ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Split Based Encryption in Secure File Transfer

Parul Rathor, Rohit Sehgal

Assistant Professor, Dept. of CSE, IET, Nagpur University, India

Assistant Professor, Dept. of CSE, IET, Alwar, Rajasthan Technical University, India

ABSTRACT: As we know today our data is not safe, it becomes easy to hack anyone data. On the other side in network security many technologies are developed to make data secure but still hackers are easily get successes in their job. So, again by using such technologies of cryptography in network security we will try to make "Strong data protection". So that data can be encrypt easily but will be difficult to decrypt it. In this paper, at first we are going to take review of such technical schemes. These schemes are none other than Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Here we create one frame, that frame is called as "Master frame" then split it into four mini frames. After these we merge above three schemes one after the other but the sequences are different in each frame. We are encapsulate here encrypted data of each scheme, and then send back to main frame which should be decrypted one. Whatever sizes of data are given by main frame the same size of data will return by each frame.

KEYWORDS: master frame; files; keys; various cryptographic schemes; transmitter.

I. INTRODUCTION

Up-till now we have study various concept of cryptography which mean the process of hiding the original message. The main aim of this paper is to introduce the new concept of security in cryptography. It will expose all such related terms of cryptography. We proceed to revise three such schemes which is mentioned above like Rivest-Shamir-Adelman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Making of these three techniques by combining them will used to offer "Strong data protection". Combination of these make one frame that frame is said to be security of trace or " Master-frame" .A master – frame is breaking down into four mini frames. Each frame we accumulate above three schemes and encrypted it. After that we provide security to this master frame by using encryption type, number & key.

II. REVIEW OF SURVEY

A. *The Rivest –Shamir –Adleman (RSA) Algorithm*:

There are number of methods/algorithms have proposed for public key system, some of them are most promising. The Diffie and Hellman introduced a new concept in cryptography which met the requirements for public key cryptographic systems. Such algorithm is called as "Rivet-Shamir-Adleman "(RSA) algorithm. This RSA algorithm is also called as asymmetric key cryptographic algorithm. The RSA algorithm is a multiplication of two large prime numbers.

And the steps for calculations are below:-

- Step 1: Take two big prime numbers i.e. R and S.
- Step 2: Multiply R and S, store it in Q.
- Step 3: Choose public key called as encryption key consider as F so it should not be factor of (R-1) and (S-1).
- Step 4: choose private key called as decryption key consider as A then the below equation is correct:

(A * F) mod (R - 1) * (S -1) = 1

- Step 5: Find encrypted text ET by original text OT as:

ET = OT^ F mod Q

- Step 6: Give encrypted text to receiver
- Step 7: Then find OT as original text by encrypted text ET as:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

OT = ET^ D mod Q

B. *Data Encryption Standard (DES)* :

DES is used to encrypt data in terms of blocks each of size 64 bits. Here original text of 64 bits as input which produces 64 bits encrypted text. The key and algorithm are used for encoding and decoding. There are two types of DES means double DES and triple DES.

Also there are two attributes of cryptography: One is substitution which is called as confusion and other is transposition which is called as diffusion. It consists of 16 steps which is said to be "round". Every round works in steps of above two techniques. These techniques are the primary ways of which original text are encoded to form encrypted text. Here in first technique that is substitution, here only characters of original text are changed by other characters, symbols or numbers. And in second technique that is transposition, it is different from first one. Transposition performs permutation over original text after changing characters or alphabets.

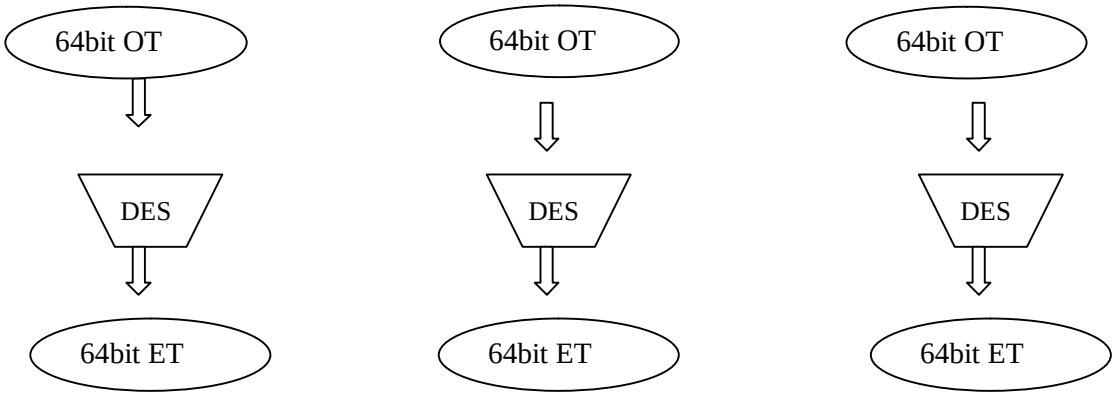

Fig 1. Original text is converted into Encrypted text each of 64 bits

Now let us discuss such steps of DES.

