Diyala Journal of Engineering Sciences

ISSN 1999-8716
Printed in Iraq

Vol. 06, No. 03, pp. 97-106, September 2013

NOVEL METHOD USING CROSSOVER (GENETIC ALGORITHMS) WITH MATRIX TECHNIQUE TO MODIFYING CIPHERING BY USING PLAYFAIR

Mohammed Sami Mohammed
Education College for Pure Science, Diyala University
E-mail: Mohammed_sami9@yahoo.com
(Received: 13/3/2013; Accepted: 14/5/2013)

ABSTRACT:- Two techniques combined with each other, to get complex one. One from technique of genetic algorithm (GA) and the other is PlayFair cipher method, in this research using one step of Genetic Algorithm (GA) which called Crossover to make offspring of two parents (characters) to get one or two new character by using these techniques then using PlayFair technique to cipher text (plain text). So the person who wants to break code, two techniques must know.

This research is a novel method of ciphering by getting a new generation of offspring from two characters, when we give a new theory of symbols as mention in research.

Keywords:- PlayFair, Genetic Algorithm, Crossover, Cipher Text, Offspring.

INTRODUCTION

The difficulties of each technique of ciphering depends on its strength and it's parameters, PlayFair one of ciphering methods which it's easy to build and break, until the modification of the researchers on this technique to difficult it make an interest to get this modification of this research.

Genetic algorithms (gas), robust and systematic optimization paradigms, have been successfully applied to many scientific and engineering problems. Their performances,

however, have been considerably limited by some problems, typically premature convergence problem [1].

Many human inventions were inspired by nature. Artificial neural networks are one example. Another example is Genetic Algorithms (GA). Gas search by simulating evolution, starting from an initial set of solutions or hypotheses, and generating successive "generations" of solutions [2].

Given the stress on recombination in holland's original work, it might be thought that crossover should always be used, but in fact there is no reason to suppose that it has to be so. Further, while we could follow a strategy of crossover-and-mutation to generate new offspring, it is also possible to use crossover-or-mutation [3].

GENETIC ALGORITHM (GA) INTRODUCTION

A genetic algorithm can be defined as a kind of biased random search technique, developed by holland, able to get optimal global solution in a complex multidimensional space. One of the advantages of genetic algorithms is that they deal with a population of simultaneous points, selecting the best ones.

Making possible to create a subset from the original population not only near the global solution but also in other regions of the search space. Evolution in a given population happens when selection, crossover and mutation operators are applied to several generations. These methods affect the success of a genetic algorithm and the associated effects can vary according to the kind of problem [4].

Biologically inspired operators like *cross*-over and *mutation* are applied on these strings to yield a new generation of strings. The process of selection, crossover and mutation continues for a "xed number of generations or till a termination condition is stashed. GAs has applications in "elds as diverse as vlsi design, image processing, neural networks, machine learning, jobshop scheduling, etc. [5].

BASICS ELEMENTS OF GENETIC ALGORITHMS

Most gas methods are based on the following elements, populations of chromosomes, selection according to fitness, crossover to produce new offspring, and random mutation of new offspring [6].

CROSSOVER

Crossover is the process of combining the bits of one chromosome with those of another. This is to create an offspring for the next generation that inherits traits of both parents. Crossover randomly chooses a locus and exchanges the subsequences before and after that locus between two chromosomes to create two offspring [6]. For example, consider the following parents and a crossover point at position 3:

Parent	1 1 0 0 | 0 1 1 1
Parent	2 1 1 1 | 1 0 0 0
Offspring	1 1 0 0 1 0 0 0
Offspring	2 1 1 1 0 1 1 1

As for the binary algorithm, two parents are chosen, and the offspring are some combination of these parents. Many different approaches have been tried for crossing over in continuous gas. Adewuya (1996) reviews some of the methods. Several interesting methods are demonstrated by michalewicz (1994). The simplest methods choose one or more points in the chromosome to mark as the crossover points. Then the variables between these points are merely swapped between the two parents [7].

