Algorithm for generating sub-keys/basins from a New Substitution Block Cipher Algorithm

Akanksha Shukla[1], Harikesh Pandey[2]

Akanksha Shukla, M.tech student , R.I.T.M, U.P, India

Harikesh Pandey, Associate Professor, R.I.T.M, U.P, India

Abstract:-*The technological advancement, the internet and information sharing has both positive and negative impacts. One of the negative impacts was the large increase in new information threats. Many of the computer incidents exploited confidential information being stored by companies in a variety of different industries, these incidents have raised a number of concerns about how the information is being secured and maintained in a proper manner. One of the main techniques to fulfil security goals is cryptography which means "secret writing". It is the science of using mathematics to encrypt and decrypt the data. Security mechanism generally involves much more than algorithm and protocols for encryption and decryption purpose and also for generation of sub keys. In the present work an effort has been made to generate an algorithm which provides security to data transmitted.*

Keywords: encryption, decryption, symmetric-key, block cipher, substitution, transposition, matrix key

1. INTRODUCTION

As the value of the data transmitted over a internet is increasing, the search for the best solution to secure the data against the attacks along with providing security services in timely manner is one of the most important subject in the security related environment. A cryptographic algorithm works in combination with a key- a word, number- to encrypt the plaintext. The security of encrypted data depends on two things:-the strength of the cryptographic algorithm and the secrecy of the key. Before starting to algorithm the definition of block cipher must be presented –"a cipher is an algorithm for performing encryption and decryption (reverse of encryption)". In block cipher data is encrypted and decrypted in form of blocks. In simple way, one can divide the plain text in to blocks which are then fed in to the cipher system to produce blocks of cipher text.

Security is often viewed a s the need to protect one or the more aspects of network's operation and permitted use(access, behavior, performance, privacy and confidentiality included).Security requirements may be global or local in their scope, depending upon the network's or internet work's purpose of design and deployment.

Primary elements of security of any computer network include security provisioning at the sending node, intermediate forwarding node, receiving node, inter-connection links and mechanism of transmission or reception at physical and logical levels. A symmetric –key modern block cipher encrypts an n-bit block of plaintext or decrypts an n-bit block of cipher text.

2. METHODOLOGY OF THE PROPOSED WORK

Step 1: Consider the sequence for n-8 to 26 values.

Step 2: Convert the sequence to ternary form of a 3 digit number.

i.e. 0--------------000

1--------------001

2--------------002 up to 26------------222

Step 3: Represent above ternary form in 27*3 matrix

$$R=\begin{pmatrix}
0 & 0 & 0 \\
0 & 0 & 1 \\
0 & 0 & 2 \\
0 & 1 & 0 \\
0 & 1 & 1 \\
0 & 1 & 2 \\
0 & 2 & 0 \\
0 & 2 & 1 \\
0 & 2 & 2 \\
1 & 0 & 0 \\
1 & 0 & 1 \\
1 & 0 & 2 \\
1 & 1 & 0 \\
1 & 1 & 1 \\
1 & 1 & 2 \\
1 & 2 & 0 \\
1 & 2 & 1 \\
1 & 2 & 2 \\
2 & 0 & 0 \\
2 & 0 & 1 \\
2 & 0 & 2 \\
2 & 1 & 0 \\
2 & 1 & 1 \\
2 & 1 & 2 \\
2 & 2 & 0 \\
2 & 2 & 1 \\
2 & 2 & 2
\end{pmatrix}$$

Step 4: Subtract 1 from each element of the above matrix and the resulting matrix R is

$$R=\begin{pmatrix}
-1 & -1 & -1 \\
-1 & -1 & 0 \\
-1 & -1 & 1 \\
-1 & 0 & -1 \\
-1 & 0 & 0 \\
-1 & 0 & 1 \\
-1 & 1 & -1 \\
-1 & 1 & 0 \\
-1 & 1 & 1 \\
0 & -1 & -1 \\
0 & -1 & 0 \\
0 & -1 & 1 \\
0 & 0 & -1 \\
0 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & -1 \\
0 & 1 & 0 \\
0 & 1 & 1 \\
1 & -1 & -1 \\
1 & -1 & 0 \\
1 & -1 & 1 \\
1 & 0 & -1 \\
1 & 0 & 0 \\
1 & 0 & 1 \\
1 & 1 & -1 \\
1 & 1 & 0 \\
1 & 1 & 1
\end{pmatrix}$$

Step 5: Consider a random matrix (user input)

$$A=\begin{pmatrix} 3 & 2 & -1 \\ 2 & 4 & 0 \\ 5 & 2 & 1 \end{pmatrix}$$

Step 6:- R= R*A

$$R*A=\begin{pmatrix} -10 & -8 & 0 \\ -5 & -6 & 1 \\ 0 & -4 & 2 \\ -8 & -4 & 0 \\ -3 & -2 & 1 \\ 2 & 0 & 2 \\ -6 & 0 & 0 \\ -1 & 2 & 1 \\ 4 & 4 & 2 \\ -7 & -6 & -1 \\ 3 & -2 & 1 \\ -5 & -2 & -1 \\ 0 & 0 & 0 \\ 5 & 2 & 1 \\ -3 & 2 & -1 \\ 2 & 4 & 0 \\ 7 & 6 & 1 \\ -4 & -4 & -2 \\ 1 & -2 & -1 \\ 6 & 0 & 0 \\ -2 & 0 & -2 \\ 3 & 2 & -1 \\ 8 & 4 & 0 \\ 0 & 4 & -2 \\ 5 & 6 & 1 \end{pmatrix}$$

