



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

A New Encryption Scheme Based on Enhanced RSA and ElGamal

Mini Malhotra

Department of Computer Science,
Lovely Professional University, Punjab, India

Abstract: 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. 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.

Keywords: Cryptography, RSA, Enhanced RSA, Elgamal, IFP, DLP, Encryption

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 ^[1].

This paper is based on asymmetric cryptosystem and introduces an algorithm based on Enhanced RSA and Elgamal cryptosystem. The Enhanced RSA is based on Integer Factorization Problem (IFP). Enhanced RSA uses three prime numbers to generate the public and the private keys. It enables faster encryption and decryption process and generates the public and the private key faster than the original RSA ^[3].

The Elgamal cryptosystem is based on Discrete Logarithm Problem (DLP) ^[2]. Now days there are many algorithms available to solve the DLP problem of small size numbers within a reasonable time span. To improve the strength of these algorithms, a combination of Enhanced RSA and Elgamal is used. This will provide a higher level of security.

This paper is based on the combination of IFP and DLP to provide a more efficient and secure system than the existing Elgamal and RSA-Elgamal system.

II. RSA and Enhanced RSA

RSA is a public key encryption algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman ^[3]. For signing as well as encryption, RSA was the first known suitable algorithm. Three steps are involved in RSA: Key generation, Encryption and Decryption.

The following are the shortcomings of RSA which are used to break the algorithm, when we use two prime numbers:

- Small encryption exponent, sending the same message to different recipients using a small exponent like $e=4$.
- Same key used for encryption and signing.

Enhanced RSA is based on the RSA algorithm. The RSA algorithm is enhanced using an additional third prime number in the generation of the N . This speeds up the encryption and the decryption process and generates the public and private key faster than the original RSA ^[4].

The steps of Enhanced RSA algorithm are as follows:

A. Generation of Public and Private keys

Following are the steps for the generation of public and private keys:

- Choose three distinct prime numbers p_1, p_2 and p_3 . Multiply them to get ' n '.
- Calculate $(p_1 - 1) * (p_2 - 1) * (p_3 - 1)$ and mention it as $\phi(n)$.
- Select ' e ' as a public key, such that e and $\phi(n)$ are relatively prime.
- Compute $e*d = 1 \pmod{\phi(n)}$ and consider ' d ' as the private key.

B. Encryption Scheme

The message M is encrypted into cipher text C using the public key 'e' such that $C = M^e \bmod n$.

C. Decryption

The cipher text C is decrypted back to its original form M with the help of the private key 'd' such that $M = C^d \bmod n$.

The following are the advantages of Enhanced RSA algorithm over RSA algorithm:

- Increased difficulty of analysis of variable N .
- Faster generation of the keys.
- Faster encryption and decryption process.

III. 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' $\in F_a$.
- Private key 'x' is chosen as a random number such that 'x' $\in \mathbb{Z}_{p-1}$.
- Public key 'y' is computed using the private key 'x'. Therefore, $y = a^x \bmod p$.

B. Encryption Scheme

The sender chooses a random integer $k \in \mathbb{Z}_{p-1}$ and computes one time key $K = y^k \bmod p$. The message M is encrypted into two parts (C_1 and C_2) as $a^k \bmod p$ and $K * M \bmod p$ respectively.

C. Decryption

The cipher text is decrypted as $M = C_2 K^{-1} \bmod p$ using one time key $K = C_1^x \bmod p$.

IV. Proposed Method

The proposed algorithm uses three large prime numbers to generate the public and private keys. The generated public and private keys are then passed to the Elgamal cryptosystem. In this method, we are integrating the IFP and DLP techniques.

The proposed method is an integration of the Enhanced RSA and Elgamal cryptosystem. This method is more efficient than the provenance of RSA, Elgamal and merge between the RSA and Elgamal algorithm^[7].

The working of proposed method is explained as follows:

A. Generation of Public and Private keys

The key generation involves the following steps:

- Choose primitive finite field F_a and a primitive root element 'a' $\in F_a$. Then choose 3 large prime numbers and multiply them to get 'n'.
- Calculate $(p_1 - 1) * (p_2 - 1) * (p_3 - 1)$ and name it as $\phi(n)$.
- Choose public key 'e': $\gcd(e, \phi(n)) = 1$.
- Compute private key 'd' = $e^{-1} \bmod \phi(n)$.