INTRODUCTION OF PLAYFAIR

The playfair cipher or playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of lord playfair who promoted the use of the cipher.

The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher and rather more complex vigenère cipher systems then in use. The playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 600 possible digraphs rather than the 26 possible monographs. The frequency analysis of

digraphs is possible, but considerably more difficult – and it generally requires a much larger ciphertext in order to be useful [8].

Between February 1941 and September 1945 the government of new Zealand used it for communication between new Zealand, the chatham islands and the pacific islands playfair is no longer used by military forces because of the advent of digital encryption devices. Playfair is now regarded as insecure for any purpose, because modern computers could easily break the cipher within seconds. The first published solution of the playfair cipher was described in a 19-page pamphlet by lieutenant Joseph o. Mauborgne [9].

DESCRIPTION OF NOVEL ALGORITHM

At first we must explain the details of algorithm, we must give some theory for letters (English Alphabetical) for A-Z, then we take each binary symbol as we assume in theory and take each two character alone to make offspring on it and then get the new generation, which it will be here two new character.

Then take these characters to fill the PlayFair matrix 5*5, then proceed with PlayFair steps to complete the full cipher text In Fig. (1) we show the simplified procedure of this novel algorithm.

As shown in Fig. (1), the plain text will pass the steps of GA and taking the only technique that he had to use which it's (Crossover), which make the Crossover to choose two point for crossover (one for beginning and the other for end of crossover). After this making binary code of each sample which give the offspring of new generation of characters to cipher it. In Fig. (2) I explain the description in details before I work on some text to cipher it.

FULL STEP OF THIS ALGORITHM

As shown in Fig(2), now we start the step of ciphering according to some initial point to start with :-

Step (1):- each letter have one binary coding we assume it in algorithm as shown in the table (1) from A to Z (English Alphabetical).

Step (2):- Making Crossover between two characters (by choosing the beginning and ending point between father and mother (character #1 and character #2).

Step (3):- getting new plain text cipher (#1) which we deal with it.

Step (4):- ciphering the new plain text which make the cipher (#2).

From table (1) the character I=J in binary coding, one of PlayFair condition, I get it in calculation so the matrix still 5*5 elements.

After many test of code for this theory, table (1) is the last performance one that I introduce it to this ciphering method, each two character as given in the plain text will be without repeating and neglected I or j if they come in the plain text (both of them), or if we have I we neglect j vise versa, which it's the PlayFair condition.

ILLUSTRATE THE RESULTS

If we have some text to cipher it in this novel algorithm like (**DAVINCHI)**, at first mention the full character that we want to deal with it except the repeating one and choosing I or J if they both mentions. As the text wanted to be ciphering will be (**DA VI NC HX**) after we choose two character with each other, then we make this:-

We denoted for **DA** like this:-

D= 1 0 0 1 0 0 1 1 1

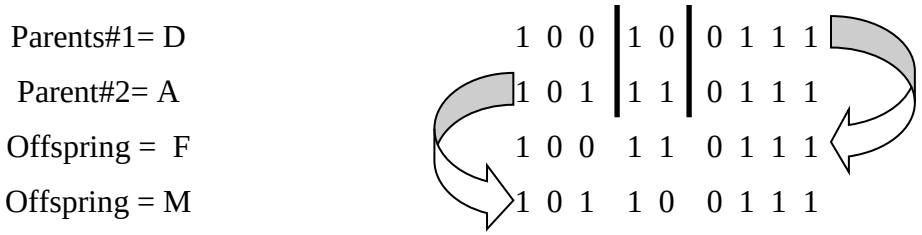
A= 1 0 1 1 1 0 1 1 1

Then we choose a point for cross over in this character we choose beginning point at 6^{th} place and the ending point is 4^{th} place as shown below:-

