PERFORMANCE ANALYSIS OF HYBRID CRYPTOSYSTEM- A TECHNIQUE FOR BETTER SECURITY USING BLOWFISH AND RSA

Suresh Timilsina[*1], Sarmila Gautam[2]

ABSTRACT

Security is the most concerned topic in this today's world of Information and Communication Technology. Single layer security can be breached easily so hybrid cryptographic system has been introduced. Hybrid system can be made by combining two or more algorithms of similar or dissimilar types. Here, combing of Blowfish algorithm along with RSA algorithm is performed. After combination their performance analysis is done based on five parameters namely Throughput, Encryption time, Decryption time, Total Execution time and Plain text size to cipher text size ratio with different key size of Blowfish algorithm ranging from 32 bit-448 bit. Among these 5 different hybrid cryptosystem we found that the Blowfish RSA system with key size 448 bit has better performance than all other bit size.

Keyboards : *Hybrid cryptography, Blowfish, RSA, Throughput*

INTRODUCTION

Cryptography is the branch of security science that deals with the art of hiding information. In communication, cryptography is necessary when communicating over any untrusted medium like internet where millions of attacker try to hack important information which is being shared between two or more other medium. There are two types of cryptosystem i.e. symmetric key cryptosystem and asymmetric key cryptosystem. Symmetric key cryptosystem is also known as private key cryptosystem whereas asymmetric key cryptosystem is also known as public key cryptosystem. But here we used the combination of symmetric key system and asymmetric key system to make a hybrid cryptographic system. The symmetric key cryptographic algorithm and asymmetric key cryptographic algorithm are used to form a strong dominating algorithm which comprises of both kinds into one system increasing the security level. But, security along with performance brings the best of each together and also minimize the disadvantages prevailing in each algorithm used individually. No matter it will certainly take some time but hybrid algorithm is not breached in finite life years. Here the concerned is just to find a best hybrid system among 5 system of same algorithms used but with different key size.

The main objectives of the system is as follows:

- To make hybrid cryptographic system using symmetric key algorithm and asymmetric key algorithm.
- To analyze the performance of the developed cryptosystem with different key length.

[1] *Department of Electronics and Computer Engineering, Thapathali Campus*
[*] *Corresponding author*
E-mail :

LITERATURE REVIEW

Khan and Khalid in 2013 researched and found that the average throughput of Blowfish was maximum as compared to individual AES and hybrid AES-Blowfish. The cipher encryption performance of AES and Blowfish was similar but the memory used by blowfish was found quite high. [1] The research Iyer, Sedamkar and Gupta focus on the implementation of system which is capable of encryption and decryption of multimedia data using hybrid approach between symmetric and asymmetric techniques. They concluded that hybrid system is always a strong one and even if the interceptor found one key he/she won't be able to decrypt the plaintext in finite amount of lifetime. [2] The author proposed hybrid cryptosystem using RSA, AES and DES. They found hybrid encryption algorithm using block cipher and symmetric key provides a more secure and convenient technique for secure data transmission for all kinds application as compared to a private key cryptography based on simple symmetric algorithm. [3] In the paper "A performance analysis of DES and RSA cryptography" It is concluded that encryption and decryption execution time consumed by DES algorithm is least as compared to RSA algorithm. [4]

Unlike all above references my research focuses on comparative analysis of hybrid algorithm made from Blowfish and RSA algorithm. Here the main thing affecting the performance is the key size of blowfish which ranges from 48 bit to 448 bit.

METHODOLOGY

A hybrid cryptosystem is the combination of two cryptosystem using two different cryptographic algorithm namely symmetric key cryptographic algorithm and asymmetric key cryptographic algorithm to form a strong dominating algorithm which comprises of both kinds into one system increasing the strength. A hybrid algorithm can even be made combining all symmetric algorithms, all asymmetric algorithms or mixer of both type of algorithms. Hybrid algorithm is considered highly secure as long as the public and private keys are secure. Hybridization will always not make higher performance result but for sure the security of the system will be highly increased.

Encryption steps using Hybrid Cryptosystem at the Source:

Before encryption process the sender must have the receiver's public key (PUK).The inputs provided are plain data Block (PDB) and symmetric key (Sk) and the output from it is the encrypted data block (EDB) which contains the encrypted plain data block along with the encrypted symmetric key.

Encryption Steps :

1. Encrypt PDB using Sk to get ED and this can be done using any symmetric algorithm.
2. Encrypt Sk using receiver's PUK to get encrypted symmetric key (ESk) and this can be done using any asymmetric key algorithm.
3. Now, the Encrypted plain data block along with encrypted Sk is send to receiver.

Decryption steps using Hybrid Cryptosystem at the Receiver

Before decryption process the receiver must have its private key (PRk). The inputs provide is the encrypted plain data block along with encrypted Sk and output is plain data block.