B. Encryption

Choose another large prime number q_1 . The message to be sent is M . Here, the message M will be converted into cipher text in two parts namely C_1 and C_2 . The cipher text is calculated using the one time key K .

The following computations are done at the encryption end:

- Select random integer k such that $1 < k < q_1 - 1$.
- Compute $K = a^k \bmod q_1$.
- Compute cipher text as $C_1 = (k^e \bmod n)$ and $C_2 = (M * K \bmod q_1)$.
- Transmit the cipher text as (C_1, C_2) .

C. Decryption

The cipher text C_1 and C_2 is converted back to its original form M . Decryption of the cipher text is done in the following way:

- Compute $k = C_1^d \bmod n$.
- Calculate $(a^{-k} \bmod q_1)$ and consider it as K^{-1} .
- Calculate $M = C_2 * K^{-1} \bmod q_1$.

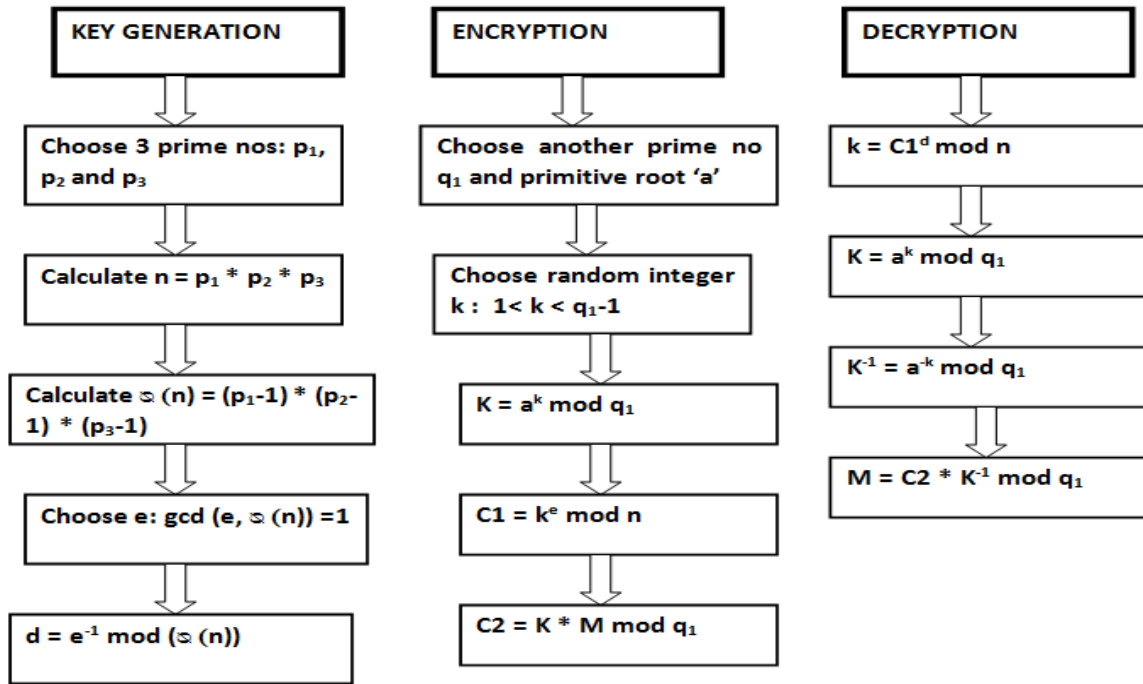


Figure 1. Working of the proposed method

V. Validity of the Proposed Method

A. Encryption Scheme

The message M is encrypted into cipher text C with the help of one time key K , and a primitive root element 'a'.

The cipher text C is computed as:

$$C = M * K \mod n \quad (1)$$

The one time key $K = a^k \mod n$. Therefore, on putting the value of K in (1) we get,

$$C = M * a^k \mod n \quad (2)$$

B. Decryption Scheme

The encrypted text C is decrypted into the original message M with the help of K^{-1} and C such that

$$M = C * K^{-1} \mod n \quad (3)$$

Putting the value of K^{-1} as $M * a^k$ in (3) we get,

$$M = C * a^k \mod n \quad (4)$$

Putting the value of C as calculated in (2), in the above equation (3) we get,

$$M = M * a^k * a^{-k} \mod n$$

On solving this, we will get $M = M$. This proves that the message M is encrypted into C and the encrypted message can then be successfully decrypted back to its original form M .

