International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

End-to-End Encryption Techniques

Kartik Giri[1], Namit Saxena[2], Yash Srivastava[3], Pranshu Saxena[4]

[1-4]*Department of Computer Science and Engineering, Inderprastha Engineering College, Ghaziabad, India*

Abstract - *Encryption manages the security of the information over a specific network. In the ongoing world there are numerous applications that assists with moving data and information over various systems which consequently urges the inclination to think about the security of our information.*

In the course of the most recent decade these encryption strategies have experienced some extreme assessments where the top long range interpersonal communication organizations were addressed. Therefore, it is imperative to know about the significance of the End-to-End encryption strategies and methods of their executions. In the race of innovation, one should not ask about 'Which one is the Best' in light of the fact that new and propelled variants and techniques are here every day. Henceforth, the paper puts together the brief highlights of various End-to-End Encryption techniques.

1. INTRODUCTION

Cryptography is a field of study and it is more broad in nature which uses a digital signature to secure digital data. Cryptography is usually stated to as the study of secret while nowadays it is very much close to the definition of encryption. Encryption is an element of cryptography. It is more of a mathematical process. It consists of only encoding the message. Encryption of data is known for shielding information from the snooping.

The encryption process transforms a given data into a pointless data (called cipher text) with the help of some cryptographic algorithms. It helps to facilitate secret messaging. It is utilized by algorithms like cipher to encrypt digital data. This new message is totally different from the original old message therefore, any hacker cannot read it so easily. It is usually done using key algorithms.

Encryption can help to protect your non-shareable personal data like passwords and pin numbers etc. It helps us to ensure that the data or message has not been altered. The encryption process also safeguards us by protecting our IP. It is a vital method which actively protects the data that you do not want to be accessed by unauthorized party.

It is theoretically possibility to break encrypted systems but it is not viable to do so by any known applied means. The growth of cryptosystem technology has put it under some questionable circumstances. There are way too many goals these day to day messengers cover, but the cybersecurity is still a great risk for all of them.

The objective is "end-to-end" encryption that could be elucidated on an example: you send a message, it gets encoded on your device and is sent to the server that brings it to the final receiver (e.g. your friend's device). Now, decoding happens only on receiver's system, certifying he is the only one to read your conversation. This research paper discusses the enactment of advanced encryption algorithms and researches related to their properties and characteristics.

2. REVIEW OF LITERATURE

a.) Rivest Shamir Adleman Algorithm

Rivest, Adi Shamir and Leonard Adleman of MIT are the designers of the RSA cryptographic algorithm in 1997. It was first portrayed in 1978. This renowned security framework is made out of three stages, which are, Prime Key generation, Encryption and Decryption. In this procedure we utilize RSA cryptosystem calculation. In which we have the private key and public key.

The public key is used to encrypt the messages only and it is open and can be used or seen to all. Therefore, it is not a secret key. The private key is utilized to decrypt the messages. The private key is also called as secret key. In this strategy we take 'n' prime number which is not easy to crack and cannot be disintegrated easily.

This method gives more effectiveness and unwavering quality over the systems. In this paper we have utilized a changed RSA cryptosystem calculate on to deal with 'n' prime numbers to give security. Two techniques are used. Firstly, the encryption strategy which is utilized to change over unique (plain content) information to cipher text which is unreadable content.

The plain content is easily pursued by anybody. Second procedure is decryption or unscrambling which is used to change over cipher text content to plain text (intelligible format). Cipher content is unreadable content i.e. opposite to plain text.

The following is the flow chart for RSA algorithm:

