[[1]](#footnote-1)

Implementation and Analysis of DES, RSA and ElGamal cryptosystems

Manika Sharma and Manasi Chaudhari

*Abstract*- This document presents an evaluation of DES, RSA and ElGamal cryptosystems. The implementation is done in Java and a comparison of runtime and memory has been done based on different input sizes. Our analysis suggests that the time taken by RSA is maximum followed by ElGamal and then DES, while the memory requirement of ElGamal is the most followed by RSA, then DES

# INTRODUCTION

Information security is one of the major key challenges in data communication. For secure information communication over public network, different cryptographic methods are applied. They can be categorized into Symmetric(private) and Asymmetric(public) encryption. In symmetric encryption, encryption and decryption keys are same. And thus symmetric encryption has one problem that participants must share a secret key in a secure way which is difficult. Asymmetric methods solve the difficulty 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.

RSA and Elgamal are asymmetric algorithms while DES is symmetric algorithm. In RSA, the key pair is derived from the product of two primes chosen according to some special rules. Elgamal is fundamental, efficient and asymmetric algorithm that is widely known as alternative to RSA. DES is a symmetric key algorithm for the encryption of electronic data. DES is now considered to be insecure for many applications. This is mainly due to the 56-bit key size being too small.

This paper presents the implementation and comparison of DES, RSA and Elgamal encryption algorithms for variable text sizes. The performance measure of encryption schemes will be conducted in terms of encryption and decryption time, memory consumption and throughput. So, our goal is to calculate time, throughput and memory requirement for each algorithm to identify which algorithm outperforms others in term of evaluation parameters.

The rest of paper is presented as follows: Section II presents Literature Review, Section III describes parameters used for the evaluation, Section IV presents experimental setting and data, Section V presents Results and Section VI presents the conclusion of this experiment.

# LITERATURE REVIEW

The main purpose of this paper is paper is to study the use of mentioned cryptographic algorithms and analyse their performance. They were implemented, and performance was compared by input files of varying contents and sizes.

## RSA algotihm:

Rivest Shamir Aldeman is the most commonly used public key encryption algorithm. RSA has been widely used for establishing secure communication channels and for authentication the identity of service provider over insecure communication medium. In the authentication scheme, the server implements public key authentication with client by signing a unique message from the client with its private key, thus creating a digital signature. The signature is then returned to the client, which verifies it using the server’s known public key. The security of RSA is inherent in the difficulty of factoring large numbers. The RSA encryption and decryption algorithms require a single modular exponentiation operation. The size of the modulus

determines the security strength of the ciphertext. The algorithm works as follows:

1. Generate 2 large primes p,q

2. Calculate n = pq,  Ø (n) = (p − 1)(q − 1)

3. Select e, where 1<e< Ø, such that the GCD(e, Ø)=1

4. Generate e, find d: ed = 1 mod Ø (n)

5. Compute ciphertext Y = x^e mod n

6. Compute plaintext x = Y^d mod n

## ElGamal algorithm:

The El-Gamal algorithm is a public-key cryptosystem based on the discrete logarithm problem. Elgamal cryptosystem requires a modular exponentiation operation. The security strength of the cipher is a function of the sizes of the modulus; it is based on the discrete logarithm. This algorithm generates required keys (private key and public key) for both encryption and decryption. The

algorithm is stated as follows:

1. Generate a large Prime number p
2. Choose a, α such that1 < a, α < p-1
3. Choose k such that 1 ≤ k ≤ p
4. Compute β = α^a mod p
5. Ciphertext Y1= α^k mod p; Y2= x\*β^k mod p
6. Plaintext =Y2\*inv(Y1^a) mod p

## DES algorithm:

DES is a block cipher, with a 64-bit block size and a 56-bit key. DES consists of a 16-round series of substitution and permutation. In each round, data and key bits are shifted, permutated, XORed, and sent through, 8 s-boxes, a set of lookup tables that are essential to the DES algorithm. Decryption is essentially the same process, performed in reverse.

