ISSN:0975-9646

A Symmetric Key Encryption Technique Using Genetic Algorithm

Sindhuja K , Pramela Devi S

Department of Computer Science and Engineering,
M.V.J College of Engineering, Bangalore, India.

Abstract **- Cryptography is a fundamental technique for securing information. In this paper, we propose a Genetic Algorithm (GA) based symmetric key cryptosystem for encryption and decryption. Here, the plain text and the user input (key) is converted into text matrix and key matrix respectively. An additive matrix is generated by adding the text matrix and key matrix. A linear substitution function is applied on the additive matrix to produce the intermediate cipher. Then the GA functions (crossover and mutation) are applied on the intermediate cipher to produce the final cipher text. The proposed algorithm has basic two steps, substitution followed by genetic crossover and mutation.**

Key Words **- Substitution, Genetic Algorithm, Encryption, Decryption.**

I. INTRODUCTION

The growing dependence on computers to process information and transmit it across virtually connected systems has increased the need for security. Cryptography follows a set of mathematical techniques to provide information security, confidentiality, data integrity, authentication and non- repudiation. Encryption and decryption are the key concepts of cryptography [5]. While sending a data from sender to receiver, the privacy of the data is protected by encrypting it (i.e) converting the data in some unreadable form. On the receiver side, the data can be decrypted to its original form. The process of encryption and decryption requires an encrypting key and decrypting key. Few cryptosystems uses same key for both encryption and decryption called symmetric key/public key cryptography, while in certain cases, encryption and decryption may use different keys called asymmetric key/private key cryptography. There are two types of cryptographic techniques namely substitution and transposition [12]. Substitution replaces each plaintext symbol with another symbol. Transposition techniques transpose symbols in the plaintext to create the cipher text.

Genetic algorithms are evolutionary algorithms based on the notion of natural selection [11]. A genetic algorithm has proven to be reliable and powerful optimization technique in a wide variety of applications. It can be applied to both texts and images. Genetic algorithm is secure since it does not utilize the natural numbers directly. The results obtained for generating keys using genetic algorithm should be good in terms of coefficient of autocorrelation. Generally genetic algorithm has two basic functions namely crossover and mutation [10]. In this paper we are using crossover and mutation function for encryption and decryption. In crossover function the child chromosome is produced by taking more than one parent chromosomes. There are many types of crossover techniques such as single point crossover, two point crossover, Uniform crossover and three parent crossover [6].

In this paper we use two point crossover techniques. In two point crossover technique, two random points are selected from the two parents and the bits between two points are swapped to produce the child chromosome.

Fig.1 shows how child chromosomes are produced from the parent chromosomes using two point crossover. Here the random points are 5 and 9.

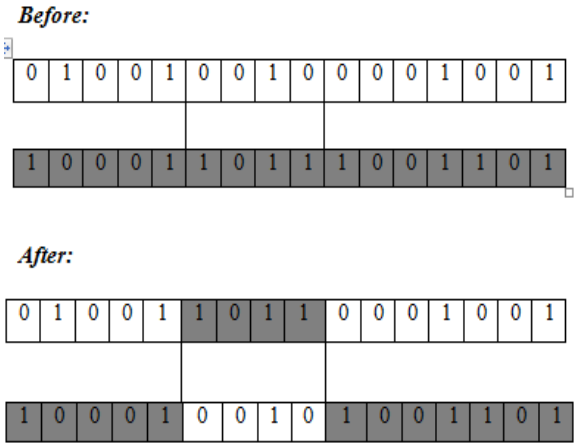

Fig. 1 Two Point Crossover

Following the crossover technique, mutation function is applied. There are many types of mutation such as flipping of bits, boundary mutation, non uniform mutation, uniform mutation and Gaussian mutation. In this paper we use flipping of bits technique. It involves selecting one or more bits of chromosome and mutate into its complement i.e a '0' would mutate into '1' and vice versa.

II. THE DESIGN

The proposed algorithm has the following phases.

