International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 6, October 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Time Performance Analysis of RSA and Elgamal Public-Key Cryptosystems

Kyaw Myo Thu[1], Kyaw Swar Hlaing[1], Nay Aung Aung[2]

[1]Assistant Lecturer, Faculty of Computer System and Technology,
Myanmar Institute of Information Technology, Mandalay Myanmar
[2]Lecturer, Information Technology Support and Maintenance Department,
University of Computer Studies, Mandalay, Myanmar

ABSTRACT

Computer and network security system are needed to protect data during their transmissions and to guarantee that data are authentic. Cryptography is useful not only for proving data to be secure but also for ensuring that data have not altered. So, it is needed to implement the public key cryptosystem in computer and network security system. In cryptography, symmetric key cryptosystems are faster than public key (asymmetric) cryptosystems. But public key cryptosystems are more secure than symmetric key cryptosystems and widely used in computer and network security system. This describes the comparison of RSA (Rivest, Shame, Adelman) public key cryptosystem and ElGamal public key cryptosystem. RSA public key cryptosystem is faster than ElGamal in encryption and decryption. This paper also describes the encryption/decryption time comparison of RSA and ElGamal.

KEYWORDS: *cryptography, encryption, decryption, RSA and ElGamal*

How to cite this paper: Kyaw Myo Thu | Kyaw Swar Hlaing | Nay Aung Aung "Time Performance Analysis of RSA and Elgamal Public-Key Cryptosystems" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-6, October 2019, pp.448-450, URL: https://www.ijtsrd.com/papers/ijtsrd28096.pdf

IJTSRD28096

I. INTRODUCTION

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. The origin of the word cryptography derived from ancient Greek. The word cryptography is made up of two components: “kryptos”, which means hidden and “logos” which means word.

There are two types of key based algorithms: symmetric (conventional) key algorithm and asymmetric (public) key algorithm. In symmetric key algorithms, the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption are the same. A public key cryptosystem is an asymmetric cryptosystem where the key is secret is constructed of a public key and a private key. The public key can be uses to encrypt messages. Only a person that has the corresponding private key can decrypt the messages.

RSA is one of the oldest and most widely used public key cryptosystems. It was the first algorithm knows to be suitable for signing as well as encryption and one of the first great advances in public key cryptography. It is still widely used in electronic commerce protocols, and is believed to be secure given sufficiently by multiplication of two very large primes. In practice, RSA has proved to be quite slow, especially the key generation algorithm. But RSA public key algorithm is faster than ElGamal public key algorithm. Because ElGamal is also based on prime number and it produces two ciphertext at the encryption process.

II. PROPOSED SYSTEM FRAMEWORK

In this section, our proposed system framework for the comparison of RSA and ElGamal public key cryptosystems is present. In Figure 1, an overview of our proposed systems for encryption process is described. In the encryption process the plaintext (text, image and audio) is encrypted with public key for RSA and ElGamal. Finally this system shows the comparison of encryption time for these two algorithms.

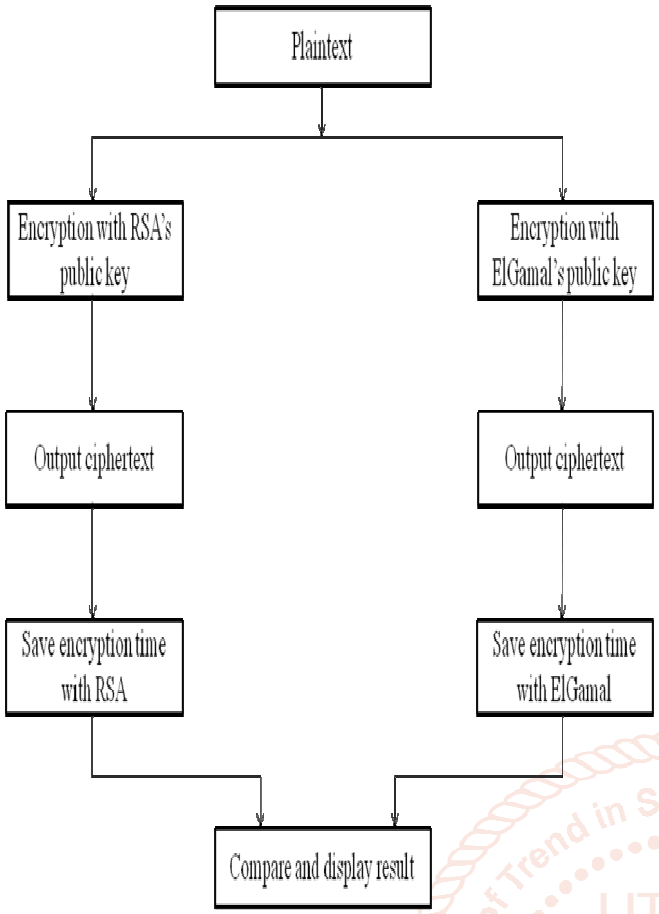

Figure.1 Blog diagram for encryption process

The decryption process is shown in Figure 2. In decryption process, the private key is use for both algorithms.

