A New Approach towards Encryption Schemes: Byte – Rotation Encryption Algorithm

Sunita Bhati[1], Anita Bhati[2], S. K. Sharma[3]

Abstract- **Information security is a challenging issue in today's technological world. There is a demand for a stronger encryption which is very hard to crack. Earlier many researchers have proposed various encryption algorithms such as AES, DES, Triple DES, RSA, Blowfish etc. Some of them are most popular in achieving data security at a great extent like AES and Blowfish. But, as security level is increased, the time and complexity of algorithm is also increased. This is the major cause of decreasing the speed and efficiency of the encryption system. In this paper we have proposed a new encryption algorithm "Byte – Rotation Encryption Algorithm (BREA)" with "Parallel Encryption Model" which enhances the security as well as speed of the encryption scheme. The BREA is applied on different blocks of plaintext and executes in parallel manner through multithreading concept of single processor system. This paper is an attempt to invent a new encryption model which is secure and very fast.**

Index terms- **Encryption, decryption, multithreading, random hash function.**

I. INTRODUCTION

Cryptography is an art of hiding information. A lot of research has been done in the field of cryptography. There are various encryption algorithms used for secure data transmission. The AES has been adopted as a Standard for Encryption by NIST (National Institute of Standards and Technology's). The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized users for malicious purpose. Therefore, it is necessary to apply effective encryption / decryption methods to enhance data security. The multiple encryption and multilevel encryption system provides sufficient security. But the performance and speed of these systems is low. Their complexity is very high. In this research paper, a new encryption algorithm named "**Byte – Rotation Encryption Algorithm (BREA)"** is proposed which is applied on different blocks of plaintext and executes in parallel manner through multithreading concept of single processor system. This paper is an attempt to invent a new encryption model which is more secure and very fast to others.

II. RELATED WORK

Cryptography is the study of transmitting secret messages securely from one party to another. To accomplish this task, the original text, called plaintext, is translated into an encrypted version called cipher text, which is sent to the intended recipient. The recipient decrypts the text to obtain the original message. Cryptography is considered not only a part of the branch of mathematics, but also a branch of computer science. There are three main forms of cryptosystems: Symmetric Encryption System, Asymmetric Encryption System and Hash Functions. These models of encryption have been developed to provide security of information but each of them having some merits and demerits. No single algorithm is sufficient for this purpose. As a result researchers are working in the field of cryptography to remove the deficiency and finding better solution. In this paper, an effort has been made to develop a new algorithm BREA which is a block cipher and used with Block Wise Parallel Encryption Model [6]. The model has been written into two steps. In the first step, the plaintext has been broken into number of blocks. Each block size is of 16 bytes. So the number of blocks depends on the total input bytes of plaintext. Each block is represented by 2D array. These arrays of blocks are passed into BREA in parallel manner to execute simultaneously by using multithreading concept. The concept will allows all the blocks to process parallel in CPU. Because of parallel execution, the processing speed of the system will enhance.

III. PROPOSED BYTE -ROTATION ENCRYPTION ALGORITHM

The BREA algorithm has the following features…

1. It is a Symmetric Key Block Cipher Algorithm.
2. Each block size is of 16 bytes.
3. Size of Key matrix is 16 bytes.
4. Values of Key matrix are randomly selected and ranging from 1 to 26.
5. Mono alphabetic substitution concept is followed.
6. Byte-Rotation technique is used.

The steps of proposed Byte-Rotation Encryption Algorithm:

1. The letters of alphabet are assigned numerical values from 1 to 26 in sequence i.e. A, B, C, ..., X, Y, Z assigned numerical values 1, 2, 3, ..., 24, 25, 26 respectively, the digits from 1 to 9 assigned numerical values from 27 to 35 respectively and the zero (0)

Manuscript received June 19, 2012; revised August 10, 2012.

