Volume 1, No. 3, Sept-Oct 2010
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

FBR Cryptosystem for Enhanced Security

Akhil Kaushik*
Assistant Professor, Computers Department
T.I.T&S College
Bhiwani, Haryana, India
akhil.kaushik@yahoo.com

Manoj Barnela
Assistant Professor, Electronics Department
T.I.T&S College
Bhiwani, Haryana, India
m.barnela@gmail.com

Satvika Khanna
Assistant Professor, Computers Department
T.I.T&S College
Bhiwani, Haryana, India
satvika16oct@gmail.com

Abstract: In aspect of information security, cryptography is one of the conventional used techniques for secure communication. In contrast to Steganography, Cryptography mechanisms deal with encoding the data into unintelligent information rather than hiding it. Primarily, the cryptography algorithms are categorized into two types which are symmetric key cryptography and asymmetric key cryptography algorithms. The symmetric encryption is much faster and occupies less memory; however its chief disadvantage is distribution of the secret key. On the contrary, asymmetric encryption is more secure but comparatively slower. The focus of this paper is to combine BEST algorithm, a fast and novel technique for symmetric cryptography and RSA, a popular asymmetric key algorithm; to yield a more authentic, secure and faster way of communication. This new hybrid system called Fusion-BEST-RSA (FBR) is developed with aim to achieve advantages of both approaches.

Keywords: Cryptography, Symmetric cryptography, Asymmetric cryptography, FBR, BEST, RSA.

I. INTRODUCTION

Cryptography is an earliest art and it became a prominent saviour for information security with the commercialization of internet. Now, internet has spread over more than 205 countries in the world and with this tremendous growth, the attacks and breaches while sending the information across internet has also increased. The basic need of global corporate world is faster access to accurate information. This aim to secure and faster access of information can be achieved through cryptography. It enables corporate to accomplish three principal goals of security- Availability (information is accessible to authorized parties when needed), Confidentiality (information assets are accessed only by authenticated users) and Integrity (information is altered only by authorized users and only in authorized way)[1][11]. Cryptography can be broadly classified into two categories: Symmetric and Asymmetric encryption.

The first category is known as Symmetric Key Cryptography (Private Key Encryption) as it uses the same key for encryption and decryption of data. It is much faster and efficient technique as the decryption is exactly reverse of the encryption process. Nevertheless this technique also has a shortcoming, which is distribution of the secret key[8]. Suppose if any eavesdropper invades the secure channel and copies all encrypted data but is unable to decode it in sufficient time, but if he finds the encryption key while transferring from sender to receiver, then every bit of data can be decoded easily and the purpose of secure transmission is defeated[12].

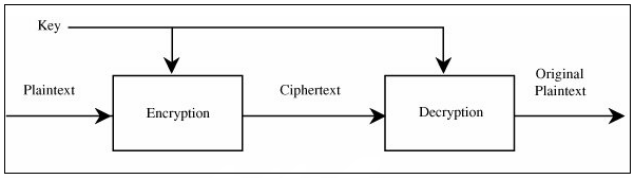

Figure 1. Symmetric Key Cryptography

Another category is known as Asymmetric Key Cryptography (Public Key Encryption) which uses two mathematically associated keys: public key & private key for encryption. When one party needs to send data it will use public key (available to everyone) of receiver to encrypt data. This encoded data can be decoded only by a private key (specific to the receiver) which is associated mathematically to the public key. Asymmetric key cryptography solves the issues of key-exchange, scalability and non-repudiation[5] but it may be slow and occupy more memory than asymmetric encryption.

