Optimized Security Enhanced System for File Transfer using Classical Encryption Technique

S. Sindhu*1, P. K .Saran*2, J. S. Tharun*3

**Department of Information technology, Sri Krishna College of Engineering and Technology,*
(An Autonomous Institution affiliated to Anna University, Chennai.), Coimbatore, Tamil Nadu, India.

Abstract— **Communication has taken an irreplaceable position in our life. To enhance the communication networks became an imperative one. Due to these communications, networks are prone to security attacks and preventing it is important to provide a secured communication and to protect sensitive information. Hence, security assurance is one of the major requirements for any user. This paper discusses about ventilate on the various ciphering and deciphering algorithms on a file by using secret key, use of RSA algorithm for ciphering and deciphering.**

Index terms— **Decryption, Encryption, RSA algorithm, Security attacks.**

I. INTRODUCTION

The Internet termed as “network of networks” is been used as a vital part of communication from one part to the other part of the earth in just fraction of seconds. Earlier it was impossible to do communication in such a terse period of time. Communication developed with the help of computers, networks and efficient communication channels. Now, these type of communications has become a normal one for the people. But, with the development of technology the risks are also tied up together. This creates a situation of thinking about the security of the data communicated, which is of a greater concern nowadays. For instance, one can break into another person's system very easily. One way is to remove the disk drive out of the system, connect it to another system, and use it. Even the process of breaking into any system is available on the internet and hence an intruder who wants to break into a system can easily get access to those solutions available. Then, the intruder can even reset the administrator password. Then can access the system as an administrator, thereby, can access all the information available in the system.

By ensuring the security of communication, users can make a better use of available information services. File encryption serves as a basic means of protection. Even when the intruder gets an encrypted file and if the key information is also got and if that can be hardly deciphered, then it ensures the increased security of the documents transferred.

II. PUBLIC KEY CRYPTOSYSTEM

Xin Zhou (2011) proposed a novel which detailed the explanation about use of RSA algorithm for ciphering and deciphering. The public key cryptography entrust on one key for encryption and another key for decryption [8]. It is infeasible computationally to determine decryption key from the insight of cryptographic algorithm and encryption key. In addition, the public key encryption scheme such as RSA has six ingredients such as plain text, encryption algorithm, public and private keys, ciphertext and decryption algorithm. In this approach, all the members have access to the public key and the private key is available to access locally to each member and therefore, it is never distributed [1].

The major steps carried out are the following,

1. Each user generates a set of two keys for ciphering and deciphering of the messages.
2. One of two keys is placed in an accessible file, for use of all members. Other key is kept as private.
3. If user1 imposes to send a confidential message to user2, user1 ciphers the message using the key in accessible file of user2.
4. When the user2 receives the message, it can be deciphered by his/her own private key. No other user can decipher the ciphered text because only user2 knows user2’ s private key. This scheme is one which is based on integers. It makes use of exponential expressions [10]. Process of ciphering and deciphering proceeds as follows, for an original text O and decrypted text D.

$$D = O^{\text{receiver's public key}} \text{ mod public key}$$
$$O = D^{\text{receiver's private key}} \text{ mod public key}$$

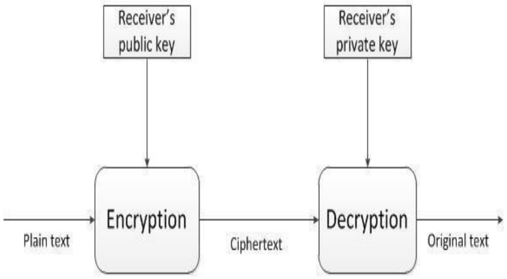

Fig. 1. Public key cryptosystem flow diagram.

The keys are set up based on following steps,

1. Select two prime numbers, l and m
2. Calculate public key = lm.
3. Calculate f(public key) = (l-1)(m-1)
4. Select receiver’s public key such that it is comparatively prime to f (public key) and less than it.
5. Determine receiver’s private key using extended Euclid’s algorithm.

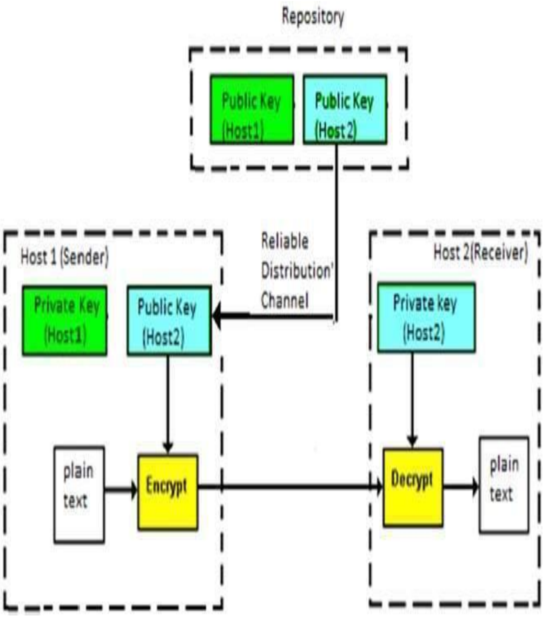

Fig. 2. Process of public key cryptosystem.

