# An Encryption and Decryption Time Efficient Elgamal Cryptosystem

**Mr. Jaydip Thakkar**[1]
[1]Student
[1]Department of Computer Science & Engineering
[1]Narnarayan Shastri Institute of Technology, Jetalpur

*Abstract*— Encryption and Decryption are two fundamental approaches in network security and cryptography. Both of these tools or we can say techniques are most commonly used nowadays. If we want to perform secure communication between sender and receiver than encryption and decryption are very useful. For this purpose, public key cryptography and private key cryptography is used. Here we present, we present an overview of the existing cryptographic system and will see some of the problems that arise in the existing cryptosystem. Then after we present the brief introduction of the proposed system and provide advantages of our proposed system.

***Key words:*** Cryptographic**,** Elgamal algorithm, Discrete Logarithm Problem

## I. Introduction

### A. Definition Of Cryptography:

“Cryptography is the science of using mathematics to transform the contents of information in secure mode and also immunes to attack”.

### B. Cryptographic Goals:

However, there are other natural cryptographic problems to be solved and they can be equally if not more important depending on who is attacking you and what you are trying to secure against attackers. The cryptographic goals covered in this text (in order of appearance) are Confidentiality, Integrity, and Availability [7].

These concepts form what is often referred to as the CIA triad. These concepts embody the fundamental security objectives for both data and for information and computing services. A useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

### C. Confidentiality:

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

### D. Integrity:

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

### E. Availability:

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Although the use of the CIA triad[7] to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are:

### F. Authenticity:

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission of a message, or message originator.

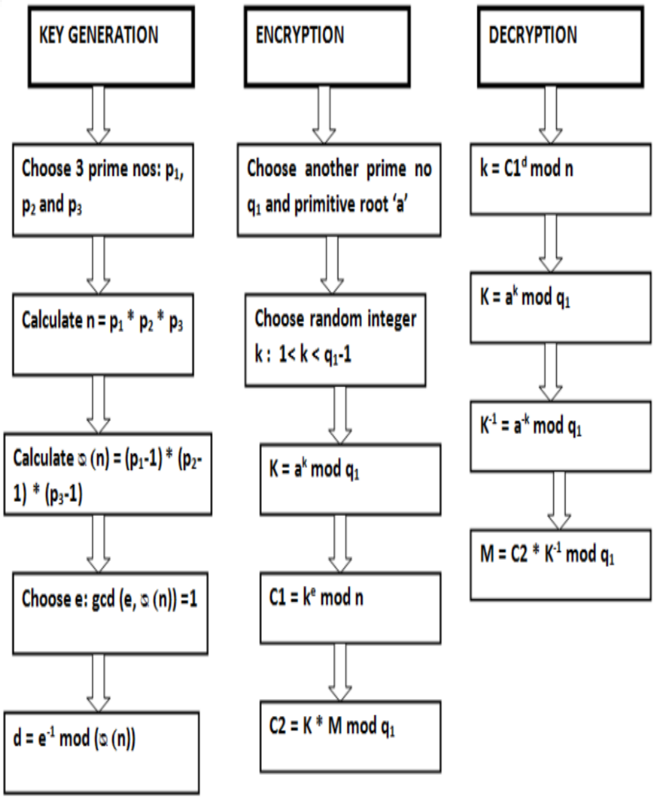
### G. Accountability:

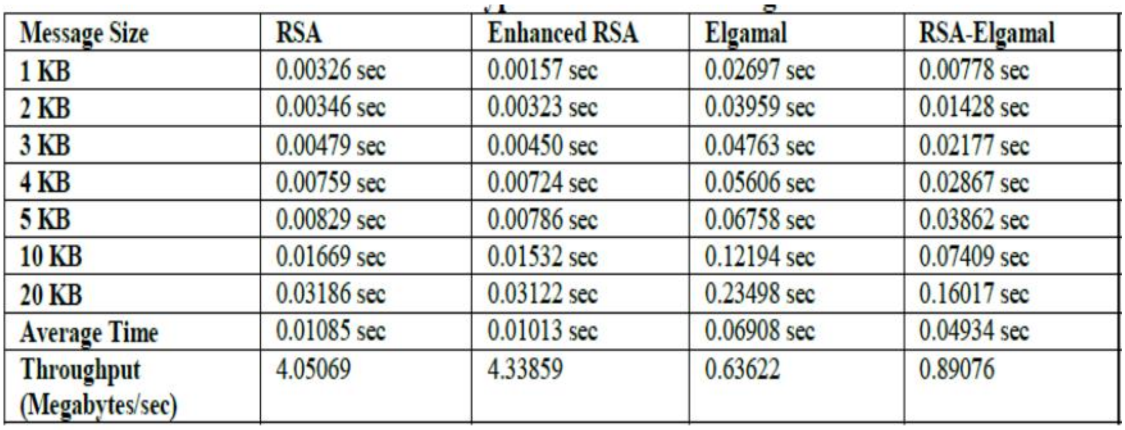
The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

## II. Related work

An encryption scheme based on the integration of Enhanced RSA and Elgamal algorithm is introduced. Enhanced RSA algorithm is based on Integer Factorization Problem (IFP). On the other hand, Elgamal algorithm is based on Discrete Logarithm Problem (DLP). A combination of IFP and DLP is proposed. A comparison has been conducted for different public key encryption algorithms at different data size[5],[6],[9]. The encryption time and throughput of the naive scheme is computed and compared with the hybridized system of RSA and Elgamal algorithm. The aim of this paper is to make the novel algorithm efficient than the existing system as described above. As a result, the proposed algorithm holds an increased throughput and decreased encryption time as compared to the Elgamal and existing hybridized system of RSA-Elgamal.

