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 1, January 2015

Application of Genetic Algorithm in Communication Network Security

SomalinaChowdhury, Sisir Kumar Das, Annapurna Das

Assistant Professor, Dept. of C.A,Guru Nanak Institute of Technology, Kolkata, India.

Professor and Dean – Research & Administration, Guru Nanak Institute of Technology, Kolkata, India.

Professor &Principal, Guru Nanak Institute of Technology, Kolkata, India.

ABSTRACT: In this paper an Encryption and Decryption algorithm have been designed for communication network using Genetic Algorithm (GA) to make the total cryptography process much faster, robust, and highly secure. Here block cipher and one point crossover is used for simplification. GA is used as a part of Encryption and Decryption technique. It is a complex and highly secured concept to break by intruders, but easy to implement in the design.

KEYWORDS: Encryption, Decryption, Selection, Crossover, Mutation, key, Fitness Value, XOR, Permutation, block cipher.

I. INTRODUCTION

Online transaction is nowadays most common practice in our daily life. So network security has become one of the most concern era. *Cryptography* is one of the techniques to communicate through insecure network securely. At the same time *Genetic Algorithm (GA)* is one of the newly emerging problem solving techniques which is gaining popularity due to its robustness. GA offers significant benefits over other optimization techniques in searching a large state space.

Cryptography is the art of processing information secretly. The basic element of cryptography is **Algorithm** for encryption and decryption of information and the other one is the **key** used.

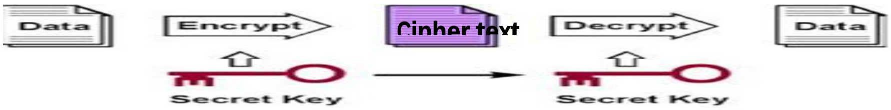


Fig.1 Cryptography Scheme

Geneticalgorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as **mutation, selection, and crossover**. Here we have used two point cross over. And the **fitness function** is used for taking decision of further movement.

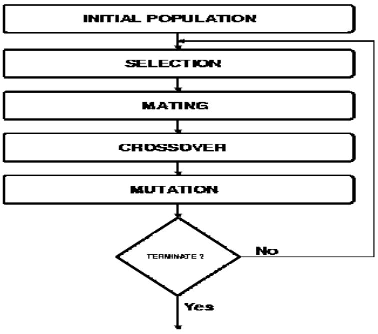


Fig.2 Genetic Algorithm flow chart

10.15680/ijircce.2015.0301057

II. RELATED WORK

In literature to date, there are many popular encryption technique are present namely DES, RSA etc.[1] And many GA based encryption algorithms have also been proposed. A. Tragha et.al [2] have describe a new symmetric block cipher system namely, ICIGA (Improved Cryptographic Inspired by Genetic Algorithm) which generates a session key in a random process. The block size and key length are variables and can be fixed by the end user in the beginning of the cipher process. ICIGA is an enhancement of the system GIC (Genetic Algorithm inspired Cryptography) [3]. There are various proposed methods for image encryption such as quad tree approach, cellular automata [4, 5]. There are wide applications of GA in solving non-linear optimization problems in various domains [6]. But very few papers exist which exploit the randomness in the algorithm for implementation of security. Chaos theory and entropy have large application in secure data communication and the desired disorder is provided by inherent nature of genetic algorithm [7, 9]. Mohammad SazzadulHoque et.al [10] have presented an intrusion detection system by applying GA to efficiently detect various types of network intrusions. They have used evolutionary theory to filter the traffic data and thus reduce the complexity [11]. There are several papers related to IDS all of which use GA in deriving classification rules [12, 14].

In this paper we have made an attempt, to build an encryption algorithm inside which we have introduced genetic algorithm. It's Strength lie in its key size i.e., 64 bit.

III. PROPOSED ALGORITHM

A. *Proposed Encryption Algorithm*

Step: 1

Divide the plain text in 64 bits block each and encrypt each block.

