An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms

[1]SHAHZADI FARAH, [2]M. YOUNAS JAVED, [3]AZRA SHAMIM, [4]TABASSAM NAWAZ

[1,4]Department of Software Engineering,
University of Engineering & Technology, Taxila, Pakistan

[2]Dept. of Computer Engineering, CE & ME, National University of Science and Technology,
Islamabad, Pakistan

[3]Faculty of Computer Science and Information Technology,
University of Malaya, Kuala Lumpur, Malaysia

shahzadifarah5@gmail.com, myjaved@ceme.nust.edu.pk, azra.majeed864@yahoo.com,
tabassam.nawaz@uettaxila.edu.pk

Abstract: - This paper presents the evaluation of RSA, ElGamal & Pallier asymmetric encryption algorithms. Encryption algorithms provide a secure communication over the internet and play main role in any security system. These algorithms consume a considerable amount of time and resources such as memory, CPU time, battery power and computation time to encrypt and decrypt data. In this paper, different experiments have been conducted to compare these algorithms in term of encryption time, decryption time, memory usage and throughput over variable text file and private key sizes.

Key-Words: -Asymmetric Algorithms, Encryption Time, Decryption Time, Throughput, Encrypted File Size, Decrypted Files Size

1 Introduction

Information security is one of the key challenges in data communication. For secure information communication over public network, different cryptographic methods are applied. The cryptographic methods are widely classified as symmetric and asymmetric. In symmetric methods, encryption and decryption keys are same or decryption key is easily calculated from the encryption key. The problem with symmetric method is that participants must share a secret key in a secure way which is difficult [2]. Asymmetric methods solve the problem of key distribution by using a pair of keys. It is computationally infeasible to determine the decryption key given only the knowledge of cryptographic algorithm and the encryption key [2].

RSA, Elgamal and Paillier encryption scheme belongs to asymmetric algorithms. RSA is one of the oldest and most widely used encryption algorithm [3]. In RSA, the key pair is derived from the product of two prime numbers chosen according to special rules [1]. Elgamal is fundamental, efficient, and simple asymmetric algorithm [4] and widely known as alternative to RSA. Paillier is and additive homomormphic algorithm and is widely known for its semantic security.

This paper presents the implementation and comparison of RSA, Elgamal and Paillier for variable text files sizes. Our goal is to calculate encryption time, decryption time, throughput, encrypted file size, and decrypted file size for each algorithm to identify which algorithms outperforms others in term of evaluation parameters.

The rest of the paper is organized as follows: Section 2 presents literature review. Section 3 describes parameters used for the evaluation. Section 4 presents experimental setting and data. Results are discussed in section 5 and Section 6 concludes the research work.

2 Literature Review

The performance evaluation of different symmetric and asymmetric encryption algorithms was extensively study in the literature. Seth et. al. [1] conducted a comparative analysis for the performance evaluation of symmetric and asymmetric encryption algorithms i.e. AES, DES and RSA in term of computation time, memory usage and output bytes on different file sizes. The result of their experiments showed that DES algorithm performed better among others in term of encryption time, AES has least memory usage and RSA algorithm generated least output file. Challa et. al. compared the performance of RSA and NTRU asymmetric algorithms on variable text file sizes with the key size of 51 bits and 20 bits for encryption and decryption process respectively [5]. They concluded that NTRU performed better in term of encryption, decryption and authentication than RSA. Vijayalakshmi et. al. compared the performance of RSA and Elliptic Curve Cryptosystem (ECC) asymmetric algorithms over execution time and memory size for encryption and decryption process with variable word lengths and different key sizes. Their results showed the superiority of ECC over RSA in term of execution time and memory requirement [9].

Elminaam et. al. conducted various experiment for performance evaluation of symmetric algorithms i.e. AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6 encryption in term of energy, power consumption, different key sizes, data types and packet size in [7]. Their results showed that Blowfish performed better than other encryption algorithms on variable packet size. Elminaam et. al. compared the performance of these algorithms on different sizes of data blocks, different data types, battery power consumption, data transmission over wireless network [8] and experimental results showed that Blowfish again performed better on variable packet size. Mittal conducted a study to compare the performance in term of processing time and throughput of symmetric algorithms i.e. DES, 3DES, and AES (Rijndael) algorithms over different in [6]. AES (Rijndael) algorithm has shown lesser execution time as compared to other algorithms and Processor 2.00 GHz (dual) showed best throughput over other hardware processors.

