Volume 3, Issue 2, February 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Network Security using Genetic Algorithm

Inadyuti Dutt*
Dept. of Computer Application & WBUT
India

Soumya Paul
Dept. of Computer Application & WBUT
India

Dr. S.N. Chaudhuri
Director &WBUT
India

Abstract-Information security has become one of the most important concerns of the total information technology development process. And all the technologies that are used to support the management and maintenance of most of the enterprise are commonly online. So network security is the subject which is applicable anywhere in the business world. Genetic algorithm is such an algorithm that helps the developer to show their creativity not only in the IT field but also in the other fields like robotics, mechanical etc, especially where we are developing any technology for the first time.

Index Terms - Network security, Genetic Algorithm, Crossover, Mutation, Fitness value

I. INTRODUCTION

Nowadays in telecommunication, bandwidth, performance, reliability, cost efficiency resiliency, redundancy and security are the key measures that are placed as demands. Optical networks have had the almost all the advantages being coined above in comparison to copper-based and wireless telecommunications solutions [1]. The biggest hindrance that became a disadvantage to fibre-optic implementation was its cost. But with the recent advancements in fibre-optic technology and the fast-growing demand for bandwidth, the cost of installing & maintaining fibre optics systems has been reduced drastically. With this growing need and efficiency, there will be continuing rise in using fibre-optic systems and thereby replacing copper-based communications with such advancement in technology. The security issues also increase manifold, thereby making path to network attackers / intruders. A Genetic Algorithm (GA) is a search heuristic that mimics the process of natural evolution. This heuristic is routinely used to generate useful solutions to optimization and search problems Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover[2]. Different crossover techniques are stated below:

One-point crossover – In this crossover a single point of both parents'strings are selected. All data beyond that point in either string is swapped between the two parents. The resulting strings are the children with changes in single position.

Two-point crossover- Two-point crossover has for two points to be selected on the parent strings. The information between the two points is swapped between the parent strings, rendering two child strings.

The mutation operator involves modifying a bit in a string by deletion, inversion and other operations. There is a random change which tells whether or not and where a particular bit will be modified.

Outline of the remaining section is as follows. The paper is organized with Section 2 states the security of data that contains confidential information (data in order to provide confidentiality, authentication. When the encrypted message is send to the receiver then it is subjected to this application program, and hence it is decrypted to get the original message.

II. PROPOSED ALGORITHM

A. *Proposed Encryption Algorithm Heuristic:*

Input: A plain text is taken as input file.

Output: A plain text is converted in to a cipher text using a secrete key.

Step 1: Read the I/P file.

Step 2: Set a variable n, where n depends on the position of alphabet according to the order in the table.

If position of x = even then x = (pos – 1)

If position of x = odd then x = (pos + 1)

Step 3: The Function is defined as: -

$F(x) = x^2-x+1$ when, 1=x<10 [If f(x) =31, then f(x) =f(x) +1]

F(x) = x-1 when, x=10
F(x) = 2x+1 when, x>10 and odd [If f(x) = 43, then f(x) = f(x) +2]
F(x) = 3x + 2 when, x>10 and even.

[Note: Using these functions we will get distinct value of f(x) for all alphabet from A to Z.]
Step 4: a block of character of length x is taken from the input string.
Step 5: From an x x x, matrix for strong the storing the values of
Sum(x), where S = 1, 3,5,7,9
Step 6: Store the value of f(x) in an array of length "n".
Step 7: Set the value of sum (x)
Such that sum (x) = f (x) + &
Sum (n) $_{ij}$ = s[i] + f [j]
Where s [ ] =array for &
f [ ] =array for f(x)
Step 8: From the table maximum value of the table is found out.
Step 9: Allocate the value and omit the corresponding row and column.
Step 10: Repeat step 7 and step 8 until the number of allocated cell in equal to the order of the matrix.
Step 11: Allocated values are called and its corresponding column value, i.e. s[i]; is saved in array R [ ] of length "n";
Step 12: Print the encrypted data
Step 13: d: = 65
Step 14: d=R[i] +d-1;
Step 15: R[i] is encrypted by the character of corresponding ASCII value "d".
Step 16: If "i" less than or equal to n then repeat the step 14 and step 15 else go to step 17.
Step 17: Print the encrypted data;
Step 18: STOP