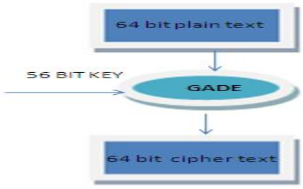


Fig.3 Skeleton of Proposed Algorithm

Step: 2

Arrange these 64 bits into 4 x 16 table format. For example*:*

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	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Step: 3

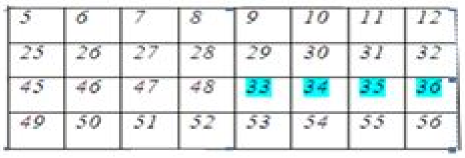
Four bit shifting per row in a cyclic fashion as highlighted

5	6	7	8	9	10	11	12	13	14	15	16	1	2	3	4
25	26	27	28	29	30	31	32	17	18	19	20	21	22	23	24
45	46	47	48	33	34	35	36	37	38	39	40	41	42	43	44
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Step: 4

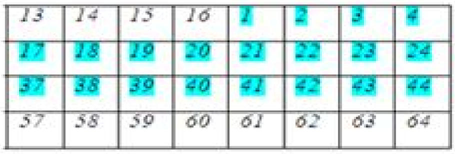
Now divide into two block (32 bits per block). Left part(LP) and Right part(RP).

LP=



5	6	7	8	9	10	11	12
25	26	27	28	29	30	31	32
45	46	47	48	33	34	35	36
49	50	51	52	53	54	55	56

RP =



13	14	15	16	1	2	3	4
17	18	19	20	21	22	23	24
37	38	39	40	41	42	43	44
57	58	59	60	61	62	63	64

Step: 5

*Perform Expansion permutation with RP.*As shown:

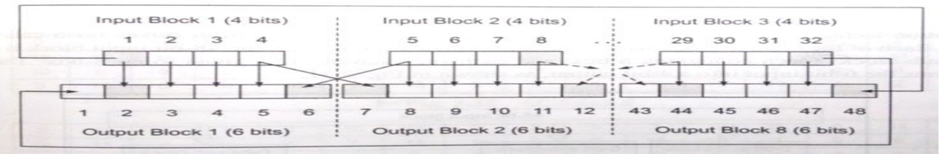


Fig.4 Example of Expand permutation

Here some bits from the input are duplicated at the output; e.g. the fifth bit of the input is duplicated in both the sixth and eighth bit of the output. Thus, the 32-bit half-block is expanded to 48 bits.

Step: 6

Now generate key of 48 bit (Explained later).

Step: 7

Apply XOR with 48 bit key and 48 bit RP to get new RP of 48 bit.

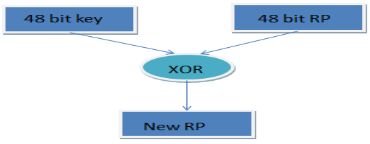


Fig.5 Key XOR with RP

Step: 8

Now with the result apply genetic algorithm operations like selection, crossover and mutation.

Fitness Function:

From new 48 bit RP make 4 x 12 table. Let the table be:

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12

Fitness will be calculated for each row of the above table. The fitness function will count the number of ones in each row. If the number of one's is 6 then fitness is 6 for that row. Similarly calculate for other rows.
Then finally count the total fitness. Now perform selection.

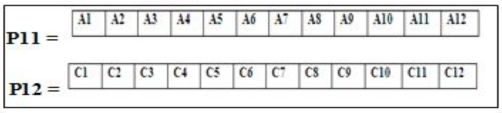
Selection:

Consider 1st and 3rd row as 1st pair of parent and other as 2nd pair of parent.
Let the new RP of 48 bit in 4 x 12 table as:
Before selection:-

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12
D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12

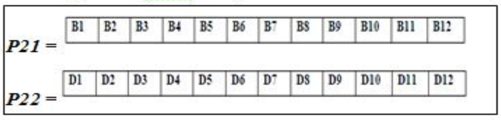
After selection:-

1st two parents (P11, P12) :



P11 =	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
P12 =	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12

2nd two parents (P21, P22) :

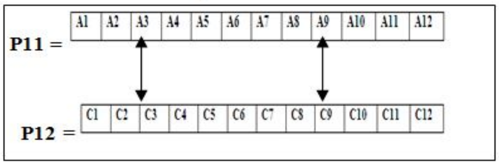


P21 =	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
P22 =	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12

Crossover *(Two point crossover):*

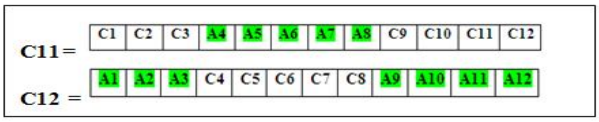
We will randomly choose any two numbers from 1 to 12 as cross over point and implement crossover. Here the points are (3,9).

