JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

STUDY ON ENCRYPTION DECRYPTION OF RSA AND ELGAMAL

[1]Seema Kute, [2]Dr. Chitra Desai, [3]Dr. Mukti Jadhav

[1]Research Student, [2]Professor, [3]Assistant Professor
[1]Dept. of CS & IT,
[1] Dr. B.A.M.U., Aurangabad, India

Abstract : The technological developments in the field of computer science has grown exponentially with the growing use of internet in open environment. The communication for various purposes has increased between two parties over internet through various applications on wide range of devices. Most of these communications are require same and encrypted using reliable tools and algorithms. The period before 1970's which relied more on symmetric key cryptographic systems which was used methods in closed network of various government organizations, military etc. started experiencing limitations. These limitations were addressed by public key cryptographic algorithms. These algorithms were based more on mathematical ideas such as integer factorization, discrete logarithms etc. of the various public key cryptographic algorithms, the most trusted and used cryptographic algorithms are those based on integer factorization and discrete logarithms. One such algorithm based on integer factorization is RSA and one based on discrete logarithm is Elgamal. Though today we see there are various modern cryptographic algorithms based on elliptical curve, the fundamental functioning of public key cryptographic algorithms can be best studied using RSA and Elgamal.

This paper studies the encryption decryption process involved in RSA and Elgamal with respect to varying key lengths and time taken for the process. The practical results will be useful to understand the impact of mathematical complexity involved in encryption and decryption process of these two algorithms with respect to time taken in each case.

IndexTerms **- RSA, Elgamal, Result and Discussion.**

I. INTRODUCTION

In this current era we use networking to send information from sender to receiver for this purpose we want to store information securely.[1] Cryptography is the best solution on this. Cryptography is the process to encode the information and make it secure. In our day to day activities like send and receive our secrete emails. ATM card safety, financial transaction process to send and receive our private messages in any form like text, image, audio, and video by using what's app like applications cryptography takes main part. Cryptography is vastly use in various areas due to digitalization process.[2]

There are two types of Cryptographic algorithms --- Symmetric and Asymmetric key Cryptography. Asymmetric cryptographic algorithms are widely known as public key cryptographic algorithms were designed to overcome problems with symmetric key algorithms. There are second public key algorithms which are based on either integer factorization, discrete logarithm, elliptic curves etc. RSA [3] is integer factorization based algorithm while elgamal [4] is discrete logarithm based algorithm. RSA, Elgamal are called public key algorithms because in these algorithms the encryption key is public and can be computed by anyone. Here, the decryption key is private without which it is hard to reverse.

Compared to Elgamal, RSA algorithm has been more popular because of being first of its kind in public key cryptography and may be because of the marketing by commercial compromises. RSA is claimed to be more efficient for encryption from Elgamal or its variants, while, decryption is more efficient in Elgamal variants than RSA [13]

This paper presents experimental results to compare the encryption and decryption time with respect to RSA and Elgamal.

II. LITERATURE REVIEW

RSA algorithm known as the most well liked cryptographic algorithm in network security world.[5] Generally, to find the product of two numbers are easy but from product value to numbers are not easily possible in case of large numbers. The RSA security is totally depends on this base point.[5] The weakness of RSA algorithm is the small size key generation that make it vulnerable but if the key size is increases like 2048 to 4096 bits then this algorithm is very difficult to break because to find out the factors of these numbers are very difficult.[6] Discrete logarithm over a finite field is the base of Elgamal algorithm for performing the encryption and decryption process.[7] ElGamal's drawback is its need for randomness and its slow process.[8] Comparative study of RSA and Elgamal showed that when takes text file of different sizes as input it was described that RSA takes more time for both encryption and decryption process and also uses more memory space while producing small output byte.[9] The Time complexity of RSA during different text encryption

process is good but Elgamal give better result in decryption process[10]. In case of secure file transmission on the basis of key length value, algorithm sort, security threats, pace usability of the model, key usages, energy consumption, hardware or software implementation Elgamal algorithm is more secure than RSA algorithm.[11] When audio(.mp3) file use as input data with different sizes examined time complexity of encryption and decryption process the experimental outcome showed that RSA algorithm is faster than Elgamal algorithm in audio file encryption process.[12]

III. EXPERIMENTAL SETUP

The system utilized during this experiment has 8.00 GB DDR4 RAM, Intel® Core(TM) i5-8265u processor and 1.60GHz-1.80GHz clock speed and implementation is done in Python 3.9.5.