Key generation, Encryption and decryption are performed in the following way:


KEY GENERATION
Choose 3 prime nos: $p_1$, $p_2$ and $p_3$
Calculate $n = p_1 * p_2 * p_3$
Calculate ø (n) = $(p_1\text{-}1) * (p_2\text{-}1) * (p_3\text{-}1)$
Choose e: gcd (e, ø (n)) =1
$d = e^{-1}$ mod (ø (n))
ENCRYPTION
Choose another prime no $q_1$ and primitive root ‘a’
Choose random integer k : $1< k < q_1\text{-}1$
$K = a^k \bmod q_1$
$C1 = k^e \bmod n$
$C2 = K * M \bmod q_1$
DECRYPTION
$k = C1^d \bmod n$
$K = a^k \bmod q_1$
$K^{-1} = a^{-k} \bmod q_1$
$M = C2 * K^{-1} \bmod q_1$



| Message Size | RSA | Enhanced RSA | Elgamal | RSA-Elgamal |
|---|---|---|---|---|
| 1 KB | 0.00326 sec | 0.00157 sec | 0.02697 sec | 0.00778 sec |
| 2 KB | 0.00346 sec | 0.00323 sec | 0.03959 sec | 0.01428 sec |
| 3 KB | 0.00479 sec | 0.00450 sec | 0.04763 sec | 0.02177 sec |
| 4 KB | 0.00759 sec | 0.00724 sec | 0.05606 sec | 0.02867 sec |
| 5 KB | 0.00829 sec | 0.00786 sec | 0.06758 sec | 0.03862 sec |
| 10 KB | 0.01669 sec | 0.01532 sec | 0.12194 sec | 0.07409 sec |
| 20 KB | 0.03186 sec | 0.03122 sec | 0.23498 sec | 0.16017 sec |
| Average Time | 0.01085 sec | 0.01013 sec | 0.06908 sec | 0.04934 sec |
| Throughput (Megabytes/sec) | 4.05069 | 4.33859 | 0.63622 | 0.89076 |

Fig. 1: Encryption time and Throuput for each method

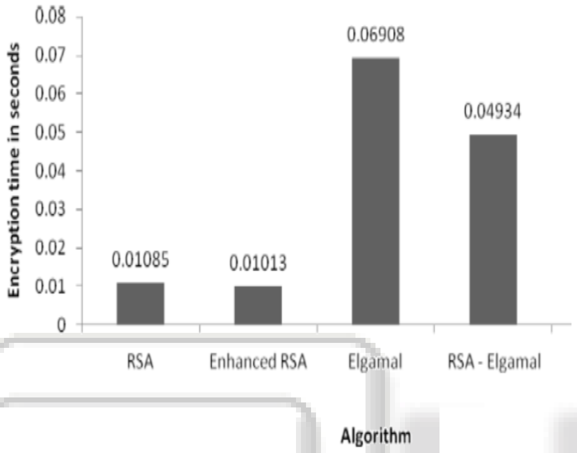


Fig. 2: Encryption time of each algorithm

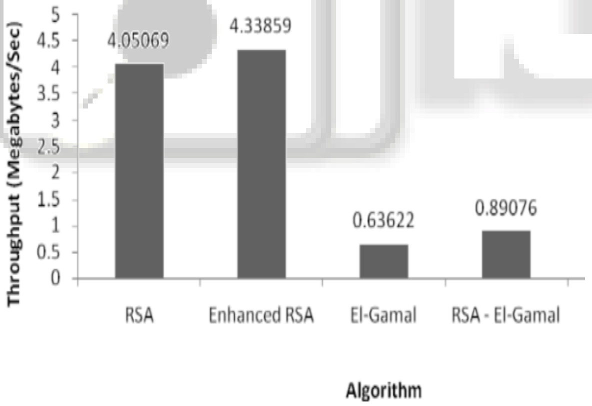


Fig. 3: Throughput of each algorithm

## III. Existing System

The elgamal system is public key Cryptosystem Based on discrete logarithm problem.

It consists of both encryption and signature algorithm.

The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol [6].

