Cryptographic Technique using Substitution through Circular Path Followed by Genetic Function

Subhranil Som[#], Mandira Banerjee[*]

[#]Department of Computer Application, JIS College of Engineering
[*] Department of Computer Application, Kalyani Government Engineering College

ABSTRACT

In this paper a new algorithm for encryption and decryption is introduced. The process of substitution and genetic function is the core of the proposed algorithm. In this encryption technique two keys are required for the encryption or decryption of a message. Input stream will be produced intermediate cipher text on which two stages of crossover will be used in the process of encryption and decryption to produce final cipher text.

Keywords

Substitution, Encryption, Decryption, Key, Crossover, Cipher text, Plain text.

I. INTRODUCTION

The demand for effective internet security is increasing exponentially day by day [1]. So for high protection, maintaining integrity of the data a robust and secure security system is needed. Cryptography is the science of making communications unintelligible to everyone except the intended receiver(s) [2]. A cryptosystem is a set of algorithms which are indexed by some key(s), for encoding message into cipher text and decoding back into plain text [3, 4].

This paper gives a new algorithm for encryption and decryption. The algorithm is based on the process of substitution and genetic function. In this technique each letter of a plain text is placed into a circular path of the proposed model, by using a random number, substitution of the plain text into intermediate cipher text, is done in a unique way. Genetic function at bit level is used using another key, named 'pivot'. Finally, the cipher text is obtained and just in the inverse way (using all keys) plain text will be achieved from the cipher text. Using the two keys give secure strength to this algorithm. When some intruder attacks the text, the pivot point cannot be found to create the intermediate text. Even if one can calculate the pivot point by trial or error method then also it is near to impossible to calculate the plain text from intermediate text. Because here we have been used a random number, it may be 7896 or 12596846214 depending on the pivot.

In section II the Scheme has been discussed. Flow chart of crossover for encryption and decryption is given in the section III. Example has been discussed in the section IV. Conclusive discussion is written in section V. Future scope followed by References is given in the section VI and VII respectively.

II. THE SCHEME

In the proposed model each letter of an input stream is placed into a circular path where each head holds one letter. All are shown in Figure – I.

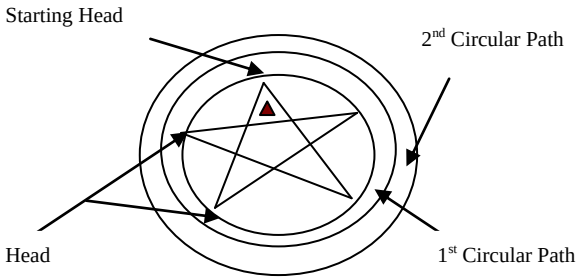

Figure – I

A random number has been chosen which is not a prime. The random number is modulated by 26. The modular result is added with the position number of original letter, which is placed on the first circular path. The addition result is the position number of the substituted letter. The next letter of the first circular path is substituted in the same way but the modular result is incremented by one in each time. When second circular path is started, the substitution value is calculated by the addition of position value of original letter, incremented value of modular result and the position value of original letter(s) which is held by the same head in previous Circular path. By this way substitution of all the letters of the input stream will generate the intermediate cipher text. After that all the letters are converted into its binary code. The bits are divided into five sections. If there is any remainder part, discard it and is store for future use.

After that genetic function is followed. A pivot point is used as a key which is used for two stages cross over between two blocks of bits. In the reverse way plain text can be retrieved from the cipher text. At the time of decryption pivot = n-(pivot as secret key) +1[where n = number of bit present in a section].

III. FLOW CHART REPRESENTATION OF CROSSOVER FOR ENCRYPTION AND DECRYPTION

Encryption:

Each set of bits in a section is denoted by a number such as 1, 2, 3, 4, 5 and 'X' is indicating crossover between two blocks of bits. Crossover between block 1 and block 5 will generate two blocks 1.1 and block 1.5. Crossover between block 2 and block 4 will generate two blocks 2.2 and block 2.4. In this first stage of crossover block 3 will remain same. Second stage crossover between block 1.1 and block 2.4 will generate two set of blocks 3.1 and 3.4 respectively and crossover between block 2.2 and

block 1.5 will generate two blocks 4.2 and 3.4 respectively. Block 3 remains same in this stage also. The block diagram of these 2 stages of crossover in the process of encryption is given Figure – II.