Crossover for 1st two parents:



P11 =	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
P12 =	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12

Result or child of crossover:

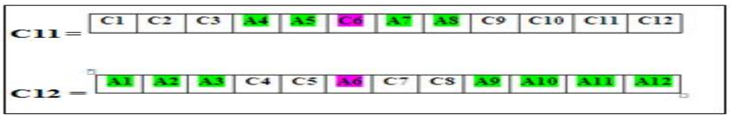


C11 =	C1	C2	C3	A4	A5	A6	A7	A8	C9	C10	C11	C12
C12 =	A1	A2	A3	C4	C5	C6	C7	C8	A9	A10	A11	A12

Similarly the other two parent pair will also create another two child.

Mutation:

We will randomly choose any one numbers from 1 to 12 as mutation point and implement. Here the point is 6(let). Shown the result after mutation.



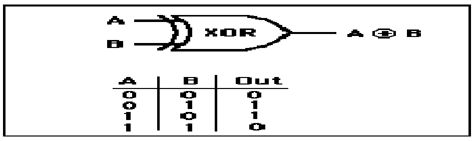
C11 =	C1	C2	C3	A4	A5	C6	A7	A8	C9	C10	C11	C12
C12 =	A1	A2	A3	C4	C5	A6	C7	C8	A9	A10	A11	A12

Now combine C11, C12, C21 and C22 to get RP.

Now again calculate Fitness same way. If the new fitness is lower then go to next step else again perform **mutation, selection, and crossover.**

Step: 9

Perform XOR operationwith LP of step 4 and the result of step 8 which is new RP. XOR gate work as:-



A	B	Out
0	0	0
0	1	1
1	0	1
1	1	0

Fig.6 Key XOR with RP

Step: 10

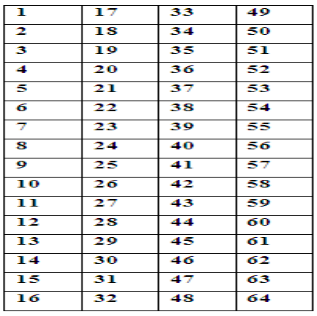
And the RP of step is taken as LP.

Step: 11

Now recombine LP of step10 and RP of step 9 to transform in 16 x 4 table.

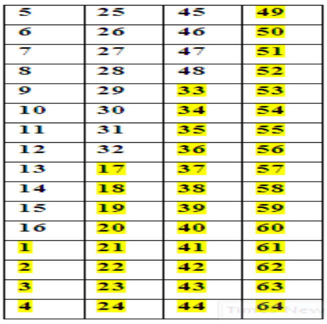
Step: 12

Four bit shifting per column in a cyclic fashion as given below.



1	17	33	49
2	18	34	50
3	19	35	51
4	20	36	52
5	21	37	53
6	22	38	54
7	23	39	55
8	24	40	56
9	25	41	57
10	26	42	58
11	27	43	59
12	28	44	60
13	29	45	61
14	30	46	62
15	31	47	63
16	32	48	64

Recombine set before shifting



5	25	45	49
6	26	46	50
7	27	47	51
8	28	48	52
9	29	33	53
10	30	34	54
11	31	35	55
12	32	36	56
13	17	37	57
14	18	38	58
15	19	39	59
16	20	40	60
1	21	41	61
2	22	42	62
3	23	43	63
4	24	44	64

After Shifting the result is

Step: 13

The resultant is the original cipher text.

B. *Proposed Key Generation Technique:*

Step: 1

At first random 64 bit are taken. And arrange them into table of 8 x 8format.

