A Hybrid Cryptosystem Approach for File Security by using Merging Mechanism

Meenakshi Sharma
Dept. of CSE, SSCET
Badhani (Punjab), India
E mail- sharma.minaxi@gmail.com

Vishu Sharma
Dept. of CSE, SSCET
Badhani (Punjab), India
E mail- vishusharma459@gmail.com

***Abstract*— The expeditious growth of internet and networks applications has given rise to many data security issues. Encryption algorithm plays a crucial role in information and network security systems. One of the efficient directions of achieving security data communication is File Splitting mechanism and Hybrid Cryptosystem. This paper presents the hybrid encryption scheme which combines the quick encryption scheme of symmetric algorithm (Blowfish) with the security of asymmetric cipher algorithm (SRNN). The proposed approach includes file splitting and merging mechanism along with hybrid encryption where each slice is encrypted by its corresponding key.**

Keywords—Hybrid cryptosystem; blowfish; SRNN; RSA; file splitting

I. Introduction

A network [12] is a series of individual elements transmitting and receiving various data. Whenever sensitive or confidential information is transmitted, there is a possibility of an unauthorized third party "eavesdropping" on a transmission and learning the contents of the sensitive message. "Cryptography is the art and science of designing or generating the secret message i.e. code or ciphers of the original message for the secure communication between sender and the receiver."Cryptography [1] is the process of transmitting a message into form which is unreadable to everyone except the intended recipient. This is typically done with the help of keys. The process of converting the plain text into cipher text is called encryption and the alter is called decryption. Two types of cryptographic scheme are :

1) Symmetric Key Cryptography: The cryptographic scheme in which sender and receiver share a common key for encoding and decoding the message. The key is distributed before transmission between entities. The size [6] and strength of the symmetric key algorithm depends on the size of key being used.

2) Asymmetric Key Cryptography: In this two different keys are used for encryption and decryption. Public key is used for the encryption process and Private key is used for the decryption process. Public key is known to everyone and private key is known to the intentional user only. So, there is no need of dispensing the keys for the communication earlier.

II. A Hybrid cryptosystem

The term "hybrid" [4] is borrowed from natural sciences, it means "crossbreed". It is basically the combination of symmetric and asymmetric algorithms and hence, fulfil the utility of both symmetric and asymmetric cryptosystems, because it is more secure as compared to symmetric cryptosystems and faster in comparison to asymmetric cryptosystems. The [4] ISO/LEC standardization committee suggests that hybrid cryptosystem can be defined as the branch of asymmetric cryptography that makes use of convenient symmetric techniques to remove some of the problems inherent in normal asymmetric cryptosystem.

A. Blowfish

Bruce Schenier, one[6] of the world's toppest cryptologists, he designed the Blowfish algorithm and made it available in the public domain. Blowfish is a (64- bit block cipher) variable length key, it is used for the protection of the data. Its algorithm was first designed in 1993, and has not been ruptured yet. It can be optimized in hardware applications due to its abruptness.

It consists of two parts: a key-expansion, converts a key of 448 bits into many sub-key arrays completing 4168 bytes. Encryption of the data takes place via 16-round (commonly). Each of the 16 rounds consists of a key-dependent permutation, and a key and data dependent substitution. All XORs and additions working are performed on 32-bit words. The working operations include 4- indexed array data lookups per round.

Bruce Schenier[10]demonstrated that differential cryptanalysis on Blowfish is possible either against a less number of rounds or with the type of information which describes the F-function. However, the boxes are properly designed to exsist to on attacks while they are arbitrary generated in Blowfish. Because, there is no successful cryptanalysis against Blowfish since 1993. It is one of the quickest symmetric algorithms among other symmetric algorithms. Blowfish is haughty in terms of throughput, processing of the time and consumption of power. The working is explained in the following figure1.

