International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 5, Issue 1, 2018, PP 34-36
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: http://dx.doi.org/10.20431/2349-4859.0501005
www.arcjournals.org

Computational Time of Modified RSA Approach for Encrypting and Decrypting Text using Multi-Power and K-Nearest Neighbor Algorithm (April 2018)

Dr. Vijay Tiwari[1]*, Kumar Shanu Singh[2]

[1]*Supervisor, India.*

[2]*Fellow Centre for Advanced Studies, India.*

Corresponding Author: *Dr. Vijay Tiwari, *Supervisor, India.*

Abstract: *The efficiency of the cryptographic algorithm is generally not based on encryption and decryption time, but also depends upon the numbers of levels used to convert plain text to cipher text. RSA is one of the widely used algorithms of the public key cryptosystem. Since every algorithm has some certain limitations. And sometimes it may be not guaranteed that the cipher text can be fully secured. ASCII characters for representation of text are one of such limitations in the past cryptosystem. To overcome the above-mentioned limitation, an innovative algorithm namely modifies RSA was proposed with K-Nearest Neighbor, in which computational time for encryption and decryption was tabulated. This paper chapter presents the literature survey on the result of above-done experiment and tried to find how encryption and decryption time vary.*

Keywords: *RSA, RSA protocol, cryptography, indexes, public key, private key, Offline storage, prime number*

1. Introduction

Security means keeping your information safe and secure by unauthorized users. It must be prevented from unauthorized access (confidentiality), prevented from any modifications during data transfer (integrity), and always available to authorized persons when needed (availability). In today's era, the various algorithms are present to secure your data. And these algorithms have variation in computational time and complexity. We used modified RSA for public key exchange and K- nearest increase the complexity of encryption and decryption.

2. Methodology Used

We have used a modified form of RSA cryptosystem with 4 prime numbers and K- Nearest Algorithm to increase the complexity and randomness of the algorithm, resulting in more security.

3. Key Generation

Steps for public and private keys generation:

- Make a set of prime numbers PR, which has ‘n’ prime numbers.
- Choose any four prime numbers A, B, C, and D from the set PR.
- Calculate L (product of prime numbers)L=A*B*C*D.
- Calculate Φ (L)Φ (L) = (A−1)*(B−1)*(C−1)*(D−1).
- Calculate J (public key), such that GCD (J, Φ (L)) =1.
- Calculate K (private key), such that K*J mod Φ (L) =1.
- Choose random number N and O.
- Choose two numbers P and Q, such that Q = PJ.

3.1. Encryption

Steps used for encryption of a message:

- The process of encryption encrypts the message character by character.
- Convert the message into their respective ASCII values.
- Calculate 'E' for each individual ASCII value of the message, such that E= $(\text{ASCII VALUE}^{Q/P})^{K}$ mod L.
- Calculate R1, as it encrypts the message and gives back cipher text of given plain text R1 =$(\text{message})^{k}$mod L.
- If the ASCII values and values of R1 come same, then apply K-nearest neighbor algorithm – Choose alternative prime A′ from the set PR.

– Calculate L′ (product of prime numbers)L′ =A ′ *B*C*D.

– Calculate Φ (L′) = (A′ −1)*(B−1)*(C−1)*(D−1).

–Calculate J′ (public key), such that Gcd (J′, Φ (L′) =1.

– Calculate K′ (private key), such that K′ *J ′ mod Φ (L′) =1.

– Calculate R′ 1, as it encrypts the message and gives back cipher text R′ 1 =$(\text{message})^{K'}$ mod L′.

– Loop back the whole process until the ASCII value is not equal to R1 value.

- After that calculate

R2 = (message)*N_1^R mod L.

Verification

H$(\text{m})^{Y}$Y= (R_1^{O} *E_1^R) mod L.

3.2. Decryption

These are the steps used for decryption of a message:

- Calculate plain text back again from cipher text using the equation

H (m) =R_1^{J} modL.

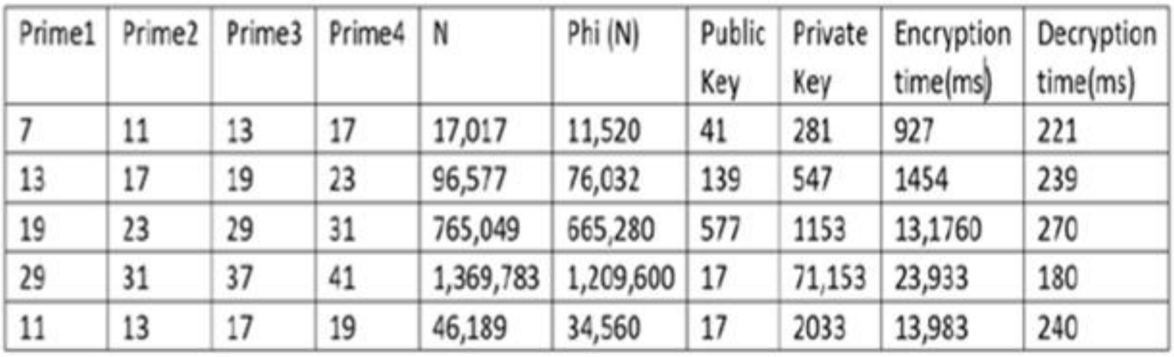
Verification

H $(\text{m})^{Y}$ modL.