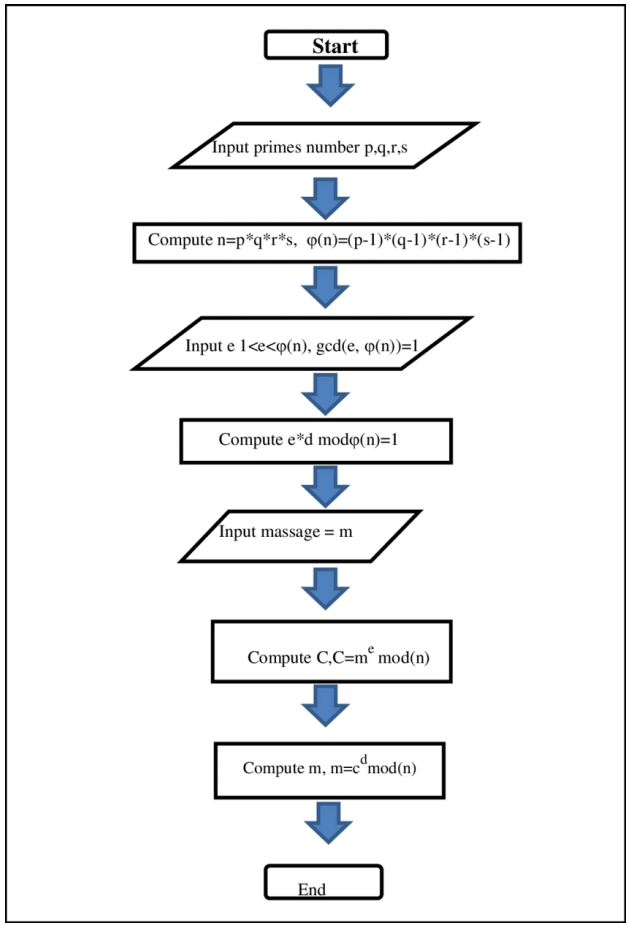

Fig - 1: The Flow Chart

1) How to Use the Keys for Encryption

Consider a sender "A" that needs to send a message to a recipient "B", the sender will make the following procedures: -

i.) Obtains the beneficiary B's open key (e, n)

ii.) Represents the plaintext message as a positive number M.

iii.) Computes the cipher text C = M e Mod n.

iv.) Send the cipher text C to B.

2) How to Use the Keys for Decryption

For the recipient "B" to receive the message sent by the sender "A", the recipient will take the following steps: -

i.) Uses the private key (n, d) to compute

M = Ce Mod n

ii.) Extracts the plaintext from the integer representative M.

This is actually the smallest possible value for the modulus n for which the RSA algorithm works.

b.) DNA Fractal-based Image Encryption

At present, DNA cryptography-based picture encryption has become a hot research field. DNA cryptography [2] is another conceived cryptography, where DNA is utilized as data transporter and the cutting edge organic innovation is utilized as usage instrument, and the tremendous parallelism, outstanding vitality productivity and remarkable data thickness intrinsic in DNA atoms are investigated for cryptographic purposes, for example, encryption, authentication, signature, etc.

The principle security premise relies upon the limitation of biotechnology, which has nothing to do with computing power. For instance, Clelland et al. [3] proposed a methodology dependent on smaller scale spots. In this methodology, the analysts delivered artificial DNA strands, which contained mystery messages. A triplet encodes one character or number. It is a basic replacement figure which encodes characters into DNA sequences.

Leier et al. [4] encoded double data into DNA groupings. A short DNA arrangement represents 1, another is 0. They tie straightforwardly to the corresponding binary data. Qiang Wong et al. [5] introduced another methodology, which can store data in living life forms. The information is converted into a DNA arrangement which is embedded into a vector.

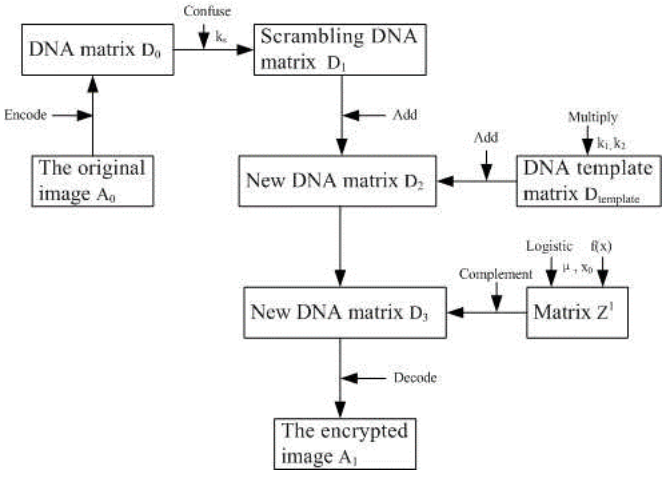

Fig - 2: The Flow Chart

This methodology isn't the one dependent on the genuine DNA cryptography, however utilizes the characteristic DNA sequences as the secret keys. The principle security premise relies upon the assortment of DNA sequence, since the common DNA succession is the regular one-time cushion. The permutation process is actualized by utilizing Hao's fractal succession portrayal [6] in particular. This approach is practical and compelling as per the performance investigation and the performance examination.

c.) Triple DES

The Triple DES algorithm was required as an advancement for DES algorithm because of advances in searching of key [7]. The algorithm utilizes three rounds of DES algorithm for encryption process which has a key length of 168 bits i.e. (56 * 3). Either a few 56-piece keys are used in the arrangement for Encrypt-Decrypt-Encrypt (EDE).