978-1-5090-2399-8/16/$31.00 ©2016 IEEE

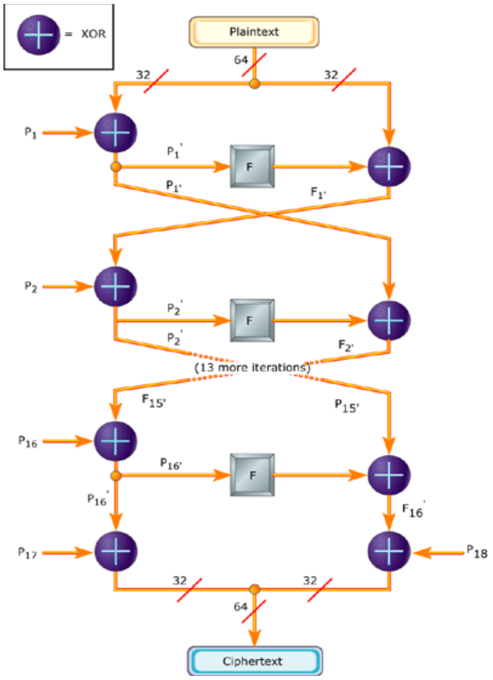


Fig. 1. Blowfish algorithm [4]

B. RSA

The Rivest-Shamir-Adleman(RSA) It is one of the best public key cryptosystems used for encryption of data blocks. The variable size encryption block and a variable size key is used in RSA. The paired key is derived from a very large number n, where n is the product of two prime numbers chosen according to special rules. The prime numbers are very large in length. The public key includes n and a derivative of one of the factors of n such that an attacker cannot get the prime factors of n from this information alone and this key feature make RSA algorithm so secure. To overcome the speed , natural numbers are used in pairs which include the keys in addition to existing parameters of RSA which gives the good balance between speed and security. This modification lead to algorithm named SRNN (Short Range Natural Number).

C. SRNN

The SRNN [2] algorithm, a public key cryptography algorithm which is similar to RSA with some modifications. This algorithm includes the two prime numbers. In addition, the short range natural numbers are used as pairs of keys. This modification increases the security of cryptosystem [11]. So it is named as short range natural number public key algorithm.

SRNN Key generation is as follows:

- Generate two large random primes p and q , such that their product n= p x q .
- Compute phi where,
  phi = (p-1)(q-1)
- Choose an integer , 1<e<phi such that, gcd(e,phi) = 1
- Compute the secret d, 1<d<phi, such that, (e x d)mod phi=1
- Choose a short range natural number u, such that, u< phi-1
- Choose another short range natural number a, such that, phi> a > u , and compute u^a
- Find d such that, e * d mod ((p-1)*(q-1)) = 1
- The public key is (n,e,u^a) .The private key is (d,a,u).

The encryption is performed using equation 1.

- $c =(mu^a)^e \bmod n \qquad (1)$

where, c is the cipher text, m is the plain text.

The decryption is performed using the equation 2

- $m = (v^e c)^d \bmod n \qquad (2)$

where, v= u^(phi-a) mod n.

III. PROPOSED SYSTEM

At the remote server, resources like files, audio, images and other data are shared among all of the servers, users and individuals. So, it becomes tough for the data owner to ensure file security. As a result, it is very easy for an intruder to access, misuse and destroy the original form of data. In case of compromise at any cost; entrusting data owner side is of no use. A need for strong and impracticable to get ambush technique is important for file security:

•The existing security models are ruptured on any time whenever any effective analysis of cryptographic algorithms is done.

•There is need to discover the more gleam and taut the encrypted system for file information protecting system on remote server.

Hence, a file security approach is needed that maintain a good balance between speed and security. The approach uses hybrid encryption algorithm. In this approach Blowfish algorithm along with SRNN algorithm is used for encryption and decryption. If the data stored is in encrypted form, it would effectively solve various security issues. Splitting and merging mechanism is used for en-ciphering and de-ciphering the data. In the file joining phase, En-Ciphered files are obtained from the different En-Ciphering techniques are merged and then transmitted to other side as a single file, by this the file becomes impossible to rupture. At the receiver's end, the files are again splitted and decrypts it by using the same algorithm and again join all the splitted files together to get the original message. The modified version of blowfish algorithm is used for the encryption of the file and then again file is encrypted and decrypted by using SRNN algorithm. Merging mechanism to split the file as shown in the following diagram (Fig. 2).