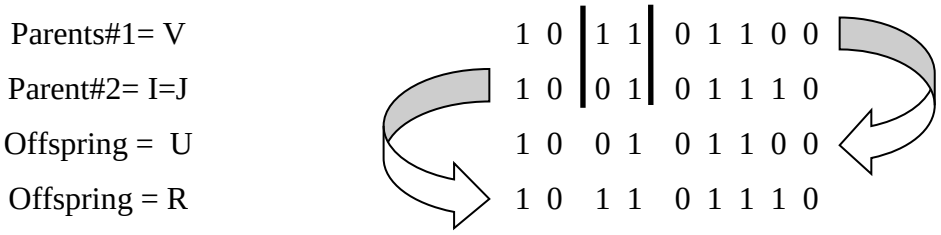
D= 1 0 | 0 1 | 0 0 1 1 1

A= 1 0 | 1 1 | 1 0 1 1 1

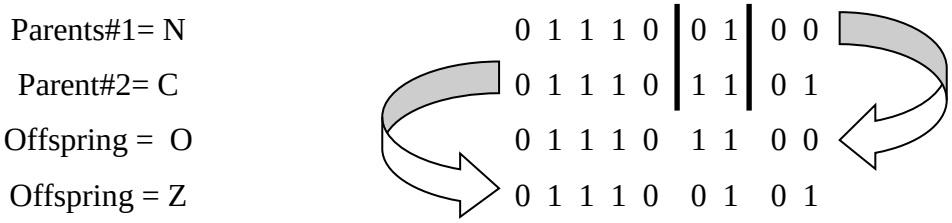
So after we make crossover (swab between binary bits) we get this results:-



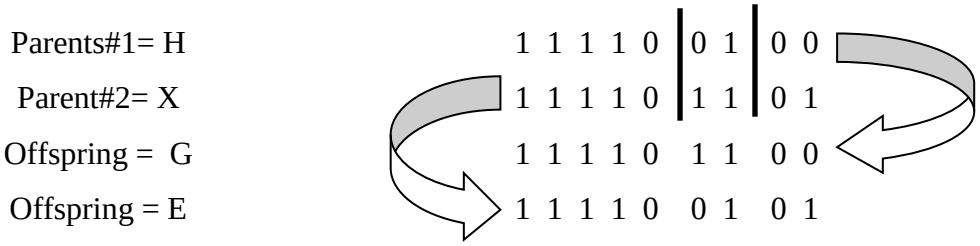
As we see we get the new generation (offspring) for D we have F, and for A we have M, so the cipher text #1 will be before entering the PlayFair for DA = FM, so on; we get the whole text as shown below:-



As we see we get the new generation (offspring) for V we have U, and for I we have R, so the cipher text #1 will be before entering the PlayFair for VI = UR, so on; we get the whole text as shown below:-



As we see we get the new generation (offspring) for N we have O, and for C we have Z, so the cipher text #1 will be before entering the PlayFair for NC = OZ, so on; we get the whole text as shown below:-



As we see we get the new generation (offspring) for H we have G, and for X we have E, so the cipher text #1 will be before entering the PlayFair for HX = GE, so on; we get the whole text as shown below:-

Then the full text we have to cipher it again to duplicate the complexity of text (so the hacker can't break it twice), because the binary coding for character unknown for hacker, so it's impossible to break it. The text (plain text) original (DAVINCHI) will be (FMUROZGE),

Then we choose a key word for PlayFair matrix to cipher it again (here we take this key word novel **method**) as shown:-

N	O	V	E	L
M	T	H	D	A
B	C	F	G	I
K	P	Q	R	S
U	W	X	Y	Z

Then we get the cipher text as the rules of PlayFair method and its condition will be:-

(FM UR OZ GE) = (HB KY WL RD)

CONCLUSION

To destroy this code we must know PlayFair technique and then we recoding the character according to table (1) to get the original text, when we know and tell the receiver of this message at what point the cross over will be, we must mention that we can make a crossover at many point not only single point, also we have pattern, this help us to get a matching between two characters.