First choice is to use three distinct keys for the encryption calculation to create cipher message on plaintext message t.

$$C(t) = Ek1(Dk2(Ek3(t))) \quad (1)$$

where C(t) is the figure content of plaintext message t, Ek1 is the encryption technique utilizing key k1, Dk2 is the unscrambling or decryption strategy using the key k2 and Ek3 represents the encryption strategy using key k3. Another alternative is to use two distinct keys for the encryption calculation which in turn uses low memory for keys in working of algorithm.

$$C(t) = Ek1(Dk2(Ek3(t))) \quad (2)$$

TDES with three keys requires 2168 potential mixes and that of two keys requires 2112 potential mixes which is difficult for powerful attackers to guess and is nearly impractical. This gives TDES as a most grounded encryption algorithm which provides its application in banking industry. The weakness of this calculation is that it is too tedious [8].

d.) Two-fish Encryption Algorithm

Two-fish is a symmetric key algorithm which entails that encryption and decryption can be done by using only one key. The block size of this encryption algorithm is 128 bits and can take key of any length of up to 256 bits. It tends to be used in the applications where there is no RAM or ROM accessible and where the keys are adaptable which implies the keys are oftentimes changed.

It has a straightforward and adaptable plan with 128-bit Feistel network. Twofish has something many refer to as "pre-brightening" and "post-brightening" in which extra subkeys are XORed into the content block both before the first round and when last round is over.

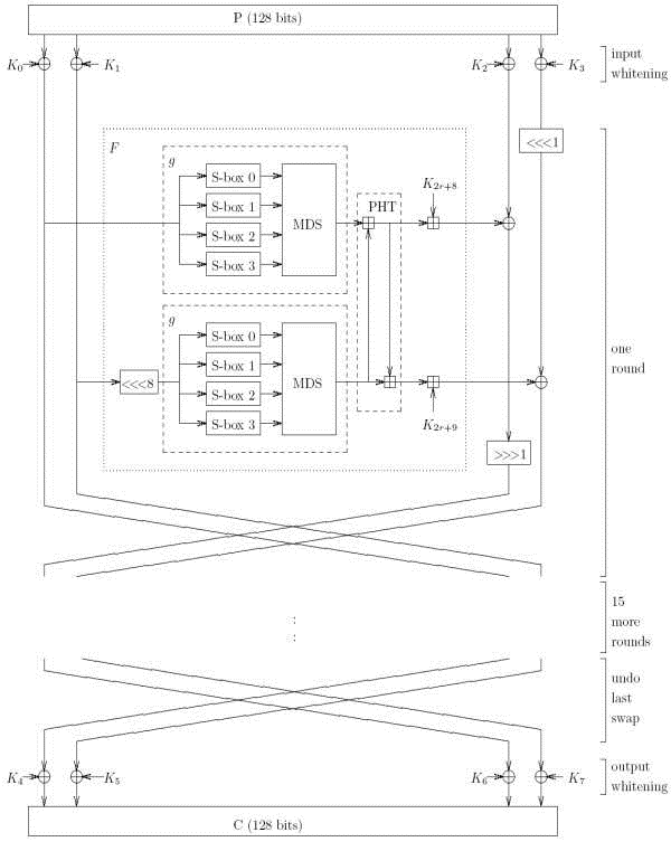

Figure 1: Twofish

Fig - 3: *Block Diagram of Twofish*

The plain content experiences input brightening or pre-brightening before the first round and afterward it experiences different phases of S-Boxes, MDS lattices and PHT. After a few rounds, it experiences yield brightening or post-brightening. After every one of these stages and a few adjusts, a cipher text is produced. In brightening, both input and output information are XORed with eight subkeys.

These XORed activities are called input brightening or pre-brightening and yield brightening or post-brightening. [9] In input brightening or pre-brightening, the partitioned four bytes word is XORed with the 128-bit key through key scheduler. The XORed blocks are currently passed in rounds. In each round, the content block is broken into two halves.

The first half is sent over the F function and the other portion of content block is XORed with it. In each round of Twofish, two expressions of 32 bit each go about as a contribution to the F function. Each word is then divided into four bytes and those words are sent to the four distinctive key reliant S-boxes.

The four output bytes are joined with the help of a Maximum Distance Separable (MDS) grid and consolidated into a 32-bit word. At this point the two 32-bits words are unified by applying Pseudo-Hadamard Transform (PHT), added to two round subkeys, at that point XORed with the other half of the content. [10].

Formulae for PHT:

a0 = a + b Mod 232 (3)

Key-reliant S-boxes are not chosen arbitrarily as they were get selected in blowfish calculation. Rather, the S-boxes are deliberately structured and tried with every single imaginable keys to affirm that all the developed S-boxes are sufficient.

e.) Keyed-Hashed Message Authentication Code (HMAC)

HMAC is a mix of hashing and cryptography. It uses secured hash functions and secret key cryptography. It tends to check the information integrity and realness of a message all the while. Any hashing calculation, for instance, SHA-1, SHA-2, SHA-

256 can be utilized to figure the HMAC. The quality of the HMAC calculation relies upon the quality and size of hash function and that of the key.

