Multi Key XOR Cipher with Parity Check (MX-PC)

Mr.Vinay.S
DOS in Computer Science, Davangere University, Shivagangotri, Davangere-577002, Karnataka(S), India.
vinaygnanesh@yahoo.com

Mr.Shivamutrthaiah.M
DOS in Computer Science, Davangere University, Shivagangotri, Davangere-577002, Karnataka(S), India.
shivamurthaiah@gmail.com

***Abstract*--This paper presents a new Cryptography method which is based on the concept of Symmetric Key Cryptography, bit Cipher Method and Error detection method called Two Dimensional Parity Bit method. This deals with generating a pair of Symmetric keys by using a Key Generator which is a utility in this cryptography system and is available on both sender and receiver side. The Key Generator performs a predefined mathematical calculation on a key value, which is shared between communication parties and generates two unique keys. Encryption includes series of transformations like performing XOR operation, grouping bit stream, adding parity bits and finally bits shifting. These all operation results in obtaining cipher text. In the destination Same Key Generator generating a pair of Symmetric keys and encryption operation performed in reverse order to get back the plain text. This technique provides many benefits like advantage of secondary security in key exchange where key shared between two parties is not the actual crypto key and parity check method for error detection. This entire concept will be implemented as an application program and made available in industries and organizations to provide security in exchange of confidential documents.**

Keywords-Bit Cipher, Transposition cipher, Symmetric key, Parity check method.

I. INTRODUCTION

The Cryptography is a science of securing data from an unauthorized entity. The process of Encryption hides the contents of a message in such a way that the original information is recovered only through a Decryption process. Modern cryptography is strongly based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, the branch of mathematics encompassing both cryptography and cryptanalysis [1]. There are two major categories of cipher methods to perform Encryption, First is Bit Stream method where plain text is converted into cipher text by one bit at a time and the second is Block Cipher method where plain text is divided into block of 8, 16, 32 or 64 bit block and whole block converted at a time into cipher text [2]. Examples for cryptographic algorithms are, Substitution Cipher, Transposition Cipher, Hill Cipher, Vernam Cipher, Running key Cipher, etc. There are two general categories for key-based Encryption: Symmetric Encryption which is also called Private key Encryption [4] here it uses a single key to encrypt and decrypt the message. Asymmetric Encryption is one which uses two different keys – a public key to encrypt the message, and a private key to decrypt its [3].Strength of the encryption depends on size of key. Increase in size of key increases the strength of encryption. For example if number of bits is 32 then estimated Time to crack the code is 8 min & if key size is 56 then it takes 285 years and 32 weeks.[2]. Security policies describe precisely which actions the entities in systems are allowed to take and which ones are prohibited. Entities include users, services, data, machines, and so on.

During transmission of data in the network there may be possibilities of errors in bit stream due to electrical interference or thermal noise and there may be possibilities of Modification of data by intruder in an active attack [6]. There are two most frequently used error detection techniques are CRC and Parity check method. Parity method is the one which involves adding one additional bit for every 7 bits to balance no of 1"s in bit stream [6].

Here in our application we are using both type of parity check methods named single dimension parity check and two dimension parity check for finding errors and active attacks in transmission. We are using XOR cipher which is one of the Bit cipher method to encrypt the data.

Our new Cryptography method presenting in this paper will works on basic principles of symmetric Key cryptography, Bit cipher method and error detection method called Two Dimensional Parity Check method.

This new approach mainly consists of three major steps: Key Generator, Encipher and Decipher.

The key Generator algorithm takes a single character or a symbol as an input which we call it as Primary Crypto key (Pck) and generates two different keys which can be used one after another in encryption and decryption process which we call those as Secondary Crypt keys(ScK1 and Sck2). This Key Generator algorithm runs on both sides to provide keys. The character key which is used to generate symmetric keys is shared between two parties. The Encipher algorithm works on sender side where Encryption starts with performing XOR operation with bits of a primary key shared between pair communication parties. Ten in next step that bit stream is splitting into 49 characters fixed size blocks and a single block of variable size bits when exact 49 bits are not available to create a fixed size block. These both type of blocks are manipulated separately. On each block parity bits are added and row and column shifting is performed then these all operations results in production of cipher text.

