JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Study of Cryptographic Algorithms and its analysis on Data Security during Transmission

Sachin Pandey[1*], Rajendra Gupta[2], Pratima Gautam[3]

[1,2,3]Rabindranath Tagore University, Raisen, India

DOI: https://doi.org/10.26438/ijcse/v7i3.976980 | Available online at: www.ijcseonline.org

Accepted: 05/Mar/2019, Published: 31/Mar/2019

Abstract- The cryptographic cipher is the terminology used for securing the web user data over the network. It is closely related to the discipline of cryptology and cryptanalysis. Using mathematical equations, the cryptography make sure the data when transferred over network is not altered. The important things for the study of mathematical equations on data security, it is almost not possible to break the encryption algorithm without knowing the correct key value. This paper focuses on the study of cryptographic algorithms and its functioning over the data transmission. The throughput is calculated for encryption algorithms during encrypting of text data in different time period and it is found that the Diffie-Hellman Key Exchange Algorithm shows better performance as compared to other studied algorithms.

***Keywords* :** Cryptographic algorithm, Cipher, Diffie-Hellman Key Exchange Algorithm

I. INTRODUCTION

The process of encryption and decryption is called cryptography. It includes techniques such as microdots, merging words with images, and other ways to hide information in storage way. However, in the present information technology, cryptography is most often associated with scrambling of plaintext (ordinary text, sometimes referred to as plain text) into cipher text (a process called encryption) and then reversible process (known as decryption). Individuals who practice this field are known as cryptographers. The classical ciphers work by changing or shifting the plaintext as substitution (replacing each character with another), or by transposition (shuffling the characters from its place). In the present study, the cipher techniques like Substitution, Transposition has been discussed with its functioning and effectiveness on the data security.

II. LITERATURE SURVEY

Several researchers have been worked on the issues of cryptographic network security and suggested different asymmetric and symmetric encryption and decryption algorithms. Chia Long et.al. have given the idea of time-efficient and space-efficient algorithms, such as RSA cryptography and Elgamal cryptography [1]. In RSA cryptography, the encryption and decryption operations are accomplished by modular exponentiation. The study also shows that the fast modular exponentiation algorithms often considered of practical significance in this cryptosystem. Qing Liu et al. aimed at speeding up the RSA decryption algorithm [2]. The implemented algorithm EAPRSA (Encrypt Assistant Multi-Power RSA) was proposed to improve RSA decryption performance by transferring some decryption computations to encryption. The experimental result of this implemented algorithm showed the speed of the decryption has been substantially improved.

Mandal et al. has proposed an algorithm to merge both RSA algorithm &Diffie-Hellman Algorithm to provide data security at a higher level [3]. In the proposed system, they have given focus on to secure data of smaller as well as larger size by obtaining one arbitrarily chosen key pair from the set of RSA keys and a randomly chosen secret key by using Diffie-Hellman algorithm and then applying RSA encryption to make even public components of Diffie-Hellman algorithm inaccessible for any eavesdropper freely. Wang et.al. explained a complete set of practical solution to the file encryption using RSA algorithm [4].

As compared to analysis with the present situation of the RSA algorithm, the author found feasibility of using it for file encryption. The conventional algorithm of RSA by used C++ Class library to develop RSA encryption algorithm and they have realized Groupware encapsulation with a 32-bit windows platform. Silva et al. suggested a very simple and direct algorithm for encryption [5]. The proposedmethod only applied to the product of two different but equalsized primes. This algorithm needed a little bit memory to execute the operation. Geethavani proposed a modified blowfish algorithm for converting the text in cipher and resultant cipher text was embedded into a cover audio file by using discrete wavelet transform [6]. This audio file was transmitted to the receiver and the reverse process was done to get back the same plain text. The method was based on the steganographic technique along with the cryptographic scheme which has improved the security of the algorithm.

