An Efficient Cryptosystem to Perform Encryption and Decryption of Data

Manila Vishwakarma[1] and Sourabh Jain[2]
[1]PG Student, [2]Assistant Professor, Computer Science and Engineering, Institute of Engineering and Science, Indore Professional Studies Academy, Uttar Pradesh, India

Abstract **- The backbone of the modern world is electronic communication. Data is transferred from one place to another in almost no time using the electronic medium. But it also exposes the confidential data to the intruder. RSA is the most common and efficient cryptography technique that is used for the purpose of encrypting the content and then sending it over the channel, then than at receivers end the content is decrypted and converted in to original form. Although there are many security mechanisms are available. But there is a continuous need to improve the existing methods. Cryptography is a security mechanism which caters the security services of world in perfect manner.**

Keywords: **Network Security, Cryptography, Elgamal Cryptosystem, Two key cryptography, Complexity**

I. INTRODUCTION

The network security becomes more important with the development of various techniques of network development. With the growth in the use of World Wide Web, this has become even more important as the users can access tools and edit the information. While communicating any information via an unsecure channel to its righteous owner, security issue becomes important. To avoid such problem, cryptography and steganography are the main ways of communicating such information in a stealth mode without anyone knowing what it is.

The global society has faced many changes because of the digital revolution. Along with all, this has also increased the number of hackers and viruses. There is a need of a system which can control the curious eyes from getting in a harm way. In such a situation, steganography and cryptography emerge as a savior for such important information [].

With the increase in the content on the web, the increase of viruses and bad eyes in the form of hackers, privacy has become an important issue among many. In such situation, Image Steganography has many important roles and application specially, when two parties want to communicate secretly.

In today's world, security is a major problem especially when it comes to hiding secret information from total strangers. So, converting a message into a form that cannot be easily cracked is an ultimate option for all. Due to the new and improved techniques used by hackers, sharing information on the internet is less secure now a day. To overcome such problems have evolved techniques like steganography and cryptography.

If we uncover the pages of history we find that in those times too, secret information was passed from one party to another via various means like invisible ink, tattoos and much more and that has become the brain child for the present techniques like cryptography where the online secret information sharing has become more secure for parties who have a sensitive information that cannot fall in wrong hands.

A. Cryptography

Cryptography is the art and science of achieving security by encrypting information to make them non-readable format.

B. Basic terms used in cryptography

1. Plain text-Clear text is a readable format or original message understand by any person. For example, if A wants to send a message to B + “Hello” then here “hello” is a plain text message.
2. Cipher text-It is unreadable message or after the encryption the resulting message is called cipher text. For example, “sd45@#$” is a Cipher Text produced for “hello”.
3. Encryption-The process of plain text converts cipher text called encryption
4. Decryption-The process of cipher text converts plain text called decryption.

II. RELATED WORK

Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices has done by D. S. Abdul. Elminaam *et. al.*, (2009) presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points can be concluded from the Experimental results. First; in the case of changing packet size with and without transmission of data using different architectures and different WLANs protocols, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6 [5].

A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms *designed by* S.A.M Rizvi1 *et. al.*, All algorithms run faster on Windows XP. The CAST runs slower than AES for text. Blowfish encrypts images most efficiently on all 3 platforms, even CAST runs faster on Windows XP for image data. But on Windows Vista and Windows7, AES and CAST perform at the similar speed .CAST performs better than BLOWFISH and AES on Windows XP for encrypting audio files, but on Windows Vista and Windows7, there is no significant difference in performance of CAST and AES, however BLOWFISH encrypts audio files at less speed for audio files [14].

ThroughPut Analysis of Various Encryption Algorithms presented by Gurjeevan Singh et al.,(2011)- For experiment a Laptop with 2.20 GHz C.P.U., 4GB RAM Core-2-Dou Processor and Windows 7 Home Premium (32-Bit) is used in which the performance data are collected. In this experiment software encrypts the text file size that ranges from 20 Kb to 99000 Kb. Their implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm. The performance matrices are throughput. The throughput of encryption as well as decryption schemes is calculated but one by one. In the case of Encryption scheme throughput is calculated as the average of total plain text in k bytes divided by the average Encryption time and in the case of Decryption scheme throughput is calculated as the average of total cipher text is divided by the average Decryption time. This work presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. The presented simulation results show the numerous points. Firstly it was concluded that Blowfish has better performance than other algorithms followed by AES in terms of throughput. Secondly 3DES has least efficient of all the studied algorithms [15].

