An Encryption Technique using Randomized Region Swapping Approach

Mogili Ankamma Rao[1]
M.Tech Student
Department of Computer Science & Engineering
VVIT, Nambur (V), Guntur (Dist.), India

R. Sudha Kishore[2]
Assistant Professor
Department of Computer Science & Engineering
VVIT, Nambur (V), Guntur (Dist.), India

***Abstract*-- In today's digital communication world information has become more valuable; hence its security becomes crucial and plays an eminent role. To provide such security we propose a new encryption mechanism that operates on sixteen byte blocks of data in two stages. Entire plaintext is divided into number of blocks and in the first stage inner region swapping is done on each block followed by key application. Second stage merely does outer region swapping where two randomly selected blocks are exchanged for some number of rounds. The basic advantage of this approach is, it uses simple operations and is simple to use, understand and feasible to implement. Security provided by this mechanism is also high as all the operations are done based on randomness induced by generated random values.**

***Keywords*-- Cipher Text, Plain Text, Enciphering, Deciphering, Symmetric and Asymmetric key, BREA.**

I. INTRODUCTION

The prominence of information sharing in day to day life now has increased a lot, since the world has become a village with usage of Internet. Security has become a challenging issue and is concerned with making sure that nosy people cannot read or worse yet modify messages intended for the receiving parties. Various public and private organizations such as defense, financial organizations and social networking groups require network security to achieve confidentiality and integrity of the information in the network transit. To withstand several security attacks we should consider sending data or information using several security mechanisms to receiving parties. These mechanisms include several various cryptographic techniques which are categorized as symmetric and asymmetric algorithms [1][2][3][4].

Cryptography is the conversion of plain text (meaningful data) into cipher text (unmeaningful data). Conversion of plain text into cipher text involves substituting or transposing the plain text data itself. Till now various algorithms have been proposed which are based on either substitution or transposition and each has their own advantages and pitfalls. As a result researchers are striving hard to enhance the security further in the domain of communication over networks. Our security mechanism proposed is a block symmetric algorithm which does both scrambling (transposition) and modification (substitution) on the plain text blocks using a secret key at sender and receiver reverses the operations to recover original message from cipher text.

In this paper, we propose an encryption scheme that applies simple operations on given data based on random values and hence provides high security to data. Proposed encryption scheme divides data into several blocks of size 16. For each block it generates an eight bit key value. It operates in two stages. In the first stage, each block undergoes two rounds. First round divides block of size 16 into four sub blocks of size 4. Out of these 4 sub blocks, two sub blocks are swapped based on key value for that block. In the second round, Caesar cipher type of encryption is applied on block x based on key of 16 bits which is obtained by concatenating key x and key x+1. The keys are selected in circular fashion. After completion of two rounds, each block contents gets transposed and substituted which completes first stage of proposed approach. Second stage goes through number of Rounds (w) to operate on data obtained from first stage based on number of blocks (N). In each round it randomly selects two blocks and swaps their contents. Finally key file is generated and is sent along with cipher text.

In the next sections we discuss the following issues. In section II, we present related work, and section III details proposed encryption process with detailed analysis. An illustrative example is given in section IV. A Decryption process is given in section V. Final section concludes and presents future work of the proposed approach.

II. RELATED WORK

Different encryption mechanisms Hill Cipher, AES, DES and Triple DES have been developed so far operating on blocks of data. F. Y. Li Min's queue transformation based digital image encryption algorithm [5] works efficiently with low time complexity, but it signifies some regularity. Efficient Digital Encryption [6] proposed by Kiran Kumar et al yields good scrambled cipher text but it does only transposition. Byte Rotation Encryption algorithm [BREA] [7] proposed by Sunita Bhati et al. operates in four stages. Firstly it reads data into different blocks of size 16. It then transposes each block contents. Second stage applies ceaser cipher type of encryption on each block based on key. Third stage does row operations by shifting first row one position to left, second row two positions to left and so on. Final stage shifts first column one position upwards, second column two positions upwards and so on. Though it is simple to understand and implement, it has certain shortcomings. It uses only 16 bit key for all the blocks which is very limited. Matrix Transposition is done in first stage which has no special significance. Row and column operations are fixed which presents monotony in the process. Our Encryption is enhancement to BREA algorithm which tries to increase key size and tries to avoid monotony in the process by random selection of operations.

