**APTIKOM Journal on Computer Science and Information Technologies**
Vol. 4, No. 3, 2019, pp. 105~111
ISSN: 2528-2417
DOI: 10.11591/APTIKOM.J.CSIT.147


# Performance comparison of asymmetric cryptography (case study-mail message)

**Zarni Sann*[1], Thi thi Soe[2], Kaythi Wyut Mhone Knin[3], Zin May Win[4]**
[1,3,4]Faculty of Computer Systems and Technologies, University of Computer Studies (Mandalay), Myanmar
[2]Faculty of Computer Science, University of Computer Studies (Mandalay), Myanmar
*Corresponding author, Zarni Sann, e-mail: zarnisann@gmail.com[1], haling.nn@gmail.com[2], kaythiwuthmonekhin29@gmail.com[3], snowqueen.zmw@gmail.com[4]

***Abstract***

*Data encryption is well known as essential for today's technology. ElGamal encryption and RSA algorithm is made before storing mails to mail server. ElGamal decryption and RSA decryption is made after retrieving mails from mail server. This system is implemented to secure mail server system for local government's important mail messages. These algorithms consume a considerable amount of time and resources of memory, CPU time, and computation time to encrypt and decrypt data. This paper discuss the results comparison of these algorithms in term of encryption time, decryption time, and memory usage over variable file sizes. The results show that RSA does faster encryption process in compare with ElGamal. However, ElGamal decryption process is quicker than RSA. This system is also expressed comparison of storage Size between RSA and ElGamal. Both of these algorithms are cryptographic public-key algorithms but have roles in different techniques. This system is using C# programming language and SQL Server to store mail messages.*

***Keywords****: ElGamal algorithm, RSA algorithm, Secured mail communication*



## 1. Introduction

Asymmetric key encryption or also known as public-key encryption is used to solve the problem of key distribution. Two keys are used in asymmetric keys; private keys for decryption and public keys for encryption. ElGamal and RSA algorithm serves encryption and decryption of the mail messages. Government's records must be secure for particular department.

ElGamal encryption-decryption is established on the complexity of the discrete algorithm problem where is directed to increase numbers of big powers. However, it is much harder to do the reverse calculation of the discrete logarithm. The ElGamal algorithm's performance, speed, and security depend on certain parameters [1-3].

Modular escalation and exponentiation are used by the RSA algorithm for encryption-decryption. Different keys are used for encryption-decryption processes as in public-key cryptography or asymmetric key cryptography standard. There are public and private key which both are generated by executing some computational effects on the product of two huge prime numbers. The public-key is sent to everyone in the system but the Private Key is kept secret in RSA. The private key can only be calculated by the public key. The RSA cryptosystem security is determined by the complexity of factoring large prime numbers [4, 5].

The rest of this paper has been structured in the following way. Section 2 designates the theoretical background of the asymmetric algorithm of ElGamal encryption and decryption and key generation for secured message communication. Section 2 also expresses RSA algorithm and its parameters. These two algorithms include three parts in each. Section 3 describes System Design and Architecture. Section 4 illustrates Implementation Result for mail messages security using ElGamal and RSA algorithm as well with Performance Parameters and comparison results with diagrams. Finally, section 5 concludes with advantages, limitation and further extensions of the system.

## 2. Elgamal and RSA Cryptography

The El-Gamal algorithm is known as a public-key cryptosystem which developed based on the discrete logarithm problem. The algorithm provide both the encryption and signature algorithms. The original or the plaintext is unencrypted message. The unencrypted message is readable to anyone who have

*Received August 10, 2019; Revised September 20, 2019; Accepted October 16, 2019*

access to intercept the message. The original text is processed in encryption process resulting a cipher text. The encryption process is shown in Figure 1.

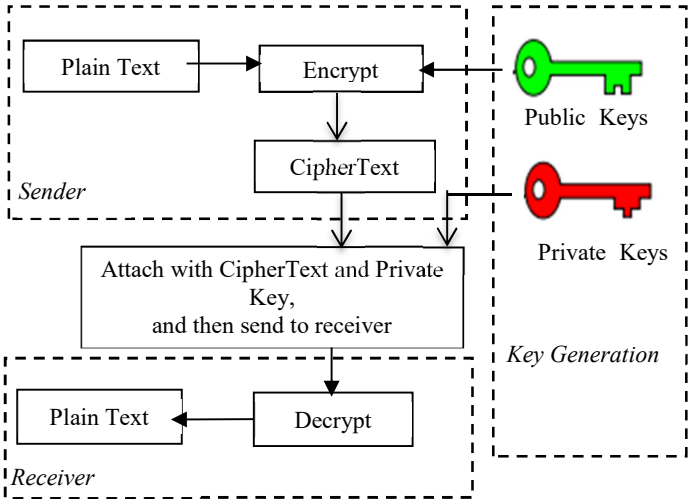


Figure 1. ElGamal algorithm structure

ElGamal algorithm is performed in three parts:

- Key generation for public keys and private keys
- Encryption for original plaintext message to receive cipher text, and
- Decryption for cipher text to generate original plaintext

For current security, a key length 1024-2048 is considered to be save for encryption. The ElGamal key can range from 256-bit to arbitrarily long which is consider to be save for its random length for at least 20 years forward. The private Key can range from 160 bit to 240 bit. The ElGamal algorithm is an asymmetric key cryptography, so, it converts message strings to digit using "String to digit conversion table".

### 2.1. Key Generation for ElGamal Algorithm

Key Generation is the first stage of Elgamal algorithm. ElGamal describes the working steps of key generator as follows:

*(1) Select a large prime p;*
*(2) Select d to be a member of the group;*
*(1<=d<=p-2)*
*(3) Select e1 to be a primitive root;*
*(4) $e2 = e1^d \bmod p$;*
*(5) public-key = (e1, e2, p);*
*(6) private key = d;*
*(7) return public-key and private key*

The following algorithm is the key generation algorithm in ElGamal [5, 6].

### 2.2. Elgamal Encryption

Encryption is the second stage of Elgamal algorithm. ElGamal proves and illustrates the encryption theory in the following algorithm: Message sender chooses a random integer 'r' for encryption and calculates ciphertexts using prime number 'p', random integer 'r' and plaintext 'P', and generates pair of ciphertext for each block (C1,C2). The following algorithm lines are the encryption stage in ElGamal [3].

*(1) Incoming parameter is (e1, e2, p, P)*
*(2) Select a random integer r*

*(3) C1 = e1$^r$ mod p*
*(4) C2 = (P x e2$^r$) mod p*
*(5) return (C1, C2)*
*(6) (C1 and C2 are ciphertexts)*

Notice that one can easily find the h$^y$ if one knows the m'. Therefore, a new y, or also called an ephemeral key, is generated for each new message to improve security encryption.

### 2.3. Elgamal Decryption

Decryption is the third stage of Elgamal algorithm. ElGamal proves and illustrates the decryption theory in the following algorithm. The recipient may retrieve the message by using public keys and private keys. Decryption process uses ciphertexts to generate plaintext, again. The result of decryption process from the ElGamal algorithm and original incoming messages are the same. The following algorithm lines are the decryption stage in ElGamal [2, 6].

*(1) Incoming parameter is (d, p, C1, C2).*
*(2) P = [C2 (C1$^d$)$^{-1}$] mod p*
*(3) return P*
*(4) (P is the plaintext).*

The result of decryption process from the ElGamal algorithm and original incoming messages are the same.

### 2.4. RSA Methodology

In RSA algorithm generate unique two number public or called as public-key namely (*e, n*). It also generate a number secret also called private exponent namely (*d*) is for each users. The key works in following term; If a user A send a mail to user B, user A should know user B's public-key and have mail M (written in the form of integer value) then user A creates the block of message of size < *n* and then sends the cipher text $C=M^e \bmod (n)$ to user B. then the receiver user B decrypt the text by $M=C^d \bmod (n)$. The choice of public and private keys will affect the security of algorithm [4, 5].

### 2.5. Key Generation for RSA algorithm

The keys generator for the RSA algorithm are work on the following procedure:

1. It takes two random primes, *p* and *q* of approximately equal size such that *n=pxq*.
2. Compute *n=p x q*, and *Ø(n)=(p-1)(q-1)*
3. Choose an integer *e, 1<e<Ø(n)*, such that approaches, all equivalent in effect to factoring the *gcd (e,Ø(n))=1*
4. Compute *d, 1<d<Ø(n)*, such that *ed=1 mod Ø(n)*
5. The public-key is *(n, e)* and the private key is *(n, d)*.

The Figure 2 shows Encryption, Decryption and Key Generation in RSA.

