Secure Use of RSA. *RSA Laboratories' CryptoBytes*.1(3).
5. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.
6. Lloyd, S. (2002). PKI Forum: Understanding Certification Path Construction. *White Paper (September 2002)*.
7. PKCS #7 Cryptographic Messaging Syntax Concepts
8. https://en.wikipedia.org/wiki/Triple_DES
9. http://www.vocal.com/cryptography/tdes/
10. https://en.wikipedia.org/wiki/Envelop_DATA