International Conference on Recent Innovations in Management, Engineering, Science and Technology
Rajshree Institute of Management & Technology, Bareilly (India)
28th - 29th January 2018, www.conferenceworld.in
(RIMEST 2018)
ISBN: 978-93-86171-95-5

FINDING THE BEST KEY FOR PLAYFAIR CIPHER BY USING GENETIC ALGORITHM

Ashish[1], Rajat Kumar[2]

[1]Assistant Professor, [2]Student, Department of CSE, RIMT, Bareilly (India)

ABSTRACT

The objective of the paper is to provide security for the data that contains alphabets, numerals and special characters during its transmission in transposition cipher. This paper proposed a optimization technique i.e. Genetic algorithm for searching the best key among the various keys which may be combination of alphabets, letters, and special characters, and that key is used for security of data. Various types of cryptography attacks have been taken under consideration for transposition cipher.

Keywords- Genetic Algorithm, transposition cipher, programming in java

I. INTRODUCTION

Security is a state of protection and a basic requirement in today's world. Security deals with two situations which are related to each other .first is to analyses the danger and thread around situation and second is to take appropriate and effective action against the first situation. Need for security is not only in some particular situation but in almost every situation and the need is higher when it comes to protection of some data.

There are various encryption techniques in today's world. there are many requirements which is used for security of cryptography. Confidentially, integrity, availability, authentication and non-repudiation are some used for security. Confidentiality is the concept of ensuring that data is not made available or disclosed to unauthorized people. Confidentially is achieved through encryption.

Genetic algorithm (GA) is generally composed of two processes. The first process is selection of individuals for the production of the next generation and the second process is manipulation of the selected individuals to form the next generation by crossover and mutation techniques. [2]The selection mechanism determines which individuals are chosen for mating (reproduction) and how many offspring each selected individual produces. The main principle of selection strategy is "the better is an individual; the higher is its chance of being parent."

II. GENETIC ALGORITHM

The genetic algorithm is an optimization and search technique based on principle of genetic and evolutionary algorithm. Genetic algorithm is initialized with a population of guesses these are usually random and will be spread throughout the search space. A typical algorithm the uses 3 operators selection, crossover and mutation. The initial guesses are held in binary codes called string. We can say that genetic algorithm is a method of optimization with is introduced by the john Holland in 1970[5].genetic algorithms works very well in mixed

(RIMEST 2018)
ISBN: 978-93-86171-95-5

combinatorial problems. For solving a problem we must represents the solution of the problem as a cromosoms. then genetic algorithm create a population for further calculation or we can say for produce a netter next generation with the help of operators that is selection, crossover and mutation. it uses many criteria of selection so that it picks the best individual for matting. the population is the candidate solution that are consider for further process new population are born into the old population while other is dies.

Genetic algorithms [5] are search and optimization algorithms based on the principles of natural evolution, which were first introduced by john Holland in 1970. Genetic algorithms also implement the optimization strategies by simulating evolution of species through natural selections.

2.1 STEPS OF THE GENETIC ALGORITHM

Step 1: Randomly generate an initial population

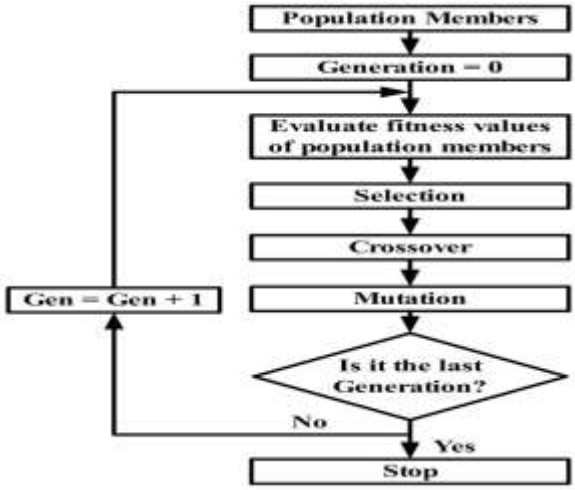
Step 2: Compute and save the fitness for each individual in the current population.

Step 3: Define selection probabilities for each individual.

Step 4: Generate probabilistically selecting individuals from population to produce offspring via genetic operator.