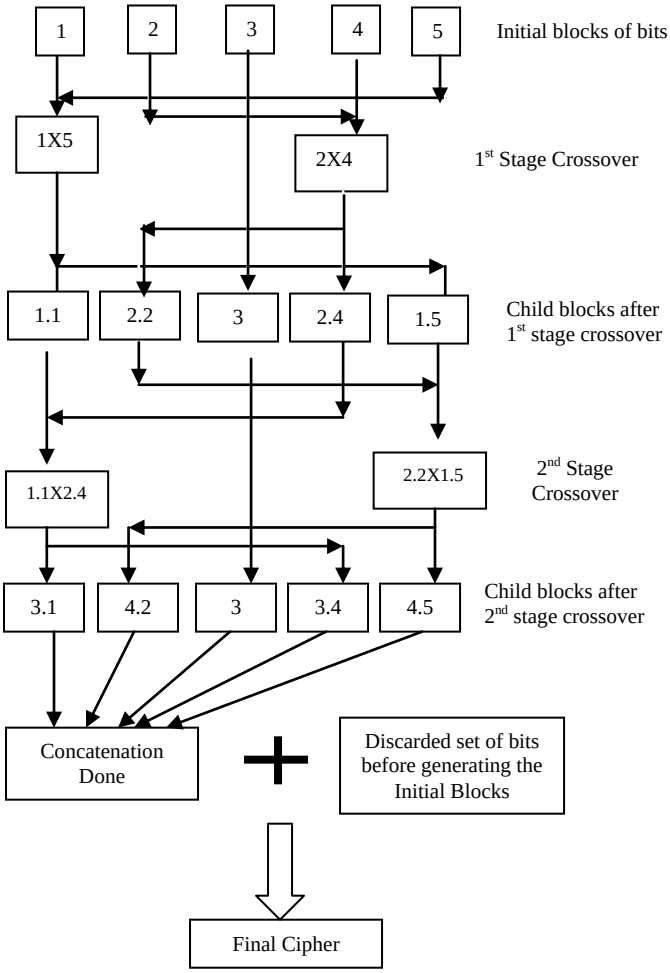

Figure – II

Decryption:

At first discard the set of bits which is added lastly at the time of encryption. Cipher text is divided into five blocks. Crossover between blocks 1 and block 4 to produce blocks 1.1 and 2.5. Crossover between blocks 2 and 5 to produce blocks 2.2 and 1.4. Block 3 will remain same. In second stage of crossover blocks 1.1 and 2.5 will produce the blocks 3.1 and 4.4. Crossover between blocks 2.2 and 1.4 to produce blocks 4.2 and 3.1. Block 3 remains same in this stage also. The block diagram of these 2 stages of crossover in the process of encryption is given Figure – III.

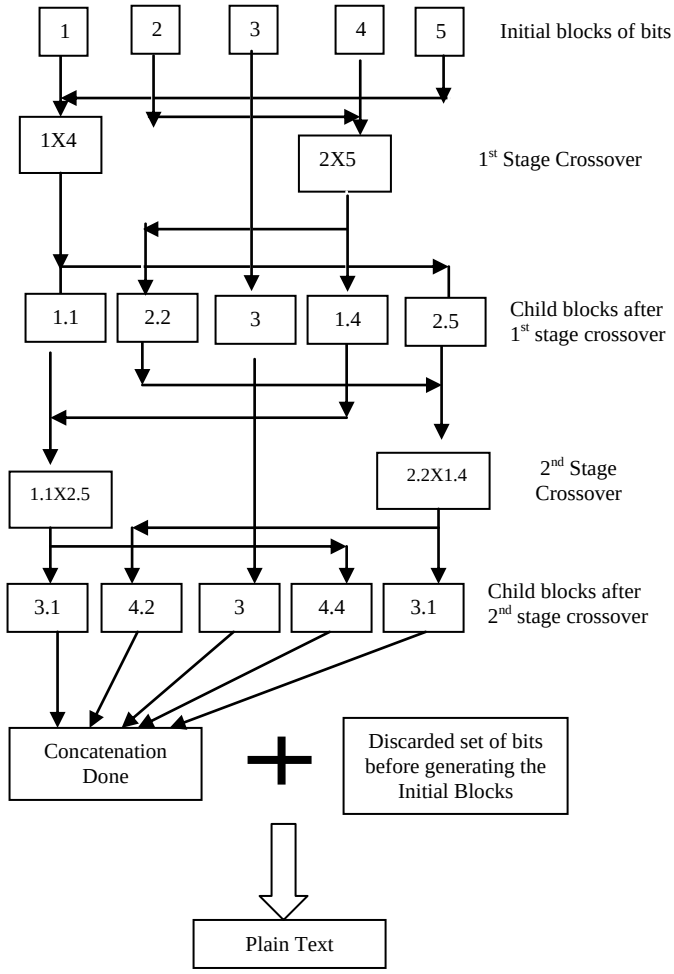

Figure - III

IV. EXAMPLE

Encryption:

Say for example the Plain text is: MANDIRA

Each letter of plain text is placed in a proposed circular model in Figure –IV.