B. Proposed Encryption Heuristic Using Genetic Algorithm

Input: Encrypted text.
Output: Proposed encryption Heuristic Using Genetic algorithm into a cipher text.
Step 1: Initialize population size = 5, Maximum no of generation = 100, crossover Probability (Pcross) =0.99, Mutation Probability (pmut) =0.99.
Step 2: Input String are placed in to a square matrix whose size is immediate square value of the string length.
Step 3: a fitness function f_i is defined as,
f_i = maximum number of common term in a row 'i' and find f_i ?
Step 4: Apply crossover on the matrix with mate number and X-site.
Where, X-site = the position of string where crossover has occurred.
Mate number (i, j)= Crossover done between i^{th} and j^{th} row at X-site position.
Step 5: Find the fitness value and compare with the previous result, If better obtain then go to step 4 else go to step 6. The final matrix is stored in temp_pop.
Step 6: apply mutation on the result where 1^{st} bit of each string of temp_pop is exchanged with node position "n_k". The output string is stored in matrix final_pop1.
Step 7: Apply mutation on the result, where 1^{st} bit of each string of final_pop1 is exchanged with node position "n_k". The final string is stored in matrix final_pop2.
Step 8: STOP.

C. Proposed Decryption Heuristic Using Genetic Algorithm
INPUT: - A Cipher text value of allocated cell(according to order) and position of the allocated cell is taken as I/P.
OUTPUT: - cipher text.
STEP 1:- Read the Input file.
STEP 2:- Apply the reverse mutation on Input file where 1^{st} bit of each string of I/P is exchanged with node position nk.
The result is stored in Matrix named Pop_1.

STEP 3:- Apply the Reverse mutation on the matrix Pop_1 same as STEP 2, and result is stored in matrix Pop_2.
STEP 4:- The Pop_2 text is placed in a square matrix of same size as used in Crossover during encryption.
STEP 5:- Applying Crossover on the matrix with mate no and x-site,
Where, x-site =the position of string where Crossover has occurred.
Mate No (i, j) =Crossover done between i^{th} and j^{th} row at x-site position.
STEP 6:- The Cipher text got from the output of 1^{st} Crossover, becomes Input for the 2nd Crossover.
STEP 7:- The output of 2^{nd} Crossover is named as Temp_out.

D. Proposed Decryption Heuristic Using General Algorithm
INPUT - cipher text named temp_out.
OUTPUT - Original plaintext
STEP 1:-Taking four characters sequentially at a time from "temp_out".
STEP 2:-Match each group of characters with their corresponding allocated values which was selected at the time of encryption in the 1^{st} encryption matrix.
STEP 3:-Subtract the characters value from each group with their corresponding allocated cell value. Let it be 'y'.
STEP 4:- Get the corresponding character for each 'y'.
STEP 5:- Now we have to match the column sequence (that we get at the time of encryption) with the four characters of each group from step 4.
STEP 6:- Sort the column number in ascending order and then arrange the character that we associate with column number accordingly.
The resultant character set will be the original plaintext.
STEP 7:- END

E. Proposed Cryptographic Algorithm
STEP 1: Call Function 3.1 i.e. Proposed Encryption Algorithm Heuristic:
STEP 2: Call Function 3.2 i.e. Proposed Encryption Algorithm Heuristic Using General Algorithm:-
STEP 3: Call Function 3.3 i.e. Proposed Decryption Heuristic Using Genetic Algorithm:-
STEP 4: Call Function 3.3 i.e. Proposed Decryption Heuristic Using General Algorithm:-
STEP 5: END;

IV. Illustration of Proposed Algorithm with Example

Working Example of Network Security Using Genetic Algorithm
[Pos = position] As shown in the table below.

POSITION	1	2	3	4	5	6	7	8	9	10
ALPHABATE	A	B	C	D	E	F	G	H	I	J
Value	2	1	4	3	6	5	8	7	10	9
11	12	13	14	15	16	17	18	19	20	21
K	L	M	N	O	P	Q	R	S	T	U
12	11	14	13	16	15	18	17	20	19	22
22	23	24	25	26						
V	W	X	Y	Z						
21	24	23	26	25						

Functions: -

$F(x) = x^2 - x + 1$ when, $1 = x < 10$ [If $f(x) = 31$, then $f(x) = f(x) + 1$]
$F(x) = x - 1$ when, $x = 10$
$F(x) = 2x + 1$ When, $x > 10$ and odd [If $f(x) = f(x) = 2$]
$F(x) = 3x + 2$ when, $x > 10$ and even