3 Evaluation Parameters

Authors selected following parameters for evaluation of RSA, ElGamal & Pallier asymmetric encryption algorithms for both encryption and decryption schemes.

- Encryption time (Computation Time/ Response Time)

The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text.[1]

- Decryption time (Computation Time/ Response Time)

The decryption time is considered the time that an encryption algorithm takes to reproduces a plain text from a cipher text.

- Throughput

Throughput is equal to total plaintext in bytes encrypted divided by the encryption time [1]. Higher the throughput, higher will be the performance.

- Encrypted File Size

The size of encrypted file is called encrypted file size.

- Decrypted File Size

The size of decrypted file is called decrypted file size.

4 Experimental Setting and Data

We performed experiments on Intel(R) Core(TM) 2 Duo CPU 2.09 GHz processor with 4 GM of RAM on Windows XP operating system. Compiler used for experiments is Python(x,y) 2.7.2.3. We carried out experiments on 68 KB, 105 KB, 124 KB, and 235 KB text file sizes. In this paper private key bit sizes are selected as suggested by NIST recommendation. Private key size of 1024 bit for RSA, 160 bits for ElGamal and Paillier was used for experimental purpose because RSA provides same amount of security on 1024 bit key size as provided by Elgamal and Paillier on 160 bit.

5 Results and Discussion

Figure 1 shows the comparison of encryption time in seconds among RSA, ElGamal, and Paillier. The secondary Y-axis represents the encryption time of Paillier because of huge time difference of Paillier as compared to RSA and ElGamal. RSA showed better performance over ElGamal and Paillier in term of encryption time and ElGamal showed better performance over RSA and Paillier in term of decryption time as shown in Figure 2.