- Matrix Addition
- Substitution
- Genetic crossover and mutation

*A. **The Encryption Logic***

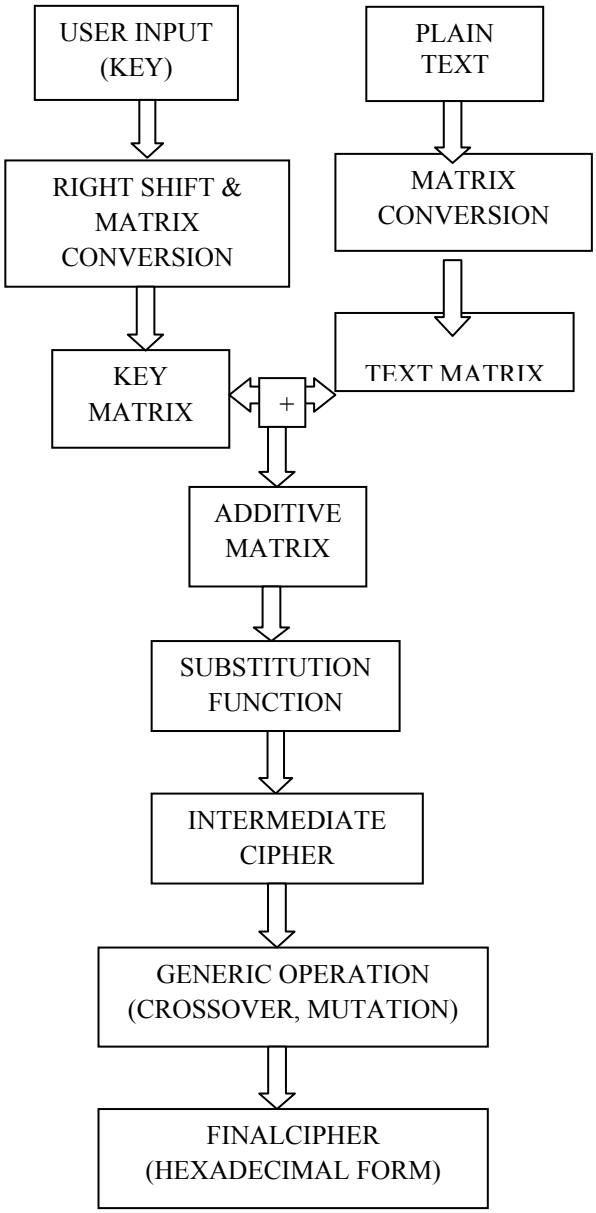

Fig. 2 Flow Chart

*B. **Encryption Process:***

1) Key Generation Algorithm:

- Choose the block size n.
- Divide the user input (key) into block size of n and append the character z to the last block if it is not equal to n.
- Represent the user input in terms of ASCII characters and perform shift operation on its equivalent binary to get the key matrix whose order is nxn.

2) Substitution Algorithm:

The substitution algorithm is of the form C(x) = (ax + b) MOD 26. Here x is the numerical equivalent of the given plaintext letter, and a and b are chosen integers. And the decryption is of the form $C^{-1}(y) = a^{-1}$ (y − b) MOD26. Here y is written in terms of x i.e., y = C(x) = (ax + b) MOD 26. We consider the following conversion table for the English alphabet for performing substitution [12].

TABLE I
CONVERSION TABLE

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

For example the following steps are used to encrypt the message “beach” using the substitution algorithm with encryption key (3, 1):

- Using the above table, we can represent the letters in our message “beach” with their corresponding numbers: 1 4 0 2 7.
- Now we multiply each of the numbers from step 1 by the first number in the encryption key, (3 in this case), to get 3 12 0 6 21
- Next, add the second number in the encryption key, (1 in this case), to each of the numbers from step 2 to get : 4 13 1 7 22
- Now use the alphabet table to replace the numbers from step 3 with their corresponding letters to obtain the cipher text: ENBHW.

3) Encryption Algorithm:

- Get the plain text and convert it into a text matrix.
- Generate an additive matrix by adding key matrix and plain text matrix.
- Apply substitution algorithm on the generated matrix to produce the intermediate cipher.
- A generic function (crossover, mutation) is applied on the intermediate cipher to produce the cipher text.
- The cipher text, user input (key), block size, substitution key and cross over points are sent to the receiver to get back the plaintext.

*C. **Decryption Algorithm:***

The steps for decryption algorithm is just reverse of encryption algorithm. First the reciprocal of cross over and mutation is used to get the intermediate cipher. Then the reverse substitution function and matrix subtraction is used to get the original plaintext.

*D. **Example***

1) Right Shift and Key Matrix generation

Let the user input (key) be NETWORK

Let the block size n=3. The ASCII equivalent for the give example after converting the user input into block of size n.