IV. RESULT AND DISCUSSION

3.1 Key Generation

RSA generates six variables (p, q, n, φ, e, d) at the time of key generation. Variables "n" and "e" are keys utilized for encoding and "n," and "d" are keys utilized for decoding. ElGamal generates four variables (p, E1, E2, D) at the time of key generation. Variables "p," "E1" and "E2" are used in the encoding process while variables "p" and "D" are used in the decoding process. The below example shows is RSA as well as ElGamal key generation and encryption and decryption process.

3.1.1 RSA

p = 687998767
q = 951579319
n = p * q = 654685398174699673
φ(n) = (p - 1) * (q - 1)
= 687998766 * 951579318
= 654685396535121588
Select e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 536034049548371329
Calculate a value for d such that (d * e) % φ(n) = 1.
d = (601999670499049825 * 536034049548371329) % 654685396535121588
Public key: (e, n) = (536034049548371329, 654685398174699673)
Private key: (d, n) = (601999670499049825, 654685398174699673)
Message = 54321
Encryption: $c = m^e \bmod n$
$= (54321)^{536034049548371329} \bmod 654685398174699673$
Encrypted Message: 3115191530730265104833096127786447613997883013670124224685855918232867275069205472455830 17
Encryption time is:
0.019562244415283203
Decryption:
$m = c^d \bmod n =$
$(3115191530730265104833096127786447613997883013670124224685855918232867275069205472455830 17)^{601999670499049825} \bmod 654685398174699673$

Decrypted Message: 54321
Decryption time is: 0.042539358139038086

3.1.2 ELGAMAL

p = 961751257
private key(d): 495056703
$E_1 = 15$
R = 312901900
Message(PT)=54321
$E_2 = 116372180$

$C_1 = E_1^R \bmod p$
$C_2 = (PT \times E_2^R) \bmod p$
C_1: 270101390
C_2: 812548098

CT = (C_1 , C_2)
= (1270101390, 812548098)

Encryption Time: 0.050986528396606445

Decrypted Message= 54321

$PT = [C_2 \times (C_1^D)^{-1}] \bmod p$

Decryption Time: 0.016278505325317383

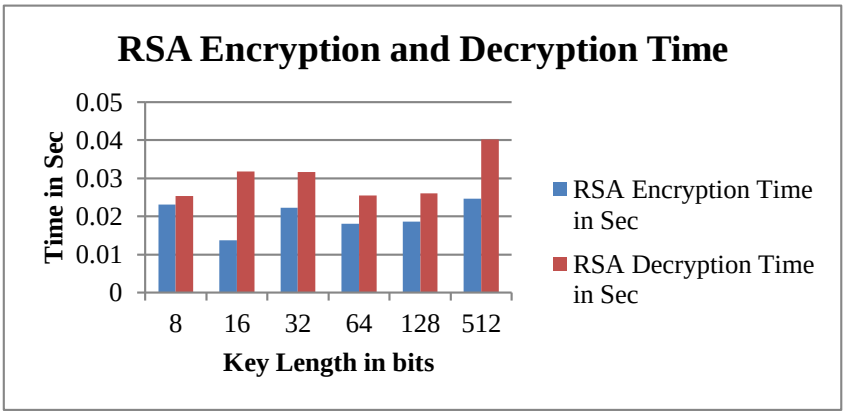

Fig.1 RSA Encryption and Decryption Time

Figure. 1, shows that RSA used less time during the encryption process of various key sizes than in the decryption process of various key sizes.