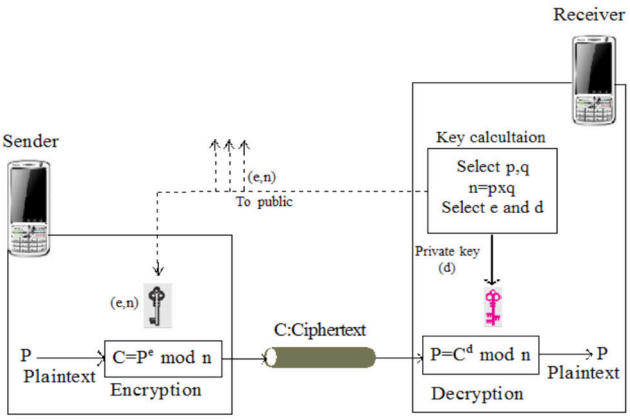


Figure 2. Encryption, decryption and key generation in RSA

### 2.6. RSA Encryption

The encryption begin in the sender's key. The sender device then to calculates the cipher text *C*: equivalent to $C=P^e \bmod n$. This can be completed quickly using the method of exponentiation by squaring. Sender then sends *C* to receiver. The letter will be used to refer the public-key *e,* since the public-key is used when encrypting a message. RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts [4 5].

### 2.7. RSA Decryption

The receiver can decode *P* from *C* by using its own private key exponent *d* by the following formula: $P=C^d \bmod n$. The letter *d* will be used to decrypt a message [1, 2]. The result of the process will be the cipher text of the product [5].

## 3. System Design and Architecture

The constructed system can be divided into three main parts: the server computer with SQL database, one mail sender client and another one mail receiver client. The sender/receiver clients can be further divided into two sub sections: messages sending and message receiving [7].

ElGamal or RSA encryption is made before storing mails to mail server. ElGamal or RSA decryption is made before retrieving mails from mail server. ElGamal or RSA converts the mail messages as encrypted text and then again decrypted text. Mail server stores mail messages until mail are not retrieved from receiver clients [7 6].

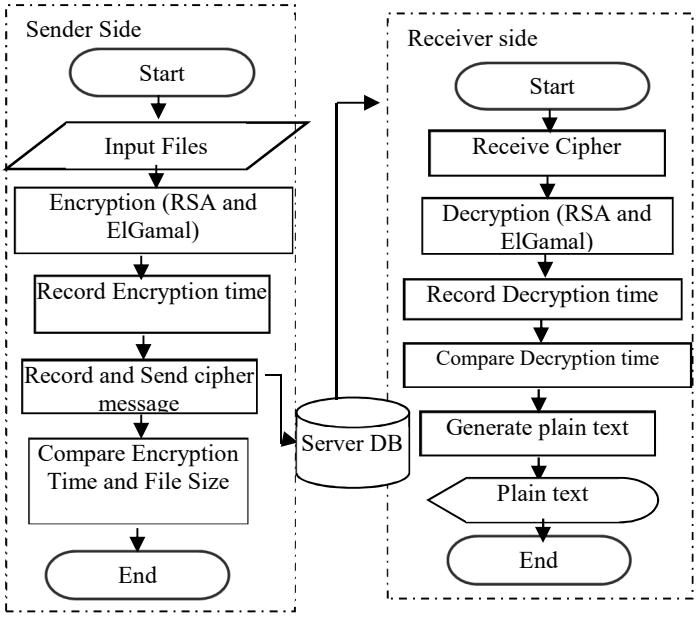


Figure 3. System flow for comparison process

Receiver client generate prime number and random key and decrypt this cipher text using ElGamal or RSA decryption algorithm to obtain plain text. This system can generate different size of attachment files and encrypt these files. In receiver side, user accepts attachment file for cipher reports from receiver inbox. So uses decrypt to gain the original message. This system records encryption time for two algorithms and decryption time for these two algorithms. Different attachment file encrypt and record to compare these two algorithms as shown in Figure 3.

## 4. Implementation Result

ElGamal or RSA algorithm serves encryption and decryption of the mail messages. Client users can send and retrieve mail and messages if their computers have connections with server computer.

Connection means the local area network connection (LAN) or wide area network connection. This system can be connected using network cable or wireless adapter. This system is implemented for security of messages on mail using ElGamal and RSA algorithms. It is developed by using *C#* Programming Language.

### 4.1. Performance Parameters

This system is considered the following parameters for Performance of two encryption algorithms for both encryption and decryption patterns. ElGamal and RSA have relatively similar time in generating key. Comparison of encryption time and decryption time are as shown in Figure 4 and Figure 5. RSA algorithm and ElGamal algorithm are asymmetric algorithms and have different formulas for encryption and decryption process where RSA algorithm is faster than ElGamal algorithm.

