International Conference on Information Engineering, Management and Security
2015 [ICIEMS 2015]

ISBN	978-81-929742-7-9	**VOL**	01
Website	www.iciems.in	**eMail**	iciems@asdf.res.in
Received	10 - July - 2015	**Accepted**	31- July - 2015
Article ID	ICIEMS009	**eAID**	ICIEMS.2015.009

Accomplishment of encryption technique to secure file

Mrs. Parul Rathor
Department of Computer Science & Engineering,
Institute of Engineering & Technology, Alwar (R.J), India

ABSTRACT: *The aim of this paper is to implement the new concept of cryptography. To protect information of files in digital form and how to get a security services by network security and cryptography. Though, a general summary of such algorithms like RSA, DES and AES of network security and cryptography is provided first. A complete review of the purposed system of network security and cryptography is then presented by using transmitter. The general attacks of security were reviewed. The purpose of this implementation is to secure a huge amount of files. So that others will unable to know the original data still they know about the procedure of encryption and decryption. This implementation has many applications to secure information including authentication. Here we create new technology by using such transmitter and receiver for decrypting data which is highly secure and accurate.*

Keywords: Master-file, various keys, transmitter and receiver.

I. INTRODUCTION

As we have learn about such cryptographic algorithms like Rivest-Shamir-Adleman [RSA], Data Encryption Standard [DES] and Advanced Encryption Standard [AES]. Also in previous paper we introduce concept of security in cryptography. Here in our data we encapsulate above three algorithm schemes. The very first one is RSA which is also known for asymmetric key algorithm. RSA is a reproduction of two big prime numbers and the secret key and public key are based on this numbers. This RSA algorithm is very easy to understand.

The second one is DES which is of two types double DES and triple DES. Also substitution known as confusion and transposition known as diffusion are the two attributes of cryptography in DES. In substitution characters are altered to numbers or symbols or any other characters and in transposition, it perform permutation over original data. We used DES generally to encrypt data in blocks which have some particular size that is 64 bits. An algorithm and key are also used for encoding and decoding. And last is AES, there are various steps mainly four is used and that are substitution of bytes, shifting of rows, mixing of columns and addition of keys. All procedure is to be process in matrixes which is of four by four. Because of actual weakness in DES, AES is invented. In DES, 56 bit keys were not safe which is based on complete key searches and also 64 bit blocks were measured as weak. So AES as developed which was based on 128 bit blocks with 128 bit keys. There are three major features of AES like Symmetric and parallel structures, Adapted to modern processors and last is suited to smart cards. So these are the basic review of our three cryptographic schemes that is RSA, DES and AES.

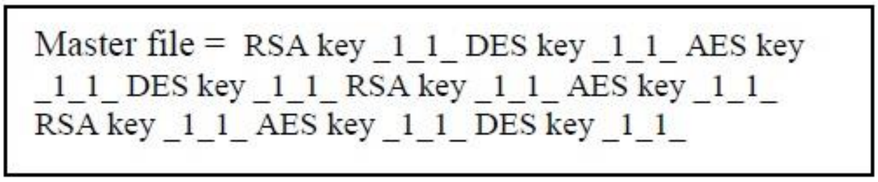
Cite this article as: Mrs. Parul Rathor. "Accomplishment of encryption technique to secure file." *International Conference on Information Engineering, Management and Security (2015)*: 56-59. Print.

II. PURPOSED METHODOLOGY

Now these three things we used in main file as a data. Firstly here we create one master file then breaking it into four parts. In all parts we used same data of above three schemes but sequences are different. Likewise for part one we encapsulate RSA on first place, DES on second place and AES on third place. Then for part two it is DES on first place, RSA on second place and AES on third place. In third part we put RSA on first, AES on second and DES on third.. In this way we merge our data in all four parts of master file.

Suppose part 1 is encrypted by RSA, part 2 is encrypted by DES, part 3 is encrypted by AES and so on. At last part 12 is encrypted by DES according to procedure of above so we get twelve encrypted parts e1 to e12 and master file contains all keys in the form. Now we used key for each algorithm but type is different. Also we have separators for each key. If there are four parts of master file then we split that four parts again into three and name them as begin with e1, e2, e3 up to e12. Means for twelve encrypted data we used here twelve separators as shown in figure below.

Fig 1. Keys with their separators.



Master file = RSA key _1_1_ DES key _1_1_ AES key _1_1_ DES key _1_1_ RSA key _1_1_ AES key _1_1_ RSA key _1_1_ AES key _1_1_ DES key _1_1_

The master file will now be separated and twelve keys which we used for encryption, the same keys obtain. Again the same twelve keys will be used for decryption. At last the decrypted file will be obtained After this we used transmitter for keeping original data that is encrypted and also with its master file. The work of this transmitter is used to transmit all above twelve parts along with its separators.

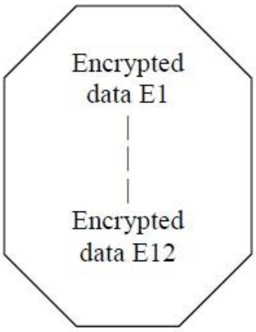


Fig 2. Transmitter

So here we have original data in encrypted form which is kept in transmitter. We can say data of transmitter are kept in input file. Now what about output file?