Decryption Steps

1. Decrypt ESk using PRk to get Sk.
2. Using this Sk decrypt ED to get PDB.

This PDB is the plain data block send by sender to receiver. [12]

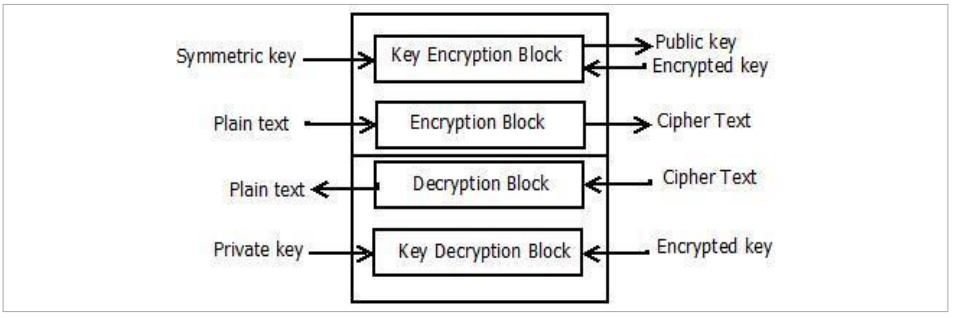

Figure: Block diagram of hybrid cryptosystem

Blowfish-RSA hybridization

Blowfish-RSA hybridization is made from combination of a symmetric key algorithm i.e. Blowfish and an asymmetric key algorithm i.e. RSA.

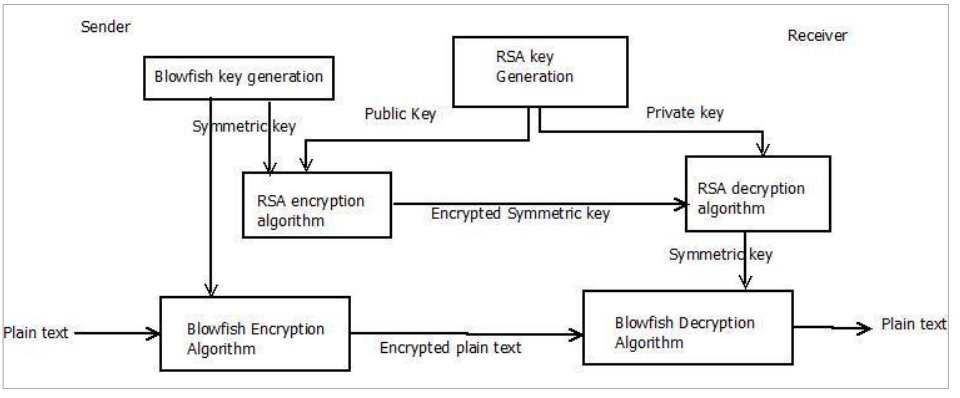

Figure: Block diagram of hybrid system using Blowfish and RSA algorithm

Here, first the key is generated of one size among 32 bit – 448 bit for blowfish algorithm which is then used to encrypt the plain text provided. The key is now encrypted using RSA public key. Both the encrypted key as well as encrypted plain text is transmitted to receiver section where the encrypted key is decrypted using private key. Thus, the then decrypted key is used to decrypt the plain text. After the system is made. This system is used to analyze various parameters for different key size.

Result and Discussion

Here, symmetric and asymmetric key algorithm are used for hybrid cryptographic algorithm are made. After that the performance analysis of the system are carried out on the basis of

following parameters. Throughput is the ratio of total plain text to total encryption time. It can also be calculated in terms of decryption time and cipher text. In case of hybrid algorithm plaintext size is the sum of size of plaintext and symmetric key. Total Execution Time is the total time required for Encryption of a plain text (i.e. combination of plaintext and symmetric key) and decryption of cipher text (i.e. combination of encrypted plaintext and encrypted symmetric key) using a hybrid cryptographic. Encryption Time is the time required for encryption of plain text (i.e. combination of plaintext and symmetric key) using hybrid algorithm. Decryption time is the time required for decryption of cipher text (i.e. combination of encrypted plaintext and encrypted symmetric key) using hybrid algorithm.

Algorithm	Total P-text (bits)	Total C-text (bits)	Plain-text to cipher ratio	Total E-time (Sec)	Total D- Time (Sec)	Total Exe Time (Sec)	Throughput
B-RSA(32)	352	422	0.83412	0.04219	0.04252	0.084712	8342.9
B-RSA(128)	448	550	0.81454	0.04372	0.04356	0.097294	10245.4
B-RSA(192)	512	648	0.790123	0.04224	0.04146	0.083712	12119.1
B-RSA(256)	576	732	0.786885	0.04122	0.04086	0.082093	13972.1
B-RSA(448)	768	1012	0.75889	0.04295	0.03773	0.080696	17878.0

From above table we can see that for a same message the total plain text size increased on increasing the size of key. Similarly the cipher text size is slightly more than the plain text size but with same increasing nature with increase in key size. The execution time for Blowfish –RSA with key size 256 bit is found to be least as compared to other hybrid algorithms with different key size this is because there is not much difference in size of total plain text and total cipher text. The decryption time for Blowfish-RSA with key size 448 bit is found to be least. Similarly the throughput is maximum for the hybrid algorithm with key size 448 bit.