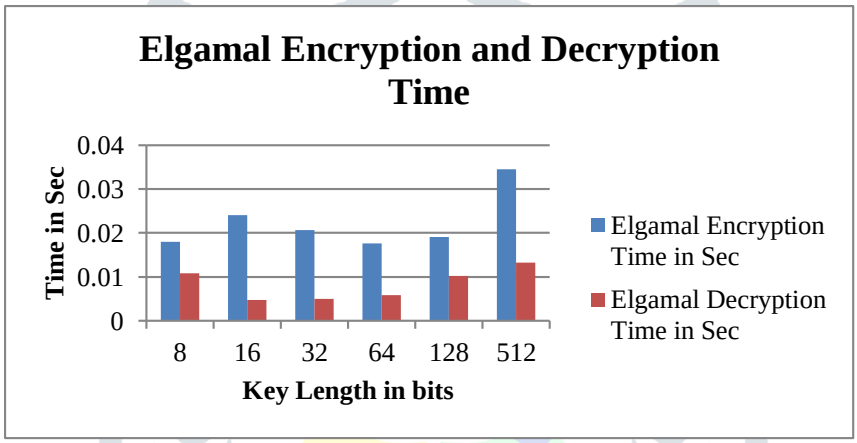

Fig. 2 Elgamal Encryption and Decryption Time

Figure. 2, shows that Elgamal used less time during the decryption process of various key sizes than the encryption process of various key sizes.

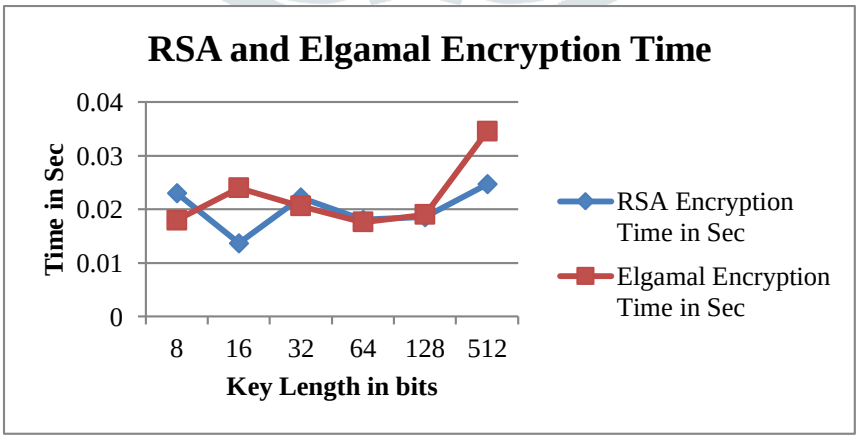

Fig. 3 RSA and Elgamal Encryption Time

Figure. 3, it can be deduced that there is no significant difference between the encryption time used by RSA and ElGamal algorithms in encryption process, but as the key size increases, RSA uses less encryption time compared to the ElGamal algorithm, so that the encryption time increases as the key size increases.