Step 7: R=Convert all positive values in to 1, negative values in to -1 and zero to 0 of resulting matrix of step 6.

$$R=\begin{pmatrix} -1 & -1 & 0 \\ -1 & -1 & 1 \\ 0 & -1 & 1 \\ -1 & -1 & 0 \\ -1 & -1 & 1 \\ 1 & 0 & 1 \\ -1 & 0 & 0 \\ -1 & 1 & 1 \\ 1 & 1 & 1 \\ -1 & -1 & -1 \\ -1 & -1 & 0 \\ 1 & -1 & 1 \\ -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ -1 & 1 & -1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & -1 & -1 \\ 1 & 0 & 0 \\ -1 & 0 & -1 \\ 1 & 1 & -1 \\ 1 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

Step 8: Add 1 to each element of the matrix R.

$$R=\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \\ 2 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 2 & 2 \\ 2 & 2 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 2 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \\ 0 & 2 & 0 \\ 2 & 2 & 1 \\ 2 & 2 & 2 \\ 0 & 0 & 0 \\ 2 & 0 & 0 \\ 2 & 1 & 1 \\ 0 & 1 & 0 \\ 2 & 2 & 0 \\ 2 & 2 & 1 \\ 1 & 2 & 0 \\ 2 & 2 & 0 \\ 2 & 2 & 1 \end{pmatrix}$$

Step 9: Convert each row of the matrix R in order to derive a decimal form to generate sequence.

i.e first row of the matrix will convert according to the following rule:

001will form $0*3^2+0*3^1+1*3^0=1$

So, the required sequence is: 1 2 11 1 2 23 4 8 26 0 1 20 0 13 26 6 25 26 0 18 22 3 24 25 15 24 25

2.1 Algorithm for generating sub-keys/basins from the generated sequence

i. Consider the values range from 0-n where n is an integer.

ii. Now read the sequence generated above.

iii. Now read the 1st element of the sequence of the step 1 and store it and then take the corresponding element of step 2 and store it in separate basin.

   a. Compare the element of step3 with element of step 2, if there is a match store it in the basin specified in step 3 and neglect the elements which are already visited.

   b. Now repeat the same procedure with the rest elements of step 3 and store it one basin.

iv. Go to next element of step 2which is not visited earlier.

Now for the above generated sequence:

n[27]=0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26

r[27]=1,2,11,1,2,23,4,8,26,0,1,20,0,13,26,6,25,26,0,18,22,3,24,25,15,24,25

iii). Read the value n[0]=0 and store the values of n[0] and r[0] in a basin i.e b(0,0)=(0,1).

a) n[0] i.e 0 is compared with the values of r[27]. There is a match found at r[0,9,12,18]. Thus b(0)=[0,9,12,18].

b) Now the above step is repeated again with the rest elements of the b[0]. For 9 and 12 there is no match found in r[27], for element 18 match is found at r[19]. Thus the updated basin b [0]=(0,9,12,18 &19).

iv) The procedure is repeated for the next element of n[27] which are not visited earlier and the other basins formed are:

b[1]=(1,3,10,21),
b[2]=(2,4,5,6,7,8,11,15,16,20,22,23,24,25,26),
b[3]=(13) and b[4]=(14,17)

3. FUTURE SCOPE:

As in the present work plain text in form of characters of English alphabets is transformed so more work is to be needed to improved so that it can support not only the English characters also other languages as well. It can also be improved to support not only text also for audio, video etc.

4. CONCLUSION:

In the present work matrix key is used. As in the present algorithm matrix key of 3*3 is considered according to which a sequence is generated as if there is change in a matrix key a sequence will also be change according to that so we found that little change in the matrix key produces significantly change in cipher text which provides maximum avalanche effect in this algorithm. Also by increasing the length of the sub-key security of the cipher text can be increased more.

REFERENCES:

[1] Vol.7 No.3 A Performance Evaluation of Common Encryption Techniques with Secure Watermark System.

[2] Performance Evaluation of Symmetric Encryption Algorithms Vol.8, 2009 ISSN.

[3] Performance Evaluation of Cryptographic Algorithms Vol.41-No.7

[4] Bruce 1996 BRUCE SCHNEIER, Applied Cryptography, John Wiley and Sons Inc.1996.

[5] www.ijaiem.org Volume 3, Issue 11.

[6] A Comparative Study and Performance Evaluation of Cryptographic Algorithms Ijartet Vol.1 issue 3.

[7] www.ijecs.in VA Literature Survey on Performance Evaluation of Encryption Algorithms Vol. 3 Issue 12.

BIOGRAPHY:

Did my B.tech with hons. from UPTU and pursuing M.tech from AKTU.

Assistant Professor at R.I.T.M since 5 years in Computer Science and Engineering department