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	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Note:

For 1st block of 64bit plain text the key creation will discard 8th column for next 64 bit it will discard 7th column so as on. And from 9th block again start from 8th column and continue.

Step: 2

Now truncate the 8th column of the table,the result will be of 56 bit key.

1	2	3	4	5	6	7
9	10	11	12	13	14	15
17	18	19	20	21	22	23
25	26	27	28	29	30	31

33	34	35	36	37	38	39
41	42	43	44	45	46	47
49	50	51	52	53	54	55
57	58	59	60	61	62	63

Step: 3

Arrange 56 bit into table of 8 x 7 format. And truncate mid or 4th row.

1	2	3	4	5	6	7	9
10	11	12	13	14	15	17	18
19	20	21	22	23	25	26	27
28	29	30	31	33	34	35	36
37	38	39	41	42	43	44	45
46	47	49	50	51	52	53	54
55	57	58	59	60	61	62	63

Step: 4

Now the key of 48 bit is ready to use. Shown in 4 x 12 format.

1	2	3	4	5	6	7	9	10	11	12	13
14	15	17	18	19	20	21	22	23	25	26	27
37	38	39	41	42	43	44	45	46	47	49	50
51	52	53	54	55	57	58	59	60	61	62	63

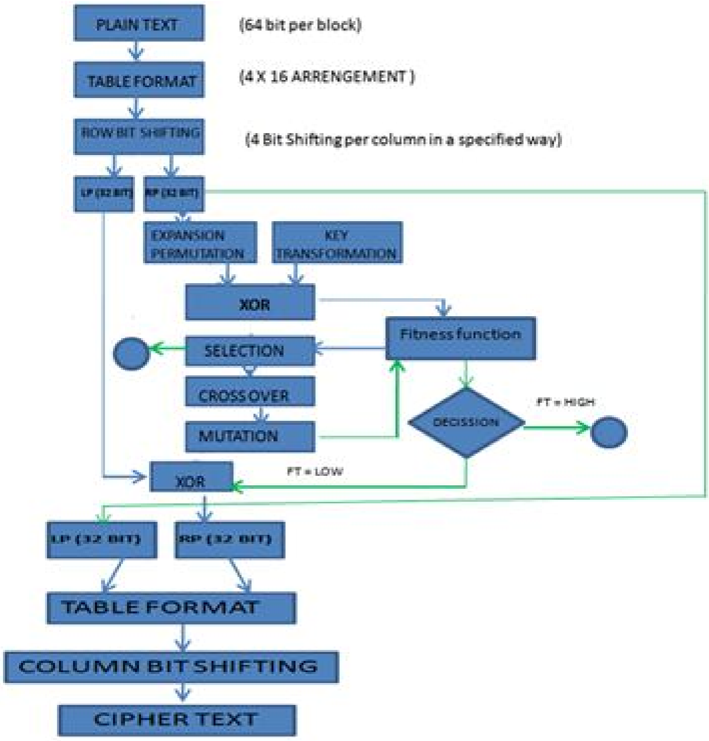


Fig.7 Proposed Algorithm flow chart

C. *Implementation in JAVA*

We can implement the above algorithm in JAVA to get the result. The files uses for the algorithm are:

Files used in the program. Filename	Description
Plain.txt	Contains the text to be encrypted
Encrypt.txt	Contains the encrypted data
Decrypt.txt	Contains the decrypted data
Key.txt	Contains randomly generated symmetric key.

IV. Conclusion and Future Work

Here in this paper an encryption technique is introduced which will prove to be a strong encryption technique for the unauthorized party to break the code. Here the key needed to share very efficiently as strength lie in key mostly. In near future it can prove to be a popular genetic-encryption technique.

Here the randomness of genetic algorithm and secrecy of cryptography has made this algorithm strong one. And the key transformation process also improved its efficiency. *Although many of its steps and key generation techniques are inspired from DES algorithm but flavour of GA makes it unique*.

References

[1] Atul Kahate, “Cryptography and Network Security- Second Edition”.