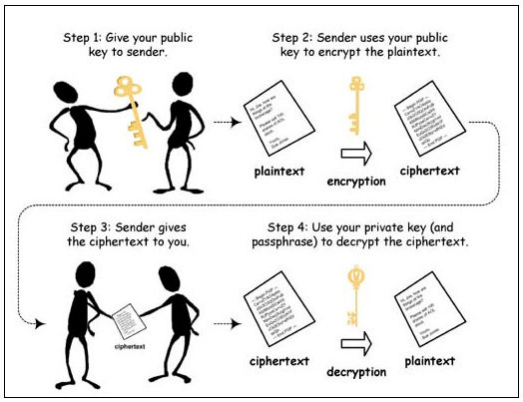

Figure 2. Asymmetric Key Cryptography

It is worthwhile to mention that both approaches are quite different and are not in competition[3]. These two approaches can be combined to form a hybrid system known as Fusion-BEST-RSA (FBR) to get all the pros of BEST and RSA algorithms without any cons. The motive behind developing a new hybrid system is to get performance of secret key cryptography over that of asymmetric encryption, and the appeal of key distribution inherent to asymmetric key cryptography. Here, a fast and highly secure Block Encryption Standard for Transfer of data (BEST) algorithm is employed for encoding the plaintext to form the cipher-text and then the symmetric key of BEST is encrypted using public key of RSA algorithm. This encrypted key will be sent along with encoded data to the receiver. On the receiver's end, private key of RSA is applied to deduce the symmetric key of BEST algorithm. Then this symmetric key is used to decrypt the cipher-text using BEST algorithm and obtain the plaintext finally.

II. BEST ALGORITHM

Block Encryption Standard for Transfer of Data (BEST) is a block cipher which works on symmetric key cryptography[2]. The prime traits of BEST algorithm are as follows:-

a. It operates on 32-bit block of data.
b. It is a partial symmetric key algorithm i.e. encryption does not depend fully on the secret key.
c. The key stream can approximate the properties of a true random stream.
d. For every block of data, a different encoding key and a random number is chosen to enhance security[10].
e. As BEST algorithm uses Unicode, hence it can be implemented in any language across the world.
f. The cipher text produced from BEST algorithm is of same size of the plaintext.
g. The encryption and decryption time of BEST is better than standard encryption algorithms like DES and AES[2].
h. Mixed operators, special symbols and a secondary key are also used to make cryptanalysis more complex.

The steps of encryption process of BEST Algorithm are:-

a. The plain text in the block size of 32 bits is read from input file.
b. The plaintext is transformed into ASCII code and then modified into binary form.
c. Then shift-left operation is performed on this 32-bit data 10 times.
d. The modified plain text is then XORed with a secondary key of 32 bits and it is made sure the result is also of 32 bits.
e. A random number is chosen from a given range and converted into 16-bit binary number.
f. A sequence symbol is randomly selected from a preselected range.
g. The selected symbol is converted into ASCII code and then finally into binary number of 8 bits.
h. The 8-bit binary code is then appended to the 16-bit binary number resulted from random number and the result is stored as the base key.
i. Then the key is applied on the modified plaintext with the help of a binary operation.
j. In the next step, a new key is generated from a different random number and different sequence symbol.
k. Every time a new key is generated, it is applied using a different binary operation on resulted cipher text of previous step and a modified cipher text is obtained.
l. This process is repeated 10 times i.e. ten times a different key is produced and ten times this key is applied on the plaintext or cipher text of previous round.
m. The encryption process is continued for next characters of file until end of file is reached.

Because of the fact that BEST is a symmetric key standard; the decryption process of BEST algorithm is exactly the reverse of the encryption process.

III. RSA ALGORITHM

The RSA algorithm (named after its creators Rivest, Shamir and Adleman) is based on asymmetric key cryptography i.e. it uses two logically related keys for encryption and decryption[4][7]. The main aspects of RSA algorithm are the following:-

a. RSA is computationally easy for receiving party B to generate the key pair (Public key KS_b, Private key KR_b).
b. It is mathematically easy for a sender A to generate the cipher text $C=E_{KSb}(M)$ knowing the public key KS_b and message to be encrypted M.
c. The process of decrypt the resulting cipher text using the private key to recover the original message $M = D_{KRb}(C)= D_{KRb}[E_{KSb}(M)]$ is computationally easy for the receiver B.
d. It is almost infeasible for an opponent to infer the the private key KR_b even by knowing the public key KS_b.
e. It is also impossible for an opponent to calculate and recover the original message M by knowing the public key KS_b, and a cipher text C.
f. The encryption and decryption functions can be applied in either order. $M=D_{KRb}[E_{KSb}(M)]= D_{KSb}[E_{KRb}(M)]$.