For decryption in some way same encryption will be performed in reverse order by using those same keys. In the sequence of decryption process before the final step error detection is performed by analyzing bit pattern. If there is an error decryption

process will be terminated and a warning message will be displayed .if no error final step will be executed to get back the plain text.

II. ALGORITHMS

Mainly there are three algorithms in this application.
A. Key Generator
B. Encryption
C. Decryption.

A. Key Generator

One of the main features of our cryptographic algorithm is of generating two symmetric keys from a single character represented as PcK and this is the key which is going to be shared between both communication entities through a secured channel.

The key Generator accepts character (PcK) and first it finds the ASCII value for that character called as PcKN then next it performs division operation; Dividing PcKN by 7. The dividend and the remainder of this calculation are considered as Secondary Crypto keys, named as ScK1 and ScK2 respectively. For the exception cases like; if the Dividend or the Remainder value is 0 or 8 then by default consider it as 7. Same key Generator algorithm is used on both the sides.
Figure 1 shows the operations of Key Generator algorithm.

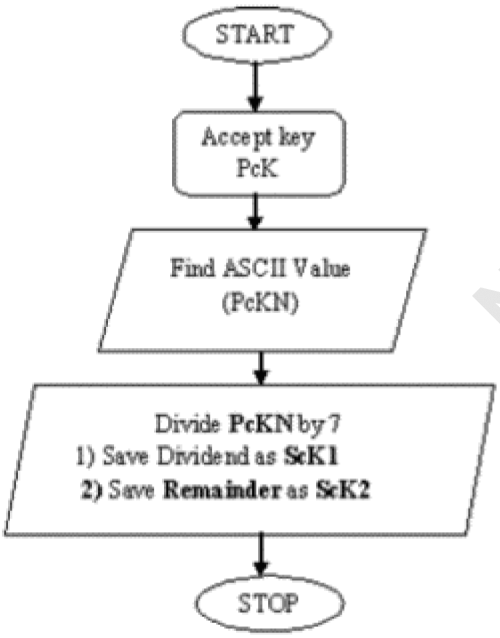

Figure 1: Key Generator.

Example Code:

```
int x, Sck1 ,Sck2,PcKN;
char Pck;

void Keygen()
{

        clrscr();
        printf("Enter a character\n");
        scanf("%c", &ck);
        x=Pck;
        printf("ASCII = %d\n", x);
        Sck1=x%7;
        ScK2k=x/7;
        printf("Dividend= %d\n",Sck1);
        printf("Remainder = %d\n",Sck2);
        }
```

B. Encryption

Encryption process consists of four stages.
First: Performing XOR operation. Second: grouping bit stream in to set of fixed size block and single variable size. Third: Adding two dimensional parity bits to fixed size blocks. Fourth: shifting rows and columns of blocks.

- FIRST: Accept the plain texts bit stream and perform XOR operation on that bit stream with Primary Crypto Key-PcK.
- SECOND: Divide the resultant bit stream of FIRST step into 49 bits fixed size blocks and represent them in 7 X 7 matrices. For exception cases like; if in the final, 49 bits are not available to create a fixed size block then those are grouped separately as a variable size Block.
- THIRD: For fixed size block two dimensional parity bit method applied .Count the number of 0"s and 1"s in each column and rows then add one parity bit 0 or 1 whichever is in odd numbers on each column and row. Now each fixed size block becomes two dimensional arrays of 8x8 sizes.
- Add on dimensional parity bit for each seven bit of variable size block.
- FOURTH: On each fixed size block bits of each Column are Right shifted for „ScK1" times then bits of each Row are shifted upward for ScK2 times.
- Bits of variable size block are Right shifted for „ScK1" times.

