Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal

Sonia Rani
M.Phil Scholar, Department of Computer Science Applications, SBBS University,
Jalandhar Punjab, INDIA

Harpreet Kaur
Assistant Professor, Department of Computer Science Applications, SBBS University,
Jalandhar Punjab, INDIA

***Abstract*:** Cryptography is a concept to protect network and data transmission over network. Data Security is the main aspect of securing data transmission over unreliable network. Cryptography is a method of storing and transmitting data in a secret form so that only those for whom it is intended can read and process it. There are two types of cryptography algorithms such as symmetric key cryptography and asymmetric key cryptography. At present there are various types of cryptographic algorithms provide high security to information on networks, but they also have some drawbacks. To overcome the drawbacks of these algorithms, we propose a new hybrid cryptographic algorithm in this paper. The algorithm is designed using combination of two cryptographic algorithms AES and Elgamal. Analyse and compare the performance of existing and proposed algorithm on parameters security, encryption time, decryption time and throughput. This new hybrid cryptographic technique has been designed to decrease encryption and decryption time and increase throughput. In this work core java + swing in NetBeans IDE 7.0.1 jdk 8.0. is used. Implementation and performance analysis of proposed model done by JAVA. Results shows the Hybrid model perform better than AES and Elgamal individually.

***Keywords*:** Cryptography, AES, Elgamal and Hybrid AES and Elgamal

I. INTRODUCTION

Cryptography is an art of writing and reading the secret information. It uses mathematics in science to protect the information. It is a method of encrypting the original information into a form that is not easily interpreted by anyone. Original message can be revealed only after decrypting the encrypted message. Public and private keys are used for this purpose. Generally, the cryptographic systems can be classified into symmetric and asymmetric. In symmetric cryptography, same key is used for the encryption and decryption whereas in asymmetric cryptography separate keys are used for the encryption and decryption process [11].

There are two types of cryptography algorithm that are given below:

- Symmetric key cryptography algorithm
- Asymmetric key cryptography algorithm

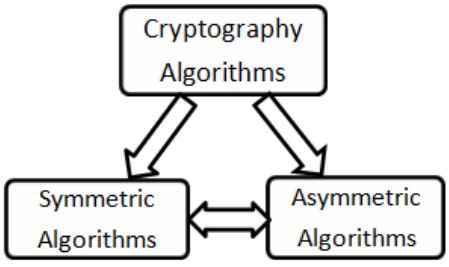

Fig 1: Cryptography Algorithms.

i. AES (Advanced Encryption Standard):

AES was developed in 1999. AES was announced by National Institute of Standards and Technology (NIST). AES is a block cipher symmetric algorithm with block length 128 bits and key lengths of 128, 192 or 256. The key size of the algorithm depends on the number of rounds in algorithm [10]. The algorithm is as shown in Figure

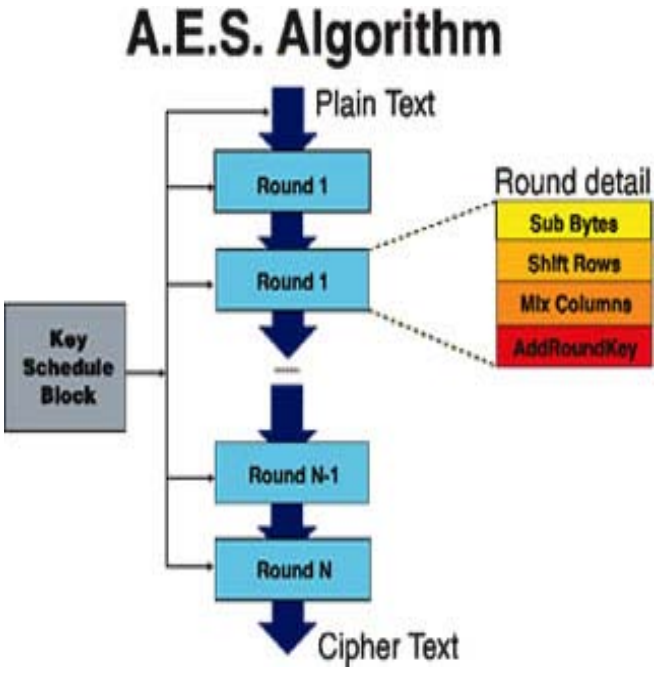

Fig 2: AES Algorithm

In AES, there are four transformations for one round
1) Sub Bytes - It's a nonlinear substitution, here each byte is replaced by another fix bytes.