1. Sunita Bhati, Research Scholar, PAHER, University, Udaipur, 313001, Raj. , India. E-mail: bhati.sunita01@gmail.com, Contact No. 009887037537.
2. Anita Bhati, Research Scholar, PAHER, University, Udaipur, 313001, Raj. , India. E-mail: anita27_bhati@rediffmail.com , Contact No. 009887037637
3. Prof. S. K. Sharma, Director, Pacific Engineering College, Udaipur, 313001. E-mail: sharmasatyendra_03@rediffmail.com, Contact No. 009352118885.

remains as it is.

2. The plaintext is partitioned into fixed-length blocks of size 16 bytes (or 128 bits) each. These blocks are represented by a matrix M_p.

3. The values of Key matrix (K) are randomly selected from the range 1 to 26. The size of Key matrix is equivalent to the block size of plaintext i.e. 16 bytes.
$K = [k_1, k_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots, k_{16}]$
$K =$ Random (1, 26, 16)

4. Calculate the Transpose matrix of plaintext block matrix (M_p), which is denoted by Mp^T.

5. Calculate encrypted Key matrix K_e using the following formula:
$K_e = K \bmod 2$

6. Add both the matrices Mp^T and K_e and the resultant matrix is denoted by C_{pk}.
$C_{pk} = Mp^T + K_e$

7. Rotate first three rows horizontally of C_{pk} matrix such that rotate one byte from first row, rotate two bytes from second row, rotate three bytes from third row and fourth row remains untouched. The resultant matrix is denoted by C_{hr} .

8. Rotate first three columns vertically of C_{hr} matrix such that rotate one byte from first column, rotate two bytes from second column, rotate three bytes from third column and fourth column remains untouched. The resultant matrix is denoted by C_{vr}.

9. Replace numeric values of C_{vr} matrix by their corresponding letters and if 36 exist in C_{vr} matrix, it is replaced by the special character #. The resultant matrix is denoted by C_e.

IV. EXPLANATION OF BREA

Example: In BREA, the letters of alphabets are assigned a numeric value as stated in the algorithm. Let the input plaintext is:

RAYMONDS SUITINGS

Its plaintext block matrix M can be represented as:

$$M = \begin{array}{|c|c|c|c|}\hline R & A & Y & M \\ \hline O & N & D & S \\ \hline U & I & T & I \\ \hline N & G & S & 0 \\ \hline\end{array}$$

Now substitute numeric values of letters in the above block matrix as shown below:

$$M_p = \begin{array}{|c|c|c|c|}\hline 18 & 1 & 25 & 13 \\ \hline 15 & 14 & 4 & 19 \\ \hline 21 & 9 & 20 & 9 \\ \hline 14 & 7 & 19 & 0 \\ \hline\end{array}$$

Find the transpose matrix of M_p

$$Mp^T = \begin{array}{|c|c|c|c|}\hline 18 & 15 & 21 & 14 \\ \hline 1 & 14 & 9 & 7 \\ \hline 25 & 4 & 20 & 19 \\ \hline 13 & 19 & 9 & 0 \\ \hline\end{array} \qquad \ldots\ldots\ldots (1)$$

Then, calculate Key matrix of size 16 bytes by random selection of any 16 numbers from 1 to 26 as given below:

$K = [k_1, k_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots, k_{16}]$

$K =$ Random (1, 26, 16)

$$K = \begin{array}{|c|c|c|c|}\hline 25 & 15 & 3 & 9 \\ \hline 20 & 7 & 13 & 8 \\ \hline 5 & 18 & 22 & 17 \\ \hline 21 & 12 & 26 & 24 \\ \hline\end{array}$$

Calculate K_e by using the following formula:
$K_e = K \bmod 2$ . ... (2)

$$K_e = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 \\ \hline\end{array} \qquad \ldots\ldots\ldots\ldots\ldots (3)$$

Add both the matrices Mp^T and K_e and the resultant matrix is denoted by C_{pk}.