VI. Results and Discussion

This section will discuss the encryption time and throughput of the proposed algorithm and will compare the results with the RSA, Elgamal and the existing hybridized system of RSA and Elgamal algorithm. All the required keys are generated by the main program. The naive scheme is implemented in Java platform. The encryption time and throughput of the RSA and Enhanced RSA is computed and compared. As a result, the encryption time of Enhanced RSA is less than the RSA. Also, the throughput of Enhanced RSA is better than the RSA. This proves that the Enhanced RSA is better than the RSA. Also, the encryption time and throughput of the proposed algorithm is compared with the existing hybridized system of RSA and Elgamal algorithm. Our proposed system holds better results than the Elgamal and existing merge between RSA and Elgamal. The algorithms are run on different data size.

The throughput is an indication of the speed of encryption. To calculate the throughput of an encryption scheme, encryption time is required. The throughput is calculated by dividing the total plain text in megabytes on the average encryption time in seconds for each algorithm^[8]. The power consumption will be decreased, as the throughput value will increase. Combination of Enhanced RSA and Elgamal is not only used for the generation of an efficient algorithm but also for the generation of a more secure cipher text.

The following table shows the encryption time and throughput of each algorithm.

TABLE I Encryption time and Throughput for each method

Message Size	RSA	Enhanced RSA	Elgamal	RSA-Elgamal	Proposed Method
1 KB	0.00326 sec	0.00157 sec	0.02697 sec	0.00778 sec	0.00678 sec
2 KB	0.00346 sec	0.00323 sec	0.03959 sec	0.01428 sec	0.03959 sec
3 KB	0.00479 sec	0.00450 sec	0.04763 sec	0.02177 sec	0.02046 sec
4 KB	0.00759 sec	0.00724 sec	0.05606 sec	0.02867 sec	0.02867 sec
5 KB	0.00829 sec	0.00786 sec	0.06758 sec	0.03862 sec	0.03422 sec
10 KB	0.01669 sec	0.01532 sec	0.12194 sec	0.07409 sec	0.07227 sec
20 KB	0.03186 sec	0.03122 sec	0.23498 sec	0.16017 sec	0.15899 sec
Average Time	0.01085 sec	0.01013 sec	0.06908 sec	0.04934 sec	0.04766 sec
Throughput (Megabytes/sec)	4.05069	4.33859	0.63622	0.89076	0.92216