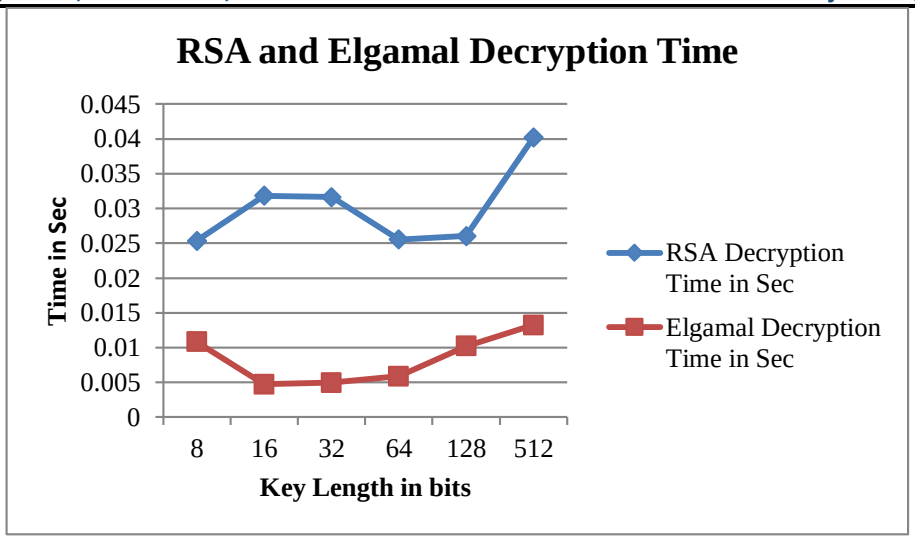

Fig. 4 RSA and Elgamal Decryption Time

Figure. 4, shows that ElGamal used less time in the decryption process of various key sizes, while the time taken by the RSA algorithm in the decryption process is comparatively high.

V. CONCLUSION

RSA and Elgamal are public key cryptosystems based on computationally hard problems. RSA is based on integer factorization and Elgamal is based on discrete logarithm. For the security of a cryptosystem, the length of key is important parameter. It is observed that for RSA and Elgamal almost equivalent security using same key length.

RSA algorithm takes less time for encryption process as compared to decryption process whereas Elgamal algorithm takes more time for encryption and very much less time for decryption process as compared to encryption process time. RSA takes less time for encryption than Elgamal algorithm. However, Elgamal takes less time for decryption than RSA.

V. REFERENCES

[1] Akansha Tuteja, Amit Shrivastava," A Literature Review of Some Modern RSA Variants", IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 08, 2014 | ISSN (online): 2321-0613.

[2] Saranya, Vinothini, Vasumathi," A Study on RSA Algorithm for Cryptography", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5708-5709

[3] D. Kurnia, H. Dafitri, and A. P. U. Siahaan, "RSA 32-bit Implementation Technique," Int. J. Recent Trends Eng. Res., vol. 3, no. 7, pp. 279–284, 2017.

[4] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469–472, 1985.

[5] https://en.wikipedia.org/wiki/RSA_(cryptosystem)]

[6] Kyaw Myo Thu, Kyaw Swar Hlaing, Nay Aung Aung," Time Performance Analysis of RSA and Elgamal Public-Key Cryptosystems", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume 3 Issue 6, October 2019, -ISSN: 2456 – 6470

[7] Rashmi Singh, Shiv Kumar," Elgamal's Algorithm in Cryptography", International Journal of Scientific & Engineering Research Volume 3, Issue 12, December-2012, ISSN 2229-5518]

[8] M. Marwaha, R. Bedi, A. Singh, and T. Singh. "Comparative analysis of cryptographic algorithms". Int J Adv Engg Tech/IV/III/July-Sept, 16,18. 2013.

[9] A. Afolabi, and O. Atanda. "Comparative analysis of some selected cryptographic algorithms". Computing Information Systems, Development Informatics and Allied Research Journal. Vol, 7, 41-52.2016

[10] Farah, Y. Javed, A. Shamim, and T. Nawaz. "An experimental study on performance evaluation of asymmetric encryption algorithms". In Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science, (EECS-12). 2012. (pp. 121-124).

[11] S. Annapoorna, S. Shravya, and K. Krithika. "A review on Asymmetric cryptography RSA and Elgamal Algorithms". International Journal of Innovation Research in Computer and Communication Engineering.Vol. 2, 2014. Special Issue 5.

[12] Z. Tin, and W. Su. "Performance Analysis of RSA and ElGamal for Audio Security". International Journal of Scientific Engineering and Technology Research. Volume.03, issue.11, June-2014, Pages: 2494-2498.

[13]A. Keith M. Martin,"Everyday Cryptography fundamental principles and applications", Oxford University Press 2016.