$C_{pk} = Mp^T + K_e$ .... (4)

$$C_{pk} = \begin{array}{|c|c|c|c|}\hline 18 & 15 & 21 & 14 \\ \hline 1 & 14 & 9 & 7 \\ \hline 25 & 4 & 20 & 19 \\ \hline 13 & 19 & 9 & 0 \\ \hline\end{array} + \begin{array}{|c|c|c|c|}\hline 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 \\ \hline\end{array}$$

$$C_{pk} = \begin{array}{|c|c|c|c|}\hline 19 & 16 & 22 & 15 \\ \hline 1 & 15 & 10 & 7 \\ \hline 26 & 4 & 20 & 20 \\ \hline 14 & 19 & 9 & 0 \\ \hline\end{array} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Now, horizontally rotate the bytes of first three rows as given below:

C_{pk} =

19	16	22	15
1	15	10	7
26	4	20	20
14	19	9	0

C_{hr} =

16	22	15	19
10	7	1	15
20	26	4	20
14	19	9	0

…............. (6)

Similarly, vertically rotate the bytes of first three columns as given below:

C_{hr} =

16	22	15	19
10	7	1	15
20	26	4	20
14	19	9	0

C_{vr} =

10	26	9	19
20	19	15	15
14	22	1	20
16	7	4	0

……………...... (7)

The numeric values of the cipher block C_{vr} is replaced by their corresponding alphabetic letters and we get the encrypted block C_e:

C_e =

J	Z	I	S
T	S	O	O
N	V	A	T
P	G	D	0

……......... (8)

The cipher texts block C_e and key matrix K sends to the recipient. At the receiver end, the above stated BREA executed in reverse order to decrypt the cipher text into plaintext. Since the proposed BREA has no complex calculation still it is very secure because of random key selection process and the key size is 128 bits which is hard to crack by the intruders. This algorithm is executed with Block Wise Parallel Encryption Model [6] as shown below:

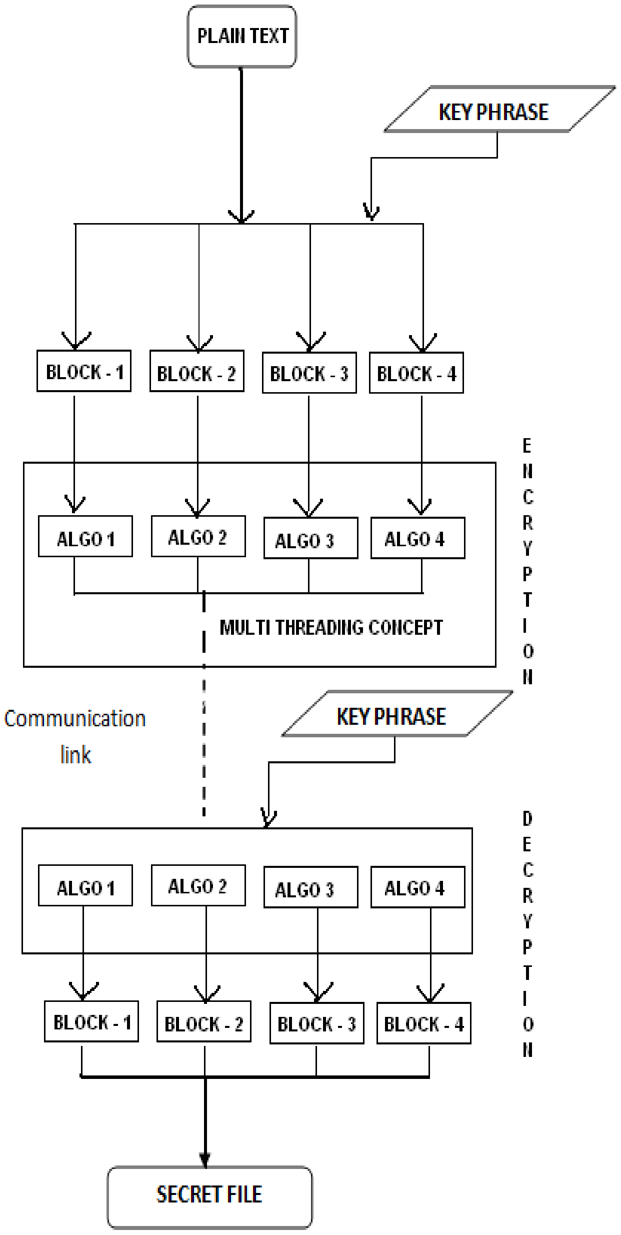

Fig 1: Block Wise Parallel Encryption Model

Block Wise Parallel Encryption System which is different and efficient from the existing systems as follows:

1. System is developed in such a way that it is platform independent. Where, the existing systems are limited to platform dependent design.
2. It is developed with the idea of multiple and multilevel encryption system.
3. The number of encryption algorithms is used; hence the security offered is very high.
4. This proposed system is developed in order to support not only text files but also images and media files. But still many of the existing systems are developed in order to suit basic text formats.

The input plaintext which is to be fed into our system is chosen at first. Then, a key phrase is entered for data authentication. Then plaintext data is divided into blocks. Four blocks passed into four threads of BREA at a time. These threads executes simultaneously by using multithreading technique. After encryption, these blocks send to receiver where the blocks are passed into the Reverse – BREA in parallel manner. Then the cipher text is decrypted into plaintext and all the blocks of plaintext scrambled together to get the original message. Since the algorithm executes parallel using multithreading technique, the execution speed and performance of the model increases. **Multithreading:** It is an ability of OS to support multiple threads of execution within a single process. A thread is a small block of a program / execution unit.

Uses of Multi Threading:
→ *Division of work*

- ➢ Foreground & background work
- ➢ Asynchronous processing
- ➢ Pipeline/Parallel execution

→ *Organization of work*

- ➢ Modular program structure

Benefits of Threads:

- ➢ Takes less time to create a new thread than a process
- ➢ Less time to terminate a thread than a process
- ➢ Less time to switch between two threads within the same process
- ➢ Threads within the same process share memory and other resources, they can communicate with each other without invoking the kernel.

So our model is very fast to other suggested models.

V. FUTURE ENHANCEMENT

The system can be easily modified to accept any encryption algorithm which would be framed in future. Just by adding or removing another module in the main function, any number of algorithms can be included or reduced. Moreover, we currently concentrate on our next work which adopts Parallelism through multiprocessor system where we can run various Encryption Algorithms in parallel environment which enhances the performance and speed of Encryption/ Decryption process.

VI. CONCLUSION

Each algorithm having its own advantages and disadvantages, our system proposed a good strategy of making most out of the advantages of BREA while trying to eliminate the limitations. The developed system ignoring the front end could be used in any network services for network security. The concept of block wise parallel encryption using multithreading technique enhances the speed of encryption system. The system also proposed a new encryption algorithm “BREA” which provides enough security. Thus the system is justified for its use in securing files.

REFERENCES

[1] Sairam Natarajan #1,“A Novel Approach for Data Security Enhancement Using Multi Level Encryption scheme”, Research paper, IJCSIT, Vol. 2 (1), 2011, 469-473.

[2] Himanshu Gupta, “Multiphase Encryption Technique”, An Article, Amity University U.P., March 2011 http://en.wikipedia.org/wiki/A_New_Concept_for_Multiphase_Encryption_Technique

[3] Daniel Lloyd Calloway, Dr. Hannon (Instructor), “Literature Review of Cryptography and its Role in Network Security Principles and Practices”, Lecture Notes, Capella University, OM8302, 8 Sept. 2008.

[4] W.Stallings, “Cryptography and Network Security: Principles and Practices”, Prentice Hall, 1999.

[5] Walter Tuchman , "A brief history of the data encryption standard", ACM Press/Addison-Wesley Publishing Co. NY, USA, pp. 275–280,1997.

[6] Sunita Bhati & Prof. S. K. Sharma, “Block Wise Parallel Encryption through Multithreading Concept”, Research Paper published in Aishwarya Research Communication Journal (ISSN : 0975-3613) Vol. 3, August 2011, pp. 100-106.