Nagar et al. proposed an algorithm to speed up the RSA algorithm functioning during data transmission between networks which is calculated to generate the security keys and after that save the values of keys in the defined databases [7]. In this research paper, a method was applied to exchange the values of security keys between gateways that contain values of public and private keys that were defined in tables inside of database. Chong Fu et al. has given the idea that RSA is most widely used in e-commerce applications [8]. The complexity of large integer operation was considered the main factor which affects efficiency of RSA. In this paper, a carry array approach was proposed to speed up the large digit calculation in RSA key generation and data encryption/decryption process is used to improve the efficiency of a RSA algorithm. The mathematics applied for RSA was discussed in detail and then feasibility of RSA algorithm was proved [10].

III. OVERVIEW OF CRYPTOGRAPHIC ALGORITHMS

Some of the cryptographic algorithms are discussed herewith with its functioning [11-15].

- **Shift Cipher**

In cryptography, a shift cipher technique is one of the easiest and most widely used encryption techniques. It is a type of substitution cipher in which each letter of the plaintext is shifted from its position by a letter or some fixed number. For example, by shifting alphabets with three letters (known as the Caesar Cipher), i.e. A would occupy letter D, B would become E, and so on. This transformation of letters can be represented by aligning the plaintext alphabet on the top of ciphertext alphabet. The following table shows the shifting of alphabets and forming cipher text.

The above mentioned process can be represented mathematically with the formula -

$$y = (x + k)\ mod\ 26$$

and after applying function notation, the above equation becomes -

$$f(x) = (x + k)\ mod\ 26$$

where x and y are integers and k is key.

- **Affine Cipher**

Since the Shift Cipher offer very less security and another problem is that the letter substitution or shifting are not mixed up enough. A scheme of Affine Cipher is proposed in which the multiplication is combined with addition, modulo m, where m is an integer, to create more options of substitution. The Affine cipher is simply a case of mono-alphabetic substitution cipher.

The Affine Cipher key uses an ordered pair of letters, suppose (a, b). While selection of security key, it is important to keep in mind the following restrictions; $a \neq 0$ and b should be chosen from the integer number 0, 1, 2, 3, …,m-1 and the letter $a \neq 0$ should be relatively prime to m. It means that a should have no factors in common with m. Suppose that a 26 character alphabet (i.e. $m = 26$) is used in which 15 and 26 have no factors in common. So we can say the number 15 is an acceptable value for a. But if we choose 12 for the value of a then it would not be a acceptable number because 12 and 26 have common factors, which is 2.

The Affine Cipher is a cipher system in which plaintext letters are enciphered using mathematical equation, which can be written as-

$$y = (ax + b)\ mod\ m$$

and the above equation using function notation can be written as -

$$f(x) = (ax + b)\ mod\ m$$

where x = numerical equivalent of the plaintext letter and m = number of letters in the alphabet

- **Transposition Cipher**

The transposition cipher is one another kind of cipher technique in which Instead of replacing characters with other characters, it just change the order of the characters. Generally, the text to be encrypted is set in a number of columns. These columns are again reordered and produce encrypted text. Here to decrypt a ciphertext using a transposition cipher, we need to find the number of columns and then rearrange the columns according to that.

Suppose the phrase is “WE ARE DISCOVERED FLY AT ONCE” – and add a bit of padding (random characters) to the end to make each column equal.

W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	Y
A	T	O	N	C	E
Q	K	J	E	U	

Now, each column can be converted vertically to create the cipher text. In this way, we can reach at a relatively secure cipher text.

- **Elliptic Curve Cryptography**

The Elliptic Curve Cryptography (ECC) is a type of public key cryptography. In public key cryptographic system, each user taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to perform the encryption and decryption. Private Key is known by only the particular user whereas the public key is distributed to all the users those who are taking part in the communication. As compared to Private Key Cryptography, the Public key cryptographydoes not require any shared secret between the communicating parties. But this cryptography is much slower than the private key cryptography.

In ECC algorithm, an elliptic curve is formed which is a set of points that satisfy a specific mathematical equation. The form of the equation is as given below :

By using elliptic curve, a number ‘d’ is generated within the range of ‘n’. Using the following equation user can generate the public key –

$$\mathbf{Q = d * P}$$

Where d = Random number used as private key and it is selected within the range of (1 to *n*-1). ‘P’ is any point on the curve and ‘Q’ is the public key.

