Implementation of Block based Data Encryption at Bit - Level

Sanjit Mazumder[1], Sujoy Dasgupta [1], Prof. (Dr) Pranam Paul [2]
[1] Student, M. Tech. (CSE), Narula Institute of Technology, Agarpara, West Bengal, INDIA
[2] Computer Application, Narula Institute of Technology, Agarpara, West Bengal, INDIA

ABSTRACT
with the growth of internet and network, the need for secure data transmission become more and more essential and important, as security is a major concern in the internet world. Data likely to be kept hide from all people except from the authorized user cannot be sent in plane text. So the plane text should be codified i.e. by the process of encryption. Each type of data has its own features, therefore different techniques should be used to protect confidential data from unauthorized access.
Here I introduced a new algorithm based on symmetric key block encryption technique. In this algorithm encryption is done on binary file. Since this encryption is done on binary file so this algorithm is applicable for any data such as text as well as multimedia data.

Key Word:
Cryptography, Encryption, Decryption, Plain Text, Cipher Text, Network Security

1. INTRODUCTION

The rapid growth of computer networks allowed larger files, such as digital image, text to be easily transmitted over the internet. Data encryption is widely use to ensure security of those data. I introduce a block based symmetric key encryption algorithm. For encryption a key is to generate. Key length and bit stream is chosen at random.
Sub-key 1 is generated from key simply taking the entire bit stream except the first two bits. From sub key 1 generate sub key 2, sub key 3 and Sub Key 4 are generated from Sub Key 1 & sub key2 and sub key3 & sub key 3 respectively.
The plane text (Binary text) is divided into four segments of same length and remaining bits are remain unchanged. Each segment is again divided successively of equal lengths length equal to the length of sub key. Each sub blocks are EXOR with sub key to produce the encrypted text.
To get back the original text the operation is called the decryption. In this process the encrypted text first divided into four segments. Each segment EXNOR with the Sub Keys. The Sub Keys are generated as the same way as in the encryption process.
In section 2, Algorithm is defined. While section 3 shows the example of whole process. An analysis along with conclusion has been done in section 4.

Manuscript received February 5, 2011
Manuscript revised February 20, 2011

2. ALGORITHM:

In this section key generation is discuss in the section 2.1. In the section 2.2 and 2.3 discussed Sub key generation from key and encryption respectively.

2.1 Key Generation:

Step-1:A bit stream say K1 having the length say 'l' bits which is less than S/4 is taken randomly. Where "S" is the length of plane text.

Step-2: The key is generated by appending K0 (which is of two bytes long) with K1 at beginning.(Key : K0, K1)

Step-3: If remainder of S/4 = 0 then Set a bit stream K0 = 00

If remainder of S/4 = 1 then Set a bit stream K0 = 01

If remainder of S/4 = 2 then Set a bit stream K0 = 10

If remainder of S/4 = 3 then Set a bit stream K0 = 11

2.2 Sub Key generation from Key:

Step-1: Generating Sub Key-1 : taking the bit stream K-1 (excluding K-0) as Sub key 1 (SK-1).

Step-2: Generating Sub Key-2 : To generating ith bit of SK-2 EXOR operation is performed on ith and (i+1)th bit of SK-1

i.e. ith bit of SK-2=ith bit of SK-1 EXOR (i+1)th bit of SK-1.(where i=1,2,3,…..,(l-1).

Appending lth bit of SK-1 at the lth bit position with the bit stream produce in above in the sequence (l-1),(l-2),(l-3),……..,3,2,1.

Step-3: Generating Sub Key 3: ith bit of SK-1 is EXOR ed with ith bit of SK-2 to produce ith bit of SK-3.

i.e. ith bit of SK-3=ith bit of SK-1 EXOR ith bit of SK-2. Where i=l,(l-1),(l-2),…..,3,2,1.