Step 5: Repeat step 2 until satisfying solution is obtained

2.2 FLOW CHART OF GA –



III. PLAYFAIR CIPHER-

The Playfair Cipher is a manual symmetric encryption cipher invented in 1854 by Charles Wheatstone, however it's name and popularity came from the endorsement of Lord Playfair. The playfair cipher starts with creating a key table. The key table is a 5×5 grid of letters that will act as the key for encrypting your plaintext. Each of the 25 letters must be unique and one letter of the alphabet (usually Q) is omitted from the table (as there are 25 spots and 26 letters in the alphabet). The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. [2]

(RIMEST 2018)
ISBN: 978-93-86171-95-5

H E L O W

R D A B C

F G I J K

M N P S T

U V X Y Z

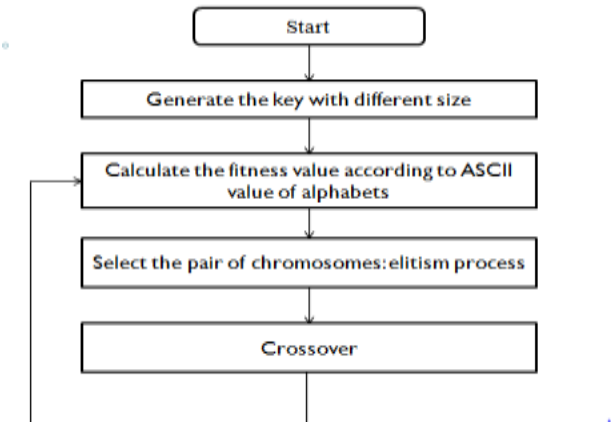
Now, we need a message to encrypt. In a playfair cipher the message is split into digraphs, pairs of two letters. If there is an odd number of letters, a Z is added to the last letter. Let's say we want to encrypt the message "hide the gold".

HI DE TH EG OL DZ

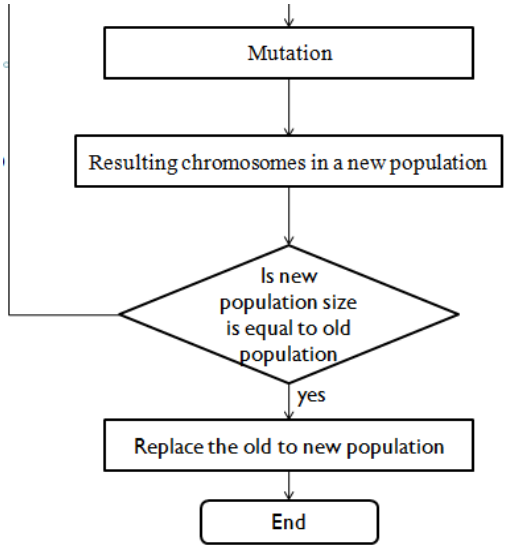
Using these rules, the results of the encryption of "hide the gold" with the key of "hello world" would be "LF GE MW DN WO CV".

IV. PROPOSED METHOD –

4.1 KEY GENERATION METHOD-



(RIMEST 2018)
ISBN: 978-93-86171-95-5



4.2 MODIFIED TECHNIQUE OF PLAYFAIR CIPHER-

To encrypt a message, one would break the message into trigraph (groups of 3 letters). If any two letters are the same or only one letter is left, add two filler letter X and Z after the first letter in the trigraph. And if any two letter is left, add a filler x after the second letter. So that BALLOON would be treated as {BAL}, {LOX}, {ONX}, and HELLOWORLDS would be treated as {HEL}, {LOW}, {ORL}, {DSX} and MASTI_M.TECH @NITJ.2012 would be treated as {MAS}, {TI_}, {M.T}, {ECH}, {@NI}, {TJ.}, {201}, {2XZ}. A letter in the trigraph will be replaced by the letter that will lay on the same row of the letter and the column of the next letter and at the floor of next-to-next letter in circular fashion. This approach can be better understood by the following diagram [4].

Plain Text Trigraph	Plain Text Trigraph			Cipher Text Trigraph
	1st Letter	2nd Letter	3rd letter	
1st Letter	Row	Column	Floor	1st Letter
2nd Letter	Floor	Row	Column	2nd Letter
3rd letter	Column	Floor	Row	3rd letter

Circular fashion means if we consider 1st letter for encryption then 2nd letter will be the next letter and 3rd letter will be the next-to-next letter and if we consider 2nd letter for encryption then 3rd letter will be the next letter and 1st letter will be the next-to-next letter and if we consider 3rd letter for encryption then 1st letter will be the next letter and 2nd letter will be the next-to-next letter**.**

V. EXAMPLE-

1. Enter the secret (password) which may contain numerals, alphabets and special symbols like: aman2012nitj@gmail.com, ravindra_1987_singh@nitj.ac.in, cipher, 29101989 etc.