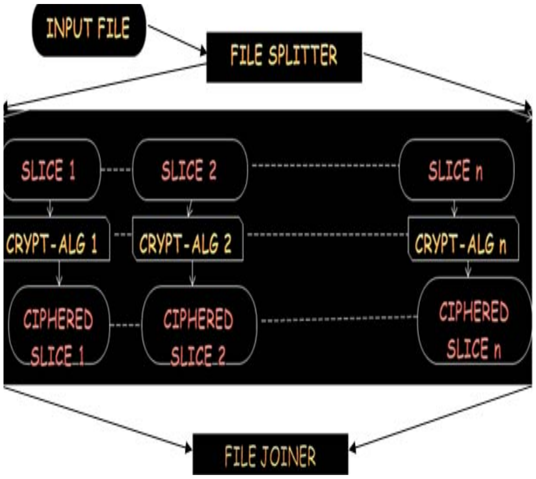


Fig. 2 File splitting and merging mechanism[6]

The original function F is defined as follows (Schneier, 1995):

F(X) = ((S1 + S2 mod 2^32) XOR S3) + S4 mod 2^32

Instead, the F- function is modified by using two XOR Operations. Thus modified F – Function is written as :

F(X) =CS ((S1 XOR S2 mod 2^32)+(S3 XOR S4 mod 2^32))

The simultaneous execution of two XOR operations are applied . In this way the security is further enhanced (Fig. 3).

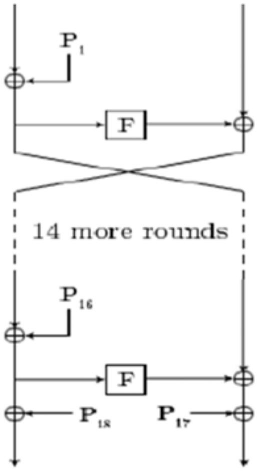


Fig. 3 Modified F-function

Steps at [5] encryption phase: The steps at encryption phase are as follows:

i) The input file is sliced into n slices upon user specification

ii) Each slice is encrypted with the corresponding password given by the user using Blowfish algorithm.

iii) Each password which served as Blowfish key is encrypted by SRNN.

k1, k2, …,kn are the blowfish keys. Cipher1, Cipher2, …, Cipher n are the corresponding ciphers.

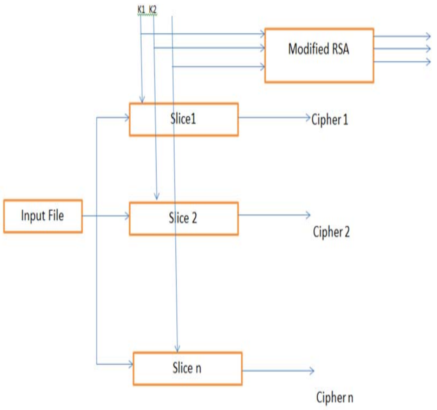


Fig. 4 Encryption phase

At Decryption Phase:

At the receiver end, firstly the n encrypted keys are decrypted by the corresponding n private keys. After decryption we are left with Blowfish keys which are served to decrypt n slices. At the end, the n slices are merged to get the original file. In this way, this proposed scheme of hybrid encryption becomes impossible to breach. The advantage of file splitting and merging is that every slice is encrypted with a different key. If the eavesdropper manages to find the key of one slice, still the remaining file is hidden from him.Ek1,Ek2, …, Ekn are the encrypted keys shown in figure.

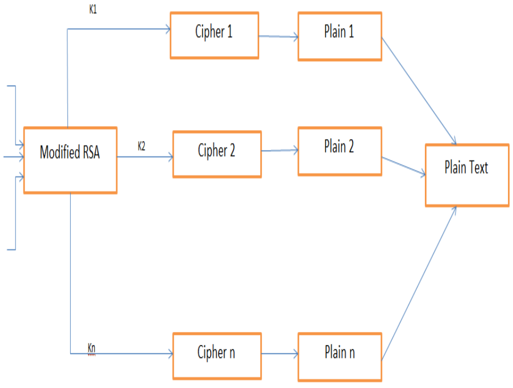
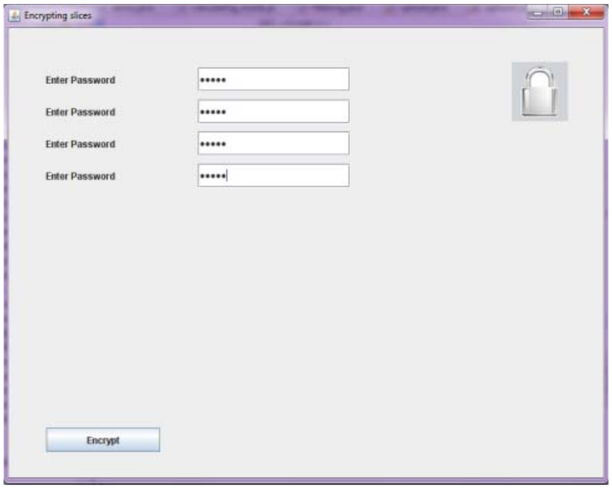


Fig. 5 Decryption phase

IV. Simulation and Results

To achieve the results for the proposed system, Java programming is used which is known for its platform independency and better GUI(Graphical User Interface) features. Various libraries have been used like javax.crypto, java.security to implement the results of hybrid cryptosystem scheme. Following figures represent the results of the proposed scheme in Java. It takes input as file and splits the file into n number of slices on the basis of user specification and finally encrypts the file slices accordingly. In decryption phase, the encrypted file slices are firstly decrypted and then merged to give the final output as a single file.