III. PROPOSED MECHANISM

This paper puts forward a symmetric key based block encryption algorithm that is applied on individual blocks of plain text. First the plain text is divided into several blocks of size 16 and padding is done in case if the last block lacks sufficient bytes of data. Let plain text size is P, then no. of blocks of size 16 possible is N where N = P/16. N keys of size 8 bits are randomly generated with binary values one for each block. After generation of blocks and their corresponding keys, the encryption process operates in two stages Inner Region Swapping and Outer Region Swapping.

A. *Inner Region Swapping:*

Each block in this stage goes through two different rounds.

Round 1: It divides each block of size 16 bytes into four independent sub blocks indexed SB0, SB1, SB2 and SB3 of size 4 bytes each as shown in Fig 1.

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

A	B
E	F

C	D
G	H

I	J
M	N

K	L
O	P

Fig 1. Block divided into sub blocks

From the figure SBO = {A,B,E,F}, SB1 = {C,D,G,H}, SB2 = {I,J,M,N} and SB3 = {K,L,O,P} where SB denotes sub block. Key of the same block is divided into four parts. Four parts decimal values are obtained and from them first two different values are identified. Based on those values, bytes of the corresponding sub blocks are swapped. Let two different values be 0 and 2 then SB0 SB2 contents are swapped.

Round 2: This round does substitution operation on each block based on 16 bit key. It expands key of a block x to 16 bits by appending key x with key x+1 in circular fashion. It means block 1 gets 16 bit key formed from appending keys of block 1 and 2. Block 2 gets key from keys of block 2 and block 3 and so on. Block N gets key from keys of block N and 1. The application of key on block values is given in the following equation.

$$B_{ij} = B_{ij} + K_{ij} \quad \text{where } 1 \leq i \leq N,\ 1 \leq j \leq 16$$

Here B and K denote a block and its corresponding expanded key. Values i and j represent a block (key) and its byte (bit) value. The same process is repeated for the remaining blocks and keys (8 bits) of the corresponding blocks are recorded in key file. Once the entire process is done, all blocks are forwarded to second stage of encryption.

B. *Outer Region Swapping:*

This stages arranges all blocks from block 1 to block N in a sequential order in FIFO basis. Based on N value, it determines number of rounds w to do outer region swapping on blocks. In each round, it randomly selects two blocks say Bx and By and swaps their contents. The blocks selected are recorded in key file.

1. Read the plain text into N blocks of size 16 bytes.
   B1,B2………..Bn.
2. Generate N keys of size 8 bits.
   K1, K2 ………..Kn
   // Inner Region Swapping
3. For each block b in {B1, B2, ……………….Bn}
   i. Divide b into 4 equal sub blocks b1, b2, b3, b4.
   ii. [x, y] = Select first two different sub blocks based on key of b.
   iii. Swap sub blocks bx and by.
   iv. New Key of b = Key of b || Key of b+1
   v. For each byte z in {1,2,……16} of block b.
   vi. Z = (Z+1). If z value of b New Key = 1
   End for.
   End for
4. Write N keys to key file.
   // Outer Region Swapping
5. W = Select number of rounds based on N.
6. Write W to key file.
7. For i=1 to W rounds
   i. U = Select a block out of N.
   ii. V = Select next block from N, U ≠ V
   iii. Swap blocks U and V
   iv. Record U and V positions in key file
   End for
8. Construct cipher text from N blocks.

Proposed Algorithm

This process is continued for the remaining rounds. The operation of one particular round is shown in following example.

B0 B1 B2 B3 B4 B5 B6 B7 ……BN

Let Bx = 1 and By = 6 then after swapping

B0 B6 B2 B3 B4 B5 B1 B7 ……BN

The detailed steps of encryption system are presented in Fig 2.

