Mixing of (Prime-Matrix) to duplicate the complexity of Ciphering (Play Fair Mixed R.S.A.)

Assistant Lecturer
Mohammed Sami Mohammed
Education for Pure Science
Computer Department
Mohammed_sami9@yahoo.com

Received 31 March 2013 ; Accepted 21 November 2013

Abstract

In this research mixing between two methods(Traditional), the first will be matrix technique from playfair method and the other is (prime) R.S.A. Technique for pair of characters , which take the rules of these two algorithms and mixed it in one algorithms called "Prime-Matrix" Algorithm, which we make it in this research, and then we compare between the two methods especially the letters will never repeat in the cipher text also the prime numbers are so many to hack.

Key Words:- Matrix, Prime Number, Cipher text, coding, Play Fair, R.S.A.

الدمج بين (تقنية الاعداد الاولية وطريقة المصفوفة) لزيادة تعقيد التشفير

المدرس المساعد محمد سامي محمد
كلية التربية للعلوم الصرفة قسم علوم الحاسوب

Mixing of (Prime-Matrix) to duplicate the complexity of Ciphering (Play Fair Mixed R.S.A.)

Mohammed Sami Mohammed

الخلاصة

لزيادة صعوبة التشفير وفك الشفرة من الممكن استخدام احدى التقنيات وايجاد بعض التغييرات الخاصة في هذه الخوارزميات لزيادة صعوبة التشفير. في هذه البحث الدمج بين طريقتين وهي طريقة المصفوفة المأخوذة من طريقة Play Fair وطريقة انتقاء الاعداد الاولية من طريقة R.S.A. لزوج من الرموز، بحيث نعتمد على قوانين هاتين الطريقتين واستنتج طريقة واحدة فقط . بالاضافة الى ان فك الشفرة يكون بنفس الطريقة ولكن بشكل معكوس كما في بقية النظريات والخوارزميات الخاصة بالتشفير، وقد تمت المقارنة مع الطريقة السابقة طريقة (R.S.A.) الاعتيادية وتم بوضوح تحديد الاختلاف بين الطريقتين وشدة التعقيد واضحة بتغير الرموز وعدم تشابه حروف النص المشفر وعند التشابه من الممكن تغيير قيمة العدد الاولي لحين الحصول على حرف اخر يختلف عن البقية وبهذه الطريقة يتم توليد اكثر من حرف اولي وهذا ما يزيد صعوبة كسر الشفرة ايضا .

الكلمات الدالة:- المصفوفة، الاعداد الاولية، النص المشفر، التشفير، خوارزمية ال play fair ،طريقة R.S.A.

Introduction

First we must deal with rules of two algorithms (playfair) and (R.S.A.) to find the text (plain text) wanted to be ciphered, must separate (two characters) each and neglected I or j if it's found, also we use x if we have double characters (or letters). Previous rules for play fair; therefore R.S.A., we must use two different prime no.So each step we change these prime no. to get a different symbol of characters to cipher it, then put each two pairs in the matrix of play fair(5*5).

Play Fair Algorithm

Playfair is a substitution cipher. Playfair cipher was originally developed by Charles whetstone in 1854 but it bears the name of lord play fair because he promoted the use of this method [1].

Playfair is a digraph substitution cipher which uses a 5*5 matrix in which the keyword is written first and the remaining cells of the matrix are filled with other letters of alphabets with I and J taken in the same cell. The message is divided into digraph, in which repeating letters in the same pair are separated by filler letter x. in case of odd Number of letters in the message a spare letter x is padded with the word to complex the pair. Then the plain text is encoded according to the four rules presented [2].

Playfair is another example of classical cipher methods, which has a square matrix of 5*5 alphabetical letters arranged in an appropriate manner [3]. We can selected a key and placed it in the matrix, the remaining letters of English alphabetic are then one by one placed in the matrix, the plain text is broken into pairs and if a pair has same alphabet then they are separated by introducing a filter letter like x, otherwise if the pair are different letters and reside the same row of matrix then each letter is replaced by the letter a head of it. If the pairs of letter are in same column then each letter is replaced by the letter below it, and if they not in the same row or column they replaced by the letter in their row that reside the intersection of paired letters [4].

R.S.A. Algorithm

One commonly used cipher is called "R.S.A. Encryption" when R.S.A. are the initial of three creators " Rivest, Shamir and Aldeman ". It's based on the following idea [5]:-

Suppose that person A wants to make a public key and that person B wants to use that key to send A a message. In this example we will suppose the message A sends B is just a number, here is the steps:-

Step 1: - Person A selects two prime number, called p and q.

Step 2: - Person A multiply p and q to get N=p*q. which it's the public key, which he tells to person B.

Step 3:- person A also choose another number called e which must be relatively prime tp (p-1)(q-1) , e is a part of a public key also, so person B must know e also.

Step4: - Now B knows enough to encode a message to A. suppose for this example, that the message is the number M.