2) Shift Rows - each row is rotating according to row position from right to left. Like 0th row rotate for 0times, 1st row rotates for 1 time, 2nd row rotates for 2 times and 3rd row rotates for 3 times.

3) Mix Columns - performs mixing operation on columns with constant and data.

4) Add Round Key - combining data's bytes column with a key's byte column. [10]

ii. **ElGamal**

Elgamal is an asymmetric key algorithm developed by Taher Elgamal in the year 1984. It is based on Diffie-Hellman key exchange algorithm [5] and works over finite fields [6]. The security of this algorithm is based on Discrete Logarithm Problem (DLP).
The steps involved in the Elgamal algorithm are as follows:

A. Initialization

Before the encryption and decryption process can start, the following initialization is done:

- Choose a random prime p and a primitive root element 'a' ε F_a.
- Private key 'x' is chosen as a random number such that 'x' ε $\cup$ F_{a-1}.
- Public key 'y' is computed using the private key 'x'. Therefore, $y^k = a^k \bmod p$.

B. Encryption Scheme

The sender chooses a random integer k ε $\cup$ F_{a-1} and computes one time key $K = y^k \bmod p$. The message M is encrypted into two parts (C1 and C2) as $a^k \bmod p$ and $K*M \bmod p$ respectively.

C. Decryption

The cipher text is decrypted as $M = C2\ K^{-1} \bmod p$ using one time key $K = C1^x \bmod p$.

II. RELATED WORK

This section gives the overview of related work by various authors in network security algorithms

Diaa Salama Abd Elminaam et al. [2010], presents evaluation of six of the most common encryption algorithms namely: AES (Rijindeal), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. [6]

Jawahar Thakur et al. [2011], provides a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since main concern here is the performance of algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. The comparison is made on the basis of these parameters: speed, block size, and key size. [2]

Shashi Mehrotra Seth et al. [2011], performs comparative analysis of three algorithm; DES, AES an RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool is used for conducting experiments. Experiments results are given to analyses the effectiveness of each algorithm. **[7]**

Jignesh R Patel et al. [2012], present an improved Hybrid AES-DES algorithm as means of strengthening the current AES architecture. The hybrid model gives a better non linearity to the plain AES and as it is merged with DES there is better diffusion hence the possibility of an algebraic attack on the hybrid model is reduced [4].

Pratap Chandra Mandal et al. [2012], provides a fair comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of these parameters: rounds block size, key size, encryption/decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is more suitable than AES. [8]

Lalit Singh et al. [2013], provides a fair comparison between five most common and used symmetric and asymmetric key algorithms: Two fish & Blowfish, IB_mRSA, RSA, RC. A comparison has been made on the basis of these parameters: rounds block size, key size, and encryption/decryption time, CPU process time in the form of throughput. These results show that IB_mRSA is more suitable than other algorithms. [9]

Jitendra Singh Chauhan et al. [2105], focuses on the comparative study of various cryptographic algorithms like AES, DES, RSA, Blow Fish, Elliptic Curve, SHA and MD5 and give a proper direction to the users for use of proper algorithm for securing of data. MD5 algorithm takes least encryption time whereas, RSA takes largest encryption time. [10]

Jitendra Singh Laser et al. [2016], surveyed the conventional algorithms, based on their benefits and drawbacks. We additionally have in comparison the significance of each these cryptographic techniques. This paper also offer an appropriate future opportunity related to these cryptographic techniques. [11]