[2] Tragha A., Omary F., Mouloudi A., “ICIGA:Improved Cryptography Inspired by Genetic Algorithms”, Proceedings of the International Conference on Hybrid Information Technology (ICHIT’06), pp. 335-341, 2006.

[3] X. F. Liao, S. Y.Lai and Q. Zhou. *Signal Processing*. 90 (2010) 2714–2722.

[4] H. Cheng and X. Li. *IEEE Transactions on Signal Processive*. 48 (8) (2000) 2439–2451.

[5] O. Lafe. *Engineering Applications of Artificial Intelligence.* 10 (6) (1998) 581–591.

[6] R. J. Chen and J. L. Lai. *Pattern Recognition*. 40 (2007) 1621–1631

[7] S. Li, G. Chen and X. Zheng. Multimedia security handbook. LLC, Boca Raton, FL, USA: CRC Press; (2004) [chapter 4].

[8] Y. Mao and G. Chen. Handbook of computational geometry for pattern recognition, computer vision, neural computing and robotics. Springer; (2003).

[9] H. S. Kwok, W. K. S. Tang, *Chaos Solitons and Fractals*, (2007) 1518–1529.

[10] Mohammad SazzadulHoque, Md. Abdul Mukit and Md. Abu NaserBikas,An Implementation of Intrusion Detection System Using GeneticAlgorithm, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[11] L.M.R.J Lobo, Suhas B. Chavan, Use of Genetic Algorithm in Network Security, International Journal of Computer Applications (0975 – 8887)Volume 53– No.8, September 2012

[12] W. Lu, I. Traore, “Detecting New Forms of Network Intrusion Using Genetic Programming”. Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing, Malden, pp. 475-494, 2004.

[13] M. M. Pillai, J. H. P. Eloff, H. S. Venter, “An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms”, Proceedings of SAICSIT, pp:221-228, 2004.

[14] S. M. Bridges, R. B. Vaughn, “Fuzzy Data Mining And Genetic Algorithms Applied To Intrusion Detection”, Proceedings of 12th AnnualCanadian Information Technology Security Symposium, pp. 109-122, 2000

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. Her areas of working interest are Genetic algorithm, Network Security, Cryptography and Wireless Sensor Network.

Sisir Kumar Das, Obtained B.Tech, M.Tech and Ph.D degree from Calcutta University, IIT kharagpur and Anna University, respectively in India. He was faculty in Delhi University during 1977-1980. Dr. Das led EMC evaluation and design of electronics products manufactured by the industry meeting International Standards and Electromagnetic Research projects in the country and abroad for 28 years under the ministry of communication and IT, Govt. of India, during 1980-2007. Presently he is Prof. and Dean – Research & Administration, GNIT, Kolkata.He is co-author of Engineering Text Book “Microwave Engineering”, published by Mc-Graw Hill, USA, Singapore and India. He is the author of the text book “Antenna and Propagation”, published by Mc-Graw Hill India. He has written three chapters in the book “Engineering EMC”, Published by IEEE press. He has nearly 120 research publications in journal and conference proceedings.

Dr Das served as associate editor for IEEE EMC journal, USA (1994-2000) and now chief Editor of EMC journal of Society of EMC Engineers (India). He is senior member of IEEE , Life member of Society of EMC Engineers (India). He received

10.15680/ijircce.2015.0301057

society of EMC Engineers (India) highest award 2002 in recognition of his contribution to the EMI/EMC Solutions for Indian Industrial Products.

Annapurna Das obtained M.Sc. degree in physics from University of Calcutta, M.Tech degree in Microwave Electronics and Ph.D degree in Electrical Engineering from the University of Delhi. She worked in the Department of ECE, Anna University during 1985-2007 as Professor. Presently she is Principal of GNIT, Kolkata.She is the author of Engineering Text Book "Microwave Engineering", published by Mc-Graw Hill, USA, Singapore and India and co-author of the text book "Antenna and Propagation", published by Mc-Graw Hill Education.

She is the life member of Society of EMC Engineers (India) and ISTE. Her current interests are microwaves, EMI/EMC and Microstrip Antenna.