REFERENCES

1- V. K. Koumousis and c. Katsaras, "a saw-tooth genetic algorithm combining the effects of variable population size and reinitialization to enhance performance,"ieee transactions on evolutionary computation, vol. 10, pp. 19–28, Feb. 2006.

2- Gen, m. And cheng, r. (2000), genetic algorithms and engineering opimization, john wiley, New York. Genetic algorithms: principles and perspectives: a guide to ga theory (2002), kluwer academic, boston.
3- L. Davis (ed.) (1991) handbook of genetic algorithms, van nostrand reinhold, New York.
4- J. A. Vasconcelos and j. A. Ram´irez and r. H. C. Takahashi and r. R. Saldanha, improvements in Genetic algorithms, ieee transactions on magnetics, 37(5), 2001, 3414-3417.
5- L. j. Eshelman (ed.), proceedings of the sixth international conference genetic algorithms, morgan kaufmann, san Mateo, 1995.
6- Mitchell, m. (1998). An introduction to genetic algorithms. Massachusetts.
7- John Wiely & sons, (2004). "Practical genetic algorithms", second edition, randy l. Haupt; sue ellen haupt, inc., hoboken, new jersey. 2004
8- http://en.wikipedia.org/wiki/electronic_codebook.
9- "the history of information assurance (ia)". Government communications security bureau. New Zealand government. Http://www.gcsb.govt.nz /about - us / history-ia . html. Retrieved 2011- 12 - 24.

Table (1): The binary coding of English letters.

Letter	Binary code	Letter	Binary code
A	101110111	N	011100100
B	100111100	O	011101100
C	011101101	P	111111100
D	100100111	Q	100111101
E	111100101	R	101101110
F	100110111	S	111110101
G	111101100	T	111111111
H	111100100	U	100101100
I	100101110	V	101101100
J	100101110	W	111110100
K	101111101	X	111101101
L	101111100	Y	111111101
M	101100111	Z	011100101

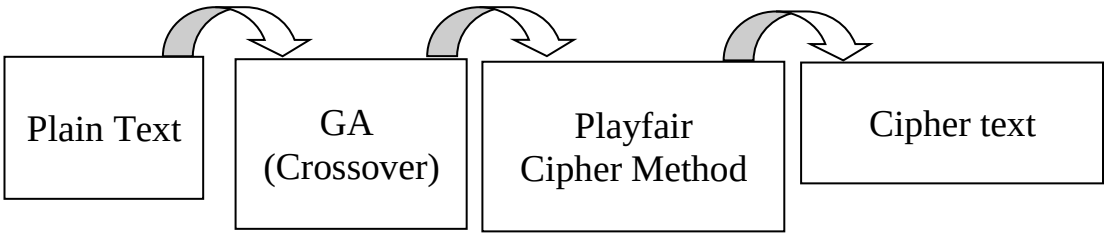


Fig. (1): Briefly Description of algorithm.