Md. Alam Hossain et al. [2016], describes the basic characteristics (Key Length, Block size) of symmetric (AES, DES, 3DES, BLOWFISH, RC4), Asymmetric (RSA, DSA, Diffie-Hellman, EI-Gamal, Paillier), Hashing (MD5, MD6, SHA, SHA256) algorithms. Also we implemented five well-known and widely used encrypt techniques like AES, DES, BLOWFISH, DES, RC4, RSA algorithms and compared their performance based on the analysis of their encryption and decryption time for different file sizes in the local system. [1]

V. Kapoor et al. [2016], a hybrid cryptographic technique for improving data security during network transmission is

proposed and their implementation and results are reported. The proposed secure cryptographic technique promises to provide the highly secure cipher generation technique using the RSA, DES and SHA1 technique. [12]

Dr. D. Vimal Kumar et al. [2016], some well-known cryptographic algorithms have been analyzed in this paper to demonstrate the basic differences between the existing encryption techniques. Regardless of the mathematical theory behind an algorithm, the best algorithm are those that are well-known and well-documented because they are well-tested and well studied. [3]

III. PROPOSED METHOD: HYBRID AES AND ELGAMAL

In proposed algorithm (Hybrid AES and Elgamal) the goal had been achieved by combining two algorithms called AES and Elgamal.

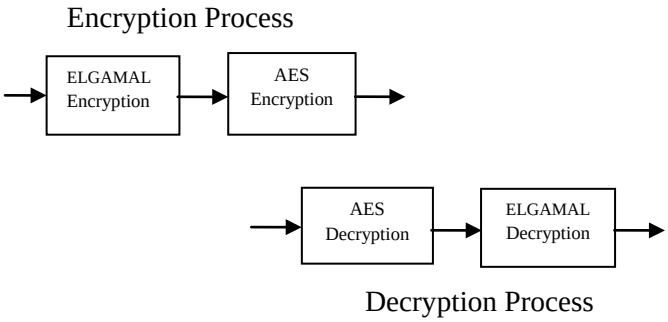

Fig 3: Block Diagram of Hybrid AES and Elgamal

IV. IMPLEMENTATION

In this system the implementation of AES, Elgamal and Hybrid AES and Elgamal is done for comparative study so it can be easily understood that time requirement for encryption of Hybrid AES-Elgamal is less than that of the time requirement of individual AES and Elgamal.

i. Encryption time

The time required to encrypt data is termed as encryption time of the cryptographic system [12]. In the figure X-axis contains data of different size for experiments and Y axis contains time required. The encryption time of the AES, Elgamal and proposed hybrid algorithm is given in below table:

Table 1: Encryption time for each algorithm

Data Size (bytes)	AES	Elgamal	Hybrid AES and Elgamal
100	128033	5855	5359
500	126531	21903	12294
1000	126039	29907	21230
1500	126018	38347	31103
2000	123639	45182	40532