Shashi Mehrotra Seth and her colleague Rajan Mishra (2011) jointly have done a Comparative Analysis Of Encryption Algorithms For Data Communication. The authors analyse the performance of encryption algorithm is evaluated considering the following parameters like Computation Time, Memory usage and Output Bytes, RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm [16].

III. PROBLEM DEFINITION AND RELATIONSHIP TO RELATED WORK

In this section, we define the problem of Elgamal system. The ElGamal system is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol.

The system parameters consist of a prime p and an integer g, whose powers modulo p generate a large number of elements, as in Diffie-Hellman. Alice has a private key a and a public key y, where $y = g^a \pmod p$. Suppose Bob wishes to send a message m to Alice. Bob first generates a random number k less than p. He then computes

$y_1 = g^k \pmod p$ and $y_2 = m \text{xor} y^k$,
wherexor denotes the bit-wise exclusive-or. Bob sends (y_1, y_2) to Alice. Upon receiving the ciphertext, Alice computes $m = (y_1^a \bmod p) \text{ xor } y_2$.

The ElGamal signature algorithm is similar to the encryption algorithm in that the public key and private key have the same form; however, encryption is not the same as signature verification, nor is decryption the same as signature creation as in RSA. DSA is based in part on the ElGamal signature algorithm.

Analysis based on the best available algorithms for both factoring and discrete logarithms shows that RSA and ElGamal have similar security for equivalent key lengths. The main disadvantage of ElGamal is the need for randomness, and its slower speed (especially for signing). Another potential disadvantage of the ElGamal system is that message expansion by a factor of two takes place during encryption. However, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys.

After that there are many variances of ElGamal cryptosystem has been proposed till now some of them are: hashed ElGamal [9], twin ElGamal [12] proposed by cash in 2009 and show if there are groups where the Computational Diffie Hellman hold, but Interactive Diffie Hellman does not hold, in such groups twin ElGamal is secure whereas classical ElGamal is not secure. But it is not known whether such groups exist or not. ElGamal-like cryptosystem proposed by Hwang in 2002 [10], use to encrypt large message by breaking large messages into small messages, whereas original ElGamal PKC is use to encrypt single message and if multiple messages are encrypted using same parameters, system is vulnerable to knownplaintext attack. With some merit in the new scheme, it come with some demerit pointed out by Wang [11].

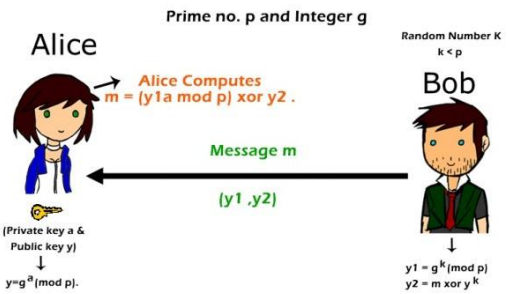

Fig. 1 The ElGamal system

A. Problems in ElGamal System

1. The main disadvantage of ElGamal is the need for randomness, and its slower speed (especially for signing).
2. Another potential disadvantage of the ElGamal system is that message expansion by a factor of two takes place during encryption. However, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys.
3. Not secure against common modulus attack
4. Not secure against known plaintext attack

IV. PROPOSED SOLUTION

The proposed algorithm begins with selection of two prime numbers P and Q. Each of these prime numbers is chosen in such a way that if it is divided by three then remainder remains 3. Public key N is calculated by product of P and Q. private key is a pair of P and Q.

At sender's side, encryption is performed by following encryption function:

$C = M^2 \bmod N$

Where
C is cipher text
M is plain text
N is public key
The cipher text is transmitted from sender's side to receiver's side. At receivers end 4 equi probable plaintexts are found by using Chinese remainder theorem and pair of keys (P and Q).

