ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Cryptographic Technique through Hexagonal Path Using Genetic Algorithm

Somalina Chowdhury

Assistant Professor, Dept. of C.A., GNIT, Kolkata, India.

ABSTRACT: In this paper some new approach for encryption and decryption is proposed. The process of block cipher and genetic function is the core of the present algorithm. In this encryption technique three secret keys are required for the encryption or decryption of a message. Input stream will be produced intermediate cipher text on which two stages of two point crossovers will be used in the process of encryption and decryption to produce final cipher text.

KEYWORDS: Block cipher, plain text, cipher text, Key, Encryption, Decryption, Crossover, mutation.

I. INTRODUCTION

This paper gives a new algorithm for encryption and decryption. The algorithm is based on the process of Block cipher and genetic function. In this technique each letter of a plain text is placed into a hexagonal path of the proposed model, by using a random number, Block cipher 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 three 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. And during cryptography process where the third key is the two point used for crossover. Now we will go for some details of the algorithm.

II. RELATED WORK

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]. Some new technique used to break transposition cipher. Here flavour of genetic algorithm is used [5]. Details implementation of Genetic algorithm in the field of cryptography [6]. Substituting cryptography using the approach of Genetic Function. Here the message is design in a circular path [7]. The detail knowledge of Cryptography [8].Basic idea of Genetic algorithm [9].

III. PROPOSED ALGORITHM

A. THE SCHEME

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

A random number has been chosen which not a prime is. The random number is modulated by 26(as we are having 26 alphabets in English). The modular result is added with the position number of original letter, which is placed on the first hexagonal path. The addition result is the position number of the substituted letter. The next letter of the first hexagonal path is substituted in the same way but the modular result is incremented by one in each time. When second hexagonal path is started, the Block cipher value is calculated by the addition of position value of original letter, incremented value of modular result. By this way Block cipher 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

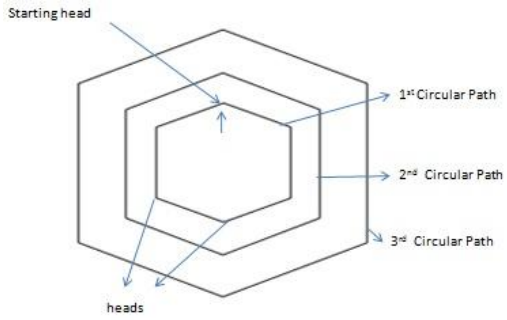

Fig: I

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. During the use of genetic function two point crossover are used. Here the two point for the crossover are used as one of the key. 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].

B. 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.

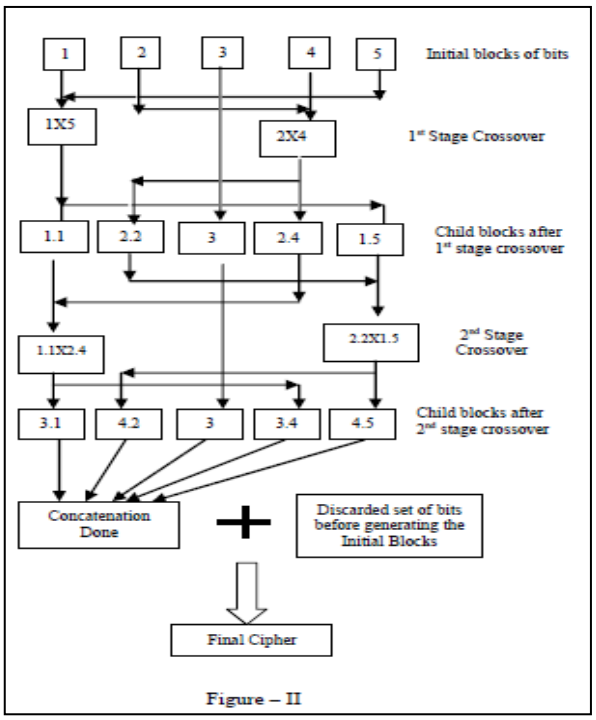

Figure – II

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

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.