78 69 84 87 79 82 75 90 90

Now converting ASCII to binary equivalent we have

01001110 01000101 01010100 01010111 01001111 01010010 01001011 01011010 01011010

Right shift the above binary streams by 2 bits

00010011 00010001 00010101 00010101
00010011 00010100 00010010 00010110
00010110

The key matrix is

19	17	21
21	19	20
18	22	22

2) Text Matrix generation

Let the plain text be SECURITY

The equivalent text matrix after converting the plain text into block of size n is given below

83	69	67
85	82	73
84	89	90

3) Additive Matrix generation

Add the key matrix and text matrix to get the additive matrix

102	86	88
106	101	93
102	111	112

4) Substitution

Apply the substitution algorithm on the above additive matrix to get the following intermediate cipher.

O G U Q H D 0 Z G

Write the ASCII code equivalent for the intermediate cipher

79 71 85 81 72 68 79 90 71

5) Genetic Crossover and Mutation

Converting the above to binary equivalent

01001111 01000111 01010101 01010001
01001000 01000100 01001111 01011010
01000111

Divide the binary streams into two halves

010011110100011101010101010100010100
100001000100010011110101101001000111

Appling two point cross on the above input, we get the following binary values

010011110100010001010101010100010100
100001000100011111110101101001000111

Apply mutation function

101100001011101110101010101011101011
011110111011100000001010010110111000

Divide into 8 bits and convert the bytes to hexadecimal equivalent which is the final cipher.

b0, bb, AA, AE, B7, 5B, 80, A5, B8

The cipher text {b0, bb, AA, AE, B7, 5B, 80, A5, B8 } along with NETWORK372916 is send to the receiver for decryption. Here NETWORK is a user input, 3 is a block size, 7 & 2 are prime numbers used in the substitution algorithm, 9 & 16 are cross over points.

III. ANALYSIS

The key operations of the proposed algorithm are right shift, matrix addition, modulo operation and genetic operations. Among the key operation the modulo function has the larger order of growth. It is expected and to be analyzed that, if a data is encrypted by the proposed method the order of growth will be O (n^2).

IV. CONCLUSION

The proposed algorithm implemented in this paper is simple and easy to implement in cryptographic system. Key generation process and intermediate cipher algorithm provides good security to the transmitted data. Here symmetric key substitution algorithm is used to ensure confidentiality in networks, which is combined and implemented with the help of genetic functions to provide added security. In the future work we are planning to modify the algorithm to support both data encryption and image encryption. Also instead of a linear substitution technique a probability based substitution technique can be used in the substitution algorithm for achieving good level of security.

REFERENCES

[1] A.Tragha , F.Omary, A.Mouloudi ," *ICIGA: Improved Cryptography Inspired by Genetic Algorithms*" , International Conference on Hybrid Information Technology ,IEEE, 335-341,2006.

[2] Behrouz A. Forouzan , " *Cryptography & Network security* ", Tata McGraw – Hill , 2007.

[3] Clark A., Dawson Ed. & Nieuwland H., "*Cryptanalysis of Polyalphabetic Substitution Ciphers Using a Parallel Genetic Algorithm",* In Proceedings of IEEE International Symposium on Information and its Applications, pages 17-20, 1996.

[4] David E Goldberg, "*Genetic algorithms in search, optimization and machine learning*", Addision – Wesley, 1989.

[5] Douglas, R.Stinson, "*Cryptography – Theory and Practice ",* CRC Press, 1995.

[6]Harsha Bhasin, Ramesh Kumr, Neha Kathuria, "*Cryptography using Cellular Automata"*. Iternational Journal of Computer Science and Information Technology, Vol. 4(2), 355-357, 2013

[7] Holland J.. *"Adaptation in Natural and Artificial Systems"* University of Michigan Press, Ann Arbor, Michigan, 1975.

[8] P. Stepaj, G. Marin, *"Comparison of a crossover operator in binary coded genetic algorithms,"* Wseas Trans. on Computers, 9 (9), 1064–1073, 2010.

[9] Subhranil Som , Niladri Shekhar Chatergee , J.K Mandal, " *Key Based Bit Level Cryptographic Technique(KBGCT)"*, 7th International Conference on Information Assurance and Security , 2011

[10] M. Mitchell, *"An Introduction to Genetic Algorithms,"* The MIT Press, Cambridge, USA, 1999.

[11] S., N. Sivanandan, S. N. Deepa, "*Introduction to Genetic Algorithm"*,Springer Verlag Berlin Heidelberg, 2008.

[12] William Stallings, "*Cryptography and Network Security"*, 3rd Edition.