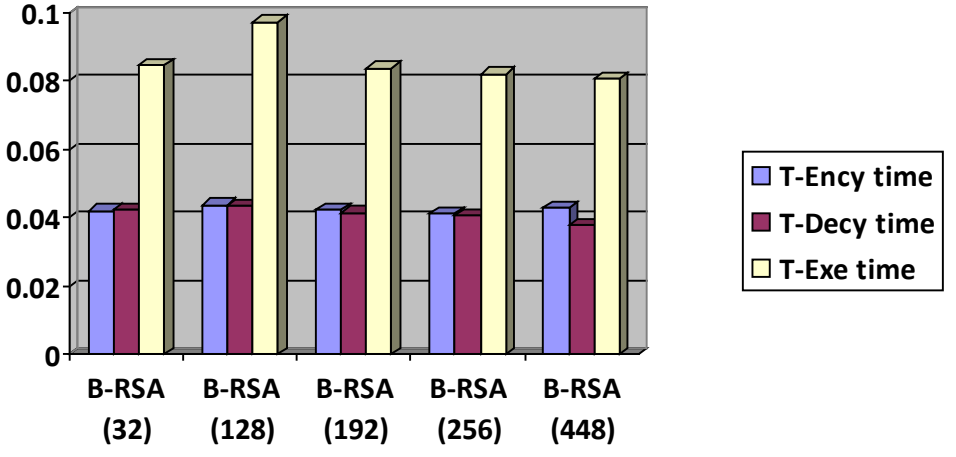

Figure: Bar Chart for hybrid algorithm showing Total encryption time,

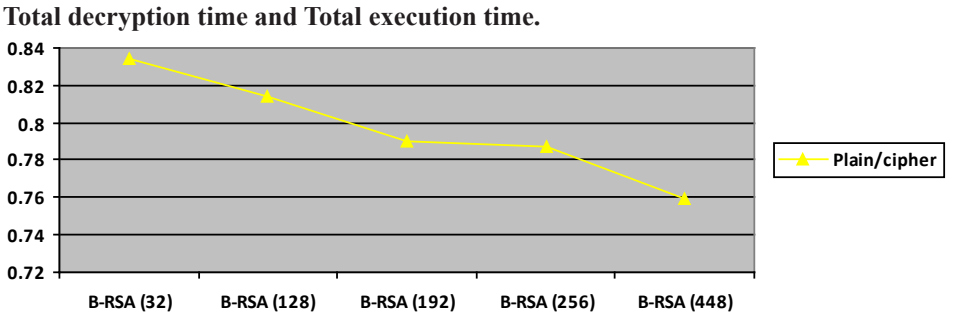

Figure: line graph for hybrid algorithm showing plain text to cipher text ratio

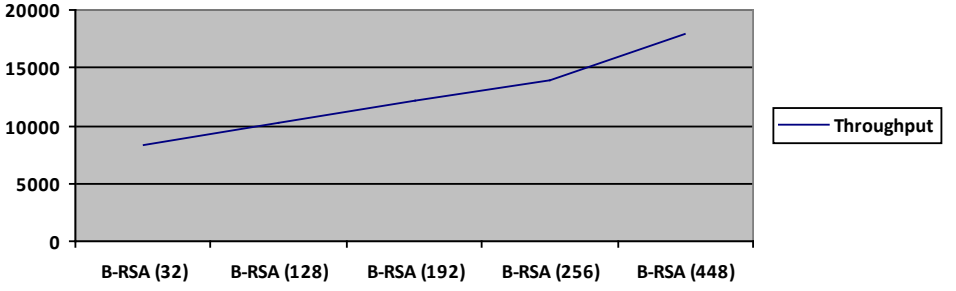

Figure: line graph for hybrid algorithm showing Throughput

CONCLUSION

From all above data it is clearly seen that the hybrid algorithm is safe no doubt then a single algorithm but among the hybrid system made using RSA and Blowfish algorithm with different key size RSA- Blowfish with key size 448 bit has better performance in terms of throughput, Execution time, decryption time and Encryption time.[2]

[1] M. Ebrahim, S. Khan, and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications, vol. 61, pp. 12–18, 2013.

[2] S.C.Iyer, R.R.Sedamkar and S.Gupta, "Multimedia Encryption using Hybrid Cryptographic Approach," International Journal of Computer Applications, May 2013, vol 56.

[3] A.K. Koundinya, Abijith C, Arunraj, Deekshith N.K. Srinath, J.Abraham, "Performance Analysis of Hybrid Cryptographic Algorithm-A^{3}D Algorithm," International Journal of Innovative Research in computer and Communication Engineering, vol 5,pp. 8961-8968, 2016.

[4] S. Singh, S. Maakar, and S. Kumar, "A Performance Analysis of DES and RSA Cryptography," International Journal of Emerging Trends & Technology in Computer Science, vol. 2, no. 3, pp. 418–423, 2013.

[5] N. Garg and P. Yadav, "Comparison of Asymmetric Algorithms in Cryptography," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 1190–1196, 2014.

[6] A.A Gutub, F.A. Khan, "Hybrid Crypto Hardware Utilizing Symmetric-key & Public-Key Cryptosystems," International conference on Advanced Computer Science Applications and Technologies , 2012.