### A. *Key Generation:*

Receiver A must do the following:

(1) Generate a large random prime number (p)
(2) Choose a generator number (a)
(3) Choose an integer (x) less than (p-2) ,as secret number.
(4) Compute (d) where

$$d= a^x \bmod p$$

(5) Determine the public key (p, a, d) and the private key (x)

### B. *Generator Number:*

How to test (a) generator or not:

(1) (a) must be between 1 and p-1
(2) Find Ø = p-1
(3) Find the all factors of Ø {f1,f2,….,fn} – { 1 }
(4) (a) is generator number if and only if $wi= a^{Ø/qi} \bmod p\ !=1$ , for all qi

### C. *Encryption:*

Sender B must do the following:

(1) Obtain the public key (p , a , d) from the receiver A.
(2) Choose an integer k such that :
   i. $1 < k < p-2$
(3) Represent the plaintext as an integer m where $0 < m < p-1$
(4) Compute (y) as follows :
   i. $y = a^k \bmod p$
(5) compute (z) as follows :
   i. $z = (d^k * m ) \bmod p$
(6) Find the cipher text (C) as follows:
   i. C= ( y , z )
(7) The sender B sends C to The receiver A.

### D. *Decryption:*

Receiver A must do the following:

(1) Obtain the cipher text (C) from B.
(2) compute (r) as follows :

$$r = y^{p-1-x} \bmod p$$

(3) Recover the plaintext as follows:

$$m = (r * z) \bmod p$$

## IV. Proposed Method

There are many cryptographic methods for encryption and decryption purpose.

AES and DES are algorithms which provide greater security for this purpose.

In our proposed work, we uses a Chinese Remainder Theorem to provide better security and designing Encryption and Decryption algorithm.

### A. *Proposed Algorithm:*

INPUT is:

(1). Keys P and Q.
(2). M (message to be encrypted) and
OUTPUT is:
Secured sending of message from A to B.

*1) Key Generation:*

```
Generate Key()
  {
  Choose P and Q two large prime numbers of the form
  4K + 3 and P != Q
  Calculate N = P * Q
  Public key = N
  Private key = (P,Q)
  }
```

(1) Generate key(B)
(2) Transmit public key to A
(3) Select the message M to be transferred by A to B.
(4) N is the product of two prime numbers in the form that if they are divided by four, the reminder remains 3.
(5) Now A sends a message to B by using the following encryption equation $C = P^2 \bmod N$
(6) At the receiver side B, the decryption is performed. It creates four equally probable plaintexts.
(7) Now B uses P and Q again while generating keys P & Q are private keys for B
$X1 = C^{(P + 1)/4} \bmod P$
$X2 = P - C^{(P + 1)/4} \bmod P$
$Y1 = C^{(Q + 1)/4} \bmod Q$
$Y2 = Q- C^{(Q+ 1)/4} \bmod Q$
(8) Now Chinese remainder theorem is called for generating four equiprobable Plaintexts
P1 = CRT (X1,Y1,P,Q)
P2 = CRT (X1,Y2,P,Q)
P3 = CRT (X2,Y1,P,Q)
P4 = CRT (X2,Y2,P,Q)

Now B choose one of the P1,P2,P3,P4 as the final answer.

## V. CONCLUSION

In future our proposed system can be upgraded for digital signaling which provides better and more efficient cryptographic algorithm than the existing algorithms. So in the proposed system we overcome the problem that arises in the previous system and it has also less time complexity and it more powerful than the existing system.

## REFERENCES

[1] A New Modular Multiplication Method in Public Key Cryptosystem. G.A.V.Rama Chandra Rao1, P.V.Lakshmi2, and N.Ravi Shankar3. s.l. : International Journal of Network Security, 2013, Vols. Vol.15, No.1, PP.23-27.

[2] A New Encryption Scheme Based on Enhanced RSA and ElGamal. Malhotra, Mini. s.l. : International Journal of Emerging Technologies in Computational and Applied Sciences, 2014, pp. 138-142. ISSN (Print): 2279-0047.

[3] "Data encryption standards”. s.l. : FIPS publication, 1977.

[4] A Survey on Various Most Common Encryption Techniques. E. Thambiraja, G. Ramesh , Dr. R. Umarani. 7, s.l. : International Journal of Advanced Research in Computer Science and Software Engineering, 2012, Vols. Volume 2,. ISSN: 2277 128X.

[5] The Elgamel Cryptosystem OVer Circulant Matrices. lanobis, Ayan Maha. 2011, Mathematics Subject Classification.

[6] A New Encryption Scheme Based on Enhanced RSA and ElGamal. Malhotra, Mini. s.l.: International Journal of Emerging Technologies in Computational, 2014. ISSN (Print): 2279-0047.

[7] Rijmen, . Daemen j and.“Rijnadael: the advanced encryption standards”. 2001.

[8] Private Recommendation Based On Elgamal Homomorphic Encryption Scheme. Sapana Borole, Prof. S. B. Javheri. 6, s.l. : International Journal of Advanced Research in Computer Science and Software Engineering, 2014, Vol. 4. ISSN: 2277 128X.

[9] Using El Gamal Cryptosystem in Message Feedback Mode for Computing Cost Reduction. Sohit Kumar, Ashish Vashistha. s.l. : International Journal of Computer Applications, 2013, Vols. 74,No.19.

[10] Stallings, William.“network security essentials”. s.l.: Pearson publication, 2004.