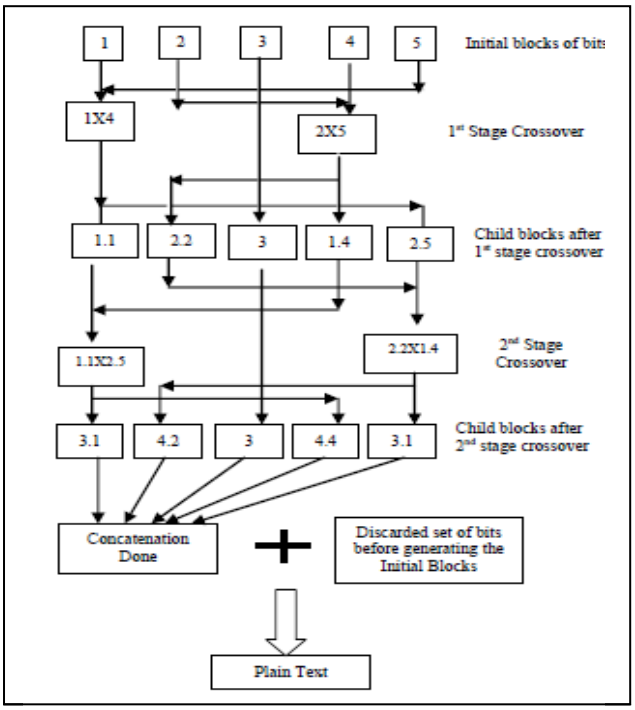

Figure - III

C. EXAMPLE

Encryption:

Say for example the Plain text is: SOMALINA

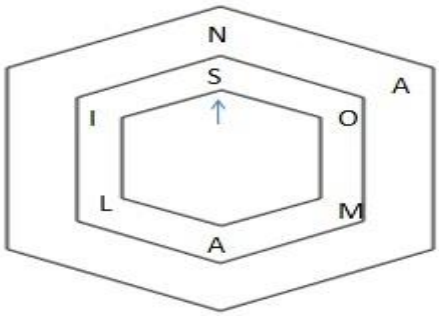

Fig: IV

Each letter of plain text is placed in a proposed hexagonal model in Figure IV. Any number has been taken as Key 1, which is not a prime number.

Let, Key 1 = 5894124

R = 5894124 % 26 =2;

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

For the 1st hexagonal path Block cipher of 'S','O','M', 'A', 'L' and 'I' are given below:
S=18+2=20=U
O=14+3=17=R
M=12+4=16=Q
A=0+5=5=F
L=11+6=17=R
I=8+7=15=P
For the 2nd hexagonal path Block cipher of 'N' and 'A' is given below:
N=13+8=21=V
A =0+9=9=J
Therefore the Intermediate cipher text will be: URQFRPVJ
Each letter of intermediate cipher text will represent 7 bits binary code.

Total bits will be: 8* 7 = 56
These 56 bits will be divided into 5 blocks.
56 % 5 = 1 [Discard last 4 bits for future use]
56 / 5 = 11 [Each block will contain 11 bits]
Randomly generate any number within 1 to 11 because each block will contain maximum of 11 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)**
U	1010101
R	1010010
Q	1010001
F	1000110
R	1010010
P	1010000
V	1010110
J	1001010

Binary representation of intermediate cipher text will be:
10101011010010101000110001101010010101000010101101001010

10101011010010101000110001101010010101000010101101001010**0**
Discard the last 1 bit „**0**" and store it for future use.
55 bits will be divided into 5 blocks as given below.
10101011010 01010100011 00011010100 10101000010 10110100101
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.
And let 4 and 9 be the randomly selected two-crossover points.
Crossover between **Block 1** and **Block 5:**
10101011**010** X **1011**0100**101**
10100100010 **[Block 1.1**]
10111011101[**Block 1.5**]
Crossover between **Block 2** and **Block 4:**
01010100**011** X 10101000010
01011000011[**Block 2.2**]
10100100010[**Block 2.4**]
Crossover between **Block 1.1** and **Block 2.4**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

10100100**010** X **1010**0100**010**
10100100010[**Block 3.1**]
10100100010[**Block 3.4**]
Crossover between **Block 2.2** and **Block 1.5**
01011000**011** X **1011**1011**101**
01011011011[**Block 4.2**]
10111000101[**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 1 bit '**0**'.
After concatenation final cipher will be generated.
10100100010101101101**100011010100** 10100100010**101110001010**
The above cipher is arranged in 7 bit per block.
1010010 0010010 1101101 1**000110**
R DC2 m F
101010 1001000 10**10111 0001010**
R H W LF