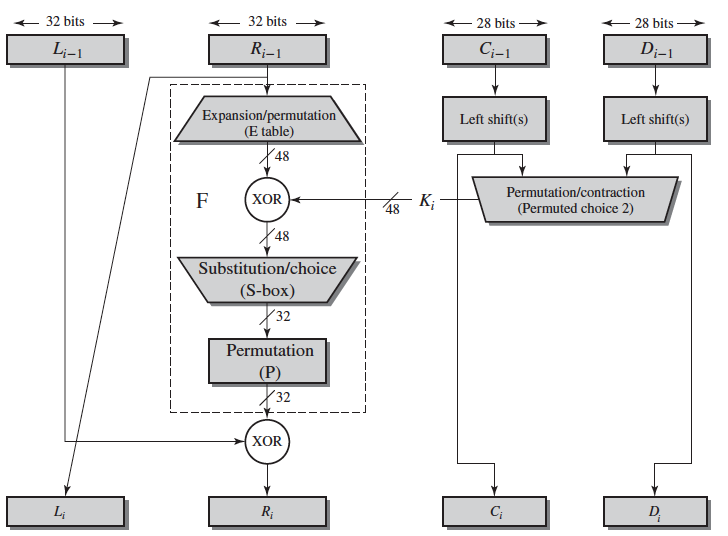


Fig 1. Each round of DES

(Image credit: Cryptography and Network Security by William Stallings)

# EVALUATION PARAMETERS

We selected following parameters for evaluation of RSA, Elgamal and DES encryption algorithm:

1. Encryption and Decryption Time:

The encryption and decryption time is considered as the time an encryption system takes to convert plaintext to ciphertext and ciphertext to plaintext  respectively

2. Memory Used:

Memory used by System computes the count of memory in kb that is being consumed by the encryption algorithm

3. Throughput:

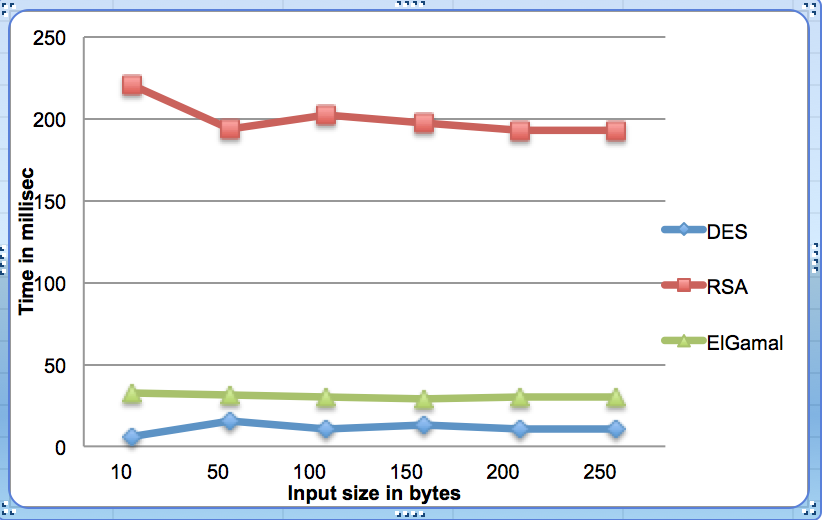
Throughput is equal to total plaintext in bytes encrypted divided by the encryption time. The value of throughput measures the performance of system. Higher the throughput, higher is the performance