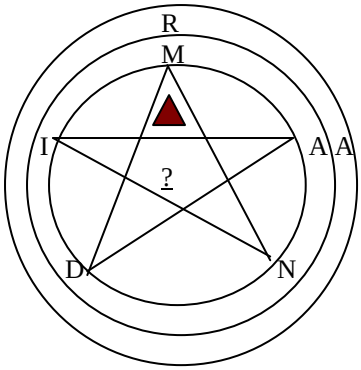

Figure - IV

Any number has been taken as Key 1, which is not a prime number.

Let, Key 1 = 5021988

R = 5021988 % 26 =10;

Alphabet weight A=0, B=1…….z=25 have been taken.

For the 1st circular path substitution of 'M', 'A', 'N', 'D' and 'I' are given below.

M=12+10=22=W
A=0+11=11=L
N=13+12=25= Z
D=3+13=16=Q
I=8+14=22=W

For the 2nd circular path substitution of 'R' and 'A' is given below.

R=17+M+15=17+12+15=44=S
A=0+A+16=0+0+16=16=Q

Therefore the Intermediate cipher text will be: WLZQWSQ.
Each letter of intermediate cipher text will represent 7 bits binary code.
Total bits will be: 7 * 7 = 49
These 49 bits will be divided into 5 blocks.

49 % 5 = 4 [Discard last 4 bits for future use]
49 / 5 = 9 [Each block will contain 9 bits]

Randomly generate any number within 1 to 9 because each block will contain maximum of 9 bits. Say for example the random number is generated is 3 and this will be called Pivot.

So, Pivot = 3 [Key 2]
Binary representation of each letter of intermediate cipher text is given below.

Letter	Binary Code (7 bits)
W	1010111
L	1001100
Z	1011010
Q	1010001
W	1010111
S	1010011
Q	1010001

Binary representation of intermediate cipher text will be:

10101111001100101101010100011010111101001110**0001**

Discard the last 4 bits '**0001**' and store it for future use.

45 bits will be divided into 5 blocks as given below.

101011110	011001011	010101000	110101111	010011101
Block 1	Block 2	Block 3	Block 4	Block 5

Now, two stages Crossover will take place between different blocks as per proposed algorithm. 'X' sign will represent the crossover.

Crossover between **Block 1** and **Block 5:**

101011110 X 010011101

101111001 **[Block 1.1]** 001110110 [**Block 1.5**]

Crossover between **Block 2** and **Block 4:**

011001011 X 110101111

100101111 [**Block 2.2**] 010111101 [**Block 2.4**]

Crossover between **Block 1.1** and **Block 2.4**

101111001 X 010111101

111100101 [**Block 3.1**] 011110110 [**Block 3.4**]

Crossover between **Block 2.2** and **Block 1.5**

100101111 X 001110110

010111100 [**Block 4.2**] 111011010 [**Block 4.5**]

Now concatenation will be performed within Block 3.1 + Block 4.2 + Block 3 + Block 3.4 + Block 4.5 + Discarded Last 4 bits '0001'.

After concatenation final cipher will be generated.

11110010101011**1100010**1010000**1111011**0111011**0100001**
y + b P { ; !

Final Cipher Text: yb+P{;!
Decryption:
Cipher Text: yb+P{;!

Character	ASCII Code	Binary Code
Y	121	1111001
+	43	0101011
b	98	1100010
P	80	1010000
{	123	1111011
;	59	0111011
!	33	0100001

Total number of bits: 7 * 7 = 49

49 % 5 = 4 [Discard last 4 bits for future use]
49 / 5 = 9 [Each block will contain 9 bits]

Pivot = (n) – (Key 2) + 1

Where n denotes number of bits in each block and Secret Key has been generated at the time of encryption.
Therefore,

Pivot = 9 – 3 + 1 = 7

Binary representation of the final cipher will be:

111100101010111100010101000011110110111011010**0001**

Discard the last 4 bits '0001' and store it for future use.

