استخدام المربعات السحرية في بناء الأنظمة الشفرية

Using Magic Squares To Create Cipher System

خلف صالح يوسف* مجيد حميد علي* نسيبه توفيق إبراهيم*

*كلية علوم الحاسبات والرياضيات- جامعة تكريت

تاريخ استلام البحث:2011/3/7 - تاريخ قبول النشر: 2011/5/3

الملخص

تمت دراسة المربعات السحرية (Magic Square) والاستفادة منها في توليد مفاتيح عشوائية "Random Key" لتشفير البيانات والمعلومات ذات الطابع السري، وتنفيذها حاسوبيا باستخدام البرنامج "Matlab"

Abstract

We study Magic Squares, and it uses to generate random keys to cipher the Data and secret information, by using Matlab programming.

المقدمة

أن الغاية الأساسية من تشفير المعلومات هي الحفاظ على سريتها، وهنالك عدة طرق للحفاظ على سرية المعلومات، منها استخدام أنظمة التشفير (Cipher Systems)، والعلم الذي يهتم بتصميم هذه الأنظمة يسمى علم التشفير (Cryptography)، وهنالك عملية أخرى مضادة لعملية التشفير إلا وهي عملية تحليل الشفرة (Cryptanalysis) التي هي عملية استخدام كافة الطرق الممكنة لمهاجمة الشفرة وإيجاد النص الصريح[3] . لذلك العلاقة بين التشفير والتحليل تناسبية. فالمشفر يحاول قدر الإمكان زيادة أمنية الشفرة التي يستخدمها في إرسال المعلومات السرية أما محلل الشفرة فيحاول باستخدام كل الطرق المعروفة في التحليل للوصول إلى النص الواضح. وتعتمد قوة الشفرة على المفتاح المستخدم " Key ". وسنتطرق في بحثنا هذا إلى استخدام المربعات السحرية (Magic Squares) كمفاتيح شفرية.

استخدام المربعات السحرية في بناء الأنظمة الشفرية

خلف صالح يوسف مجيد حميد علي نسيبه توفيق إبراهيم

الهدف من البحث:

لغرض بناء نظام تشفير رصين يصعب كسره ، تم توليد مفاتيح عشوائية من المربعات السحرية وعلى شكل أرقام عشرية (Decimal) يتم تحويلها إلى النظام الثنائي (Binary System) ، حيث يتم تحويل النص الواضح إلى شفرة الاسكي (ASCII) ونعاملها مع المفتاح "Key " المتولد من المربعات السحرية بعملية " XOR " لنحصل على النص المشفر[4].

(Plain text +Key = Cipher text)

ويعرف المربع السحري على انه مصفوفة مربعة تكون مدخلاتها أعداد صحيحة غير متساوية (مختلفة) (من 1 الى n^2) بحيث يكون مجموع المدخلات في كل سطر وعمود وكذلك الأقطار الرئيسية منها مساوية لمقدار ثابت يسمى بالثابت السحري (The Magic Constant)[2] ($\frac{n(n^2+1)}{2}$)، ونستفاد من المربعات السحرية لتوليد عدد هائل من المفاتيح العشوائية[1]. إن عدد المربعات السحرية (4×4) باستخدام الأعداد من 1 الى 16 بالثابت (34) هي 880 مربع سحري، وعدد المربعات السحرية (5×5) باستخدام الأعداد (من 1 الى 25) هو (275305224) ومسالة المربعات السحرية (6×6) فما فوق فإنها تحتاج الى كم هائل من العمليات الحسابية بحيث انه لايمكن استخدام الحاسوب العادي اليوم للتوصل للإجابة وتوجد بعض التقديرات المثبتة هو عدد المربعات السحرية (6×6) باستخدام الإعداد (من 1 الى 36) وبحسب هذه التقديرات فان العدد يفوق(1.7745×10^{19}) من خلال عمليات تبديل اسطر وأعمدة وانعكاسات متعددة ،ان الشكل العام للمربع السحري (4×4) هو

A	B	C	2S-A-B-C
D	2S-A-B-D	2S-A-C-D	2A+B+C+D-2S
3S-2A-B-C-D	A+C+D-S	A+B+D-S	S-D
A+B+C-S	S-C	S-B	S-A

حيث ان (A,B,C,D,S) هي متغيرات حرة وشكل المربع سوف يعتمد على هذه المتغيرات وهو يحتوي على عدد غير منتهي من الحلول للمربع، ولو فرضنا ان (A=16,B=2,C=3,D=5,S=17) فإننا نحصل على المربع السحري التالي:

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

الجانب النظري:

الخطوة الأولى

في البداية يتم تحويل النص المراد تشفيره إلى رمز الاسكي (ASCII code) وهي إلترميزه الأمريكية القياسية لتبادل المعلومات وهي رمز بطول (8) بت بحيث يمكن تشغيل (128) رمز مختلف وهي كافية للأحرف الكبيرة والصغيرة والأعداد والرموز الأخرى . وفي هذه الشفرة تمثل الأعداد العشرية من (65)إلى (90) (في النظام الثنائي من 1000001 إلى 1011010) للحروف الإنكليزية الكبيرة (منA إلىZ) وتستخدم الأعداد الأخرى لتمثيل علامات الترقيم والحروف الصغيرة والأرقام[5] .