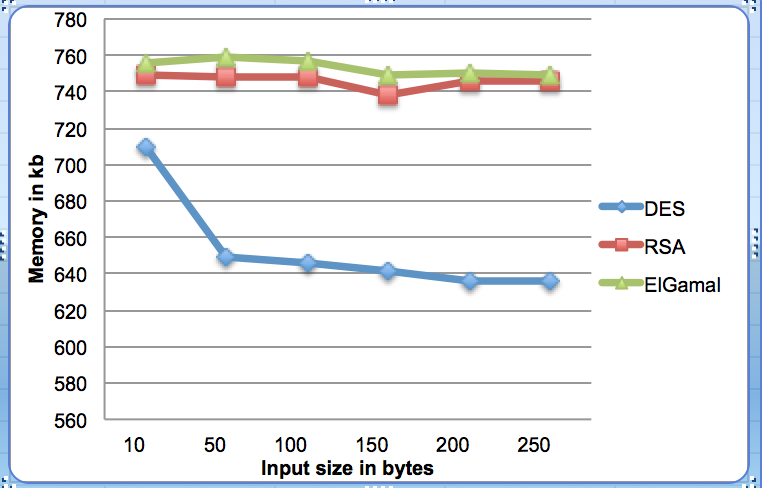
# EXPERIMENTAL SETTINGS

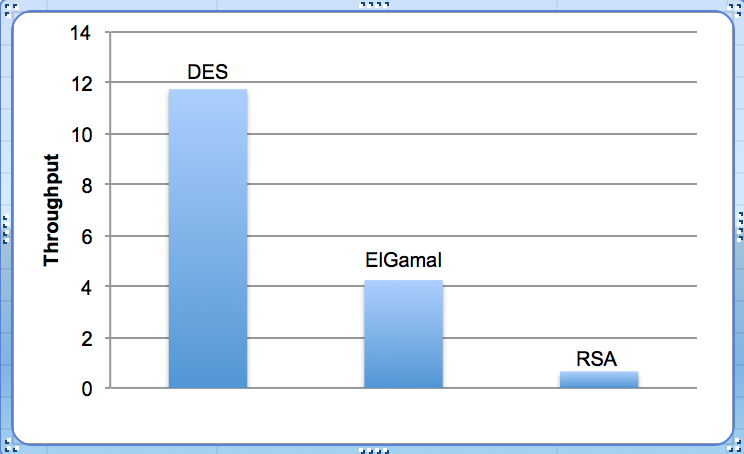
We performed experiments on Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz with 16 GB of RAM on Ubuntu operating system and on MacOSX 2.4 GHz Intel Core i5 processor at 1600 MHz with 8GB RAM. We carried out experiments on 10 B, 50 B,100 B, 150 B,200 B,250 B size text. Private key size of 2048 bit for RSA and ElGamal was used for experimental purposes.

# RESULTS

We have compared the running time, memory usage and throughput of DES, RSA and ElGamal. Figure 2 shows the comparison of encryption time in milliseconds among RSA, ElGamal, and DES. TheY-axis represents the total time while the X-axis represents bit size of input. Figure 3 shows the comparison of memory used by these cryptosystems. We see that DES is the fastest, while RSA is the slowest of the three. In terms of memory, ElGamal consumes the most while DES takes the least. So, according to these results, it is obvious that the throughput value of DES is maximum, followed by ElGamal and then RSA. Thus, we can say that DES performs better than ElGamal and RSA.

  
Fig 2. Time vs input size

  
Fig 3. Memory vs Input Size

  
Fig 3. Throughput

# CONCLUSION

Encryption algorithms play a very important role in communication security where encryption time, memory usages and throughput are the major issue of concern. We evaluated the performance of selected encryption algorithms-DES, RSA and Elgamal in respect to these parameters

Based on the plaintext used and the experimental result, it is concluded that DES algorithm consumes least encryption+decryption time and RSA algorithm consumed the most time. And time difference is not huge in case of Elgamal and DES algorithm.

DES requires the least amount of storage space. Though the difference in storage space for all the three algorithms was not too huge. Throughput is the most important parameter that demonstrates the performance of any algorithm and RSA has the least throughput as was obvious from its large encryption-decryption time, DES has the most throughput.

REFERENCES

1. Shashi Mehrotra Seth, Rajan Mishra, Comparative Analysis Of Encryption Algorithms For Data Communication, IJCST Vol. 2, Issue 2, June 2011
2. Dr. Prerna Mahajan, Abhishek Sachdeva, A Study of Encryption Algorithms AES, DES and RSA for Security, Global Journal of Computer Science and Technology, Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013
3. Annapoorna Shetty, Shravya Shetty K, Krithika K,A Review on Asymmetric Cryptography RSA and ElGamal Algorithm, IJIRCCE, Vol.2, Special Issue 5, October 2014
4. E.Thamiraja ,G.Ramesh,R.Uma rani “A Survey on

Various Most Common Encryption Techniques” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

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

1. [↑](#footnote-ref-1)