International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Application of a Recurrence Matrix to Cryptography using Genetic Algorithm

Amit Kumar Mandle, Varsha Namdeo

Abstract*: *The aim of this paper is to develop an algorithm for encryption and decryption of a message involving recurrence matrix and genetic algorithm. In this approach secrecy is maintained by using of genetic algorithm. The proposed algorithm solves various problems that we are facing now days. Thus in this paper, with the help of recurrence matrix and genetic algorithm a secret sharing scheme is established, which is designed for encryption that maintains the secrecy of the information.

Keywords*: *Recurrence matrix, Genetic Algorithm, Crossover, Mutation, Encryption and Decryption.

I. INTRODUCTION

Due to increase of digital media transmission and unauthorized access of import data, secure data transmission over network has become a vital and critical issue. For information security cryptography uses mathematical techniques. The concept of encryption and decryption is the base of cryptography. When data is converted to some unreadable form, then it is called encryption, while that process is called decryption when unreadable form of data is again converted to its original form. Symmetric and asymmetric cryptography are two types of algorithm. In symmetric cryptography one key is used for encryption and decryption both, while in asymmetric cryptography there are two different keys are used, one key for encryption known as public key and other is decryption key known as private key [3].

A method which is based on natural selection and used for solving constrained and unconstrained optimization is known as genetic algorithm. There are three main types of rules that are used by genetic algorithm i.e. selection, crossover and mutation. In crossover technique combining two parents to form a children for next generation, while mutation process random changes the individual parents to form children. There are various types of crossover techniques i.e. single point, two-point, uniform etc. In this paper we will use two-point crossover technique. In this technique, we choose two random points on the chromosomes and genetic material exchanged at these points. Mutation operation is also various types. Some mutation operations are insert, inversion, swap, flip, reversing, uniform etc. In this paper we will use swap mutation operation. In this operation we choose two bits random and swap their position.

When elements of a matrix are considered from a recurrence matrix then this type of matrix is known as recurrence matrix. In this paper we consider a recurrence matrix which is whose elements are taken from Fermat sequence 2,3,5,9,17,13,........Thus in this paper we define a recurrence matrix made from Fermat Sequences follows:

$$R_F = \begin{bmatrix} 1 & C_{n+2} & C_{n+1} & C_n \\ C_{n+2} & 1 & C_{n+4} & C_{n+3} \\ C_{n+1} & C_{n+4} & 1 & C_n \\ C_n & C_{n+3} & C_{n+5} & 1 \end{bmatrix} = \begin{bmatrix} 1 & 5 & 3 & 2 \\ 5 & 1 & 17 & 9 \\ 3 & 17 & 1 & 33 \\ 2 & 9 & 33 & 2 \end{bmatrix}$$

II. LITERATURE REVIEW

Kumar [1], Surya [4], Patil [2] and others are developed various cryptographic techniques using algorithm along with other tools. They studied proposed easy cryptographic secure algorithm for communication. They also designed a secure communication method for encryption and decryption with the help of genetic algorithm.

III. METHODOLOGY

Following Kumar [1], Surya [4], Patil [2] and other researchers in this paper we develop and algorithm for encryption and decryption of a message using recurrence matrix and genetic algorithm we develop a secret sharing scheme for secure communication, which is designed in such a way that encryption maintains secrecy of the message.

IV. ALGORITHM

Numerical values for alphabets and some symbols used in the paper given in the following table:

Table – 1

A – 1	O – 15
B – 2	P – 16
C – 3	Q – 17
D – 4	R – 18
E – 5	S – 19
F – 6	T – 20
G – 7	U – 21
H – 8	V – 22
I – 9	W – 23
J – 10	X – 24

Manuscript published on January 30, 2020.
* Correspondence Author
Amit Kumar Mandle*, Research Scholar in the Department of Computer Applications (MCA) at SRK University, Bhopal, India
Varsha Namdeo, Associate Professor in the Department of Computer Science and Engineering at SRK University, Bhopal, India

K – 11	Y – 25
L – 12	Z – 26
M – 13	0 – 0
N – 14	

4.1 ENCRYPTION:

1. Convert the Plain text and arrange them in a block size of 16 bytes i.e. 4×4 order matrix.
2. Correct each alphabet of plaintext matrix into numeric value using Table I. Called this matrix M (say).
3. Multiply key matrix K(say) and Plaintext matrix M under modulo p, here we take p= 27, we get another matrix M1(say).
4. Convert the numeric value of each element of matrix M1 into 5-bit binary code and divided them into two segments.
5. Apply two point (agreed by sender and receiver) crossover technique.
6. Apply swap mutation operation on that positions which are shared with receiver.
7. Convert each decimal value of element of above resultant matrix into their corresponding alphabet/symbol using table I to get required cipher text.