الأحرف	ASCII	الأحرف	ASCII	الأحرف	ASCII
A	01000001	J	01001010	S	01010011
B	01000010	K	01001011	T	01010100
C	01000011	L	01001100	U	01010101
D	01000100	M	01001101	V	01010110
E	01000101	N	01001101	W	01010111
F	01000110	O	01001111	X	01011000
G	01000111	P	01010000	Y	01011001
H	01001000	Q	01010001	Z	01011010
I	01001001	R	01010010		

الخطوة الثانية

نولد أرقام عشوائية من المربعات السحرية وبأبعاد (n×n) .وبأخذ (mod 128) ، ثم نقوم بتحويلها إلى النظام الثنائي.

الخطوة الثالثة

نقوم بعملية جمع النص المشفر بالاسكي مع الأرقام العشوائية (Key) المتولدة من المربعات السحرية وبطريقة (XOR)المنطقية وجدولها كآلاتي :

X	Y	XOR
0	0	0
0	1	1
1	0	1
1	1	0

وبذلك نحصل على النص المشفر .

أما عملية حل الشفرة: فنقوم بجمع النص المشفر مع المفتاح (Key) للحصول على النص الواضح حيث إن المفتاح يكون معروفا لدى الطرفين (المرسل والمستلم).

الجانب العملي : إذا أردنا تشفير النص الواضح (UNIVERSITY) وباستخدام المربع السحري (13×13)

الحل: نحول النص الواضح إلى رمز ال(ASCII)، نقوم بتوليد المربع السحري (13×13) باستخدام برنامج ال(Matlab)

93	108	123	138	153	168	1	16	31	46	61	76	91
107	122	137	152	167	13	15	30	45	60	75	90	92
121	136	151	166	12	14	29	44	59	74	89	104	106
135	150	165	11	26	28	43	58	73	88	103	105	120
149	164	10	25	27	42	57	72	87	102	117	119	134
163	9	24	39	41	56	71	86	101	116	118	133	148
8	23	38	40	55	70	85	100	115	130	132	147	162
22	37	52	54	69	84	99	114	129	131	146	161	7
36	51	53	68	83	98	113	128	143	145	160	6	21
50	65	67	82	97	112	127	142	144	159	5	20	35
64	66	81	96	111	126	141	156	158	4	19	34	49
78	80	95	110	125	140	155	157	3	18	33	48	63
79	94	109	124	139	154	169	2	17	32	47	62	77

لو أخذنا المجاميع العشرة الأولى (المستخدمة كمفاتيح للتشفير) وباستخدام (mod 128) ثم نقوم بتحويلها إلى النظام الثنائي فتصبح كالأتي.

Key	Key (mod 128)	Binary
93	93	01011101
108	108	00011011
123	123	00101111
138	10	00101000
153	25	01001100
168	40	00001010
1	1	01000000
16	16	00000100
31	31	01111100
46	46	00111010

اختبار عشوائية المفاتيح المتولدة من المربعات السحرية:

تم إجراء عدة اختبارات إحصائية على السلسلة المتولدة من المربعات السحرية والتي استخدمت كمفاتيح بعد تحويلها الى النظام الثنائي وهي

01011101, 00011011, 00101111, 00101000, 01001100, 00001010, 01000000, 00000100, 01111100, 00111010

ومن هذه الاختبارات:

1-اختبار التردد (frequency test): القانون الرياضي

حيث (n_0) عدد الاصفار في السلسلة

(n_1) عدد الواحدات في السلسلة

(n) طول السلسلة (المفتاح)

علما" بان الاختبار يكون ناجحا" اذا كان $\chi^2 < 3.84$ لدرجة حرية واحدة حيث ان $\chi^2_{0.05} = 3.84$ (من جدول χ^2) وعليه فان الاختبار ناجح لان $3.2 < 3.84$.