Step 5: - B calculate the value of $c = M^e (\mathrm{Mod}\ N)$.

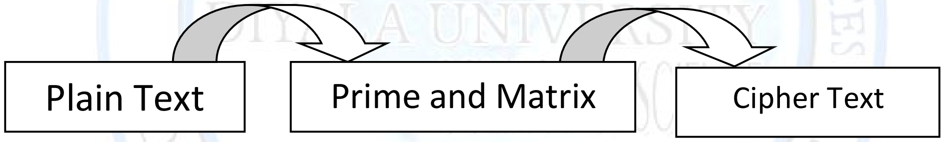
Step 6: - The C is the number that be encoding B sends to A.

Step 7: - Now to decode it for A have to find d such that:-

$$ed=1(\mathrm{mod}\ (p-1)(q-1))\text{-------}1$$

Description of Mixed Algorithm

The algorithms that we can describe it in the figure (1) below, it will be the main research by mixing these two methods:-



Fig(1) Mixed Algorithm

We can explain this algorithm in details so we have a plain text like" IRAQ is better now", we take two character separated of each to other so it will be (the plain text) like this:-

ir ⇨ **aq** ⇨ **sb** ⇨ **et** ⇨ **no** ⇨ **wx**

Then after we put x with last letter mention in the plain text we can use put it without frequently the letter in matrix 5*5 as:- Peace ⇨ Peac

Before we cipher text each two character (remaining in matrix 5*5) enter to R.S.A. algorithm with different prime No. such as the Figure(2) shown .