P1 = CRT (X1,Y1,P,Q)
P2 = CRT (X1,Y2,P,Q)
P3 = CRT (X2,Y1,P,Q)
P4 = CRT (X2,Y2,P,Q)

Then receiver selects one of the plaintext as the final answer.

Algorithm:

The proposed algorithm is as follows:
Input: 1. keys p and q
2. M i.e. message to be encrypted
Output: Secured sending of message from A to B

Procedure:

1. Generate_key(B)
2. Transmit public key to A
3. Select the message M to be transferred by A to B, call it as P
4. N is the product of two prime numbers in the form that if they are divided by four, the reminder remains 3.
   // n used in step 4 is same as n used in generate_ key(B) in step 1
5. Now A sends a message to B by using the following encryption equation
   $C = P^2 \bmod N$
   // This encryption is in $<Zn^*,*>$
6. At the receiver side B, the decryption is performed. The decryption is non deterministic. It creates four equally probable plaintexts.
7. Now B uses P and Q again which was used in step2 while generating keys i.e. P & Q are private keys for B
   $X1 = + C^{(P+1)/4} \bmod P$
   $X2 = - C^{(P+1)/4} \bmod P$
   $Y1 = + C^{(Q+1)/4} \bmod Q$
   $Y2 = - C^{(Q+1)/4} \bmod Q$
8. Now Chinese remainder theorem is called for generating four equi probable
   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)
9. Now B choose one of the P1,P2,P3,P4 as the final answer.

Generate_Key(USER)
{
1. Choose P and Q two large prime numbers of the form 4K + 3 and P != Q
2. Calculate N = P * Q
3. Public key = N
4. Private key = (P,Q)
5. Relim public key and private key
}

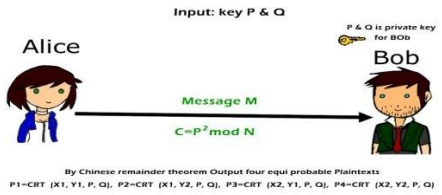

Fig. 2 Proposed Algorithm

V. RESULT ANALYSIS

A. Complexity Analysis of the proposed method

Encryption Complexity : $O(M^2)$, where n is the length of the vector
Decryption: O(M)
Key generation: O(1)

B. Complexity Analysis of Elgamal Method

Elgamal is a hard problem. It takes a lot of time for encryption and decryption. It depends on diffie- hellman. Whose complexity is $O(M^3)$.

TABLE I RESULT COMPARISON

Method	Encryption Complexity	Decryption Complexity
Proposed Method	$O(M^2)$	O(M)
Elgamal method	$O(M^3)$.	$O(M^3)$.

From above it is clear that time complexity of proposed method is less than existing elgamal cryptosystem.

C. Encryption Time Complexity

M is the plaintext, if the size of input/M is 3 then the number of machine instructions executed by elgamal cryptosystem for encryption is 27. Because its time complexity is $O(M^3)$ and number of machine instructions for encryption executed by proposed system is 9. Because its time complexity is $O(M^2)$. It is shown below in graph.

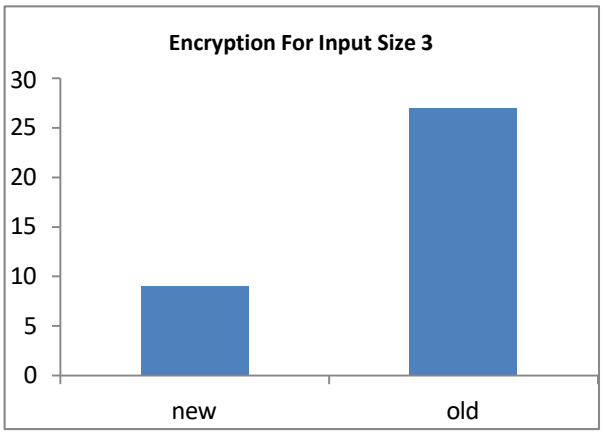

Fig. 3 Time comp lexity (no of instructions executed) comparison for encryption

D. Decryption Time Complexity

M is the plaintext, if the size of input/M is 3 then the number of machine instructions executed by elgamal cryptosystem for decryption is 27. Because its time complexity is $O(M^3)$.
and number of machine instructions executed by proposed system for decryption is 3. Because its time complexity is O(M). It is shown below in graph.