III. SECRET KEY CRYPTOSYSTEM

Guy-Armand Yanji(2011) proposed a novel which described in detail about the methodology and functionality of AES. The symmetric key cryptosystem is based on using one key for both ciphering and deciphering [8]. It would be a more secured one as same key is used [4]. AES (Advance Encryption Standard) is a type of symmetric block cipher. It processes on plain text of 16 bytes. Its key size can be of 16, 24 or 32 bytes [9][10]. In this method of encryption, it has greater level of cryptographic key based on the deep analysis of standard cryptographic algorithms [6]. This algorithm plays an indispensable role to encrypt and provide high security to the data. In this methodology AES describes the issues influence of design processor. And the MD5 is placed for the verification of proposed algorithm for the verification of IPV6. The third party is registered and encrypts data with other party. It uses MD5 algorithm to encrypt files using second pass through algorithm. MD2 and MD5 are the encryption algorithm and it goes usefulness while new algorithm are found these are the algorithm demonstrated that much of motivation for the hash functions as wide range. The most widely used hash function is MD5. The main strategy used in the process is flag encrypted status and the data Encrypted [2].

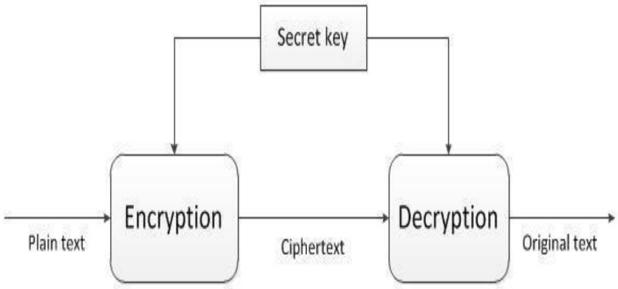

Fig. 3. Symmetric key cryptosystem flow diagram.

In ciphering process, flag is simplifier is used to check and give information about the file is already encrypted or not. The method of encryption and decryption refers to operations on flags. The main importance of this flag is to make faster processing and need not open a file to view it is encrypted or decrypted. The hash key will protect the file from any other intruder trying to determine the password. The Status encryption is an added advantage to block any attempt to decode the message, and then AES is used to ensure enhanced security [2].

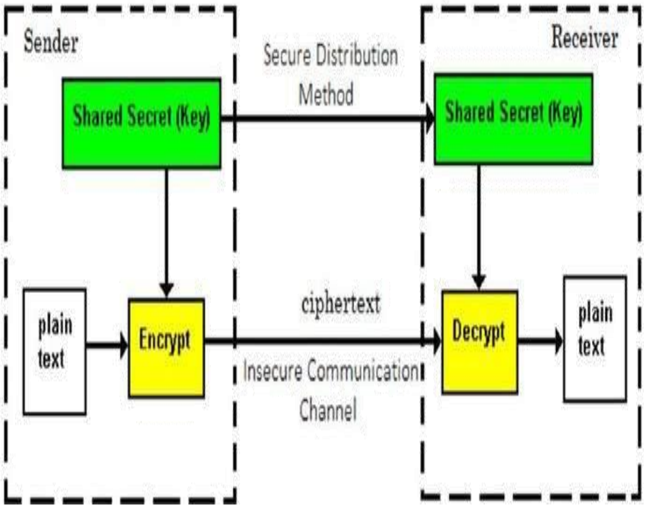

Fig. 4: Process of secret key cryptosystem

In deciphering process, verifying the flag refers to the use of function that checks whether the password entered in this process is same as that in the prior process. In case, if the password does not match, decryption does not take place and the process will abruptly stop [2].

IV. FILE CRYPTOGRAPHY FUNCTIONALITY

Balasaheb B. Gite1 (2014) proposed a novel which described in detail about the methodology and functionality of MD5 and Data signatures. This is about transfer of files using Keys as private and public ,normally the file is transferred by using some hardware and through software, it cause some security breach and it has no security to protect the files while transferring the files to the receiver. So those to rectify and provide greater security to the users through the cryptography technique as encryption and decryption by using online files transfer. However, the way of algorithm plays important modules in this project [3].