Final Cipher Text: **RDC2mFRHWLF**
Decryption:
Cipher Text: **RDC2mFRHWLF**

Character	ASCII Code	Binary Code
R	82	1010010
DC2	18	0010010
m	109	1101101
F	70	1000110
R	82	1010010
H	72	1001000
W	87	1010111
LF	10	0001010

Total number of bits: 78* 7 = 56
56% 5 = 1[Discard last 4 bits for future use]
56 / 5 = 11 [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 = 11– 3 + 1 = 9
Binary representation of the final cipher will be:
10100100010010110110110001101010 0 10100100010101110001010**0**
Discard the last 1 bit '**0**' and store it for future use.
Rest of the bits will be divided into 5 blocks as given below.
10100100010 01011011011 00011010100 10100100010 10111000101
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.
And let 4 and 9 be the randomly selected two-crossover points.
Crossover between **Block 1** and **Block 4**:
10100100**010** X **10100100010**
10100100010[**Block 1.1**]
10100100010[**Block 1.4**]
Crossover between **Block 2** and **Block 5**:
01011011**011** X 10111000101
01011000011[**Block 2.2**]
10111011101[**Block 2.5**]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Crossover between **Block 1.1** and **Block 2.5**:
10100100**010** X **1011**1011**101**
10101011010[**Block 3.1**]
10110100101[**Block 3.5**]
Crossover between **Block 2.2** and **Block 1.4**:
01011000**011** X **1010**0100**010**
01010100011[**Block 4.2**]
10101000010[**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 1 bit '0'
After concatenation Intermediate cipher will be generated.
1010101101001010100011**00011010100**10101000010**10110100101**0

The above cipher is arrange in 7 bit per block .
1010101 1010010 1010001 1**000110**
U R Q F
1010010 1010000 10**10110 1001010**
R P V J

Intermediate Cipher Text: **URQFRPVJ**
Let, Key 1 = 5894124
R = 5894124 % 26 =2;
Each letter of intermediate cipher is placed in a proposed hexagonal model in Figure – V.

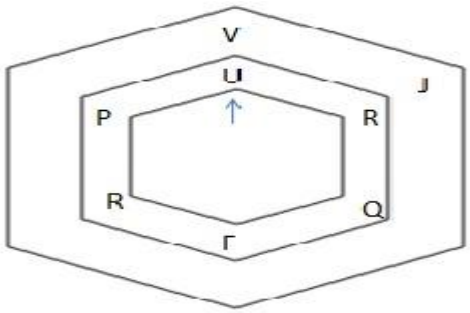

Fig: IV

Alphabet weight A=0, B=1…….z=25 have been taken.
For the 1st hexagonal path Block cipher of '**U**', '**R**', '**Q**', '**F**', '**R**', '**P**' are given below:
U=20-2=18=S
R=17-3=14=O
Q=16-4=12=M
F=5-5=0=A
R=17-6=11=L
P=15-7=8=I
For the 2nd hexagonal path Block cipher of '**V**' and '**J**' is given below.
V=21-8=13=N
J=9-9=0=A
Therefore the Plain Text will be: SOMALINA

IV. DISCUSSION

Message transformation needs intact security with integrity of the content. The aim of this paper is to present a highly secure cryptographic technique with the favor of genetic algorithm in a hexagonal path. In the proposed technique three

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

keys are 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 hexagonal path model also makes the proposed technique unique.

V. FUTURE WORK

Simulation In near future the security of message will get a new enlightens. As Existence of new technology simplifies our life it also increases the chance message corruption. 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.
And also any software implementation can also used to automate the technology.

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]Subhranil Som, Mandira Banerjee, "Cryptographic Technique using Substituting through Circular Path Followed by Genetic Function",Special issue of IJCA.
[8] Atul Kahate, "Cryptography and Network Security" 2nd edition, TATA McGRAW HILL
[9] Melanie Mitchell, "An introduction to Genetic Algorithms". A Bradford book.

BIOGRAPHY

Somalina Chowdhury, Obtained BCA and MCA degree in 2008 &2011 respectively, from West Bengal University of Technology, INDIA. She is the member of Computer Society of India. She is presently working as Assistant Professor in GNIT, Kolkata. Three International journal published her paper.Her areas of working interest are Genetic algorithm, Network Security, Cryptography and Wireless Sensor Network.