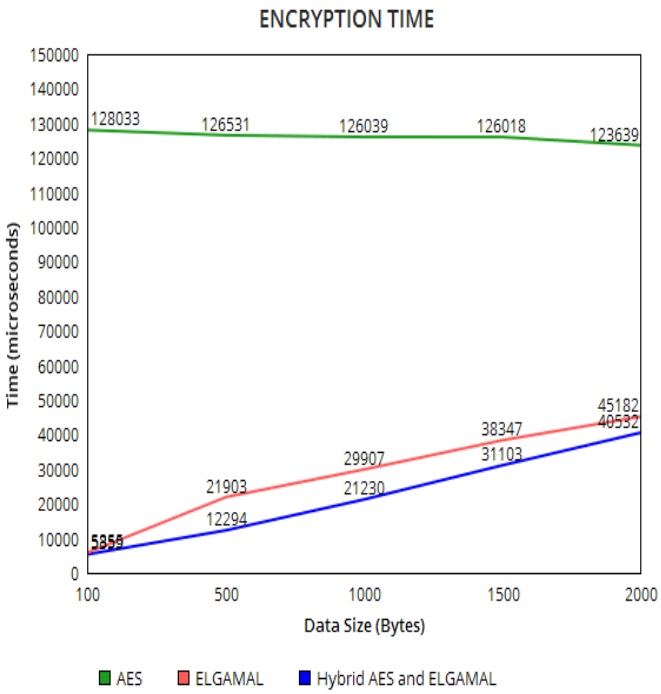

Fig 4: Encryption time for each algorithm.

The diagram contains data of different data size in X axis by which experiments are conducted. Similarly Y axis contains amount of time in microseconds. The results show proposed algorithm consumes less time as compared to AES and Elgamal algorithm. According to mean performance proposed Hybrid algorithm consumes less amount of time with respect to AES and Elgamal algorithm.

ii. Decryption time

The time to recover original data from cipher is known as decryption time [12]. Figure shows comparative performance of AES, Elgamal and proposed Hybrid algorithm. In this figure X-axis contains data of different size for experiments and Y axis contains time required. The decryption time of the proposed algorithm is efficient as compared to individual AES and Elgamal algorithm.

Table 2: Decryption Time for each algorithm

Data Size (bytes)	AES	Elgamal	Hybrid AES and Elgamal
100	533	1723	176
500	824	2146	345
1000	976	2442	432
1500	1243	2678	763
2000	1426	2929	865

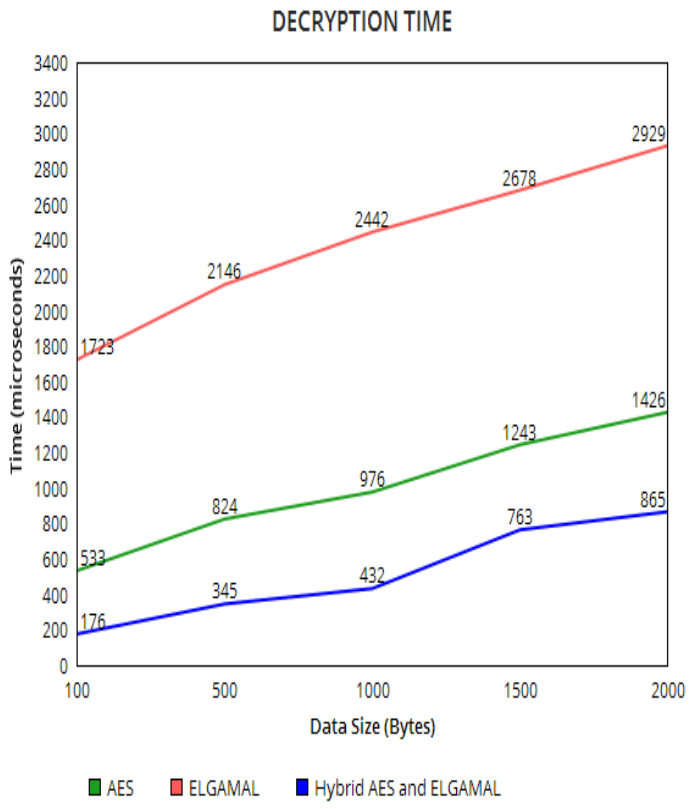

Fig 5: Decryption time for each algorithm

The results as defined in figure shows, the proposed technique is efficient as compared to AES and Elgamal algorithm. The results shows proposed Hybrid algorithm provides advantage over AES and Elgamal algorithm. Thus proposed technique reduces the time consumption as compared to both AES and Elgamal algorithm.

iii. Throughput

The throughput of each algorithm is depicted in figure 5. The throughput of proposed hybrid model is better than the throughput of AES.