The key function is for deciphering the ciphered file while receiver received the correct file to decipher, and the MD5 algorithm is applied to transfer the file very fast and secured way. The file algorithm is done by using javascript and digital signature used to verify each file to decipher the content. A digital trademark is the symmetric representation for the authentication of documents or files [7]. The digital trademark is created and verified using signature class. Once data is transferred to signature object, one can check the digital signature of that data and report the result. While the signature was read into an array of bytes where it is verified. Verified value will be true if the stated signature matches with the real signature of the specified data file. The result of the process is conversion of original message into non-readable format. In many, the word deciphering refers to the reversal process of ciphering, to make the ciphered information to readable format. It uses inbuilt package "javax.crypto". To provide higher security and confidentiality it uses both the digital trademark and ciphering mechanisms. The sender digitally makes a sign on the original document and the document is encrypted. The message being transferred is reformed into non-readable format. The receiver will then use a particular key or a group of keys for deciphering. This method enhances the security level to avoid security breach [3].

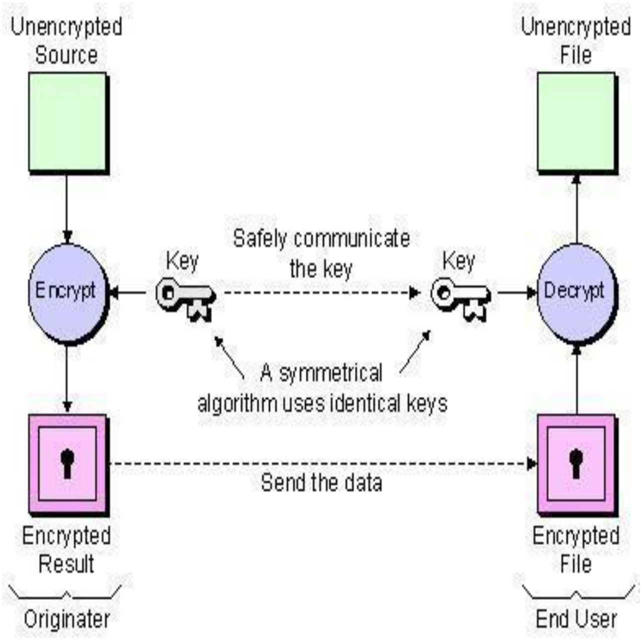

Fig. 5. File encryption using symmetric algorithm.

V. ANALYSIS

Based on the concepts studied in this paper, various factors of the ciphering and deciphering algorithms are analysed and are listed as follows,

TABLE I
ANALYSIS OF VARIOUS ALGORITHMS

S.NO.	**FACTORS**	**AES**	**RSA**	**MD5 and Digital Signature**
1	Key Size	16 or 24 or 32 bytes.	>1024 bits	>256 bits
2	Algorithm type	Symmetric	Asymmetric	Symmetric
3	Usage of keys	Same key is used on the sender as well as receiver side.	Different key is used on sender and receiver side.	Symmetric key cryptosystem to transmit secret key to receiver.
4	Security attacks	Highly secured.	Timing attacks.	Highly secured.

A. Size of key

Specifies the length of the key used in the algorithm.

B. Algorithm type

Determines the sort of algorithm based on count of keys used on both the sides of communication. It can be of two types.

C. Usage of keys

Determines the keys used on both the ends of communication.

D. Security attacks

An attack happens to either get the key or the original message. It determines the attacks possible in the system.

VI. CONCLUSION

As communication over networks plays a major part in everyone's life, the encryption also plays an inevitable part of communication. In this paper, the study about most widely used algorithms is made, from which it can be concluded that in case of computation of ciphertext bytes, RSA is advanced than AES. Increasing the count of rounds in AES algorithm increases security but the disadvantage is that steps of decryption differ from that of encryption process. In case of RSA, the determination of private key from key in accessible file is computationally infeasible.

REFERENCES

[1] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", IFST,2011.
[2] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf and Jules Ehoussou , "Research on a Normal File Encryption and Decryption", IEEE transactions, 2011.
[3] Balasaheb B. Gite1, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, vol.16, Nov., 2014.
[4] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Performance Evaluation of Symmetric Cryptographic Algorithms", IGECT, vol. 2, Issue 3,Sep.,2011.
[5] Pratap Chandra Mandal "Superiority of Blowfish Algorithm", IJARCSSE, vol. 2, Issue 9, Sep.,2012.
[6] Daemen.J and Rijmen, "The Advanced Encryption Standard", Dr. Dobb's Journal, March 2001.
[7] R.L.Rivest, A.Shamir, L.Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystem", Communication of the ACM, vol. 21, Feb., 1978.
[8] E.Thmbiraja, G.Ramesh, Dr.R.Umarani, "A survey on various most common encryption techniques",IJARCSSE, vol. 2, Issue 7, July, 2012.
[9] Monika Agrawal, Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", IJCSE, vol. 4, May, 2012.
[10] B. Padmavathi and S. Ranjitha kumara, "A Survey on Performance Analysis of DES, AES and RSA algorithm with LSB Substitution Technique", IJSR, vol. 2, Issue 4, April, 2013.