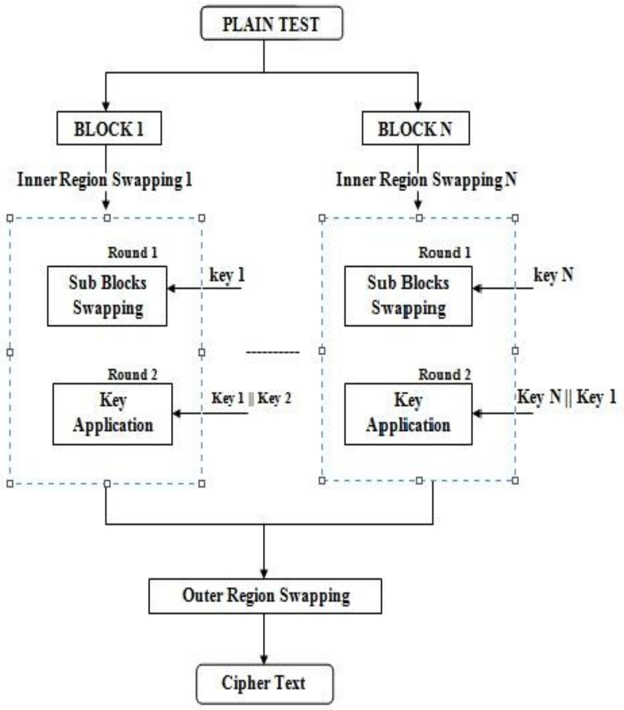

Fig 2: Encryption process

IV. ILLUSTRATIVE EXAMPLE

This section explains the encryption mechanism with a simple example. Let the plain text size is 64 bytes and takes the following values

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43, 44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63 , 64

Based on plain text size four blocks are possible of size 16 and for each block eight bit key is generated and let the key values are

00110110, 10100100, 00001010, 01010110

Round 1 operations of Inner Region Swapping process is given in Fig 3 where in block 1 sub blocks 0,3 are swapped, in block 2 sub blocks 2,1, in block 3 sub blocks 0,2 and last block sub blocks 1,2 gets swapped.

Locations and swapped sub blocks locations are highlighted in the Fig 3 and Fig 5.

1	2	3	4	17	18	19	20	33	34	35	36	49	50	51	52
5	6	7	8	21	22	23	24	37	38	39	40	53	54	55	56
9	10	11	12	25	26	27	28	41	42	43	44	57	58	59	60
13	14	15	16	29	30	31	32	45	46	47	48	61	62	63	64

00	11	01	10	10	10	01	00	00	00	10	10	01	01	01	10

11	12	3	4	17	18	25	26	41	42	35	36	49	50	57	58
15	16	7	8	21	22	29	30	45	46	39	40	53	54	61	62
9	10	1	2	19	20	27	28	33	34	43	44	51	52	59	60
13	14	5	6	23	24	31	32	37	38	47	48	55	56	63	64

Fig 3: Round 1 of Internal Region Swapping

11	12	3	4
15	16	7	8
9	10	1	2
13	14	5	6

0	0	1	1
0	1	1	0
1	0	1	0
0	1	0	0

11	12	4	5
15	17	8	8
10	10	2	2
13	15	5	6

key application for block 1

17	18	25	26
21	22	29	30
19	20	27	28
23	24	31	32

1	0	1	0
0	1	0	0
0	0	0	0
1	0	1	0

18	18	26	26
21	23	29	30
19	20	27	28
24	24	32	32

key application for block 2

41	42	35	36
45	46	39	40
33	34	43	44
37	38	47	48

0	0	0	0
1	0	1	0
0	1	0	1
0	1	1	0

41	42	35	36
46	46	40	40
33	35	43	45
37	39	48	48

key application for block 3

49	50	57	58
53	54	61	62
51	52	59	60
55	56	63	64

0	1	0	1
0	1	1	0
0	0	1	1
0	1	1	0

49	51	57	59
53	55	62	62
51	52	60	61
55	57	64	64

key application for block 4

Fig 4: Round 2 of Inner Region Swapping

Key application of round 2 of Inner Region Swapping is shown in Fig 4 where block's values get changed where there are 1's in keys.Outer Region Swapping mechanism is presented in figure 6. Suppose rounds selected in this phase is w = 2 then random selection of two blocks and their swapping.