A. *Encryption frame*


Encrypting slices

Enter Password •••••

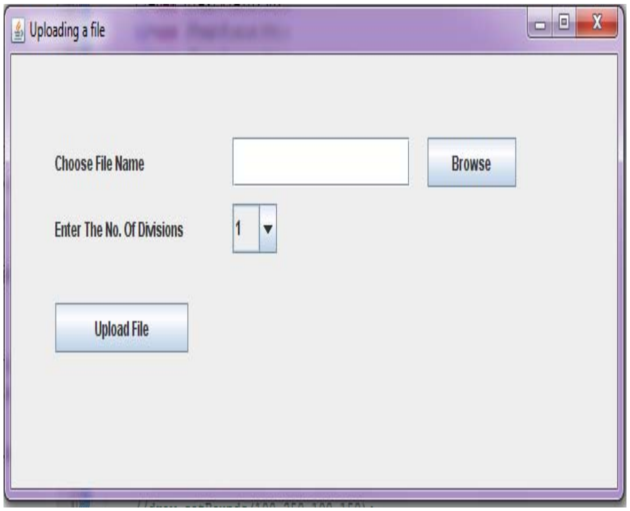
Enter Password •••••

Enter Password •••••

Enter Password •••••

Fig. 6 Encryption frame

This frame (Fig.6) provides an interface for the user to specify the passwords (Blowfish key) for each file slice which will encrypt the corresponding file slices using Blowfish algorithm.


Uploading a file

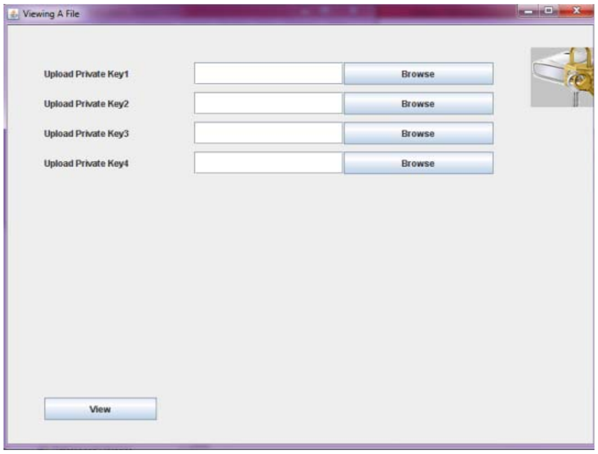
Choose File Name

Enter The No. Of Divisions 1

Fig. 7 File splitting

The above frame (Fig.7) lets the user to specify the filename along with the number of slices in which the user wishes to split the file.

B. *Decryption frame*


Viewing A File

Upload Private Key1

Upload Private Key2

Upload Private Key3

Upload Private Key4

Fig. 8 Decryption frame

Here(in Fig.8), the user need to provide SRNN private key which will decrypt the encrypted Blowfish keys and then the decrypted Blowfish keys decrypts the corresponding file slices. The decrypted files slices are finally merged to give the final output(Fig. 9).

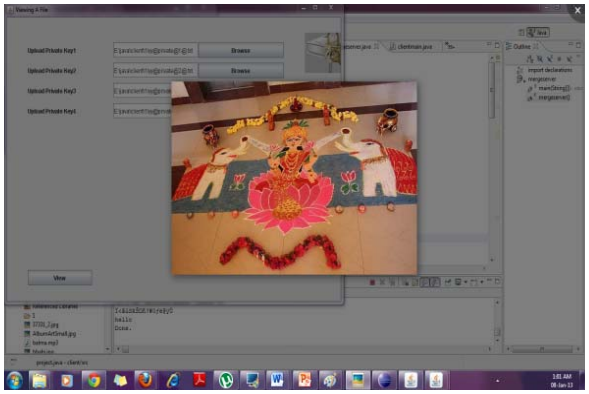


Fig. 9 Decrypted file

C. *Algorithm versus time*

The approximate time taken when tested on file size of 36 bytes and SRNN of 256 bits key is shown in the graph.