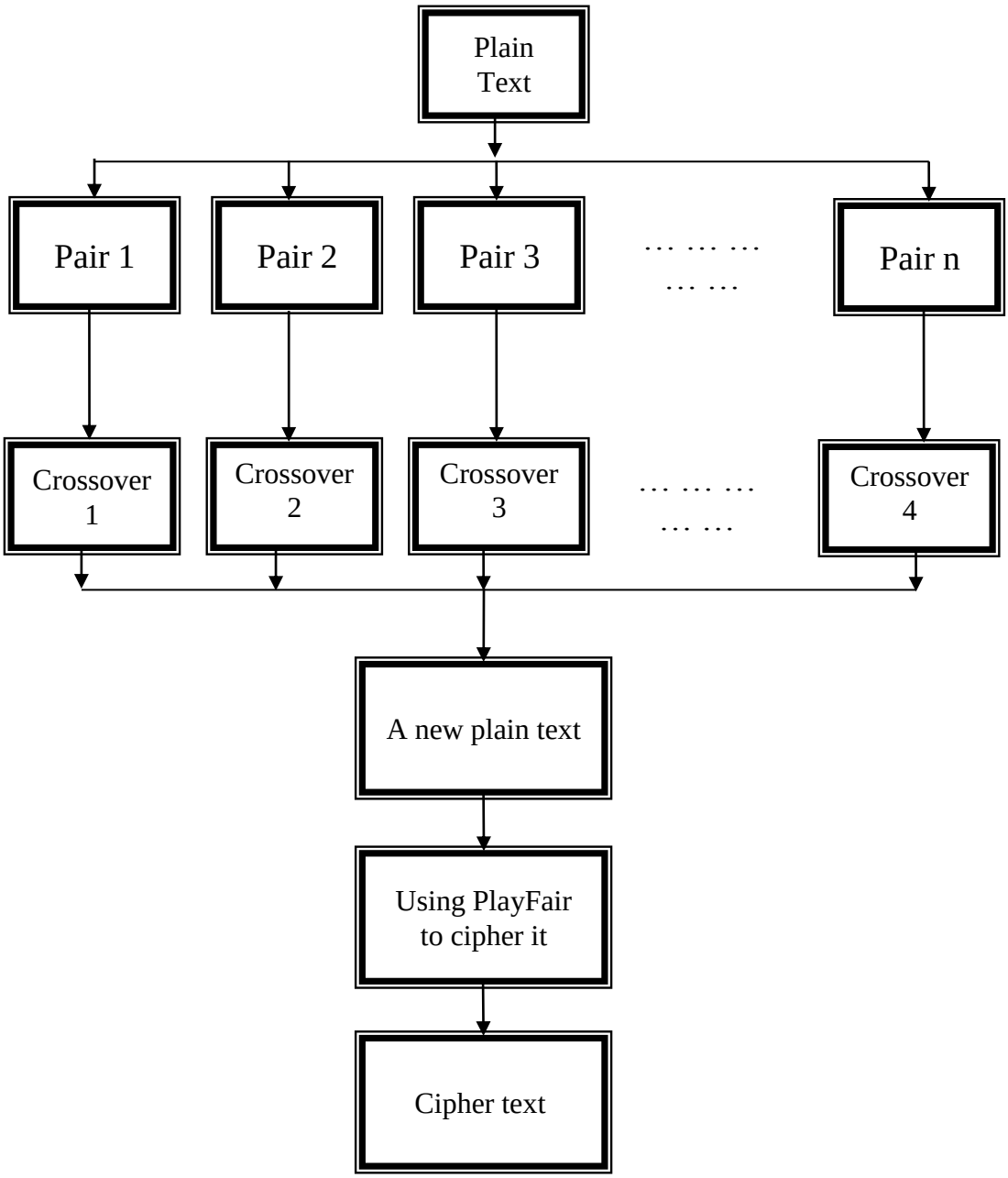


Fig. (2): Final modifying algorithm.

طريقة الدمج بين تقنية التصالب (الخوارزميات الجينية) مع طريقة المصفوفة لزيادة صعوبة التشفير

محمد سامي محمد

مدرس المساعد

كلية التربية للعلوم الصرفة – جامعة ديالى

الخلاصة:-

طريقتان تم الدمج بينهما للحصول على تقنية جديدة وذات صعوبة تشفير اكبر من النظريتان الأساسيتان، إحداهما من نظرية الخوارزمية الجينية والأخرى من طريقة التشفير باستخدام المصفوفة . في هذا البحث استخدم تقنية واحدة من الخوارزمية الجينية وهي التصالب لعمل ذرية من أبوان (رموز) للحصول على واحد أو أكثر من الرموز الجديدة باستخدام طريقة المصفوفة لذلك فعند كسر هذه الشفرة يجب على المستخدم معرفة التقنيتين.

في هذا البحث تعتبر الطريقة طريقة جديدة وذلك بالحصول على جيل جديد من الرموز وذلك باستخدام تقنية التصالب بفرض رموز ثابتة من الممكن العمل عليها في كافة أنواع وطرق التشفير.