1) Encryption time (Computation Time/ Response Time) is the time needed for an algorithm to do encryption and produce cipher text. The detail comparison of encryption time in shown in Table 1.
2) Decryption time (Computation Time/ Response Time) it the time need to revert the cipher text into plain text by algorithm. The comparison time of both algorithm is shown in Table 2.

Table 1. Comparison of encryption time (Second)

| File Sizes (KB) | RSA | ElGamal |
|---|---|---|
| 64 | 54 | 5142 |
| 96 | 81 | 7713 |
| 150 | 126 | 12051 |
| 208 | 175 | 16711 |
| 298 | 250 | 23941 |

Table 2. Comparison of decryption time (Second)

| File Sizes (KB) | RSA | ElGamal |
|---|---|---|
| 64 | 205 | 179 |
| 96 | 307 | 268 |
| 150 | 480 | 419 |
| 208 | 666 | 580 |
| 298 | 954 | 831 |

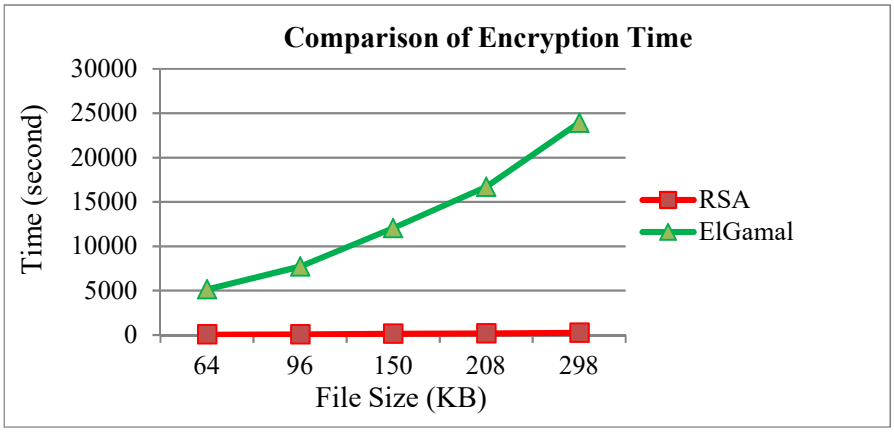


Figure 4. RSA and ElGamal encryption time comparison

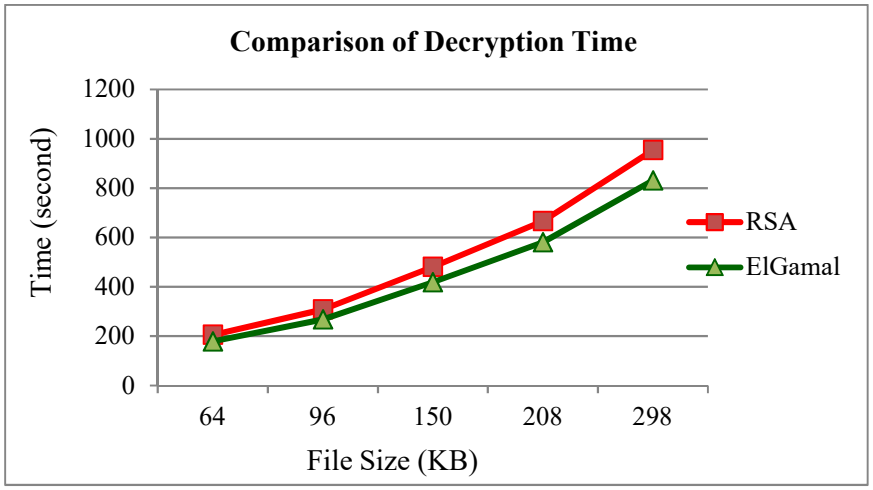


Figure 5. RSA and ElGamal decryption time comparison

3) Encrypted File Size: The size of encrypted file is called encrypted file size in Figure 6. The encryption time of ElGamal is more than RSA encryption time. The decryption time of ElGamal is little less than RSA algorithm. RSA requires least amount of storage space for encrypted files. These two algorithms is concluded that RSA made better in term of encryption time, ElGamal made better in term of decryption time. The comparison detail is shown in Table 3.
RSA Ciphertext has less numbers than ElGamal algorithm made. The ElGamal algorithm has a ciphertext pair. Each encrypted plaintext will create two ciphertext values. RSA requires least amount of storage space for encrypted files. Decrypted files sizes of two algorithms chosen for this paper, are equivalent to the original file sizes as shown in Figure 6.