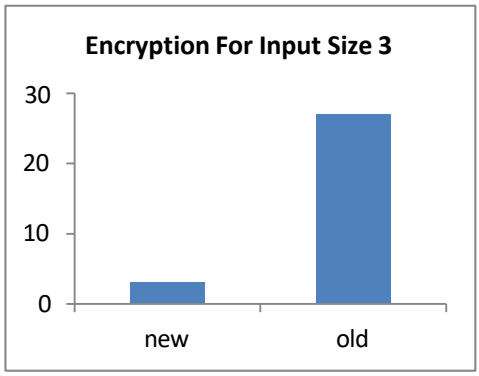

Fig. 4 Time complexity (no of instructions executed) comparison for decryption

V. CONCLUSION

We have elaborated the basic concept of cryptography and the key management schemes. A review of modern methods is also done in brief. The most of the modern data security techniques have been reviewed. Each of the method has been analyzed with the advantages and the disadvantages. Then a list of common problems in the current version has been identified. On basis of the research gap identified, the problem was formulated. Proposed method is having following advantage, encryption and decryption complexity is less in comparison to present system.

VI. FUTURE WORK

Following enhancements can be done in future:

1. The present system works for small scale applications. In future it can be extended for the large scale applications.
2. The proposed algorithm can be extended to handle rich text, audio, video etc.
3. The proposed methodology can be enhanced to work with any key size.
4. The proposed method can be upgraded to perform image encryption in the same efficient manner.

REFERENCES

[1] W. Stallings. *Network Security Essentials (Applications and Standards)*. Pearson Education. 2004.
[2] National Bureau of Standards. *Data Encryption Standard*. FIPS Publication. 46. 1977.
[3] P. Sharma, "Modified Integer Factorization Algorithm using V-Factor Method", *Second International Conference on Advanced Computing & Communication Technologies, IEEE*. 2012.
[4] A Hamami, I. A. Aldariseh, "Enhanced Method for RSACryptosystem Algorithm", *International Conference on Advanced Computer Science Applications and Technologies, IEEE.* 2012.
[5] S A Minaam, M Hatem, A Kader and M M. Hadhoud, "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", *International Journal of Network Security*, Vol. 11, No. 2, pp.78-87. Sept.
[6] V. Rijndael, "The Advanced Encryption Standard", *Dr. Dobb's Journal*. March 2001.
[7] S Mehrotra and R.Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication", *IJCST*, Vol. 2, No. 2. pp. 192-192. June 2011.
[8] S A M Rizvi1, Hussain S Z and N. A Wadhwa, "Comparative Study of Two Symmetric Encryption Algorithms across Different Platforms".
[9] J A. Jose, "Possible Attack on RSA Signature. Research scholar", Sathyabama University. Chennai.
[10] M Abdalla, M Bellare and P. Rogaway, "The oracle Diffie-Hellman assumptions and an analysis of DHIES", In David Naccache, editor, CT-RSA 2001. Vol. 20, of LNCS. pp. 143–158.Springer-Verlag.
[11] M S Hwang, C C Chang and K F. Hwang, "An ElGamallike cryptosystem for enciphering large messages", *IEEE Trans. Knowledge and Data Engineering*, Vol. 2. pp. 445- 446. 2002.
[12] M N Wang, S M Yen, C D Wu and C T. Lin, "Cryptanalysis on an ElGamal-like cryptosystem for encrypting large messages", *Proceeding of the 6th WSEAS International conference of Applied Informatics and communications*. pp. 418-422. 2006.
[13] D Cash, E Kiltz and V.Shoup, "The Twin DiffieHellman problem and applications", 2009.
[14] S A M Rizvi1, S Z Hussain and N.Wadhwa, "A Comparative Study of Two Symmetric Encryption Algorithms Across Different Platforms".
[15] G Singh, A K Singla and K S.Sandha, "Through Put Analysis of Various Encryption Algorithms", *IJCST*. Vol. 2, No. 3, 2011.
[16] S M Seth and R.Mishra, "Comparative Analysis of Encryption Algorithms For Data Communication", *IJCST*. Vol. 2, No. 2. pp. 192-192. 2011.