Resultant of all these steps gives the cipher text.
Figure 2 shows the working of Encryption.

Example Code:

```
int a[100][100], i, j, b[7][7];

int BlockCreate()
    {
      for(i=0;i<=3;i++)
         {
          for(j=0;j<=4;j++)
                scanf("%d",(*(a+i)+j));
                }
 for(i=0;i<=3;i++)
        for(j=0;j<=4;j++)
              {
                *(*(b+i)+j)=*(*(a+((i-2+4)%4))+j);
              }
              for(i=0;i<=3;i++)
                {
                 for(j=0;j<=4;j++)
  printf("%d\t",*(*(b+i)+j));
```

```
            printf("\n");
        }
    return 0;
}
```

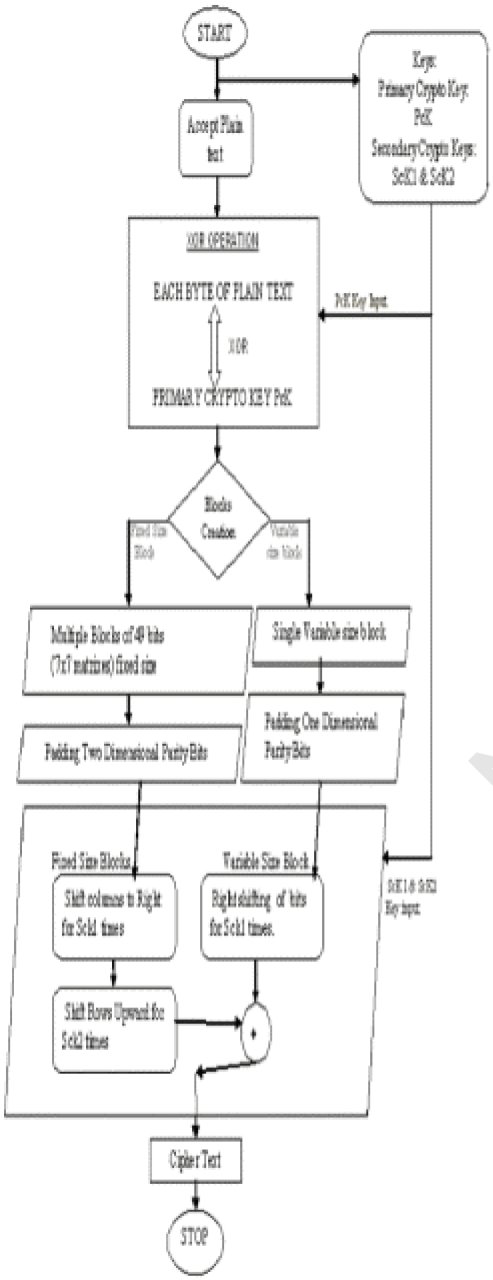

Figure 2: Encryption process

C. *Decryption*

Decryption process consists of four stages which is quite similar to encryption process but in reverse order. Here before completing decryption process error detection should be made by checking the bit pattern of cipher text by grouping them in eight bit each. If there is no error control is moved to final step of decryption process to get the plain text. If there is an error then decryption process is terminated and receiver will get an error message.

FIRST: grouping bit stream in to set of 64 bit fixed size blocks and single variable size block. SECOND: Shifting rows and columns of blocks in reverse to the encryption order. Third: Check bit patterns for error detection. If there is no error, then remove parity bits from each block. FOURTH: Performing XOR operation on bit stream using PcK value.