Table 3. Comparison of encrypted file (MB)

| File Sizes (KB) | RSA | ElGamal |
|---|---|---|
| 56 | 1.1 | 3.3 |
| 96 | 1.8 | 5.1 |
| 150 | 2.41 | 7.72 |
| 208 | 3.8 | 10.6 |
| 298 | 5.15 | 14.8 |

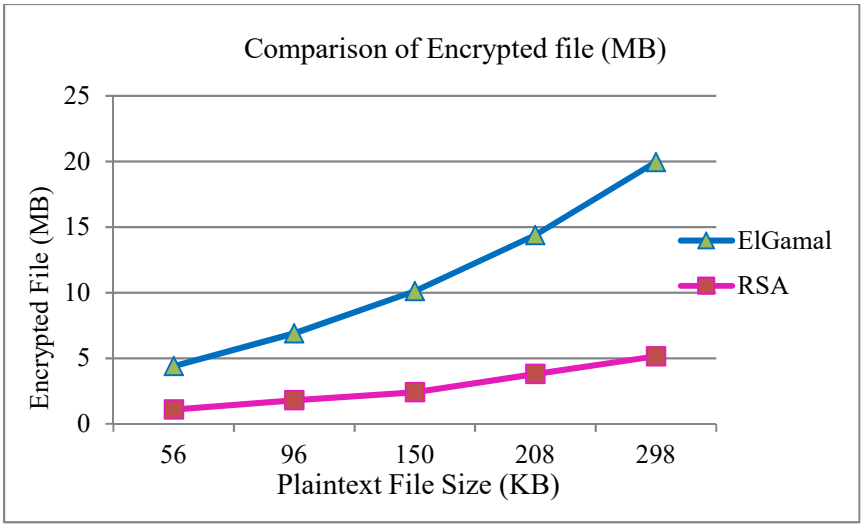


Figure 6. Comparison of storage size among RSA and ElGamal

## 5. Conclusion

To sum up, two encryption techniques like ElGamal and RSA algorithms are implemented. Also, it is necessary to compare their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption. In the use of email, the users will find that they can't send a files in large scale because of the encryption take longer time. The advantages of the system are: can make efficient and flexible mail services for user, can implement mail sending and receiving architecture.

The security for mail message is must for preventing our message from different attacks. It's necessary to make sure that our message to be interrupted or hijacked by unitended users. Therefore using cryptographic algorithm: ElGamal and RSA provide solution for mail security system. It provides security services in terms of privacy, authentication, integrity and nonrepudiation. RSA encryption is faster than RSA decryption.

Further extension of this system can use performance parameters such as throughput, bandwidth and different key size, etc. This system can extend the security of different data types. Future research on image data and audio data encryption using existing cryptograpgy to improve the encryption and decryption time algorithm like ElGamal and RSA.

## References

[1] Czeslaw Koscielny, A new approach to the Elgamal encryption scheme, Academy of Management of Legnica, Faculty of Computer Science, ul. Reymonta 21, 59–220 Legnica, Poland. *Int. J. Appl. Math. Comput. Sci*. 2004. Vol.14(2): 265-267.

[2] Mustafa Dulegerler, & M.NusretSarisakal. A secure e-mail application using the ElGamal algorithm, Instanbul University. Engineering Faculty. Computer Engineering Department. 34850. Turkey. 1998.

[3] Rashmi Singh, & Shiv Kumar. Elgamal's Algorithm in Cryptography. *International Journal of Scientific & Engineering Research*. Dec 2012. Vol.3(12).

[4] AnnapoornaShetty, Shravya Shetty K, Krithika K. A Review on Asymmetric Cryptography - RSA and ElGamal Algorithm, *International Journal of Innovative Research in Computer and Communication Engineering.* Oct 2014. Vol.2(5).

[5] M. Preetha, & M. Nithya. A Study and Performance Analysis of RSA Algorithm. *IJCSMC.* Jun 2013. Vol.2(6): 126-139.

[6] Zarni Sann, May Thiri Win, San Thiri Aung. Secured Mail System using Asymmetric Cryptography - RSA and ElGamal Algorithm, *Journal of Networking, Computer Security and Engineering*, Vol.4(1).

[7] Jae-Young Kim & James Won-Ki Hong. *Design and Implementation of a Web-based mail server management system.* 1996.