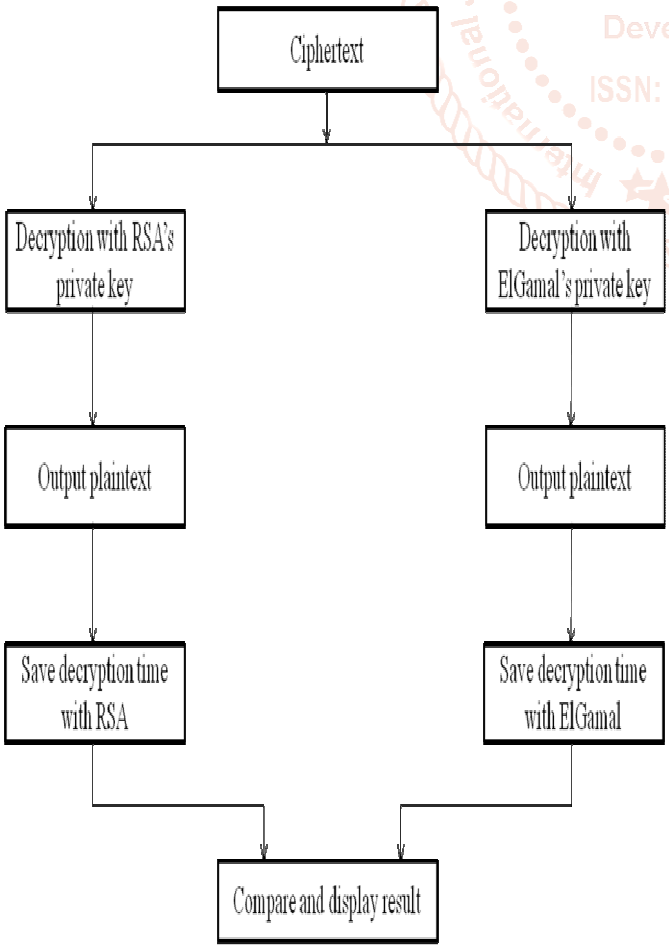

Figure.2 Blog diagram for decryption process

III. BACKGROUND THEORY

A. Rivest-Sharmir-Adleman (RSA) Algorithm

RSA algorithm is used for public key encryption. The security of RSA is based on factoring integers. RSA laboratories currently recommend key sizes of 1024 bits for corporate use and 2048 bits for extremely valuable keys like the root key pair used by a certifying authority. RSA involves two keys, public key and private key. The public key is known to everyone and is used to encrypt message. The private key is kept secret form knowing everyone except owner. The messages can only be decrypted by use of the private. Anybody can encrypt a message, but only the holder of a private key can actually decrypt the message and read it.

RSA encryption scheme can be divided into three stages:

- **Key Generation Stage**

RSA public key and private key can be generated by the following procedure. Choose two random prime number p and q such that p and q are not equal.

- Compute **n** such that **n = p * q**.
- Compute **Φ (n)** such that **Φ (n) = (p-1) (q-1)**.
- Choose a random integer **e**, **e< Φ (n)** and
- **gcd (e, Φ (n))= 1** that **e*d=1** modulo **Φ (n)**.
- **[n,e]** is private key .
- **[n,d]** is public key.

- **Encryption Stage**

Person **A** transmits public key **n & e** to person **B** and keeps the private key secret.

- **B** then wishes to send message **M** to **A**.
- **B** first turns **M** into a number, such that **M<n**.
- **B** then computes the **cipher text C** = $\mathbf{M^e}$ **mod n**.
- **B** then transmits **C** to **A**.

- **Decryption Stage**

Person A can recover message **M** from **C** by using the private key **d** and **n.**

- Decrypted value = $\mathbf{C^d}$ **mod n**.
- Given decrypted value, **A** can recover the message **M**.

B. ElGamal Algorithm

The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1984. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems.