4. Simulation Result And Discussion

The proposed algorithm was tested on varying length messages, the performance of the proposed algorithm in terms of encryption time, decryption time along with N, Phi (N), public key, and the private key is shown in Tables 1. We have taken five samples (S1, S2, S3, S4, and S5). In each sample, four prime number was randomly chosen. Encryption and decryption time is calculated following the above-proposed algorithm. Encryption and decryption time was plotted in the Graph (Figs. 1, and 2). Since while looking at the graph it is clear that encryption time of each sample keeps increasing but the decryption time of S3 and S4 was decreasing.

Table1. *Encryption and decryption time using Proposed approach including for Prime numbers*



Prime1	Prime2	Prime3	Prime4	N	Phi (N)	Public Key	Private Key	Encryption time(ms)	Decryption time(ms)
7	11	13	17	17,017	11,520	41	281	927	221
13	17	19	23	96,577	76,032	139	547	1454	239
19	23	29	31	765,049	665,280	577	1153	13,1760	270
29	31	37	41	1,369,783	1,209,600	17	71,153	23,933	180
11	13	17	19	46,189	34,560	17	2033	13,983	240

5. Conclusion And Future Work

The proposed algorithm includes modified RSA with four prime numbers and K- nearest algorithm for encryption and decryption. This modified approach introduced an additional level of security and also enhance the randomness in the cipher text. It also removes the redundancy in cipher text as in plain text. By adopting this, it is very difficult to hack the information being transmitted. It increases the efficiency and security of the approach. One of the conclusions that were missed by the previous researchers was the computational time of this algorithm, we can clearly see that the encryption time was constantly increasing at every sample but the decryption time at sample S3 and S5 was dropping. There was no justification for that.

Future researchers may be directed to investigating how decryption time was decreasing and also further improvement in the algorithm. Future work can also be continued to study the encryption and decryption of characteristics of audio and video files through their proposed algorithm.

References

[1] Mathur S., Gupta D., Goar V., Choudhary S. (2018) Implementation of Modified RSA Approach for Encrypting and Decrypting Text Using Multi-power and K-Nearest Neighbor Algorithm. In: Perez G., Mishra K., Tiwari S., Trivedi M. (eds) Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies, vol 4. Springer, Singapore

[2] M. Thangavel, P. Varalakshmi, Mukund Murrali, K. Nithya, “An Enhanced and Secured RSA Key Generation Scheme”, Department of Information Technology, Anna University, Chennai, 2014, Elsevier.

[3] Amare Anagaw Ayele, Dr. Vuda Sreenivasarao, “A Modified RSA Encryption Technique Based on Multiple public keys”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, ISSN 2320-9798, June 2013.

[4] Norhidayah Muhammadi, Jasni Mohamad Zaini, Md Yazid Mohd Saman, “Loop-based RSA Key Generation Algorithm using String Identity”, 13th International Conference on Control, Automation and Systems (ICCAS 2013). International Journal of Computer Applications (0975 – 8887) Volume 114 – No. 7, March 2015.

[5] Ms. Ritu Patidar, Mrs. Rupali Bhartiya, 2013, “Modified RSA Cryptosystem Based on Offline Storage and Prime Number”, IEEE.

[6] Liang Wang, Yonggui Zhang, 2011, “A New Personal Information Protection Approach Based on RSA Cryptography”, IEEE.

[7] Malek Jakob Kakish, “Enhancing The Security Of The RSA Cryptosystem”, IJRRAS August 2011.

[8] Dr. D.I. George Amalarethinam, J. Sai Geetha, “Enhancing Security level for Public Key Cryptosystem using MRGA”, World Congress on Computing and Communication Technologies, 978-1-4799-2876-7/13/, 2014, IEEE.

[9] Dr. Abdulameer K. Hussain, “A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm”, IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2, Issue 1, ISSN 2348-7968, January 2015.

[10] Xianmeng Meng, Xuexin Zheng, “Cryptanalysis of RSA with a small parameter revisited”, Information Processing Letters 115, 858-862, 2015, Elsevier.

[11] Ritu Tripathi, Sanjay Agrawal, “Critical Analysis of RSA Public Key Cryptosystem”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, ISSN 2277-128X, July 2014.

[12] Shilpi Gupta, Jaya Sharma, “A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman”, International Conference on Computational Intelligence and Computing Research, 978-1-4673-1344-5/12, 2012, IEEE.

Citation: *Dr. Vijay Tiwari & K. S. Singh. (2018)” Computational Time of Modified RSA Approach for Encrypting and Decrypting Text using Multi-Power and K-Nearest Neighbor Algorithm (April 2018)”, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 5(1), pp.34-36. DOI: http://dx.doi. org/10.20431/2349-4859.0501005*