III. SYSTEM ARCHITECHTURE

After transmission of data encryption are converted into decryption and these decrypted data are to be found in output file. This file is kept in receiver, just like we used transmitter for keeping input file after transmission output file is kept in receiver. The receiver receives all twelve encrypted parts and separates them with its separators. This is only because to get master file and all its parts. The transmitter contains codes of encryption only. While at receiver codes of decryption are kept.

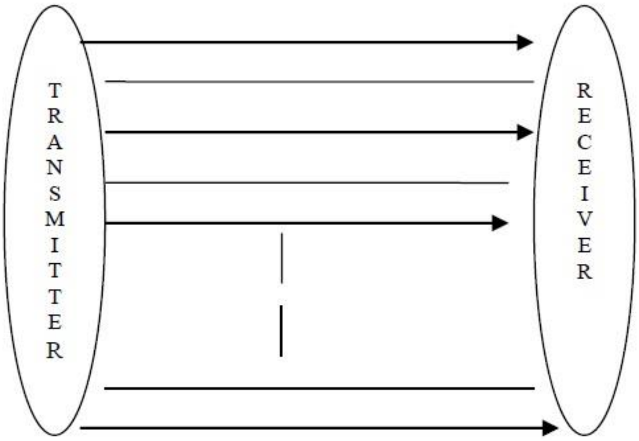


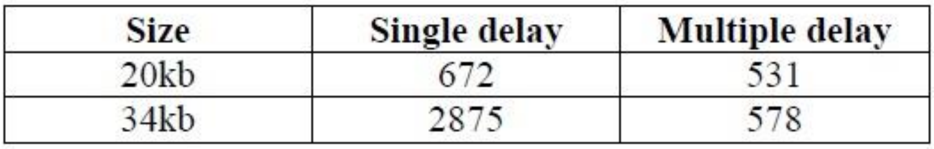
Fig 3. Conversion of original data to decrypted data.

Cite this article as: Mrs. Parul Rathor. "Accomplishment of encryption technique to secure file." *International Conference on Information Engineering, Management and Security (2015)*: 56-59. Print.

In above figure, there are two sides one side we kept transmitter and on the other side there is receiver. In between this figure shows arrows and lines. An arrow is known for file and lines known for separators. The arrow 1 is for master file then kept one separator below this file that shows like single line. In the same way we arrow 2 is known for encrypted data part E1 and kept separator below it. Likewise we arrange all twelve encrypted parts from E1 to encrypted part E12 with its separators.
In other side receiver obtained output file which contains decrypted data.

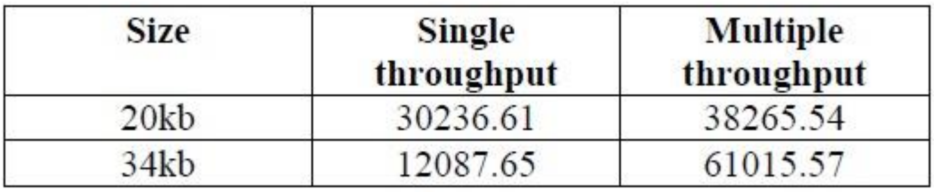
IV. EXPERIMENTAL RESULTS

We can observe it with the help of results.



Size	Single delay	Multiple delay
20kb	672	531
34kb	2875	578

Fig 4. Single delay versus multiple delays



Size	Single throughput	Multiple throughput
20kb	30236.61	38265.54
34kb	12087.65	61015.57

Fig 5. Single throughput versus multiple throughputs

Here at receiver mode we have transmitter for single connection and for multi connection. Its depend on our choice. According to size of file we have single delay with its throughput and multiple delays corresponding to its throughput. So we find here what will be range between single delay versus multiple delays in figure 4 and in figure 5 single throughput versus multiple throughputs. As well for file size 20 kilobytes there are 672 observe in single delay and 531 observe in multiple delay. And 30236.61 find in single throughput and 38265.54 obtain in multiple throughput. In the same way we can find for file size 34 kilobytes and so on to get desire output. Also we can express more deeply these output with the help of graph as shown below figure 6. There are some advantage and disadvantage to every research, lets discuss about first advantage. An advantage of transmitter (input file) and receiver (output file) for encryption and decryption is make data highly secure. Also it is accurate and gives high throughput.
On the other side if there are good points so it should have bad points also. The disadvantage is here like multiple types of encryption is used, so because of this computation complexity is high. Also as there are twelve parts and for these parts each having its own separators so large amount of space is required which mean memory requirement is high.