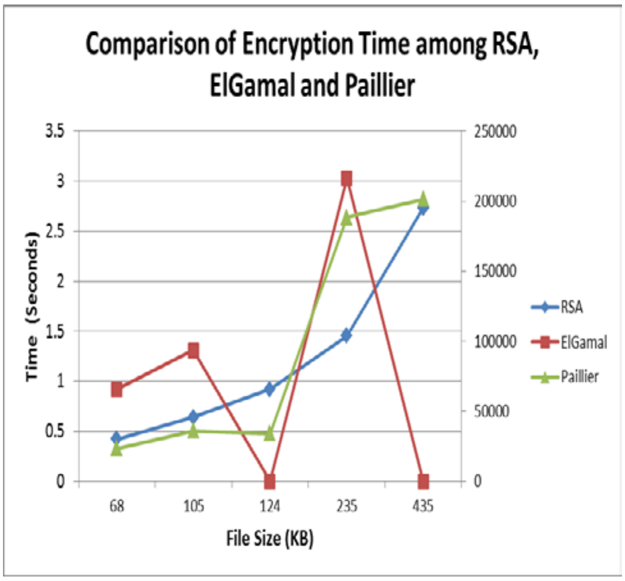

Figure 1: Comparison of Encryption Time among RSA, ElGamal and Paillier

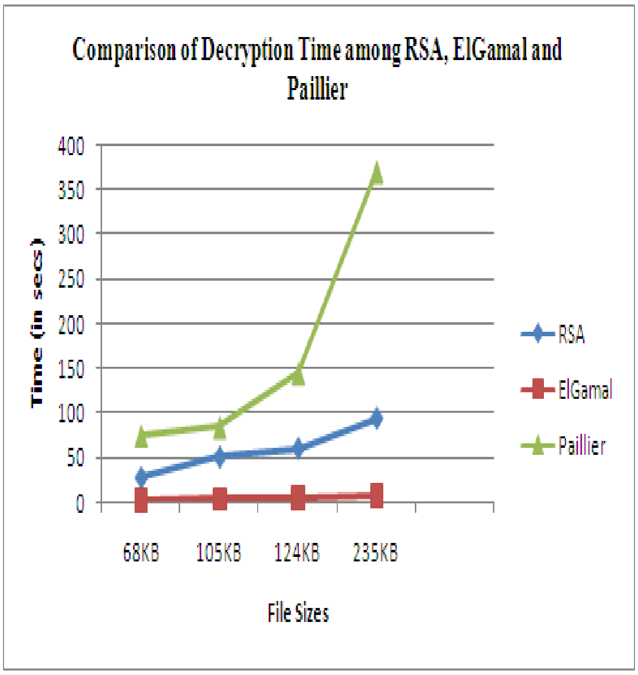

Figure 2: Comparison of decryption Time among RSA, ElGamal and Paillier

Figure 3 shows throughput of RSA, ElGamal and Paillier for encryption process and Figure 4 shows throughput of RSA, ElGamal and Paillier for decryption process. It is concluded from Figure 3 and Figure 4 that RSA showed better throughput over ElGamal and Paillier in encryption process and Elgamal showed better throughput over RSA and Paillier in decryption process.

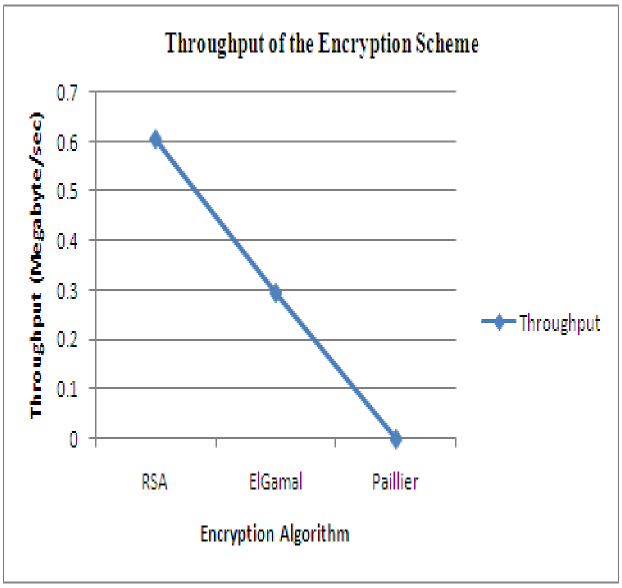

Figure 3: Throughput of RSA, ELGamal and Paillier for Encryption Process

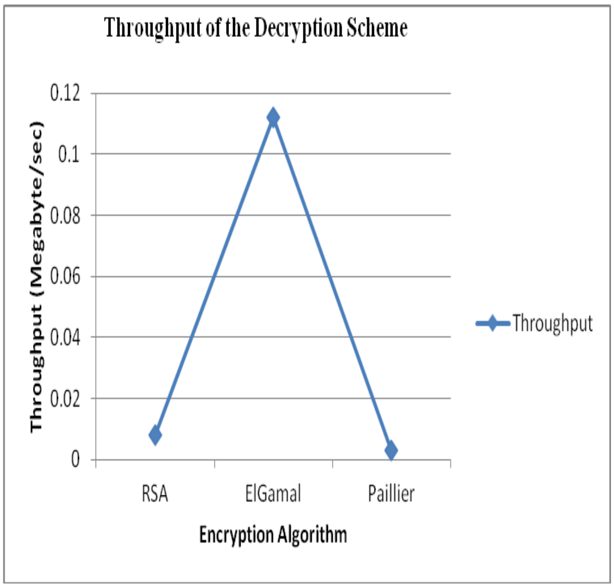

Figure 4: Throughput of RSA, ElGamal and Paillier on Decryption Process

Figure 5 and Figure 6 shows the comparison encryption and decryption file sizes among RSA, ElGamal and Paillier. Paillier showed worst result in encrypted file size and its encrypted file size increased exponentially with increase of input file size. The best result was shown by RSA. ElGamal, RSA, and Paillier showed same exponential increase in decrypted file size with increase in input file size.