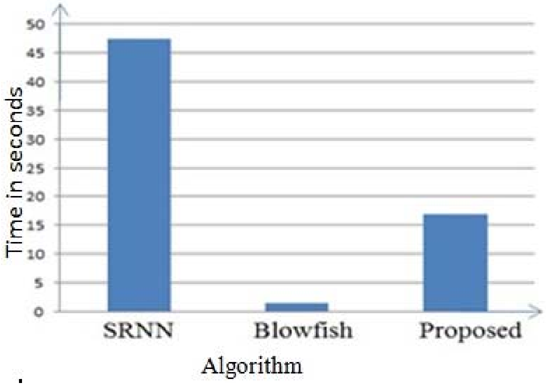


Fig. 10 Algorithm vs time

The graph demonstrates the relationship between the various algorithms and the respective time taken by them to encrypt and decrypt the file and any other data. It can be shown from the algorithmic results ,the proposed hybrid encryption scheme has a good speed as compare to SRNN Algorithm, but the speed is less as compare to Blowfish algorithm. The results are tested for image and audio files.

V. Benefiets of proposed model

The proposed model is liable to meet the required security needs of data. Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. Modified RSA (SRNN) has increased security than RSA. The idea of splitting and merging adds on to meet the principle of data security. The hybrid approach makes the server more secure and thus, helps the Providers to fetch more trust of their users. The various benefits are:

- The public key cryptography used helps to facilitate authorization of user for each file.
- The file splitting and merging makes the model unfeasible to get attacked.

VI. Conclusion

The combination of hybrid cryptosystem along with splitting and merging mechanism along with encryption makes the proposed system better in terms of speed, time and security. It provides more security to the file while transmission. The proposed scheme is more secure than blowfish and also better than SRNN in terms of both time and security as. The hybrid approach serves a good purpose where security needs are prominent. It can be further improved by increasing its throughput compared to symmetric algorithm.

Acknowledgment

Nothing concrete can be achieved without an optimum combination of inspection and perspiration. Generating this mechanism has been time consuming and an arduous task and has involved various contributions. It is our pleasure to acknowledge the help we have received from different individuals we are thankful to SSCET, Badhani for providing us the Infrastructure and Facilities for carrying out this work.

References

[1] Stallings, W., 1999. Cryptography and Network Security: Principles and Practices. 2nd Edn., Prentice Hall, Country.

[2] Manikandan.Get al.(Jan 2012), “A modified cryptographic scheme enhancing data”, Journal of Theoretical and Applied Information Technology, Vol. 35, No.2, pp.149-154, 2012.

[3] Sonal Sharma,Jitendra Singh Yadav and Prashant Sharma ‘Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm’, International Journal of Advanced Research in Computer Science and Software Engineering,vol.2, Issue 8 August 2012.

[4] Y. P. Singh M. Ayoub Khan. "On the security of Joint Signature and Hybrid Encryption", 2005 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic, 2005.

[5] Srinivasarao D et al., “Analyzing the Superlative symmetric Cryptosystem Encryption Algorithm”, Journal of Global Research in Computer Science, vol. 7, Jul. 2011.

[6] Tingyuan Nie. "Performance Evaluation of DES and Blowfish Algorithms", 2010 International Conference on Biomedical Engineering and Computer Science, 04/2010.

[7] S. J. Aboud, M. A. Al-Fayoumi, M. Al-Fayoumi, and H. S. Jabbar, "An efficient RSA public key encryption scheme," in Proceedings of the International Conference on Information Technology: New Generations (ITNG '08), pp. 127-130, April 2008.

[8] Behrouz,A.Forouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security" 2nd Edition Tata McGraw Hill pvt ltd, New Delhi.

[9] Domenico, B. and I. Luca, 2007. Image based Steganography and cryptography. International Conference on computer vision.

[10] Bruce Schneider, http://www.schneier.com/paper-blowfishfse.

[11] Solanki, Devendra Singh, and Savita Shiwani. "A model to secure e-commerce transaction using hybrid encryption", 2014 International Conference on Control Instrumentation Communication and Computational Technologies (ICCICCT), 2014.

[12] Kenneth W. Hsu. "High speed SOC design for blowfish cryptographic algorithm", 2007 IFIP International Conference on Very Large Scale Integration, 10/2007.