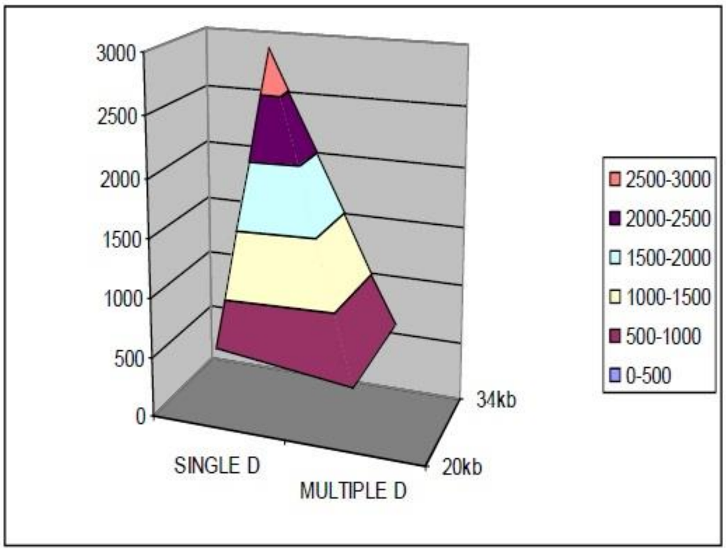


Fig 6. Graph for single delay versus multiple delay.

Cite this article as: Mrs. Parul Rathor. “Accomplishment of encryption technique to secure file.” *International Conference on Information Engineering, Management and Security (2015)*: 56-59. Print.

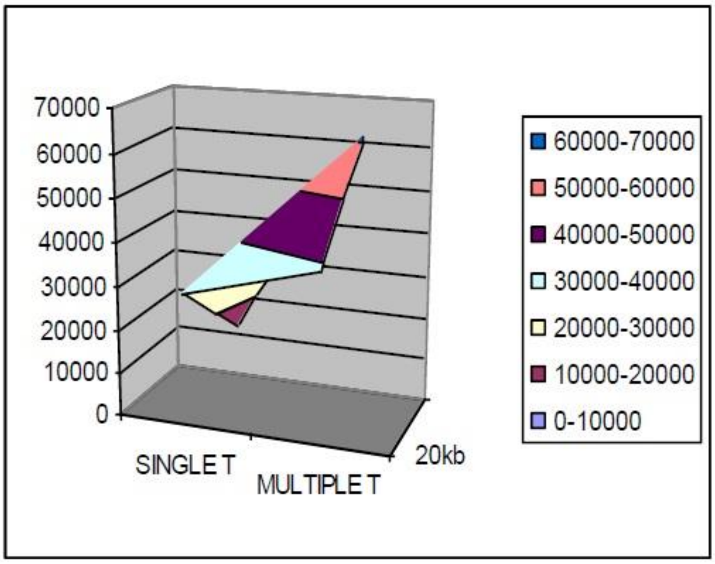


Fig7. Graph for single throughput versus multiple throughput.

V. CONCLUSION

The main purpose for this is today any one can know about cryptographic techniques and about encryption/decryption. They can easily encrypt data but will make difficult for them to decrypt it. This above procedure is somewhat complicated for others to hack it. Hence we discuss by taking shortest review of all algorithms like RSA, DES and AES which were used here. Also try to implement the procedure of conversion data from encryption to decryption in different format. We were found some results which were shown with respect to graph.

ACKNOWLEDGEMENT

It is with deep sense of appreciation and veneration that I express my sincere thanks to my highly respectable supervisor Prof. Rohit sehgal. He has played a pivotal role for my guidance, encouragement, help and useful suggestion throughout. His untiring and painstaking efforts, methodological approach and individual help made it possible to complete this work in time. I like to thank our Principal Prof.(Dr.) Anil Kumar Sharma , H.O.D(CS/IT) Dr. B.K.Verma for providing all the facilities and working environment in the institute.

REFERENCES

[1] Parul Rathor, "Implementation of split based encryption technique for securing file transfer over a network", in International Conference on Industrial Automation and computing [ICIAC-2014].
[2] Parul Rathor, "SPLIT BASED ENCRYPTION IN SECURE FILE TRANSFER",
[3] Rajani Devi.T, "Importance of cryptography in network security", in 2013 International conference on communication systems and network technologies.
[4] Atul kahate, "Cryptography and Network Security" book, tata McGraw-Hill publishing company limited, 2003.
[5] "Cryptography And Network Security" principles and practice, Fifth edition, pearson by William Stallings.
[4] Trappe, W., & Washington, L.C. (2006). *Introduction to Cryptography with Codin Theory*, 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall.
[5] Denning, D.E. (1982). *Cryptography and Data Security*. Reading, MA: Addison-Wesley.
[6] Ferguson, N., & Schneier, B. (2003). *Practical Cryptography*. New York: John Wiley & Sons.
[7] Electronic Frontier Foundation. (1998). *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. Sebastopol, CA: O'Reilly & Associates.
[8] Schneier, B. (2000). Secrets & Lies: Digital Security in a Networked World. New York: John Wiley & Sons.
[9] Network Security Essential, William Staling, Pearson Publications Ltd

Cite this article as: Mrs. Parul Rathor. "Accomplishment of encryption technique to secure file." *International Conference on Information Engineering, Management and Security (2015)*: 56-59. Print.