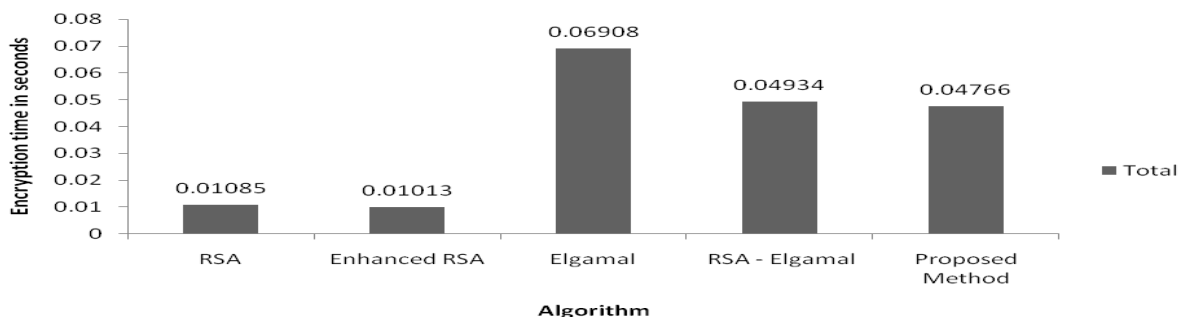


Figure 2. Encryption time of each algorithm

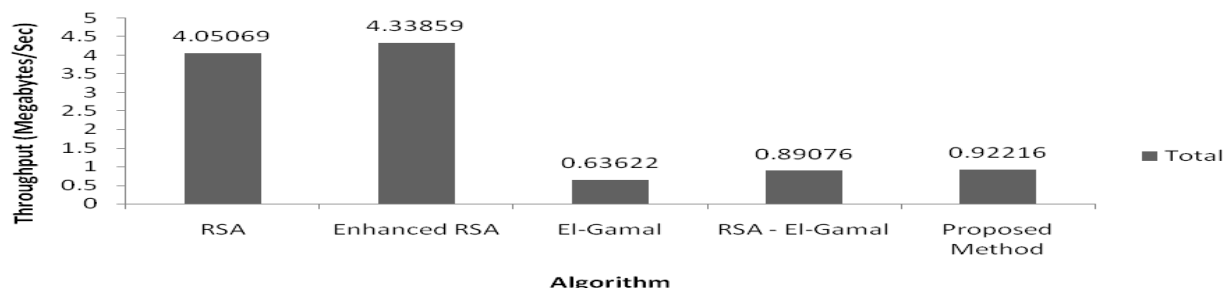


Figure 3. Throughput of each algorithm

Figure 2 shows the average encryption time of each algorithm. It clearly shows that the encryption time of Enhanced RSA is better than RSA. Also, the encryption time of the proposed method is better than the encryption time of Elgamal and the integration of RSA and Elgamal. The throughput of each algorithm is depicted in figure 3. The throughput of Enhanced RSA is better than the throughput of simple RSA. Another point noticed is that the throughput of the integration of Enhanced RSA and Elgamal is higher than that of the Elgamal and the integration of RSA-Elgamal. This leads to high performance of the naive approach. Figure 4 and 5 depicts the encryption time for 1 KB and 5 KB data respectively.

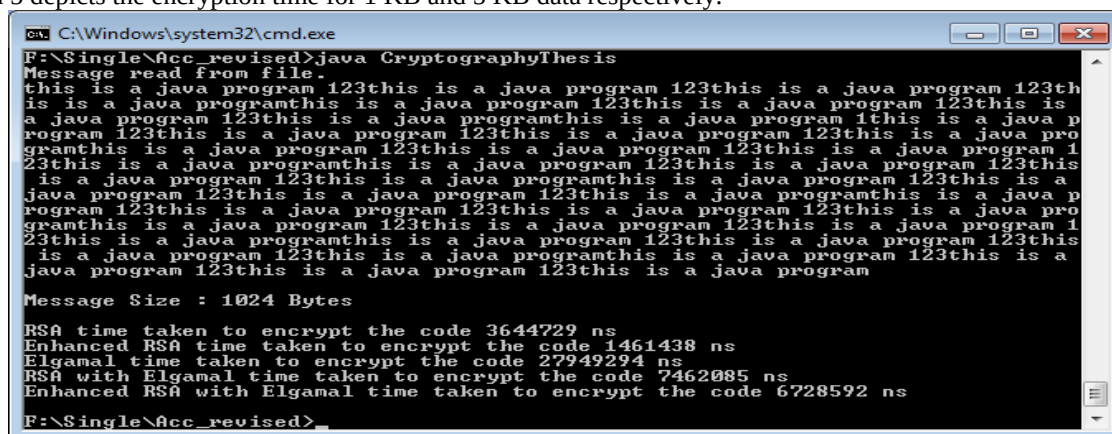


Figure 4. Encryption time of each algorithm for 1KB (in nanoseconds)

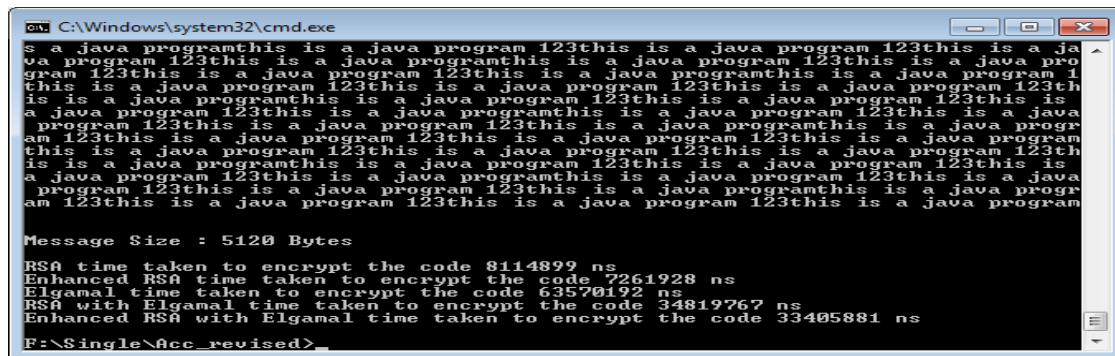


Figure 5. Encryption time of each algorithm for 5KB (in nanoseconds)

VII. Complexity

This section discusses the computational complexity of the proposed method in terms of the big O-notation. The complexity is computed as $O(f(n))$; in terms of some function f .