Table 3: Throughput of each algorithm

Data Size (bytes)	AES	Elgamal	Hybrid AES and Elgamal
100	5.23	20.67	17.75
500	7.56	25.78	20.67
1000	5.59	23.89	19.78
1500	8.9	43.23	23.54
2000	6.69	40.42	25.78

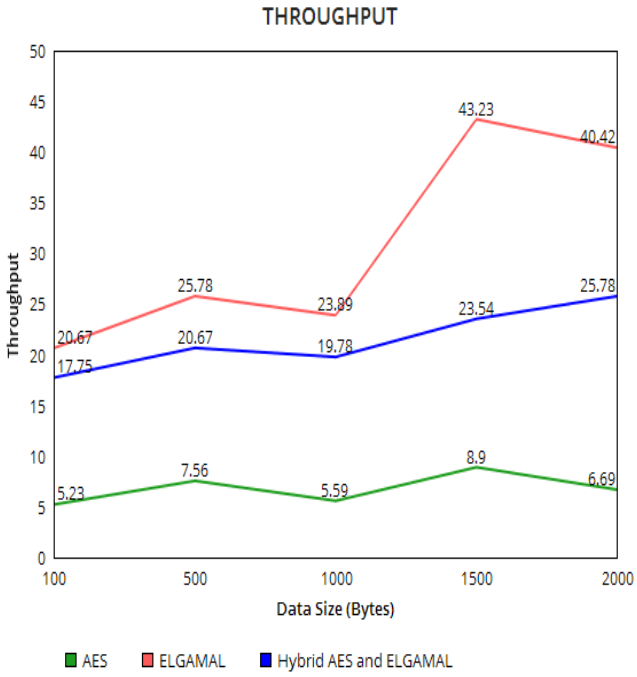

Fig 6: Throughput of each algorithm

V. CONCLUSION

In order to protect the intended data from hacking, cryptography is performed. In this paper we discussed about cryptography AES and Elgamal and our proposed hybrid algorithm using AES and Elgamal algorithms. Cryptographic algorithms play a very important role in Network security. In the review of literature work there are some drawbacks. The hybrid algorithm is better than AES and Elgamal in terms of encryption time and decryption time and security. Future work can be done on other symmetric and asymmetric algorithms by merged them.

REFERENCES

[1] Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 3, March 2016.

[2] Swati Kashyap, Er.Neeraj Madan "A Review on: Network Security and Cryptographic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, April 2015.

[3] Dr. D. Vimal Kumar, Mrs. J. Divya Jose, "Over View of Cryptographic Algorithms for Information Security" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 5, May 2016.

[4] Jignesh R Patel, Rajesh S. Bansode Vikas Kaul, "Hybrid Security Algorithms for Data Transmission using AES-DES" International Journal of Applied Information Systems (IJAIS), Volume 2– No.2, February 2012.

[5] Shaina Arora, Pooja, "Enhancing Cryptographic Security using Novel Approach based on. Enhanced – RSA and

Elgamal : Analysis and Comparison " International Journal of Computer Applications (0975 – 8887) Volume 112 – No 13, February 2015.

[6] 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.213-219, May 2010.

[7] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication" IJCST Vol. 2, Issue 2, June 2011.

[8] Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish" Journal of Global Research in Computer Science Volume 3, No. 8, August 2012.

[9] Lalit Singh Dr. R.K. Bharti, "Comparative Performance Analysis of Cryptographic Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[10] Jitendra Singh Chauhan, S. K. Sharma, "A Comparative Study of Cryptographic Algorithms" INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD, Volume - 1, Issue - 2, Sept – 2015.

[11] Jitendra Singh Laser, Viny Jain, "A Comparative Survey of various Cryptographic Techniques" International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 03 | Mar-2016.

[12] V. Kapoor, Rahul Yadav, "A Hybrid Cryptography Technique for Improving Network Security" International Journal of Computer Applications (0975 – 8887) Volume 141 – No.11, May 2016.