Step-4: Generating Sub Key 4: In the same way stated above SK-4 is generated by OR ing ith bit of SK-2 with ith bit of SK-3.

i.e. ith bit of SK-4=ith bit of SK-2 OR ith bit of SK-3. Where i=l,(l-1),(l-2),…,3,2,1.

2.3 Encryption Process:

Step-1: Decomposed the plane text into four segments having same length. If "S" be the length of the plane text then length of each segments (say STi, where i=1,2,3,4.) is
Length of STi = ⌊S/4⌋ where i=1,2,3,4.
Let the remaining bits be UB (UB<4)

Step-2: STi where i=1,2,3,4. is again decompose into n numbers of segments having length equal to SKi say "l" which is discussed in section 2.2.

Let each sub block is SSTin where i=1,2,3,4 and l n = 1,2,3,……, ⌊S/4⌋ . The remainder is taken as usual, say USBi (Unchanged sub Block) where i=1,2,3,4. .

Step-3: An EXOR operation has been done with SSTin and SKi to produce to produce a block of text say SETin.

i.e. SST i1 EXOR SKi = SET i1
SST i2 EXOR SKi = SET i2
. .
. .
SST in EXOR SKi = SET in.

Step-4: Appending all SET i1, SET i2, SET i3,……, SET in and USBi (in this sequence) , ETi is generated where i=1,2,3,4.

Step-5: Appending all ETi in the sequence of UB, ET1, ET2, ET3 and ET4 to generate encrypted text.

2.4 Decryption Process:

Step-1:Takes decimal value of the first two bits of the key as " V " .

Step-2: Take first V- bits from the encrypted text as Unchanged Block, UB.

Step-3:Sub Key are being generated according to the process discuss in section 2.2.

Step-4: Rest of the encrypted text (length say S) has been decomposed into four equal blocks. ETi Where i= 1,2,3,4.

Let length of the ETi is "L"
There fore, L= ⌊S/4L⌋

Step-5: ETi (i=1,2,3,4), is again decomposed into n number of segments (as SETin) (i=1,2,3,4 and n=1,2,3,……., ⌊S/4L⌋),having length equal to SKi (i= 1,2,3,4). The remainders are taken as usual say, SUBi.

Step-6: An EXOR operation has been done on SETin and SKi to get SSTin.

SET i1 EXOR SKi = SSTi1
SET i2 EXOR SKi = SSTi2
SET in EXOR SKi = SSTin.

Step-7: Appending all SSTi1, SSTi2, SSTi3,…….SSTin and UEBi (in this sequence) to generate STi (i=1,2,3,4).

Step-8: Appending all STi in the sequence ST1,ST2,ST3,ST4 and UB to obtain decrypted text.

3. EXAMPLE

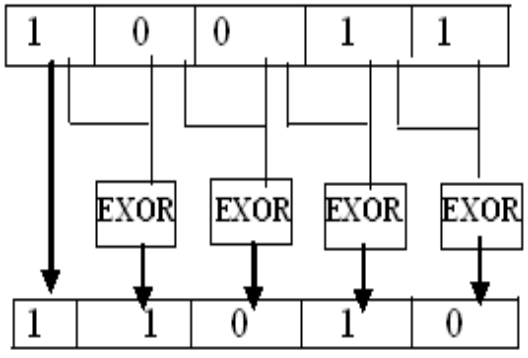
Consider the text 011101010110111101110011
The length of the plane text = S = 24
Let consider the randomly generated bits is 10011= K1. Since the remainder of S/4=0 so K0=00