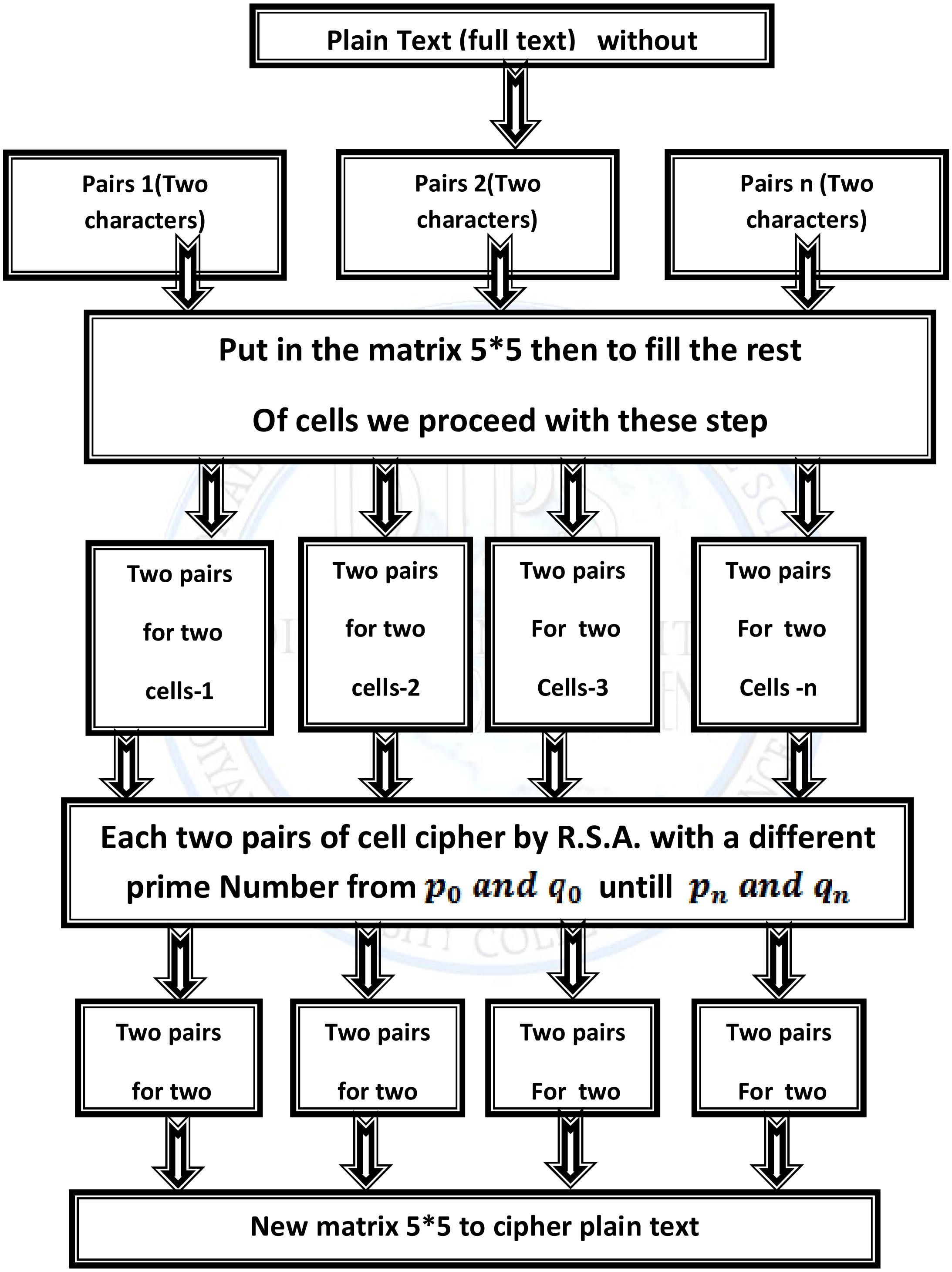

Plain Text (full text) without
Pairs 1(Two characters)
Pairs 2(Two characters)
Pairs n (Two characters)
Put in the matrix 5*5 then to fill the rest
Of cells we proceed with these step
Two pairs for two cells-1
Two pairs for two cells-2
Two pairs For two Cells-3
Two pairs For two Cells -n
Each two pairs of cell cipher by R.S.A. with a different prime Number from p_0 and q_0 untill p_n and q_n
Two pairs for two
Two pairs for two
Two pairs For two
Two pairs For two
New matrix 5*5 to cipher plain text

Fig (2) Mixed Algorithm

<u>Illustrate the algorithm (Mixed algorithm)</u>

After we separates the plain text like this :-

"IRAQ is better now"

"IRAQsbetnow"

ir ⇨ aq ⇨ sb ⇨ et ⇨ no ⇨ wx

Then the matrix will be:-

i	r	a	q	s
b	e	t	n	o
w	x	-	-	-
-	-	-	-	-
-	-	-	-	-

We mention letter i then we neglected letter j according to the rules of play fair algorithm, the rest of the letters must put in matrix 5*5 by cipher it in R.S.A. Techniques with different prime. No.

i	r	a	q	s
b	e	t	n	o
w	x	c	d	f
g	h	k	L	m
p	u	v	y	z

Then the letter

"cdfghklmpuvyz"

must be ciphering before putting in the matrix separated (two character) and each two pairs have different prime No.

we must note if we cipher cd and cipher text result one or two of the letter in matrix 5*5 then we should change the prime Number , until we get the difference character. The receiver (person who get all the prime-No., so we get the final cipher text.

Results of Mixed algorithm

- For "cd" we choose the $p_0 = 13, q_0 = 17$.and by using R.S.A. Technique we get this result

cd = "mp"

- For "fg" we choose the $p_0 = 31, q_0 = 91$.and we get this result

fg = "kv"

- For "hk" we choose the $p_0 = 19, q_0 = 11$. we get this result

hk = "yf"

- For "lm" we choose the $p_0 = 17, q_0 = 37$. we get this result

lm = "uc"

- For "pu" we choose the $p_0 = 71, q_0 = 101$.an we get this result

pu = "dz"

- For "vy" we choose the $p_0 = 217, q_0 = 191$. we get this result

vy = "gh"

- For "z" we choose the $p_0 = 233, q_0 = 211$. we get this result

z = "l"

so the matrix will be :-

i	r	a	q	S
b	e	t	n	O
w	x	m	p	K
v	y	f	u	C
d	z	g	h	L

As we see the new matrix will be like matrix above without any arrangement of alphabetical cell.

Conclusion

Important point we should mention it below:-

1: - we depend on the rules of play fair and R.S.A. algorithms, by mixing two number with R.S.A and make a matrix of them of 5*5 array.

2: - mixed of these two methods is a new technique provided more difficulties to hacker, by comparing between the two methods for one word of (6 letters) we have two prime number with my research we have 6 prime number so the value of complicated is three times the first method.

3: - the receiver person like (B) someone must know public key and the primary numbers.

4: - To decryption we must take the backwards steps.

5: - matrix (Play Fair) algorithm has 5 rows and 5 columns without changing this rules we re-arrange alphabetical distribution on the matrix.

6: - we use in this matrix algorithm many primary no. which we provided it by using c++ language and visual basic v6.0 to implement randomly prime number until we get different character to the previous.

7:- we can use R.S.A. mixed with Play Fair by ciphering plain text before put it in a matrix (5*5) by using R.S.A. Methods then get the step of Play Fair algorithms.

8:-if we want to cipher text like PEACE we have :-

PE ---- NX, AC ---- FS and EX ---- XY

Which is difference than the traditional methods of Play Fair.

References

1. Williams stallings, cryptography and network security , principles and practice , 4th edition, Prentice Hall, 2005.
2. Http://en.wikipedia.org/wiki.
3. V. Umakanta sastry, N. Ravi shanker and S. Durga Bhavani " A modified Play Fair cipher involving interweaving and Iteration". International Journal of computer theory and Engineering , Vol.1, No.5, December 2009.
4. Thomas H. Corman, Charles E.Lieserson and Ronald L. Rivest, Introduction to Play Fair algorithm , Prentice-Hall of India, 2nd edition, 2000.
5. Tom Davis , " R.S.A. Encryption", Chapter one, p 1-4, October 10, 2003, http://www.geometer.org/mathcircles.