4.2 DECRYPTION:

1. Consider the cipher text and convert each alphabet/symbol into corresponding numeric value using table I and arrange them into a matrix D (say) of order 4.
2. Convert numeric value of each element of matrix D into 5-bit binary form and divided them into two segments.
3. Apply swap mutation operation as shared with sender.
4. Appling two point crossover technique as shared by sender.
5. Convert each 5-bit binary group into their decimal equivalent and arrange them into a matrix of order 4. Say this matrix D1.
6. Multiply D1 and inverse of key matrix K under modulo p, here we take p = 27. We get another matrix say P.
7. Convert numeric value of each element of P into corresponding alphabet using Table I, to get plain text.

Illustration:

Encryption Steps:

1. Consider a recurrence matrix as key matrix of 4×4 order (non-singular), which is made from Fermat's sequence, as follows:

$$R_F=\begin{bmatrix} 1 & C_{n+2} & C_{n+1} & C_n \\ C_{n+2} & 1 & C_{n+4} & C_{n+3} \\ C_{n+1} & C_{n+4} & 1 & C_n \\ C_n & C_{n+3} & C_{n+5} & 1 \end{bmatrix} = \begin{bmatrix} 1 & 5 & 3 & 2 \\ 5 & 1 & 17 & 9 \\ 3 & 17 & 1 & 33 \\ 2 & 9 & 33 & 1 \end{bmatrix} (\text{mod } 27)$$

$$= \begin{bmatrix} 1 & 5 & 3 & 2 \\ 5 & 1 & 17 & 9 \\ 3 & 17 & 1 & 6 \\ 2 & 9 & 6 & 1 \end{bmatrix} = K \text{ (say)}$$

2. Let a plain text be
Arrange them in a block size of 16 bytes i.e. 4×4 matrix, we get

$$\begin{bmatrix} P & UB & L \\ I & CE & N \\ C & RY & P \\ T & IO & N \end{bmatrix}$$

3. In the above block matrix substitute numeric values of letters using table I as follows:

$$M \text{ (say)} = \begin{bmatrix} 16 & 212 & 12 \\ 9 & 3\,5 & 14 \\ 3 & 1825 & 16 \\ 20 & 9\,15 & 14 \end{bmatrix}$$

4. Multiply the key matrix K and text Matrix M under modulo system, we get

M_1 = MK (mod27)

$$= \begin{bmatrix} 16 & 212 & 12 \\ 9 & 3\,5 & 14 \\ 3 & 1825 & 16 \\ 20 & 9\,15 & 14 \end{bmatrix} \begin{bmatrix} 1 & 5 & 3 & 2 \\ 5 & 1 & 17 & 9 \\ 3 & 17 & 1 & 6 \\ 2 & 9 & 6 & 1 \end{bmatrix} (\text{mod } 27)$$

$$M_1 = \begin{bmatrix} 16 & 0\,20 & 2 \\ 13 & 16\,5 & 8 \\ 11 & 8\,4 & 10 \\ 3 & 415 & 9 \end{bmatrix}$$

5. Convert the numeric value of each elements of matrix M1 into 5-bit binary code, we get
10000 00000 10100 00010 01101 10000 00101 01000
01011 01000 00100 01010 00011 00100 01111 01001

6. Apply two point crossover technique at 11 and 30, we get
10000 00000 00100 01010 00011 00100 00101 01000
01011 01000 10100 00010 01101 10000 01111 01001

7. Apply the swap mutation operation on 2nd and 4th position of bit in each 5-bit group, we get
10000 00000 00100 01010 01001 00100 00101 00010
01011 01000 10100 00010 01101 10000 01111 01001

8. Convert each 5-bit binary code into their decimal equivalent and arrange them in 4×4 matrix row wise, we get

$$\begin{bmatrix} 16 & 04 & 10 \\ 9 & 45 & 2 \\ 11 & 2\,20 & 8 \\ 7 & 1615 & 3 \end{bmatrix} = C \text{ (say)},$$

9. Convert each decimal value into their corresponding alphabet/symbol using table I, we get the following cipher text

Decryption Steps:

1. Consider the cipher text
2. Convert each alphabet symbol into their corresponding numeric value using table I and arrange them into 4×4 square matrix D (say), we get –

$$D = \begin{bmatrix} 16 & 04 & 10 \\ 9 & 45 & 2 \\ 11 & 2\,20 & 8 \\ 7 & 1615 & 3 \end{bmatrix}$$

3. Convert numeric value of each elements of matrix D into 5-bit binary form as follows:
10000 00000 00100 01010 01001 00100 00101 00010
01011 00010 10100 01000 00111 10000 01111 00011

4. Apply the swap mutation operation on 2nd and 4th position of bit in each 5-bit group, we get –
10000 00000 00100 01010 00011 00100 00101 01000

01011 01000 10100 00010 01101 10000 01111 01001
5. Apply two point crossover technique at 11th and 30th bit, we get –
10000 00000 10100 00010 01101 10000 00101 01000
01011 01000 00100 01010 00011 00100 01111 01001
Convert each 5-bit binary group into their decimal equivalent and arrange them into a matrix of order 4×4, we get –

$$\begin{bmatrix} 16 & 0 & 20 & 2 \\ 13 & 16 & 5 & 8 \\ 11 & 8 & 4 & 10 \\ 3 & 4 & 15 & 9 \end{bmatrix} = D_1 \text{ (say)}$$

6. Now apply the operation

$$D_1K^{-1} \text{ (mod 27)} = P \text{ (say)}$$

$$\Rightarrow P = \begin{bmatrix} 16 & 0 & 20 & 2 \\ 13 & 16 & 5 & 8 \\ 11 & 8 & 4 & 10 \\ 3 & 4 & 15 & 9 \end{bmatrix} \begin{bmatrix} 0 & 11 & 20 & 24 \\ 11 & 12 & 3 & 14 \\ 20 & 3 & 4 & 17 \\ 24 & 14 & 17 & 22 \end{bmatrix} \text{(mod 27)}$$

$$\Rightarrow P = \begin{bmatrix} 16 & 2 & 12 & 12 \\ 9 & 3 & 5 & 14 \\ 3 & 18 & 25 & 16 \\ 20 & 9 & 15 & 14 \end{bmatrix}$$

7. Convert numeric values of each element of matrix P into corresponding alphabet using Table I, we get the final plain text as follows:

V. RESULT AND DISCUSSIONS

In this proposed algorithm, since we used recurrence matrix and genetic algorithm, therefore it is very difficult to break the cipher text without proper key. Extraction of original information from cipher text is very complicated because the chosen of recurrence matrix, secret key and genetic algorithm. Due to the size of key brute force attack is also hard task.

VI. CONCLUSION

Proposed algorithm is based on genetic algorithm and recurrence matrix. Here secrecy is maintained at following four levels:

1. Chosen recurrence matrix.
2. Chosen genetic algorithm.
3. Secret Key
4. Different Operations.

Therefore breaking of generated cipher text is a tedious job. Even when the algorithm is known, the extraction of plain text from cipher text becomes quite difficult.

REFERENCES

1. Kumar Chandan, Dutta Sandip and Chakborty Soubhik: Musical Cryptography using Genetic Algorithm, ICCPCT, 2014, pp. 1742-1747.
2. Patil Shraddhali N, Parab. Dhanashree H, Nambly Akshay and John Linda Mary: Encryptic Message Using Musical Notes by Genetic Algorithm, IJREM, Vol.03, Issue 01, 2017, pp. 63-66.
3. Stallings William: Cryptography and Network Security Principles and Practices, Prentice Hall, 2005.
4. Surya S and Muhammad Ilyas H: Genetic Algorithm Based Cryptographic Approach using Karnatic Music, IRJET, Vol.04, Issue 06, 2017, pp. 1995-2001.

AUTHORS PROFILE

Amit Kumar Mandle is a Research Scholar in the Department of Computer Applications (MCA) at SRK University, Bhopal, India. He completed his Master in Computer Application from MPBOU, Bhopal (M.P.) in 2006.

Varsha Namdeo is an Associate Professor in the Department of Computer Science and Engineering at SRK University, Bhopal, India. She is a teacher and researcher in the field of computer science and information technology. She earned her Master in Computer Application from Barkatullah University Bhopal (M.P.) in 2000 and in Computer Science and Engineering from Barkatullah University Bhopal (M.P.) in 2009 and PhD degree from Maulana Azad National Institute of Technology; Bhopal (M.P.) in 2015.She had a long career in teaching and research.