The algorithm of RSA work as shown below:-

a. Choose two large prime numbers P and Q.
b. Calculate a number N such that, N = P * Q.
c. Select the public key (encryption key) E so that it is not a factor of (P-1) and (Q-1).
d. Select the private key (decryption key) D such that the following equation is true:
    a. (D * E) mod (P - 1) * (Q - 1) = 1
e. Encrypt the plain text PT to form the cipher text CT: $CT = PT_E \bmod N$.
f. Send CT as the cipher text to the receiver.
g. Decrypt the cipher text CT to form the plain text PT: $PT = CT_D \bmod N$.

IV. DESIGN OBJECTIVES OF FBR

This new proposed FBR cryptosystem is designed to accomplish the following objectives:-

a. The key exchange problem should be addressed.
b. The encryption/ decryption process should be faster.
c. The cryptosystem should have enhanced security.

d. The generated cipher text should be compact in size to solve memory issues.
e. The cryptosystem should be scalable to any number of users depending upon their need.
f. Key management issues should be handled effectively.

V. FBR HYBRID CRYPTOSYSTEM

The FBR Hybrid Cryptosystem is based on combining the BEST and RSA algorithms and to make it efficient, faster and securer than both of its components. Suppose that ABC is the sender and XYZ is the receiver. The working of FBR Hybrid Cryptosystem is discussed below:

a. ABC encrypts the given plaintext with the help of symmetric key (SK) of BEST algorithm and obtains the cipher-text.
b. This symmetric key (SK) is then encrypted with public key (P_BK) of XYZ using RSA algorithm.
c. The encrypted symmetric key acquired from step (b) is sent along with cipher-text to XYZ.
d. On the receiving side, XYZ now implies private key (P_RK) on the modified cipher text to determine the symmetric key (SK).
e. Then XYZ uses symmetric key (SK) and BEST algorithm to find out the plaintext.

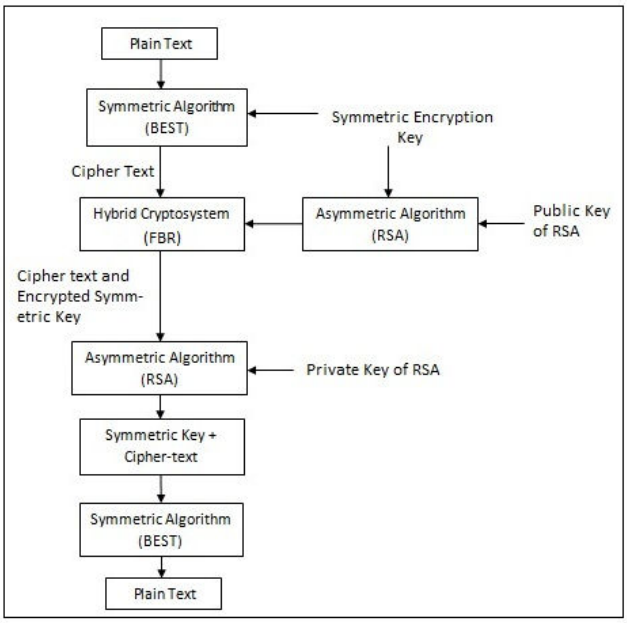

Figure 3: Block Diagram of FBR

The FBR hybrid cryptosystem is a novel approach to secure information transfer. This cryptosystem produces comparatively larger cipher text than the plaintext. Another plus point of it is that RSA algorithm is used only for encryption of symmetric key of BEST and hence the encryption and decryption process is faster. As the encryption of text is done using BEST algorithm and further secret key is encoded; hence achieving ultimate security for transfer of data. This cryptosystem is faster as comparative to RSA and also solves the key-distribution problem of BEST, thus attaining benefits of both types of cryptography.

VI. PERFORMANCE EVALUATION

FBR is basically a new proposed encryption system which combines advantages of both public and private encryption and achieves an enhanced level of security. Experiments show that FBR is immune to 'replay attacks[6]' and in case, eavesdropper comes in and discovers the key, still he will be unable to construe the key because it is encrypted using RSA.