ElGamal encryption scheme can be divided into three stages:

- **Key Generation Stage**

ElGamal_Key_Generation

{

Select a large prime p

Select d to be a member of the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$ such that $1 \le d \le p - 2$

Select e_1 to be a primitive root in the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$

$e_2 \leftarrow e_1^d \bmod p$

Public_key $\leftarrow (e_1, e_2, p)$ // To be announced publicly

Private_key $\leftarrow d$ // To be kept secret

return Public_key and Private_key

}

➢ **Encryption Stage**

```
ElGamal_Encryption (e1, e2, p, P)          // P is the plaintext
{
   Select a random integer r in the group G = < Zp*, × >
   C1 ← e1^r mod p
   C2 ← (P × e2^r) mod p                   // C1 and C2 are the ciphertexts
   return C1 and C2
}
```

➢ **Decryption Stage**

```
ElGamal_Decryption (d, p, C1, C2)          // C1 and C2 are the ciphertexts
{
   P ← [C2 (C1^d)^-1] mod p                // P is the plaintext
   return P
}
```

IV. COMPARISON OF RSA AND ELGAMAL

In this system, the testing results for encryption processing time of text files are shown in Table 1.

Size(KB)	RSA(Second)	ElGamal(Second)
1K	0.15	0.66
2K	0.18	0.69
3K	0.22	0.75
4K	0.25	0.77
5K	0.28	0.81

The testing results for decryption processing time of text files are shown in Table 2.

Size(KB)	RSA(Second)	ElGamal(Second)
1K	0.846	0.877
2K	0.860	0.885
3K	0.875	0.890
4K	0.888	0.903
5K	0.898	0.911

The testing results for encryption processing time of image files and audio files are shown in Table 3.

Size(KB)	RSA(Second)	ElGamal(Second)
5K(JPG)	0.31	1.092
12K(JPG)	0.55	2.52
14K(JPG)	0.68	2.85
242K(mp3)	0.955	3.342
312K(mp3)	1.32	4.081

The testing results for decryption processing time of image files and audio files are shown in Table 4.

Size(KB)	RSA(Second)	ElGamal(Second)
5K(JPG)	2.03	4.664
12K(JPG)	3.01	6.324
14K(JPG)	3.723	7.45
242K(mp3)	23.645	40.877
312K(mp3	30.231	42.902

According to the testing results, RSA is about 4 times faster than ElGamal at the encryption process. In the decryption, RSA is also faster than Elgamal.

V. FUTURE WORK

The cryptography is widely used for data and messages security in network and computer system. This system can be extended to the secure application of the business and organization that used the Internet such as e-Commerce, e-Banking, e-Mail and military and so on.

VI. Conclusion

The two implemented systems RSA and ElGamal are suitable for applications where it requires security based on the environment. This thesis shows the (encryption and decryption) time for RSA and ElGamal public key cryptosystems. The RSA encryption and decryption time are significantly faster than the ElGamal. RSA is ideally suitable for applications where high performance and high security.

REFERENCES

[1] D. Kahn, the Code breakers: The comprehensive History of Secret Communication from Ancient to the internet, Published 1967.

[2] AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram, "Comparative analysis of performance efficiency and security measures of some encryption algorithms", volume 2, Issue 3, May-June 2012, pp.3033-3037 in International Journal of Engineering Research and Applications (IJERA) ISSN.

[3] S. Inshi and A. Youssef, "Design and Implementation of an Online Anonymous Feedback System," in communications, 2008 24th Bi-ennial Symposium on, 2008, pp.58-61.

[4] Tzvetalin S. Vassilev, Andrew Twizell, "Cryptography: A Comparison of Public Key Systems", 2012, 1(5): 31-42.

[5] Alese, B. K., Philemon E. D, Falaki, S. O, "Comparative Analysis of Public Key Encryption Schemes", 2012, 2049-3444.

[6] Challa Narasimham, Jataram Pradhan: "Evaluation of Performance Characteristics of Cryptosystem Using Text Files", 2008 JATIT.

[7] Shahzadi Farah, M.Younas Javed, Azra Ahamim, Tabassam Nawaz, "An Experimental Study on Performance Evaluation of Asymmetric Encryption Algorithms", 987-1-61804-140-1.

[8] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh: "Comparative Analysis of Cryptographic Algorithms", July-Sept., 2013/16-18.

[9] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, 22 (1976) 644-654.

[10] T. ElGamal, "A Public Key Cryptosystem and a signature scheme based on discrete lagarithms", IEEE Transactions on Information Throry, volume 31, pages 469-492, 1985.

[11] R. L. Rivest, A. Shamir, L. Adleman: "A method for obtaining digital signatures and Public-Key Cryptosystems", Communications of the ACM 21 (1978), 120-126.

[12] W. Mao, Modern cryptography: theory and practice: Prentice Hall Professional Technical Reference, 2003.