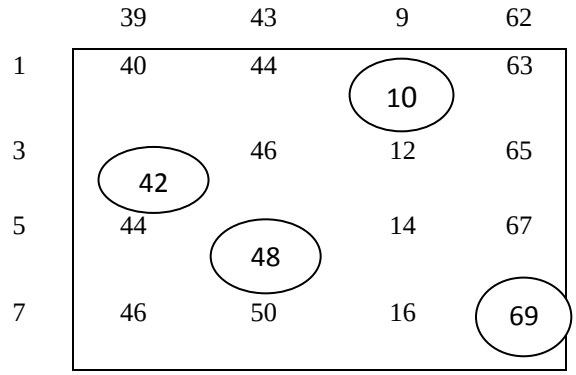
F(A)	F(B)	F(C)	F(D)	F(E)	F(F)	F(G)	F(H)	F(I)	F(J)	F(K)
3	1	13	7	31+1	21	57	43	9	73	38
F(L)	F(M)	F(N)	F(O)	F(P)	F(Q)	F(R)	F(S)	F(T)	F(U)	F(V)
23	44	27	50	31	56	35	62	39	68	45
F(W)	F(X)	F(Y)	F(Z)	Space(@)						
74	70	80	51	2						

1	3	5	7	9

Our Text: - THIS IS MY PROJECT
Array 1: -
Space is denoted as @. We will divide our text in the group of 4 alphabets.
So, our text is: - THIS @IS@ MY@P ROJE CT@@

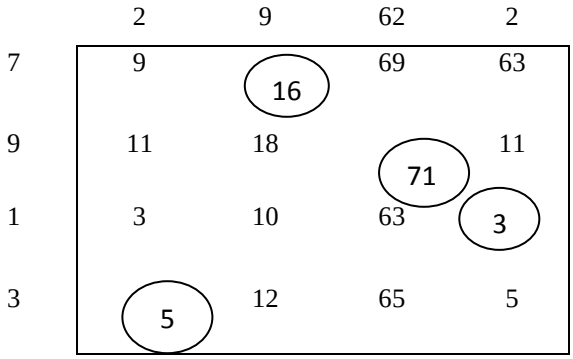
Encryption heuristic using Building Function

(i) THIS



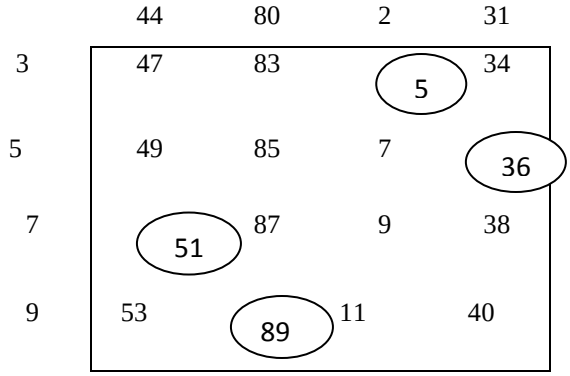
Cipher text: - 7531

(ii) @IS@



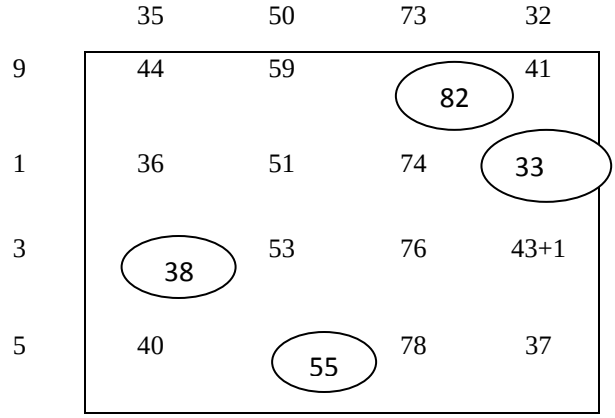
Cipher text: - 9731

(iii) MY@P



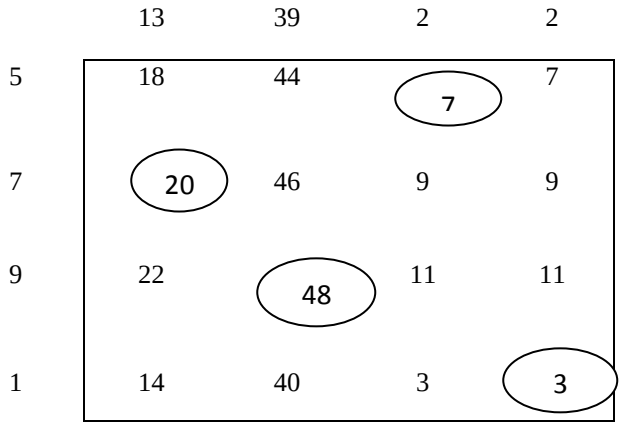
Cipher text:-9753

(iv) ROJE



Cipher text:-9531

(v) CT@@



Cipher text:-9751

Complete cipher text is: - 75319731975395319751

Encrypted ASCII values

1 → (65+1) – 1 = 65 = A
3 → (65+3) – 1 = 67 = C
5 → (67+5) – 1 = 71 = G
7 → (71+7) – 1 = 77 = M
9 → (77+9) – 1 = 85 = U
Final cipher text is: - MGCAUMCAUM, GCUGC, AUMGA