- **Diffie-Hellman Key Exchange Algorithm**

Diffie and Hellman have invented an algorithm in the year 1976 which describe a means for two parties to agree upon a shared secret key such that the secret information should not be available to eavesdroppers. Diffie-Hellman is a mathematical algorithm that allows two computers to produce an identical shared secret on both systems; even both systems never have communicated with each other. This shared secret can be utilized to safely exchange a cryptographic encryption key.

The simple mathematical procedure and the original implementation of the system use the multiplicative group of integers modulo *p*, where *p* is prime number and *g* is a primitive root modulo p. Following is the steps for sharing of data with key between two user ‘A’ and ‘B’.

i. ‘A’ and ‘B’ are agree on a prime number *p* and a base *g*.

ii. ‘A’ chooses a secret integer *a* and sends it to ‘B’

$$A = g^{a}\text{mod } p$$

iii. ‘B’ chooses a secret integer *b*, and sends to ‘A’

$$B = g^{b}\text{mod } p$$

iv. ‘A’ computes

$$K1 = B^{a}\text{mod } p$$

v. ‘B’ computes

$$K2 = A^{b}\text{mod } p$$

vi. ‘A’ and ‘B’ now share a secret data, both ‘B’ and ‘A’ can use this number as their key.

IV. RESULT AND DISCUSSION

After analysis of various cryptographic cipher techniques proposed earlier by many researchers, it is found that the cryptanalysis is very much needed for securing the web user data over the network. By applying already proposed algorithms of cipher over the users data, almost same result is found and by applying same algorithm over different types of data items, the algorithms has performed differently.

As compared to the study in [9] is done for the different security algorithms such as Blowfish, RC, DES etc. the present work has been analysed. The implementation and the performance is compared by encrypting input files of various contents and data sizes. The algorithms were tested on 2 different computers having same configuration, to compare the performance of algorithms. They configuration of two different machines was; P-V28 GHz processing power and 1 GB RAM. The results showed that Elliptic Curve Cryptography and Diffie-Hellman Algorithm had a very good performance as compared to other discussed algorithms. Also it is noticed that the Diffie-Hellman Algorithm had a better performance than Elliptic Curve Cryptography.

The analysis of the studied algorithms can be compared on various parameters like Encryption Time, Throughput, CPU speed for computing encryption speed, and transmission time. In the present work, we have calculated the performance on the basis of throughput of encryption. The *throughput* is a measure of how many units of information a system can process in a given amount of time.

The throughput of the encryption scheme is calculated as per for following equation :

$$\text{Throughput of encryption} = \frac{\text{Total Plain Text (TPT)}}{\text{Encryption Time (ET)}}$$

Fig. 1 : Throughput of Encryption Algorithms to encrypt various text data (Mb/Sec)

Diffie-Hellman is an interactive protocol with the aim that two user can compute a common secret message which derive a secret key usually used for symmetric encryption schemes. However, the algorithm is safe against passive eavesdropping but the weakness of the algorithm is that it is not necessarily protected from active attacks. Some of the limitations found for this algorithm like (a) no identity of the parties involved in the exchange of data (b)it is easily susceptible to man-in-the-middle attacks (c) third party can exchange keys with both A and B (d) it takes enough time to compute the keys (e) algorithm is not suitable for encrypting the messages.

On the other hand, Elliptical Curve Cryptography is a method of encoding data files such that only specific user can decode the data file. This algorithm is full based on mathematics of elliptic curves. The algorithm denotes the location of points on an elliptic curve to encrypt and decrypt the message. The ECC algorithm is very much successful in secure electronic mailing and web browsing but it has some disadvantages as compared to other cryptography techniques. One of the main disadvantages of this algorithm is that it increases the size of the encrypted message significantly more than other encryption algorithms. The advantages of the algorithms are (a) it is faster (b) since there is no key transmitted with the messages; the chances of data being decrypted not possible (c) a system which possesses the secret key can decrypt a message.