A. Timing Analysis

The core advantage of any cryptographic algorithm is the speed of encoding and decoding of data[9]. FBR algorithm is especially designed for this feature and some time-saving coding is done. The following table shows total (encryption and decryption) times for FBR against its components BEST and RSA.

Table 1. Timing analysis of FBR

Encryption Algorithms	Key Length (Bits)	Input Size (Bytes)	Total Time (sec)
BEST	24	45911	1.8
RSA	8	45911	0.106
RSA	12	45911	0.183
RSA	16	45911	0.183
FBR	24	45911	1.8

B. Memory Requirements

The following table shows that memory prerequisite of FBR is five times lesser as compare to RSA (16-bit key).

Table II. Memory requirement of FBR

Encryption Algorithms	Key Length (Bits)	Plaintext Size (Bits)	Cipher Text Size (Bits)
BEST	24	45911	45911
RSA	8	45911	154340
RSA	12	45911	213350
RSA	16	45911	254180
FBR	24	45911	45928

From the above tables it is concluded that the timing and memory requirements of FBR algorithm is better than BEST and RSA algorithms for the text file with addition to better defense of data.

VII. CONCLUSION AND FUTURE WORK

From the analysis of performance evaluation, it can be stated that FBR can be used as a reliable hybrid cryptographic approach which is much faster than the trendy RSA. It also solves the key exchange issue of the BEST algorithm and makes it practically immune for the eavesdropping. Thus the advantages of both cryptographic systems are preserved in the fusion system FBR. FBR cryptosystem is not only time-saving but also provides enhanced security against unauthorized attacks. Moreover the experiments also show the memory requirements of FBR are lower than well established encryption algorithms. The proposed algorithm proves to be a very efficient technique for transferring messages from sender to the receiver, in addition to confidentiality as well as message authentication. Finally it can be concluded that the newly proposed FBR encryption standard can be a one-stop solution for all information security problems for the transfer of text files.
A proposed direction for the future work could be to analyze the following factors:

a. Implementation of FBR for digital images and speech /audio data.

b. Hardware realization of FBR.
c. Improvement of execution time of FBR.
d. Make it more adjustable for larger input file size.
e. The key value along with the modified secure code sequence can be passed through cipher text by using steganography.

VIII. REFERENCES

[1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone Handbook of Applied Cryptography. New York: CRC Press, Inc., 1997.

[2] A. Kaushik, M. Barnela and A. Kumar, "Block Encryption Standard for Transfer of data", ICNIT, Phillippines, 2010.

[3] B. Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., New York, USA, 1994.

[4] Bellare M. and Rogaway P," Optimal Asymmetric Encryption", Proc. Of Eurocrypt'94,LNCS 950, Springer-Verlag 1995, pp.92-111.

[5] Fujisaki E. and Okamoto T., "How to Enhance the Seurity of Public-Key Encryption at Minimum Cost", Proc. Of PKC' 99, Springer-Verlag, LNCS 1560,1999, pp.53-68.

[6] G. Prosanta, K. Akhil, A. Kushal, and K. Neeraj, "X-MODDES (eXtended Multi Operator Delimiter based Data Encryption Standard)", ICFN, China, 2010.

[7] H. C. Williams, " A Modification of the RSA Public key Encryption Procedure", IEEE Trans. On Information Theory, Vol. IT-26, No.6, 1980, pp.726-729.

[8] Kencheng Zeng, Chung-Huang Yang, Dah-Yea Wei and T.R.N. Rao, "Pseudorandom Bit Generators in Stream-Cipher Cryptography", IEEE Computer, February 1991, pp 8-17.

[9] M. Luby, "Pseudorandomness and Cryptographic Applications", Princeton, NJ: Princeton Univ. Press, 1996.

[10] P.K. Stephen and K. W. Miller, "Random Number Generators: Good ones are hard to find", Communications of the ACM, October 1988.

[11] P.P Charles & P.L Shari, "Security in Computing: 4th edition", Prentice-Hall, Inc.,2008.

[12] W.Stallings, "Cryptography and network security principles and practice," Fourth edition, Prentice hall, 2007.