- FIRST: Divide the bit stream of cipher text into fixed size blocks of 64 characters and represent them in 8X8 matrices. For exception cases like; if in the final, 64 bits are not available to create a fixed size block then those are grouped separately as a variable size Block.
- SECOND: On each fixed size block bits of each Row are shifted downward for „ScK2" times and Column are left shifted for „ScK1" times then bits of each variable size block are left shifted for „ScK1" times.
- THIRD: Bit pattern is analyzed by counting the number of 0"s and 1"s in each column and rows analyzed for detecting errors. Then if there is no error then two dimensional parity bits from fixed size blocks are removed and one dimensional parity bits are removed from variable size block.
- FOURTH: On the resultant bit pattern got from THIRD step, XOR operation is performed on that by using PcK value.

These sequence of steps results in obtaining the plain text.
Figure 3 shows the working of Decryption.

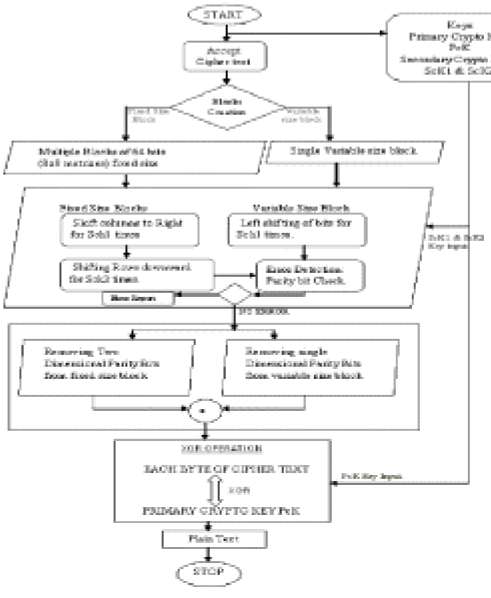

Figure 3: Decryption Process

III. CONCLUSION

This new Cryptographic technique is simple and effective to secure confidential data in transmission. It includes one of the best error detection technique called as parity check method which helps to find one of the active attack method where intruder going to modify the data stream. This technique can be implemented easily as an application with any programming language and the algorithm is simple and quite small which consumes less time to implement and size of the application is less so occupy less memory in computer system. Compare to present well-known cryptographic techniques which are similar to our proposed algorithm, our new technique is quite different because it provides advantage of secondary security in key exchange and error detection technique. Here we suggest that it is safer if Character key which is used to generate cryptographic keys and encrypted data are to be sent in separate email or message. Moreover if intruder hacks the character key they are not aware of generating those two symmetric keys by using that character key. It is best suitable to fulfill the data security of sensitive administrative documents in the organization.

For the future enhancement it can be transformed to Public key encryption and Strength of encryption operations can be enhanced by implementing sequence of different encryption algorithms.

IV. REFERENCES

[1] Bruce Schneier. Applied cryptography, 2nd edition, Author. Publication: Whitfield Diffie.
[2] William Stallings. Cryptography and network security Principal and practice, 3rd edition, Publication: Pearson Prentce.
[3] Atul Kahate. Cryptography and network security, 2rd edition. Publication:
[4] Tata McGraw Hill Edition Private Limited.
[5] Artur Ekert, Carolina Moura Alves, Ajay Gopinathan, "History of Cryptography".
[6] V.K.Pachaghare. Cryptography and information security, Publication: PHI.
[7] Behrouz A.Forouzan. Data Communication and Networking, Fourth
[8] edition. Tata McGraw-Hill Publication.
[9] Research Paper: A plain key compliment XOR Cipher Method. Vinay S & Shivamurthaiah M. Journal Publication ISBN: 978-81-92820309. (National
[10] conference on Software and information management. on 27 Sept 2013)
[11] Research Paper: Private C-Multi Key S-Matrix Block Cipher. Vinay S & Shivamurthaiah M. Journal Publication ISBN: 978-81-207-8818-3. (National conference on Convergence in Operational and Computational Technology COCT 2k14.28 March 2014)
[12] International Journal of Computer Science and Security, Volume (1) .Issue
[13] (1), 2009. Majdi Al-qdah & Lin Y