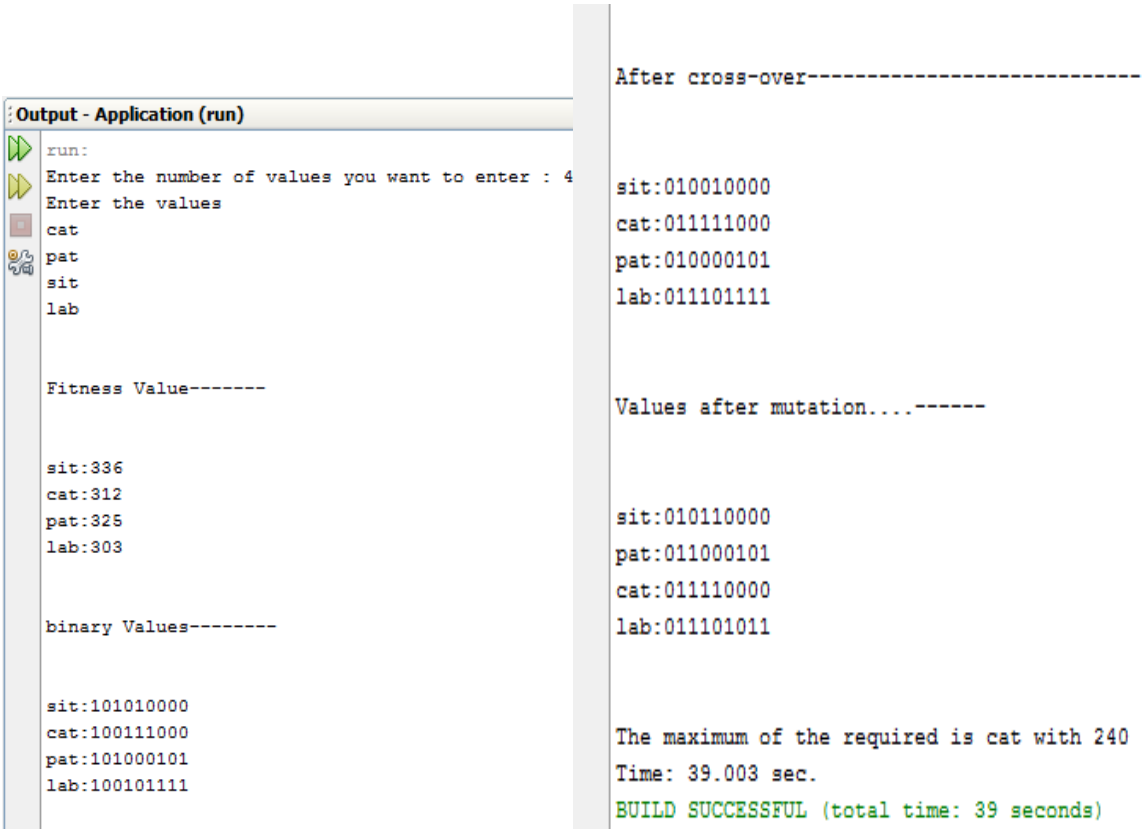
ISBN: 978-93-86171-95-5

2. Find out the keyword by dropping the duplicate letters of key. Ex: amn201itj@g.com, ravind_1987sgh@tj.c, cipher, 29108 for above keys.

3. Arrange the keyword in 5 X 5 X 5 matrix floor by floor, row-wise: left to right and then top-to-bottom.

4. Fill the remaining spaces in the matrix with the rest of numerals (0-9), alphabets (A-Z), special symbols that was not the part of our keyword.

VI. EXPEREMENTAL RESULT-



VII. CONCLUSION

Cryptanalysis of the playfair cipher is much more difficult than normal simple substitution ciphers, because digraphs (pairs of letters) are being substituted instead of monographs (single letters) and this method proposed trigraph(pairs of 3 letters),so this is more complex than plarfair cipher. Its complexity is very high because we use 26 upper and 26 lower characters, 10 numbers and 63 special characters for encryption and decryption.

REFERENCES

1. William Stallings, Cryptography and Network Security Principles and Practice. Second edition, Pearson Education.

(RIMEST 2018)
ISBN: 978-93-86171-95-5

2. Schnier B, Applied cryptography: protocols, algorithms and source code in C. New York: John Wiley and sons, 1996.
3. Menezes AJ, Oorschot PCV, Vanstone SA, Handbook of applied cryptography. Boca Raton, Florida, USA: CRC Press; 1997.
4. Impletentation of 3d approach in playfair cipher, Ashish, Anil kumar pandey ,2015
5 .Review of Crossover Techniques for Genetic Algorithms Ashish Saxena and Jyotsana panday Student Scholar, Department of Computer Science, Invertis University, Bareilly, UP, India ,2014