International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 1, January 2016

Encryption Technique To Secure File Exploitation

[1] Parul Choudhary [2] Prof Rohit Singhal
Department of Computer Science & Engineering
Institute of Engineering and Technology
Alwar, Rajasthan
[1]cparul2605@gmail.com [2]mtechrohit@gmail.com

***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.**

***Keyword*: 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 performs 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.

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. Here as we encrypted the algorithms that means we used keys for them.

As we used keys to each of them but type is different. Also we have separators for each key; which helps us to separate each encrypted algorithm with their keys and it will not get by other keys.

Now as the input data is encrypted so we transform it with their keys in master frame. Also this frame contains the information about all keys with its different algorithms.

We can illustrate it with help of figure 1 below.

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

Fig 1. Keys with their separators.

III. SYSTEM DESIGN

The master frame will now be separated and twelve keys which we used for encryption, the same keys obtain.

After this we used transmitter for keeping these data that is encrypted and also its master file. The work of this transmitter is used to keep all above twelve parts along with its separators.

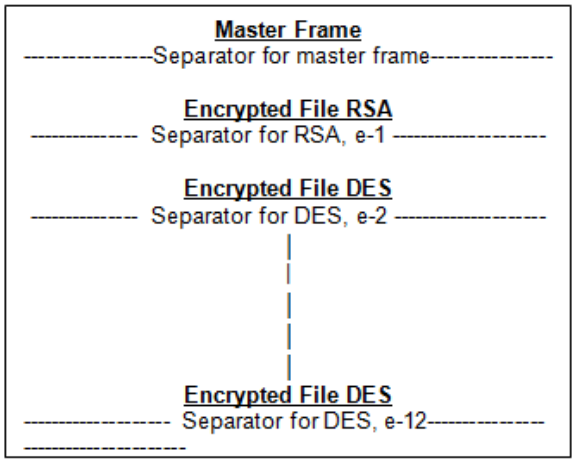


Fig 2. Transmitter

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

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.

Hence in input file we kept first real data then spitted it, encrypted it by providing keys.

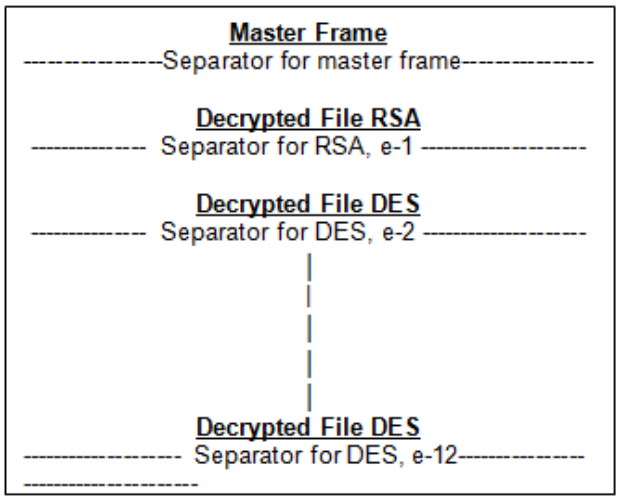


Fig 3. Receiver

Now in below 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 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.

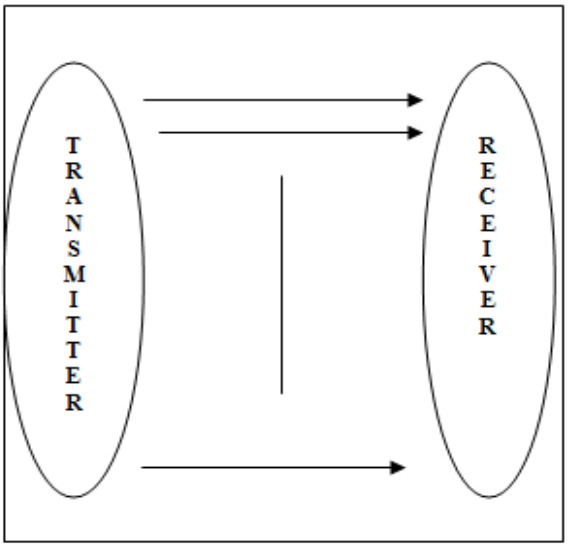


Fig 4. Transmitter & Receiver

We know that there are two types of keys like Symmetric and Asymmetric keys. So RSA and DES uses

asymmetric key for encryption, whereas AES uses symmetric key for encryption.