The encryption of the naive approach consists of the following main steps:

- Generation of one time key, $K = a^k \bmod q_1$.
- Generation of cipher text into two parts $C1$ and $C2$; where $C1 = k^e \bmod n$ and $C2 = M * K \bmod q_1$.

The complexity of the first step is $O(\log n)^3$. The computational complexity of the second step is $O(\log n)^3$ and $O(\log n) + 2 O(\log n)^3$ for $C1$ and $C2$ respectively.

The decryption of the naive approach consists of the following main steps:

- Retrieval of random integer k ($k = C1^d \bmod n$) with the help of $C1$.
- Computation of $K^{-1} = a^{-k} \bmod q_1$.
- Retrieval of original message $M = C2 * K^{-1} \bmod q_1$.

Therefore, the complexity of the first and the second step is $O(\log n)^3$. And, the complexity of the last step i.e. original message M is $O(\log n) + 3 O(\log n)^3$.

VIII. Conclusion and Future Work

In this paper, Enhanced RSA cryptosystem is combined with the Elgamal cryptosystem. The public and the private keys are generated using the Enhanced RSA. These keys are then passed to the Elgamal. A few modifications are also done in the encryption and decryption process; leading to an increased efficiency of our system than the Elgamal and existing hybridized system of RSA-Elgamal. The encryption time and throughput of Enhanced RSA is improved than the RSA. Finally, the encryption time and throughput of the proposed system comes up to be larger than the Elgamal and existing integrated RSA-Elgamal system.

We can sum up the conclusion in the following points:

- Enhanced RSA is better than RSA in terms of encryption time and throughput.
- The proposed algorithm is efficient than the existing Elgamal and integrated system of RSA-Elgamal system.
- The throughput of the proposed system is more than the Elgamal and the existing hybridized system of RSA and Elgamal algorithm, which leads to less power consumption.
- The proposed algorithm is of great use for secure data transmission.
- Encryption time and complexity is a trade-off

Presently, this system is working with the encryption, decryption and throughput. Future work can also be done for the generation of digital signature.

References

- [1] W. Mao, Modern cryptography: theory and practice: Prentice Hall Professional Technical Reference, 2003, pp. 294-296.
- [2] William Stallings, Cryptography and Network Security-Principles and Practice, Fifth Edition, Pearson publication, pp. 259-262.
- [3] Thomas H. Cormen. Charles E. Leiserson. Ronald L. Rivest. Clifford Stein; Introduction algorithms; second edition; 2003;
- [4] Al-Hamami,A.H. ; Aldariesh,I.A., "Enhanced Method for RSA Cryptosystem Algorithm", Proc. IEEE Advanced Computer Science Applications and Technologies (ACSAT), 2012, pp : 402 – 408.
- [5] Al.Hasib,A. ; Haque, A.A.M.M , "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography", Proc. IEEE, Convergence and Hybrid Information Technology, ICCIT'08, 2008, Volume 2, pp : 505 – 510.
- [6] Rashmi Singh, Shiv Kumar, "Elgamal's Algorithm in Cryptography", International Journal of Scientific & Engineering Research,2012, Volume 3.
- [7] Ahmed, J.M. ; Ali, Z.M, " The Enhancement of Computation Technique By Combining RSA and ElGamal Cryptosystems", IEEE Proc. Electrical Engineering and Informatics (ICEEI), 2011, pp : 1-5.
- [8] Diaa Salama Abd Elminaam, Hatem Md Abdual Kader, Mohiy Md Hadhoud, "Evaluating the Performance of Symmetric Encryption Algorithms", International Journal of Network Security, 2010, Volume 10, pp: 213-219.