Step1: Original text of 64 bits is handed over to Initial Permutation (IP) function. First permutation is performing on original text.

Step2: Then Initial Permutation (IP) is produces two blocks, First is Left Original Text (LOT) and Right Original Text (ROT).

Step 3: LOT and ROT having its own key follows 16 rounds of encryption processes.

Step4: Again above two blocks LOT and ROT are combined then last permutation (LP) is performed.

Step5: At the end, encrypted texts of 64 bits are formed.

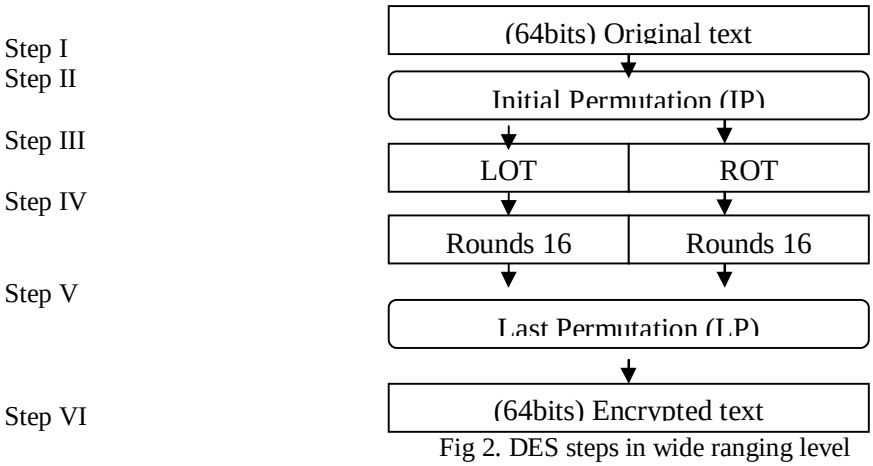

Fig 2. DES steps in wide ranging level

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

We can explain details of one round DES. So it can be discussed step by step.
1. Key transposition: In DES, 64 bit key input is transfer to produces 64 bit key by using 56 bit key this key is available in every round. In each round different 48 bit key is obtained.

2. Expansion permutation: After first permutation, it was divided into two blocks LOT and ROT. Now this expansion ROT is expanded means its increases from 32 bits to 48 bits.

3. S-Box substitution: From XOR operation, S-box accepts input of 48 bit having its key and ROT which gives 32 bit of output by using only substitution process.

4. P-Box permutation: There are 32 bits of output in S-box and this are permuting only by using P-box. Here each bit is replaced by another bit.

5. XOR and Swap: Until now we have seen all tasks are performed in ROT but not in LOT. So here we XOR-ed LOT with P-box permutation. Result of this XORing produces latest ROT so that old ROT becomes new one.

C. *Advanced Encryption Standard (AES*):
AES is not a constitution of feistel. Half block of data is used to alter another half block of data then halve are swap. Using substitution and permutation as an alternative, whole block of data as particular matrix in each round processes. The key is expanded here as an input. There are four different stages which are used. Here all the operations are done in four by four matrixes
1. Substitution of bytes: The S-box technique is used, which is same as of DES.The original text is passes to S-box and generates new text

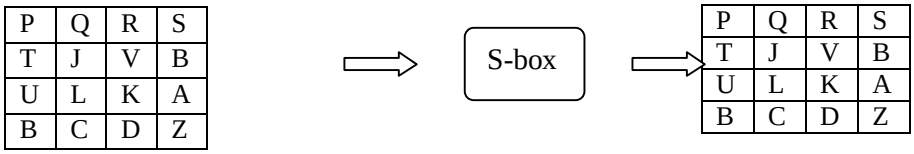

Fig 3. Bytes Substitution

2. Rows shifted: In all process there were four rows and four columns. At these step first rows was remain as it is and changes were done from second rows onwards. The very first byte that is T was shifted on right side and in same way other bytes were also follows it.