Encryption heuristic using GENETIC ALGORITHM

String no. Fit

1	M	G	C	A	U	O
2	M	C	A	U	M	2
3	G	C	U	G	C	2
4	A	U	M	G	A	2
5						5

11

Crossover:-

1st Iteration

Mate no X-site fit 11

(1, 4) 3

(2, 5)

(2, 3) 4

M	G	U	G	C	2
M	C			U	2
G	C	C	A		2
A	U	M	G	C	0
		A	U	M	2

2nd Iteration

Mate no X-site fit 8

(1, 3) 2

2

G	U	M	G	A
U	C		M	
A	C	C		G
C	U	M	A	G
	U	A		M

Mutation: -

1st Iteration

Temp _ pop_0 N_k

3	M	G	U	G	C	2
4	M	C				3
5	G	C	C	A	U	2
4	A	U	M	G	A	2
4			A	U	M	2

2nd Iteration

Temp _pop_1

U	G	M	G	A
	C		M	U
	C	C	A	G
G	U	M	A	C
U		A	U	M

Final _pop_1 Nk Final _ pop_2

U	G	M	G	A

	C		M	U	2
	C	C	A	G	5
G	U	M	A	C	4
U		A		M	5

2

M	G	U	G	C
M	C			
G	C	C	A	U
A	U	M	G	A
		A	U	M

After Mutation and Crossover,
Final Cipher Text is: - GUMGAUC@M@ACC@GCUMA@UA@M
Decryption Using Genetic Algorithm

Final _ pop

2
5
4
5

N_k

G	U	M	G	A
U	C		M	
A	C	C		G
C	U	M	A	G
	U	2 A		M

M	G	U	G	A
M	C			U
G	C	C	A	
A	U	M	G	C
		A	U	M

Decryption (Crossover):-

1st Iteration

Mate no X-site

(1, 4) 3 (2, 5)

(2, 3) 4 2

M	G	U	G	A
M	C			U
G	C	C	A	
A	U	M	G	C
		A	U	M

2nd Iteration

Mate no X-site

(1, 3)

M	G	C	A	U
M	C	A	U	M
G	C	U	G	C
A	U	M	G	A

2

T	C	@	@
2	1	3	4

→

1	2	3	4
C	T	@	@

9	7	5	3
89	51	36	5

→

9	7	5	3
2	1	4	3

Initial decrypted value is: -

MGCAUMCAUMGCUGCAUMGA

A → (65 + 1) – 65 = 1
C → (67 + 1) – 65 = 3
G → (71 + 1) – 67 = 5
M → (77 + 1) – 71 = 7
U → (85 +1) – 77 = 9

Decrypted value is: -
75319731975395319751

7	5	3	1
69	48	42	10

→

7	5	3	1
4	2	1	3

69 – 7 = 62 → S
48 – 5 = 43 → H
42 – 3 = 39 → T
10 – 1 = 9 → I

9	7	3	1
71	16	5	3

→

9	7	3	1
3	2	1	4

S	I	@	@
3	2	1	4

→

1	2	3	4
@	I	S	@

71 – 9 = 62 → S
16 – 7 = 9 → I
5 – 3 = 2 → @
3 – 1 = 2 → I@

48 – 9 = 39 → T
20 – 7 = 13 → C
7 – 5 = 2 → @
3 – 1 = 2 → @

S	H	T	I
4	2	1	3

→

1	2	3	4
T	H	I	S

So the final Plain text that we will get is

"THIS IS MY PROJECT ".

V. CONCLUSION

So the paper is concerned about sending a message securely to the receiver so that no third person who has the cipher text but cannot understand what it actually is. It provides following facilities to Sender who can enter a complete message and can encode the message using crossover & mutation of genetic algorithm. The algorithm will help the user and create new cipher text every time. Receiver on the other hand, will receive the message in encoded cipher text form and will retrieve the actual message by mapping the cipher text in the decryption algorithm.

REFERENCES

[1] Inadyuti Dutt, Soumya Paul, "Some Research on Optical Fibre Security-A Practical Approach to Optical Fibre Security", Lambert Academic Publishing, 2012, ISBN-978-3-659-22811-7
[2] Wikipedia.org/wiki/genetic_algorithm.
[3] David. E. Goldberg, "Genetic Algorithms in Search, Optimization, and Machine Learning", Pearson Education, 1989, ISBN-13: 978-020115767.