1- **اختبار التسلسل (Serial test):** القانون الرياضي

01=10 ,10 = 10 , 00 = 13 ,11 = 17

$\chi^2 = 3.2$ علما" بان قيمة χ^2 الجدولية هي لدرجتي حرية هي (5.99) وعليه $3.2 < 5.99$

فان السلسلة قد اجتازت الاختبار.

2- اختبار بوكر (Poker test): القانون الرياضي

نفرض (m=4) طول المقطع، $F = \frac{n}{m}$ عدد المقاطع من التطبيق أعلاه $\chi^2 = 2$ $\frac{\text{طول الرسالة}}{\text{طول المقطع}}$

علما" بان الاختبار يكون ناجحا" إذا كان اقل من قيمة χ^2 الجدولية لدرجة حرية (2^m-1) قيمة χ^2لدرجة حرية (2^4-1=15) تساوي *25* ، الاختبار ناجح لان $25 < 2$.

وكذلك اجتازت اختبار الجريان (Run test)، واختبار التطابق الذاتي (Autocorrelation)

ألان نقوم بعملية جمع النص المرمز بالاسكي مع الأرقام العشوائية المتولدة والتي تم تحويلها إلى النظام الثنائي

Text	X=Plain Text	Y=Key	Cipher Text
U	01010101	01011101	00001000
N	00111001	00011011	00100010
I	01001001	00101111	01100110
V	00110101	00101000	00011101
E	01010001	01001100	00011101
R	00100101	00001010	00101111
S	01100101	01000000	00100101
I	01001001	00000100	01001101
T	00010101	01111100	01101001
Y	01001101	00111010	01110111

يصبح النص المشفر كالأتي:

00001000 00100010 01100110 00011101 00011101

00101111 00100101 01001101 01101001 01110111

ويمكن تقطيعه إلى مجاميع خماسية جاهزة للإرسال وكما يلي:

00001, 00000,10001,00110,01100,00111,01000,11101,

00101, 11100,10010,10100,11010,11010,01011,10111

أما إذا أردنا حل النص المشفر أعلاه فنتبع الخطوات التالية:

الخطوة الأولى: نحول النص المشفر الأتي:

00001, 00000,10001,00110,01100,00111,01000,11101,

00101, 11100,10010,10100,11010,11010,01011,10111

إلى مجاميع ثمانية

0001000 0100010 1100110 0011101 0011101

0101111 0100101 1001101 1101001 1110111

الخطوة الثانية: نعامل النص المشفر مع المفتاح المستخدم (المتولد في المربعات السحرية) بعملية XOR ثم نستخدم شفرة الASCII لنحصل على النص الواضح.

Cipher Text	Y=Key	X=Plain Text	Text
00001000	01011101	01010101	U
00100010	00011011	00111001	N
01100110	00101111	01001001	I
00011101	00101000	00110101	V
00011101	01001100	01010001	E
00101111	00001010	00100101	R
00100101	01000000	01100101	S
01001101	00000100	01001001	I
01101001	01111100	00010101	T
01110111	00111010	01001101	Y

فنحصل على النص الواضح : University

الاستنتاجات والتوصيات:

الاستنتاجات:

1- باستخدام المربعات السحرية تكون خيارات التوليد كثيرة ومختلفة، حيث ان المربع السحري الذي أبعاده (5×5) يكون عدد المفاتيح المتولدة منه(275) مليون حيث يصعب كسره[4].

2- باستخدام المربعات السحرية حصلنا على أرقام عشوائية اجتازت الاختبارات الإحصائية الخاصة بالعشوائية.

التوصيات:

1-برمجة خوارزمية التشفير بأكملها والحل حاسوبيا" اختصارا" للوقت والجهد

وسرعة المعلومات للاستفادة منها.

2-التوسع في استخدام المربعات السحرية ذو الرتب العليا .

3-مكننة الخوارزمية لصنع جهاز يقوم بعملية التشفير والحل .

المصادر:

1- الأشهب، سليم شفيق، 2000، **نظرية المربعات السحرية برمجيا ورياضيا**، ط1،سلسلة للبحوث العلمية (1) الأردن.

2- ألآمري، مجيد حميد، **دراسة حول الفضاء الصفري للمربعات السحرية المركبة**،رسالة ماجستير، الأردن، 2008.

3- الحمداني، وسيم عبدالامير، **أنظمة التشفير**، الجامعة التكنولوجية، 1997.

4-K. Pinn and C. Wieczerkowski, **Number of Magic Squares From Parallel Tempering Monte Carlo**, ar Xiv:cond-mat/984109v1, Germany, 9 Apr. 1998.

5-Stallings, William, **Cryptography and Network Security Principles and practice**, third edition, prentice-Hall of India, New Delhi, 2005.