11	12	4	5
15	17	8	8
10	10	2	2
13	15	5	6

18	18	26	26
21	23	29	30
19	20	27	28
24	24	32	32

41	42	35	36
46	46	40	40
33	35	43	45
37	39	48	48

49	51	57	59
53	55	62	62
51	52	60	61
55	57	64	64

w = 1 , blocks selected : 1 and 3

11	12	4	5
15	17	8	8
10	10	2	2
13	15	5	6

49	51	57	59
53	55	62	62
51	52	60	61
55	57	64	64

41	42	35	36
46	46	40	40
33	35	43	45
37	39	48	48

18	18	26	26
21	23	29	30
19	20	27	28
24	24	32	32

w = 2 , blocks selected : 0 and 2

41	42	35	36
46	46	40	40
33	35	43	45
37	39	48	48

49	51	57	59
53	55	62	62
51	52	60	61
55	57	64	64

11	12	4	5
15	17	8	8
10	10	2	2
13	15	5	6

18	18	26	26
21	23	29	30
19	20	27	28
24	24	32	32

Fig 5: Outer Region Swapping

Of contents is given the figure. Cipher text produced from this entire mechanism is

41,42,35,36,46,46,40,40,33,35,43,45,37,39,48,48,49,51,57,59,53,55,62,62,51,52,60,61,55,57,60,61,11,12,4,5,15,17,8,8,10,10,2,2,13,15,5,6,18,18,26,26,21,23,29,30,19,20,27,28,24,24,32,32.

V. DECRYPTION PROCESS

The decryption of proposed approach exactly works in reverse fashion. It reads cipher text to N blocks of 16 bytes and reads corresponding keys belonging to Inner Region Swapping and Outer Region Swapping from key file. Then it first performs Outer Region Swapping process where it iterates for w rounds as recorded in key file. In each round, it swaps two blocks x and y based on key values. After completion of w rounds, N blocks become ready for Inner Region Swapping. In this, each block of size 16 is partitioned into 4 equal sub blocks similar to encryption process. Out of these, two sub blocks are exchanged based on key corresponding block. Once the entire process is done, original message is constructed by grouping contents of N blocks.

VI. CONCLUSION

This paper attempts to avoid pitfalls in BREA encryption mechanism. In BREA technique, single key of size 16 is used to encrypt all blocks where the key size is limited. But proposed approach uses 8 bit key for each block where each block contents get changed and scrambled based on key. A second phase is also operated in this scheme to do more scrambling of the blocks contents. BREA applies fixed set of row and column operations which induces monotony in the process and becomes easy for the intruder to know the plain text details with minor operations. But in the proposed approach, each operation is done based on random values. Therefore guessing of keys and all these random values out of N blocks is very complex and difficult. Hence it is very tricky and becomes complicated for the attacker to break it. For a cryptanalyst to break the encryption technique, he has to try

$(2^8 \times N) \times (Nc_2)^w$ trails where former denote trails required for breaking Inner Region Swapping and later for breaking Outer Region Swapping. Finally it is very easy to understand, implement and is feasible to operate in any environment. In our future work we try to reduce key size or try to do encryption using asymmetric key and also try to incorporate more random operations.

REFERENCES

[1] I.Tanenbaum, AS, “Computer Networks” 2nd edition, Prentice Hall, London.1989.
[2] Stinson, D.R, “Cryptography Theory and Practice”, CRC Press, London, 1995.
[3] Network Security Essentials Applications and Standards, William Stallings, Pearson Education, New Delhi.
[4] Cryptography and Network Security, 2nd Edition by Atul Kahate. Tata Mc-Graw-Hill Publications, New Delhi.
[5] F.Y. Li Min,(2005), ”A new class of Digital Image Scrambling Algorithm based on the method of Queue Transformation”, Computer Engineering ,01(31):148-149.
[6] M. Kiran Kumar., et al, “Efficient Digital Encryption Algorithm Based on Matrix Scrambling Technique”, Journal of Network Security and its Applications, vol.2, no.4: 30-41,October 2010.
[7] Sunita Bhati., et al, “A New Approach towards Encryption Schemes: Byte – Rotation Encryption Algorithm”, Proceedings of the World Congress on Engineering and Computer Science, Vol II, 2012.

AUTHORS

Mogili Ankamma Rao[1] is pursing Master of Technology in Computer Science and Engineering from JNTU Kakinada. He has received Bachelor of Technology in Information Technology form Acharya Nagarjuna University in 2011. His research interests are Information Security and Web Technology.

R. Sudha Kishore[2] is working as Assistant Professor in VVIT, Andhra Pradesh, INDIA. He has received B.Tech and M.Tech degrees from JNTU Hyderabad. This author has overall 9 years teaching experience and guided more than 10 innovative projects as a part of his academic work. His research interests are Image processing, Information security, security algorithms.