V. CONCLUSION

To protect or secure the user data over network, a number of cryptographic mathematical algorithms have been proposed and implemented at various applications where security is important. A number of governmental organizations of different countries are using these securities algorithms for protecting their confidential and sensitive data. Both types of cryptography (symmetric and asymmetric, having public, private and secret key) have their advantages and disadvantages. A combination of these two methods generates appropriate results in the system. For the personal use of the user, data is encrypted using private and secret keys while other types of activity such as e-mail, public and private keys are used.

Using mathematical equations, the cryptography make sure the data when transferred over network is not altered. The important things for the study of mathematical equations on data security, it is almost not possible to break the encryption algorithm without knowing the correct key value. A number of cipher algorithms are studied with practical example.

The analysis of the studied algorithms can be compared on various parameters like Encryption Time, Throughput, CPU speed for computing encryption speed, and transmission time. In the present work, we have calculated the performance on the basis of throughput of encryption. The results show that Elliptic Curve Cryptography and Diffie-Hellman Algorithm have a very good performance as compared to other discussed algorithms. Also it is observed that the Diffie-Hellman Algorithm has a better performance than Elliptic Curve Cryptography.

Classical encryption schemes like substitution and transposition ciphers are no longer widely used for current network security applications. After study, it is found that these methods are so weak and time consuming if operated over bulky messages.

REFERENCES

[1] Chia Long Wu, Chen HaoHu,"Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application", Innovations in Bio-Inspired computing and Applications(IBICA), 2018, pp. 307 – 311.

[2] Qing Liu, Yunfei Li, Lin Hao, "On the Design and Implementation of an Efficient RSA Variant", Advanced Computer Theory and Engineering (ICACTE), 2017, pp.533-536.

[3] Mandal, B.K., Bhattacharyya, Bandyopadhyay S.K., "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm", Communication Systems and Network Technologies (CSNT), 2017, pp. 453 – 461.

[4] Wang, Suli, Liu, Ganlai, "File encryption and decryption system based on RSA algorithm", Computational and Information Sciences (ICCIS), 2016, pp. 797 – 800.

[5] Da Silva, J.C.L, "Factoring Semi primes and Possible Implications for RSA", Electrical and Electronics Engineers in Israel (IEEEI), 2016, pp.182–183.

[6] Geethavani, B., Prasad, E.V. Roopa, R. "A new approach for secure data transfer in audio signals using DWT", Sept 2016, pp. 1-6.

[7] Nagar, S.A., Alshamma, S., "High speed implementation of RSA algorithm with modified keys exchange", Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp. 639 – 642, 2016.

[8] Chong Fu, Zhi-liang Zhu, "An Efficient Implementation of RSA Digital Signature", Wireless Communications, Networking and Mobile Computing, Oct. 2016, pp.1-4.

[9] DiaaSalama, HatemAbdual Kader, MohiyHadhoud "Studying the Effects of Most Common Encryption Algorithms, International Arab Journal of e-Technology", Vol. 2, No. 1, January 2017

[10] Turki Al-Somani,Khalid Al-Zamil, "Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems", vol. 4, issue – 6, 2015, pp. 34-45

[11] Hongwei Si, YoulinCai, Zhimei Cheng, "An Improved RSA Signature Algorithm Based on Complex Numeric Operation Function", Challenges in Environmental Science and Computer Engineering (CESCE), 2016, pp.397–400.

[12] Wenxue Tan,Wang Xiping, Jinju Xi, Meisen Pan, "A mechanism of quantitating the security strength of RSA key", Electronic Commerce and Security (ISECS), 2015, pp. 357 – 361.

[13] Dhakar, R.S. Gupta, A.K. Sharma, P., "Modified RSA Encryption Algorithm (MREA)", Advanced Computing & Communication Technologies (ACCT), 2015, pp. 426–429.

[14] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms", International Conference on Information and Communication Technologies, 2015, pp. 219-232.

[15] Li Dongjiang,Wang Yandan, Chen Hong, "The research on key generation in RSA public- key cryptosystem", 2016, pp. 578–580.