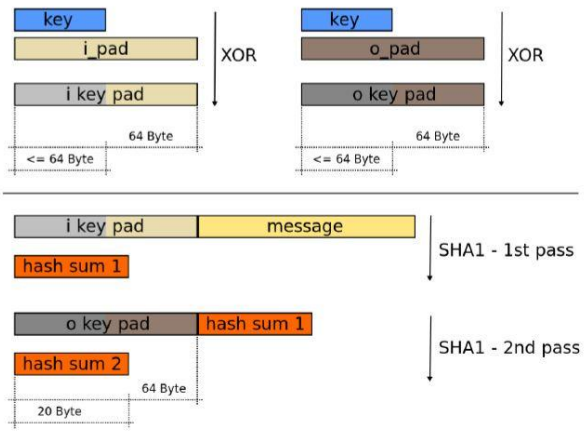

Fig - 4: HMAC-SHA1 Generation

This calculation uses two rounds to calculate the hash. The unknown key is used to calculate the two keys called as inner key and outer key. In first round, the inner key and message is used to process the inner hash. At that point in second round, the inner hash and the external key is used to deliver the HMAC code.

The HMAC can be defined as:

Where,

H is cryptographic hash function,

M is the message to be authenticated,

$$\mathrm{HMAC}(K,m) = \mathrm{H}\left((K' \oplus opad) \parallel \mathrm{H}\left((K' \oplus ipad) \parallel m\right)\right)$$

$$K' = \begin{cases} \mathrm{H}(K) & K \text{ is larger than block size} \\ K & \text{otherwise} \end{cases}$$

K is the secret key,

K' is a block-sized key derived from the secret key,

|| denotes concatenation,

XOR is the bitwise exclusive OR,

"opad" is the block-sized outer padding,

"ipad" is the block-sized inner padding.

Other than its capacity to check data integrity and message validation, one motivation behind why it is enthusiastically prescribed is because of its efficiency. Hash functions can take a message of unrestricted length and converts it into a limited length digest. This signifies, regardless of whether you have generally long messages, their relating message reviews can stay short, subsequently permitting you to expand bandwidth.

3. CONCLUSIONS

The paper briefs the different techniques used for encryption in End-to-End services. Every encryption technique has its strong points and its vulnerabilities. Where one technique may be lacking in availability, another may be weak in distribution. Among all the techniques used in modern world, the only way to really determine which one is superior is by evaluating and comparing the various methods. Thus, for deciding which encryption techniques to use, they have to decide what type of information they want to secure.

To add up in the end, all the strategies examined above are helpful for ongoing encryptions. Regular new encryption methods are advancing thus quick and secure customary encryption procedures will consistently work out with higher pace of security.

ACKNOWLEDGEMENT

We say thanks to Mr. Pranshu Saxena, Associate Professor, Department of Computer Science, Inderprastha Engineering College for the help with examination in the undertaking of the paper, and Computer Science and Engineering,

Inderprastha Engineering College for criticism and follow up that enormously improved our manuscript.

REFERENCES

[1] G. Z. Xiao, M. X. Lu, L. Qin and X. J. Lai. New field of cryptography: DNA cryptography, Chinese Science Bulletin. Chinese Science Bulletin 51 (2006), 1413–1420.

[2] A Gehani, T. H. LaBean and J. H. Reif, DNA based Cryptography, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 54 (2000), 233–249.

[3] C. T. Celland, V. Risca and C. Bancroft, Hiding Messages in DNA Microdots, Nature 399 (1999), 533–534.

[4] A. Leier, C. Richter, W. Banzhaf and H. Rauhe, Cryptography with DNA Binary Strands, BioSystems. 57 (2000), 13–22.

[5] P. C. Wong, K. K. Wong and F. Harlan, Organic Data Memory Using the DNA Approach, Communications of the ACM. 46 (2003),95–98.

[6] B. L. Hao, H. C. Lee and S. Y. Zhang, Fractals Related to Long DNA Sequences and Complete Genomes, Chaos Solltons Fractals. 11 (2000), 825–836.

[7] Aamer Nadeem and Dr M. Younus Javed , A Performance Comparison of Data Encryption Algorithms, IEEE, 2005.

[8] O.P Verma, Ritu Agarwal, Dhiraj Dafouti and Shobha Tyagi, Peformance Analysis Of Data Encryption Algorithms IEEE Delhi Technological University India, 2011.

[9] R.anderson and E. Bihan, Two practical and provably secure block cipher BEAR and LION fast software encryption, third international workshop proceedings, springer – verlag, 1996, pp. 113-120.

[10] U. Blumenthal and S. Bellovin, A Better Key Schedule for DES like ciphers pragocrypt “96 proceedings, 1996, pp.42-54.