Rest of the bits will be divided into 5 blocks as given below.

111100101	010111100	010101000	011110110	111011010
Block 1	Block 2	Block 3	Block 4	Block 5

Now, two stages Crossover will take place between different blocks as per proposed algorithm. 'X' sign will represent the crossover.

Crossover between **Block 1** and **Block 4**:

111100101 X 011110110

10**1**1111001 [**Block 1.1**] 01**1**0111101 [**Block 1.4**]

Crossover between **Block 2** and **Block 5**:

010111100 X 111011010

10**0**101111 [**Block 2.2**] 00**1**110110 [**Block 2.5**]

Crossover between **Block 1.1** and **Block 2.5**:

101111001 X 001110110

10**1**011110 [**Block 3.1**] 01**0**011101 [**Block 3.5**]

Crossover between **Block 2.2** and **Block 1.4**:

100101111 X 010111101

01**1**001011 [**Block 4.2**] 11**0**101111 [**Block 4.4**]

Now concatenation will be performed within Block 3.1 + Block 4.2 + Block 3 + Block 4.4 + Block 3.5 + Discarded Last 4 bits '0001'.

After concatenation Intermediate cipher will be generated.

10101111001100**1011010**1010001**1010111**1010011**1010001**
W L Z Q W S Q

Intermediate Cipher Text: WLZQWSQ

Key 1: 5021988

R = Key 1 % 26 = 10

Each letter of intermediate cipher is placed in a proposed circular model in Figure – V.

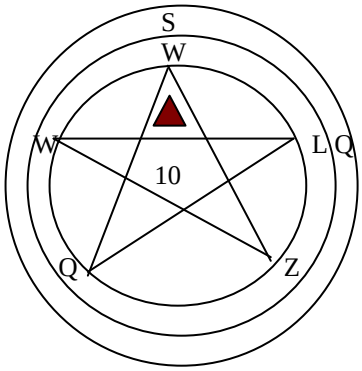

Figure – V

Alphabet weight A=0, B=1…….z=25 have been taken.
For the 1st circular path substitution of 'W', 'L', 'Z', 'Q' and 'W' are given below.

W – 10 = M
L – 11 = A
Z – 12 = N
Q – 13 = D
W – 14 = I

For the 2nd circular path substitution of 'S' and 'Q' is given below.
S – (M + 15) = S – (12 + 15) = S – 25 = R
Q – (A + 16) = Q – (0 + 16) = Q – 16 = A

Therefore the Plain Text will be: MANDIRA

V. CONCLUSIVE DISCUSSION

The objective of this paper is to facilitate the development of applications that include advanced cryptography through above said technique for secured transmission of the messages. In the proposed technique two key is used which will increase the security. Genetic function crossover is used to make the technique susceptible from the attacker. Two stages crossover are used in the proposed algorithm which confirms the more security of the algorithm. The proposed circular path model also makes the proposed technique unique.

VI. FUTURE SCOPE

The future of encryption is brighter than ever before. The demand for more control and protection of corporation information assets and third-party information is increasing dramatically. Distribution of character frequencies will be analyzed for proposed algorithms. Some testing like non-homogeneity between source and encrypted file, chi-squire value test, has to be done to measure the security of proposed technique with well known existing techniques. Comparison of Encryption, decryption time for different category of files with existing algorithm in the market will be performed in future. All above said parametric test will confirm the good security in the present age of global communication system.

VII. REFERENCES

[1] Poonam Garg, "Genetic algorithms and simulated annealing: a comparison between three approaches for the crypto analysis of transposition cipher" IMT, INDIA-2004

[2] Dr. G. Raghavendra, Nalini N, "a new encryption and decryption algorithm combining the features of genetic algorithm (GA) and cryptography" NIE, Mysore.

[3] A. J. Bagnall, "the application of genetic algorithms in cryptanalysis" School of information system, University of East Anglia, 1996

[4] N. Koblitz, "a coursein number theory and cryptography', Springer- verlag, New York, 1994

[5] R. Toeneh, S. Arumugam, "Breaking Transposition cipher with genetic algorithm", Chennai, India

[6] Bethany Delman, "Genetic algorithm in cryptography", Rochester, New York, July – 2004

[7] Atul Kahate, "Cryptography and Network Security" 2nd edition, TATA McGRAW HILL

[8] Melanie Mitchell, "An introduction to Genetic Algorithms". A Bradford book.