3.1 Sub Key generation from Key:

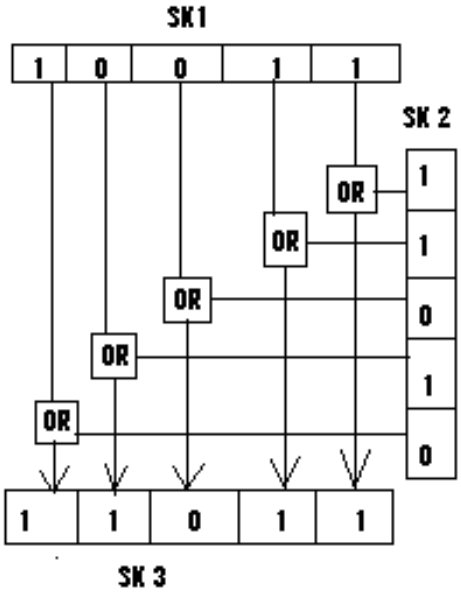
Generation of SK-1 :

1	0	0	1	1

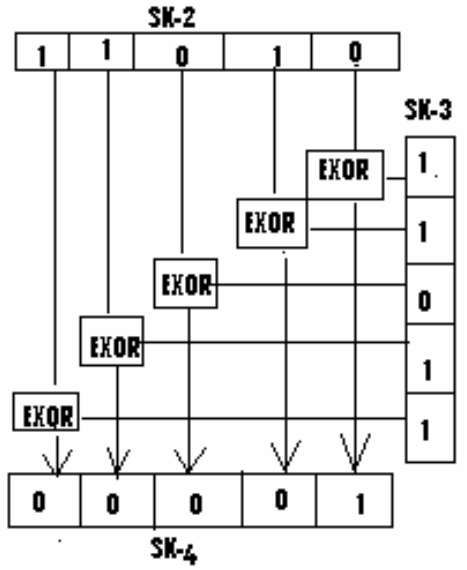
Generation of SK-2:



Generation of SK-3:



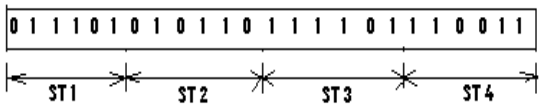
Generation of SK-4:



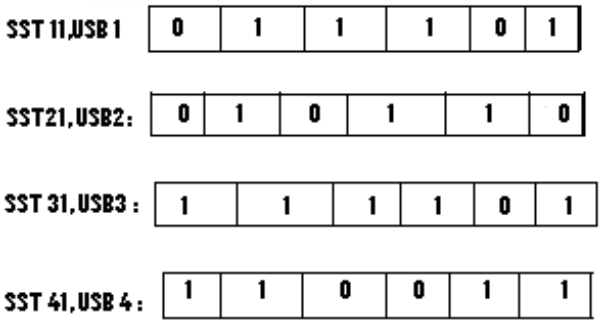
3.2 Encryption Process :