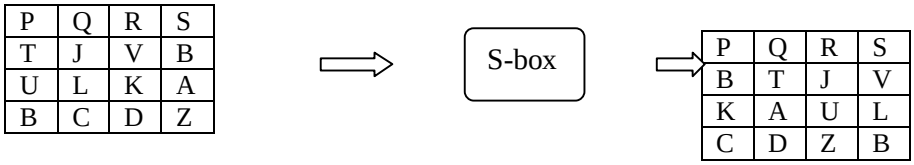

Fig 4. Shifting of Rows

3. Columns mixed

4. Key addition: In the last step that is key addition, here two boxes which were same were getting Xoring and the same third box was established.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

P	Q	R	S
T	J	V	B
U	L	K	A
B	C	D	Z

XOR

P	Q	R	S
T	J	V	B
U	L	K	A
B	C	D	Z

P	Q	R	S
T	J	V	B
U	L	K	A
B	C	D	Z

Fig 5. Add keys

III. METHODOLOGY

Here we try to merge above three schemes like RSA, DES and AES in one file that file is the main file. What happen today hackers may easily know how to encrypt the data but we will make difficult for them to access data. This process will increase randomization. We have divided this main file into four sub parts called as mini frames. We label them as part I, part II, part III, and part IV. In each part we have taken these three schemes and try to adjust them one after the other, Means here schemes are same but sequences are different. Suppose in first part the sequence is RSA – DES – AES then the second part we adjust it into DES – AES – RSA, in third part it is AES – DES – RSA and in last one fourth part it is RSA – AES – DES. Here first we send the whole data to all parts then data are arranged in above manner. After sending the data we encrypt each scheme one by one by using proper key. Whatever the size of data we kept in main file, the same size of data we have to send it again. Suppose if main file is of 100kb then each sub part of that file should be of size 25kb. So after encryption of three schemes in one part the data should be of 25 Kb. same things are happen to remaining parts of files.

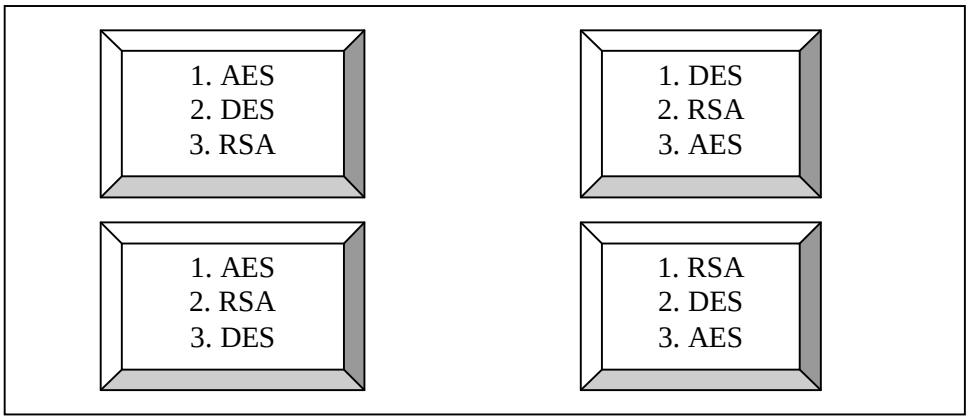

Fig 6. Main File

Now point to be noted we generate one master frame inside these main file. Master frame contains all key information which is used for encryption of each scheme. This frame having all keys with respect to their scheme and its separators. Here this separator is used to separate the particular key information which is very must.

At last we used one transmitter. It is used to keep all input files which should be encrypted. In above figure we shown main file that having four sub parts, three common schemes like AES-DES-RSA are used but sequences are changed because it increases randomization. At each sequence we used one key to encrypt it. If there are four parts and in each part having three sequences means there are total twelve numbers of sequences. So the transmitter should have data from encrypted data one to encrypted data twelve, we can named it as e1 to e12. Also separators for each encrypted

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

data are must to separate among all. These separators are look like underscore and number. We can explain it by using figure below.

.