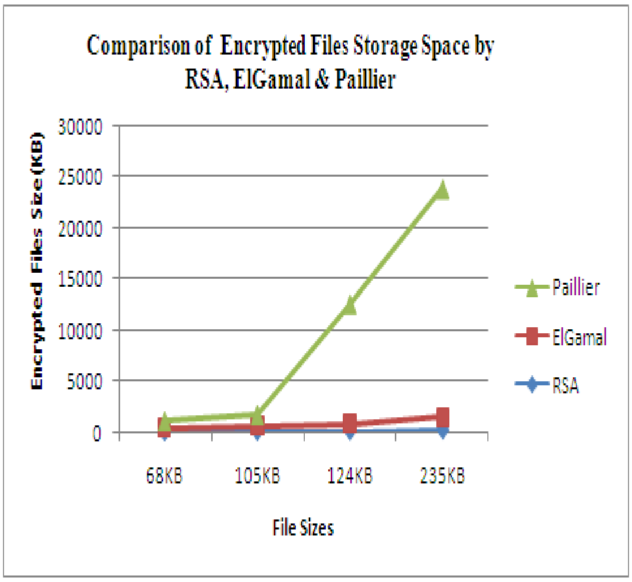

Figure 5: Comparison of Encrypted File Size by RSA, ElGamal and Paillier

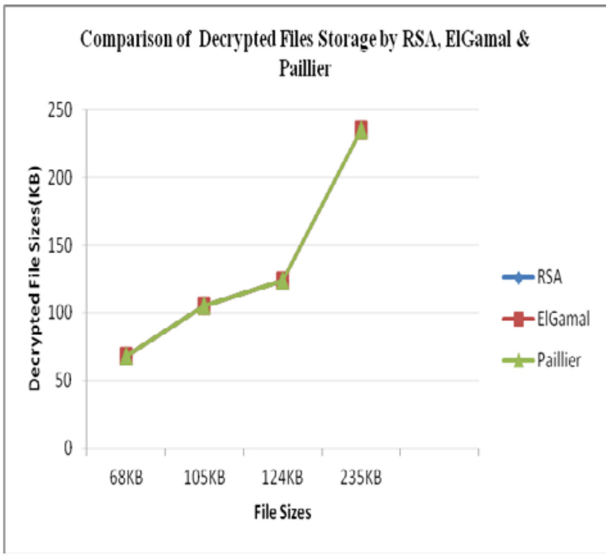

Figure 6: Comparison of Encrypted File Size by RSA, ElGamal and Paillier

5 Conclusions

This research work presents the comparison of RSA, ElGamal & Pallier in term of encryption time, decryption time, throughput, encrypted file size and decrypted file size. Different experiments were conducted for comparison of these algorithms and it is concluded that RSA performed better in term of encryption time, ElGamal in term of decryption time. Throughput is the most important parameter that demonstrates the performance of any algorithm. It is observed that throughput of RSA is better in encryption process than all others and ElGamal is better over others in decryption process. RSA requires least amount of storage space for encrypted files. Decrypted files sizes of all the three algorithms chosen for this paper, are equivalent to the original file sizes. The overall performance of RSA is better over ElGamal and Paillier in term of parameters used in this work.

References:

[1] Shashi Mehrotra Seth, Rajan Mishra, Comparative Analysis Of Encryption Algorithms For Data Communication, IJCST Vol. 2, Issue 2, June 2011

[2] Evaluation Of Performance Characteristics Of Cryptosystem Using Text Files

[3] 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.

[4] Myungsun Kim, Jihye Kim, And Jung Hee Cheon, Compress Multiple Ciphertexts Using Elgamal Encryption Schemes

[5] Narasimham Challa and Jayaram Pradhan, Performance Analysis of Public key Cryptographic Systems RSA and NTRU, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.8, August 2007

[6] Mohit Mittal, Performance Evaluation of Cryptographic Algorithms, International Journal of Computer Applications (0975 – 8887) Volume 41– No.7, March 2012

[7] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, Evaluating The Performance of Symmetric Encryption Algorithms, International Journal of Network Security, Vol.10, No.3, PP.216–222, May 2010

[8] Diaa Salama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud, Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices, International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October, 2009 1793-8201

[9] P.R.Vijayalakshmi, K. Bommanna Raja, Performance Analysis of RSA and ECC in Identity-Based Authenticated New Multiparty Key Agreement Protocol, International Conference on Computing, Communication and Applications (ICCCA), 22-24 Feb. 2012, pp 1-5