Plane text : 011101010110111101110011
Step-1

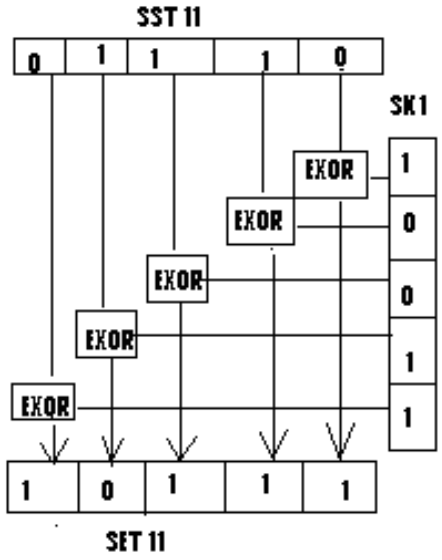
Plane Text

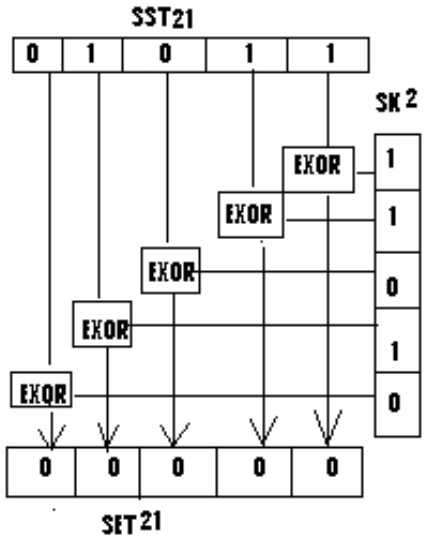


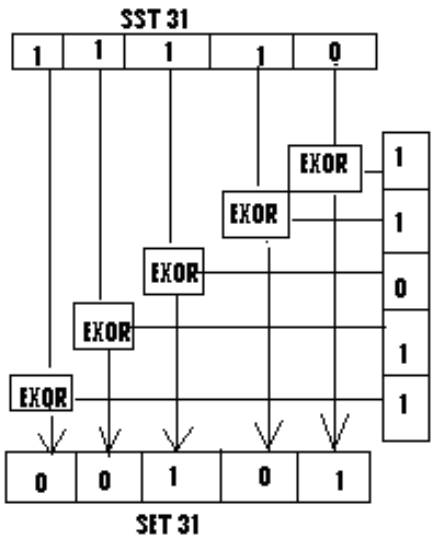
Step-2:

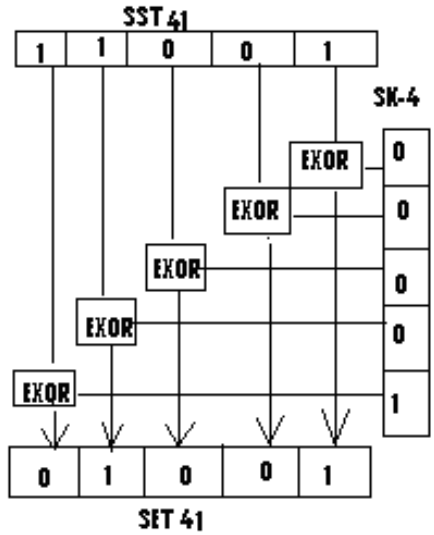


Step-3:









Step 4:

ET 1:	SET 11	USB 1
	10111	1
ET 2:	SET 21	USB 2
	00000	0
ET 3:	SET 31	USB 3
	00101	1
ET 4:	SET 41	USB 4
	01001	1

Generating encryption text:

UB	ET1	ET2	ET3	ET4

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

Step-5:

3.3 Decryption Process:

Key:

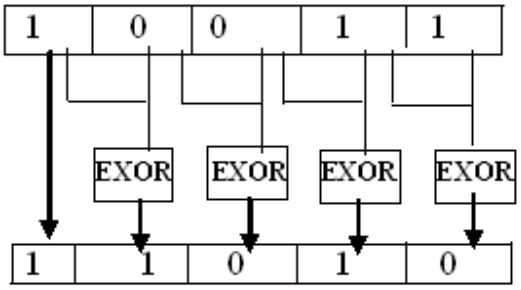
K0	K1
0 0	1 0 0 1 1

Step1: V=0(Decimal value of 00 from R0).
Step-2:

Generation of SK-1 :