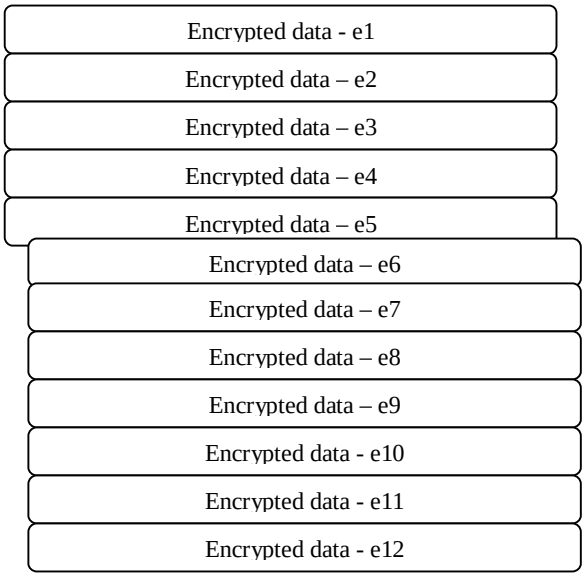

Fig 7. Transmitter

IV. CONCLUSION

This paper has described temporarily about how cryptography works. In spite of the mathematical theory behind an algorithm, the best algorithms are those that are familiar and well-documented. A permutation of algorithms is used to provide "A Strong data protection. "

The RSA algorithm is the most fashionable & verified asymmetric key cryptographic algorithm. The second one was to be called as the Advanced Encryption Standard (AES).And the third one is RC6,which is highly opposed to reverent and linear cryptanalytic attacks, which are currently the two most selective diagnostic attacks on block ciphers. Finally, all these three schemes are stored in one frame called

"Master Frame "which will be secured by using frame numbers, encrypted type & key.

In this way it will make our master frame secure.

For higher accessibility storage machine is capable for used.

At last we can say that security of frame or a file is known as main file.

ACKNOWLEDGEMENT

I would like to thanks prof. Rohit sehgal department of computer science from Institute of engineering and technology, alwar for their precious suggestion in making the final edition of this manuscript.

REFERENCES

1. Cryptography and Network Security by Atul Kahate (Tata McGraw-Hill)
2. Cryptography and Network Security by William Stallings (fifth edition, pearson)
3. T. A. Yang. Computer security and impact on computer science education. *J. Comput. Sci. Coll.*, 16(4):233–246, Apr 2001.
4. A. Yasinsac. Information security curricula in computer science departments:Theory and practice. *The George Washington University Journal of Information Security*, 1(2):135–158, 2002.
5. W. Yurcik and D. Doss. Different approaches in the teaching of information systems security. In *Proceedings of the Information SystemsEducation Conference*, 2001.
6. Electronic Frontier Foundation. (1998). *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. Sebastopol,CA: O'Reilly & Associates.
7. Schneier, B. (2000). Secrets & Lies: Digital Security in a Networked World. New York: John Wiley & Sons.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

8. Network Security Essential, William Staling, Pearson Publications Ltd.
9. S. Hansman and R. Hunt, "A taxonomy of network and computer attacks", Computers Security (2005), Volume: 24,Issue: 1, Publisher:Elsevier, Pages: 31-43.
10. Long, M., Chwan-Hwa Wu, Hung and J.Y., "Denial of service attacks.
11. E. Biham and A. Shamir. *Diferential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New York, 1993.
12. A. Biryukov and E. Kushilevitz. *Improved cryptanalysis of RC5*. In K. Ny-berg, editor, Advances in Cryptology | Eurocrypt '98, volume 1403 Lecture notes in Computer Science, pages 85{99, 1998. Springer Verlag.
13. J. Daemen, R. Govaerts and J. Vandewalle. Weak keys for IDEA. In D. Stinson, editor, Advances in Cryptology | Crypto '93, volume 773 of Lecture Notes in computer Science, pages 224{231, New York, 1994, Springer Verlag.
14. M.H. Heys. *Linearly weak keys of RC5. IEE Electronic Letters*, Vol. 33, pages 836{838, 1997.
15. T. Jakobsen and L.R. Knudsen. *The interpolation attacks on block ciphers.*
In E. Biham, editor, *Fast Software Encryption*, volume 1267 of Lecture notes in Computer Science, pages 28{40, 1997. Springer Verlag
16. 1Trappe, W., & Washington, L.C. (2006*). Introduction to Cryptography with Codin Theory*, 2nd ed. Upper Saddle River, NJ:Pearson Prentice Hall.

BIOGRAPHY

Parul Rathor is an Assistant Professor in Computer Science & Information Technology dept., Nagpur University, India. Her research interest is in computer network & security.

Rohit Sehgal is an Associate Professor In Computer Science & Information Technology dept., Alwar, RTU, India. His research interest is in computer network & security, Web, etc.