VI. EXPERIMENTAL RESULTS

Size (kb)	Single delay
22 kb	640
52 kb	688
72 kb	641

Table 1. Size with Single Delays

Size (kb)	Multiple delays
22 kb	547
52 kb	594
72 kb	640

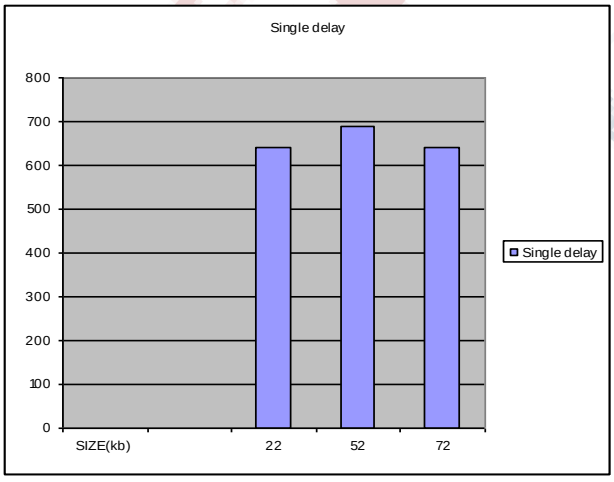
Table 2. Size with Multiple Delays

Size (kb)	Single Throughput
22 kb	34417.19
52 kb	32015.99
72 kb	34363.49

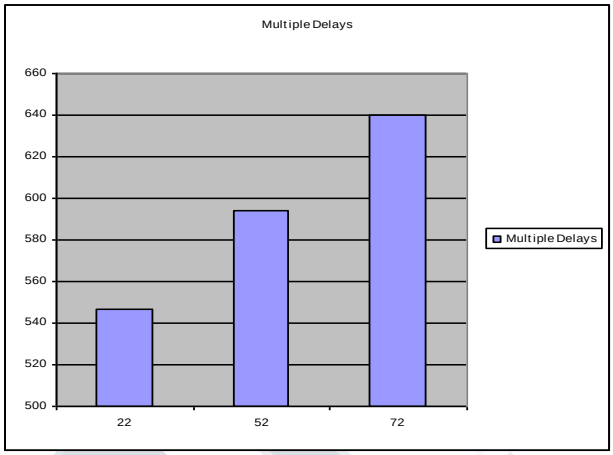
Table 3. Size with Single Throughputs

Size (kb)	Multiple Throughputs
22 kb	40268.74
52 kb	90112.8
72 kb	114623.4

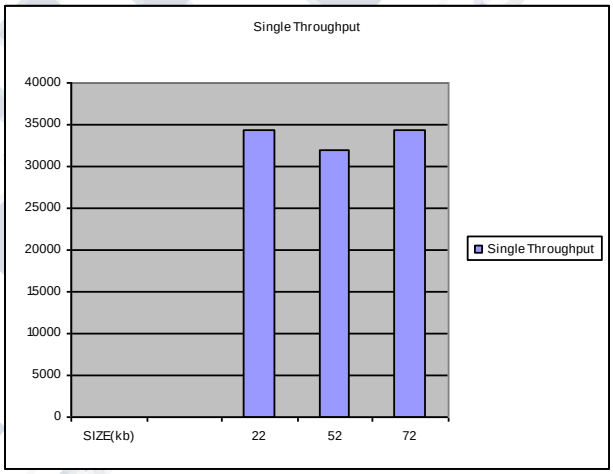
Table 4. Size with Multiple Throughputs



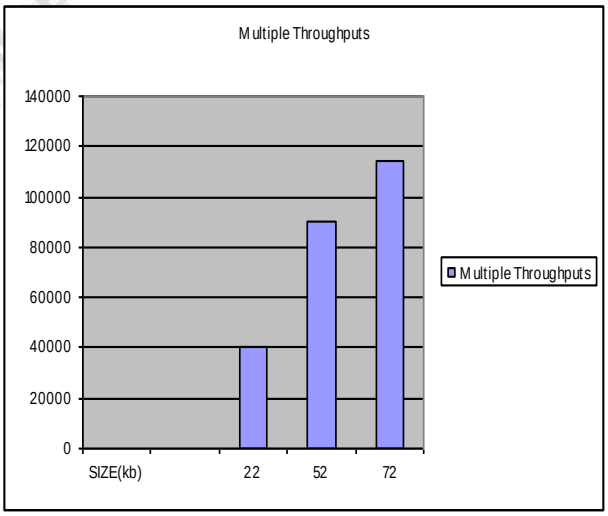
Graph 1. Single Delays



Graph 2. Multiple Delays



Graph 3. Single Throughputs



Graph 4. 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 find for

single delay with its throughput and multiple delays corresponding to its throughput.

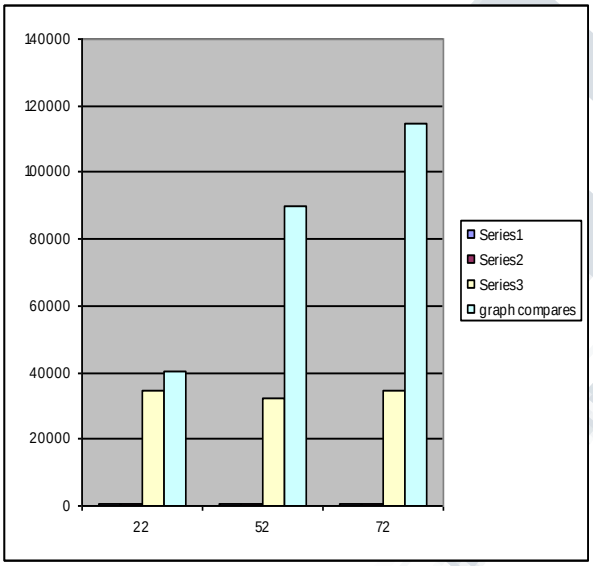
Also we can express more deeply these output with the help of graph as shown below.

Size	S.Delay	M.Delay	S.Through	M.Through
22kb	640	547	34417.2	40268.7
52kb	688	594	32015.9	90112.8
72kb	641	640	34363.5	114623.5

Table 5. Combine between tables of delays with throughputs

Thus if we want to show combine comparisons between single and multiple delays as well as single and multiple throughputs than we can able to show it again by using bar graphs.

Thus we can take any size of file but it should be in kilo bytes. It can exceed after 100 kb also. It will show us delays and its proper throughputs.



Graph 5. Comparison between Delays & Throughputs

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.

VII. 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 here we 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 Singhal**.**

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 and Prof. Rohit Singhal, "Split Based Encryption in Secure File Transfer". In International Journal of Innovative Research in computer and communication engineering, Volume 3, Issue 7, July 2015.

[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 Trappe, W., & Washington, L.C. (2006). Introduction to Cryptography with Codin Theory, 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall.

[6] Denning, D.E. (1982). *Cryptography and Data Security*. Reading, MA: Addison-Wesley.

[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 Network Security Essential, William Staling, Pearson Publications Ltd

BIOGRAPHY

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

Ms. Parul Choudhary is a M.Tech Student In Computer Science & Information Technology dept, Alwar, RTU, India. Her research interest is in computer network & security.