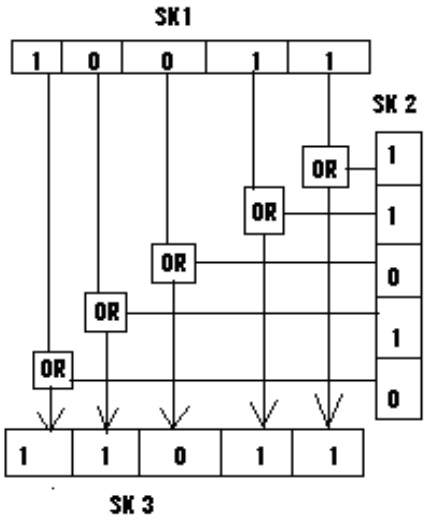
1	0	0	1	1

Generation of SK-2

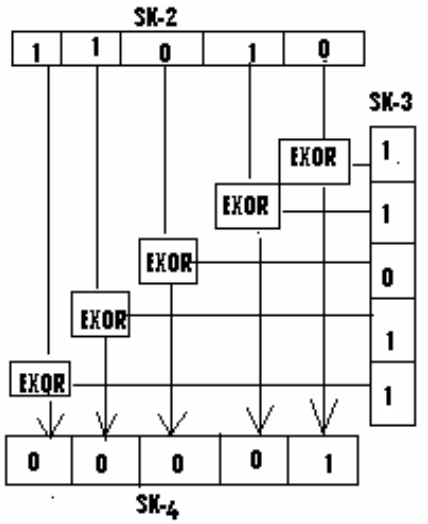


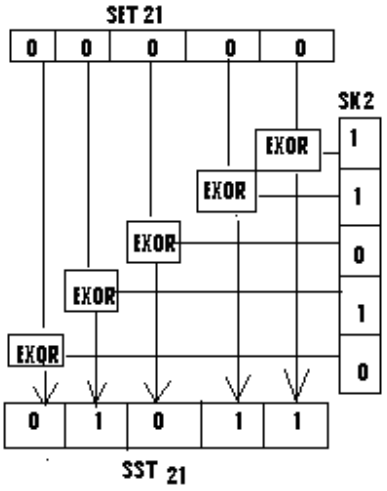
SK-2

Generation of SK-3:

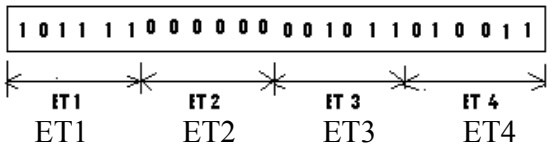


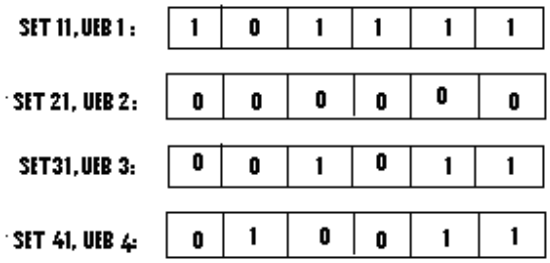
Generation of SK-4:



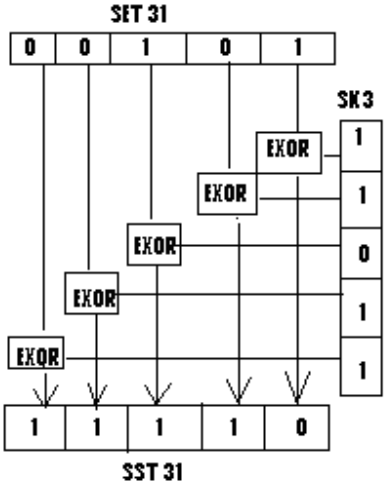


Step-3:

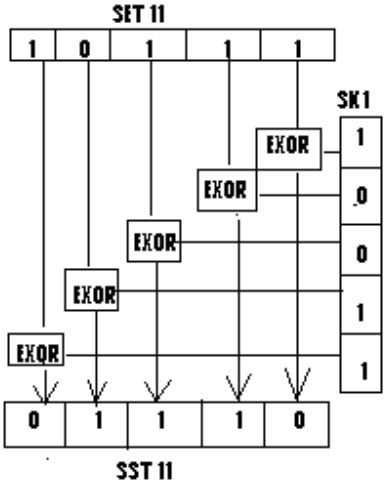


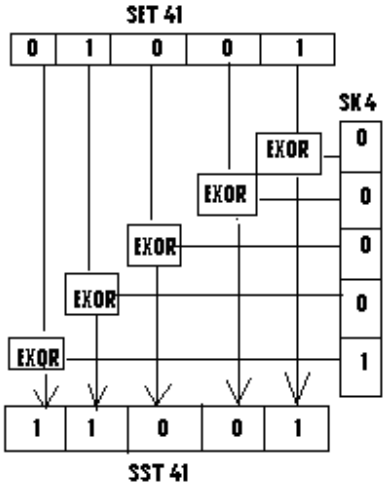


Step-5:



Step-4:





ST1 = 011101, ST2=010110, ST3=111101, ST4=110011,

Step-6:
Decrypted text:
STi:

SSTi	UEBi

UB	ST1	ST2	ST3	ST4

Decrypted text:

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

4 ANALYSIS AND CONCLUSION

In this algorithm encryption is perform on binary data. All data which is under stable by the computer is finally converted into binary bits. So it can be implemented for any data type encryption process. Such as text encryption, image encryption or sound encryption process.

Not only that, the key length is not fixed in this algorithm, so we can take large key for making it more complex. If the key length is assume 'n' then 2n-2 numbers of combination can be possible. So if one bit is increased the possible combination will be 2n-1 i.e. the complexity increased exponentially. In this case if one bit is increase the complexity is increase in exponentially.

In this algorithm the length of the plane text is not restricted so it can be applicable for any large file.

We can shuffle the segments after EXOR ing which produce more difficulties for unauthorized access.

In this algorithm the sub-keys (which are generated from key) length is large so it difficult to access the confidential data for unauthorized user but since the key, which develop the sub-keys are composed of less bits so the data transfer overhead is less.

5. REFERENCES

[1] J. K. Mandal, S. Dutta, "A 256-bit recursive pair parity encoder for encryption", Advances D -2004, Vol. 9 nº1, Association for the Advancement of Modelling and Simulation Techniques in Enterprises (AMSE, France), www. AMSE-Modeling.org, pp. 1-14

[2] Pranam Paul, Saurabh Dutta, "A Private-Key Storage-Efficient Ciphering Protocol for Information Communication Technology", National Seminar on Research Issues in Technical Education (RITE), March 08-09, 2006, National Institute of Technical Teachers' Training and Research, Kolkata, India

[3] Pranam Paul, Saurabh Dutta, "An Enhancement of Information Security Using Substitution of Bits Through Prime Detection in Blocks", Proceedings of National Conference on Recent Trends in Information Systems (ReTIS-06), July 14-15, 2006, Organized by IEEE Gold Affinity Group, IEEE Calcutta Section, Computer Science & Engineering Department, CMATER & SRUVM Project-Jadavpur University and Computer Jagat

[4] Dutta S. and Mandal J. K., "A Space-Efficient Universal Encoder for Secured Transmission", International Conference on Modelling and Simulation (MS' 2000 – Egypt, Cairo, April 11-14, 2000

[5] Mandal J. K., Mal S., Dutta S., A 256 Bit Recursive Pair Parity Encoder for Encryption, accepted for publication in AMSE Journal, France, 2003

[6] Dutta S., Mal S., "A Multiplexing Triangular Encryption Technique – A move towards enhancing security in ECommerce", Proceedings of IT Conference (organized by Computer Association of Nepal), 26 and 27 January, 2002, BICC, Kathmandu.

Sanjit Mazumder is MTech (CSE) final year student of Narula Institute of Technology, Agarpara. He had completed his MSc. in Information Technology.

Sujoy Dasgupta is MTech (CSE) final year student of Narula Institute of Technology, Agarpara. He had complete his BTech in Information Technology.

Dr Pranam Paul is an Assistance Professor cturer of Narula Institute Technology, Agarpara. He had completed his Ph.D from Electronic and Communication Engineering department of National Institute of Technology, Durgapur in the field of Cryptography and Network Security and master degree in Computer Application in 2005 under West Bengal University of Technology, INDIA. He has total 19 International Journal publications among total 32 publications, except this one.