# التشفير باستخدام التحويلات الخطية للمصفوفات السحرية الفردية

**خلف صالح يوسف الجميلي**

*قسم الرياضيات، كلية علوم الحاسبات والرياضيات، جامعة تكريت،تكريت ،العراق*

( تاريخ الاستلام: ٩ / ٦ / ٢٠٠٩ ، تاريخ القبول: ٢٣ / ٥ / ٢٠١٠ )

**الملخص**

تمت دراسة المصفوفات السحرية الفردية (Odd Magic Matrix) والاستفادة منها في التحويل الخطي للنصوص الواضحة إلى نصوص مشفرة وذلك لخاصيتها في عدم التكرار ووجود المعكوس لها، وتنفيذها حاسوبيا باستخدام البرنامج "Matlab"

**المقدمة**

تؤدي التحويلات الخطية دورا" مهما في مجالات عديدة من الرياضيات إضافة إلى دورها في عدد هائل من المشاكل التطبيقية واحدها هو علم التشفير. ويعرف التحويل الخطي بالاتي[٤]:

ليكن كل من V,W فضاء متجهات ، التحويل الخطي $L:V\to W$ هو دالة تنسب لكل متجه x في V متجها وحيدا"L(x) فيW بحيث ان:

ا) $L(x+y)=L(x)+L(y)$ لكل x,y فيV

ب) لكل x فيV ولكل عدد c فان $L(cx)=cL(x)$

توجد دراسات سابقة باستخدام المصفوفات الاعتيادية وحسب معلوماتنا لم تستخدم المصفوفات السحرية سابقا".ومن خلال دراستنا لخصائص هذه المصفوفات تم ادخالها في مجال التشفير. إما المصفوفة السحرية الفردية فتعرف على أنها مصفوفة أبعادها ( n×n) حيث إن n عدد فردي بحيث إن مجموع المدخلات في كل سطر وعمود وكذلك الأقطار الرئيسية منها مساوية لمقدار ثابت يسمى الثابت السحري[١]، ونستفاد منها في توليد عدد هائل من الأرقام العشوائية الغير مكررة، حيث n يجب ان يكون فردي لأنه لو كان زوجي تصبح شاذة لاتمتلك معكوس (غير قابلة للقلب).

**الهدف من البحث:**

لغرض المحافظة على امنية المعلومات يتم تشفيرها باستخدام المصفوفات السحرية مستفيدين من خاصية توليدها ارقام عشوائية وغير متكررة . فاذا كان A مصفوفة سحرية من الصنف n×n (n فردي) فانه نستطيع ان نعرف تحويل خطي $L:R^n\to R^n$ بالصيغة $Y=L(X)=AX$ لكل x في $R^n$

X هنا تمثل النص المراد تشفيره.

Y يمثل النص المشفر.

اما اذا اردنا الحصول على النص الواضح من النص المشفر فيتم التحويل الخطي باستخدام $A^{-1}Y= X$ [٥]

**الجانب النظري:**

**((خطوات التشفير))**

**الخطوة الأولى:**

في البداية يتم تحويل النص المراد تشفيره إلى أرقام مختلفة لكل حرف من حروف الأبجدية وحسب الجدول الترميز الأساسي الأتي[6] :

**جدول الترميز الأساسي**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| P | Q | R | S | T | U | V | W | X | Y | Z | space | , | . | |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | |

ولكن رموز من هذا النوع يمكن ان تحل بدون صعوبة بواسطة عدد من التقنيات منها تحليل تردد الحروف[٣].

**الخطوة الثانية:**

نولد مصفوفة سحرية فردية عدد عناصرها بقدر الحروف المراد تشفيرها، واذا كانت عدد العناصر المراد تشفيرها زوجي نضيف حرف x في النهاية لتحويلها الى عدد فردي.

**الخطوة الثالثة:**

نقوم باجراء عملية ضرب المتجه الصفي للنص الواضح (الرمز) في المصفوفة السحرية الناتجة من الخطوة الثانية.

**الخطوة الرابعة:**

نأخذ (mod 29) للارقام الناتجة من الخطوة السابقة وبهذا تصبح جاهزة للارسال.

**خطوات حل التشفيرة**

فنقوم بجمع النص المشفر مع المفتاح (Key) للحصول على النص الواضح.

**الخطوة الاولى:**

نقوم بايجاد معكوس المصفوفة السحرية المستخدمة في عملية التشفير وناخذ لها (mod 29) .

**الخطوة الثانية:**

نقوم بضرب عناصر معكوس المصفوفة السحرية في متجه النص المشفر المكون من ارقام.

**الخطوة الثالثة :**

ناخذ (mod 29) لناتج الخطوة السابقة.

**الخطوة الرابعة :**

نقوم بتحويل الارقام الناتجة من الخطوة السابقة الى ما يقابلها من حروف ورموز في جدول الترميز. حيث إن المفتاح يكون معروفا لدى الطرفين (المرسل والمستلم).

**الجانب العملي :**

إذا أردنا تشفير كلمة (PLANE) وباستخدام المصفوفة السحرية (5×5).

**الحل:** نحول النص الواضح إلى ما يقابلها في الارقام من (1,2,…,26)

| | P | L | A | N | E |
|---|---|---|---|---|---|
| X | 15 | 11 | 0 | 13 | 4 |

X=[15,11,0,13,4]

- نولـد عناصـر المصـفوفة السـحرية(5×5) باسـتخدام برنـامج ال(Matlab) ويكون الناتج كما يلي:

| 17 | 24 | 1 | 8 | 15 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 17 | 24 | 1 | 8 | 15 |
| 23 | 5 | 7 | 14 | 16 |
| 4 | 6 | 13 | 20 | 22 |
| 10 | 12 | 19 | 21 | 3 |
| 11 | 18 | 25 | 2 | 9 |

يصبح النص المشفر كالأتي جاهزة للإرسال وكما يلي:

[15, 5, 4, 4, 12].

**أما عملية حل الشفرة فنستخدم الاتي:**

يـتم الاتفـاق مـابين المرسـل والمسـتلم علـى ابعـاد المصـفوفة السـحرية حيـث يمكـن تمويههـا داخـل النـص المشـفر معـروف مكانهـا لـدى الطـرفين . فعنـد استلام النص المشفر نقوم بتوليد معكوس المصفوفة السحرية

| | | | | |
|---|---|---|---|---|
| 24 | 7 | 15 | 20 | 17 |
| 26 | 1 | 7 | 17 | 3 |
| 4 | 5 | 5 | 5 | 6 |
| 7 | 22 | 3 | 9 | 13 |
| 22 | 19 | 24 | 3 | 15 |

نقوم بضرب المتجه الرقمي في معكوس المصفوفة

[15, 5, 4, 4, 12].

| | | | | |
|---|---|---|---|---|
| 24 | 7 | 15 | 20 | 17 |
| 26 | 1 | 7 | 17 | 3 |
| 4 | 5 | 5 | 5 | 6 |
| 7 | 22 | 3 | 9 | 13 |
| 22 | 19 | 24 | 3 | 15 |

وتكون النتيجة متجه رقمي

[15,11,0,13,4]

**المصادر:**


١- الأشـهب، سـليم شـفيق، نظريـة المربعـات السـحرية برمجيـا ورياضـيا، ط١،سلسلة للبحوث العلمية (١) الأردن، ٢٠٠٠.

٢- الآمري، مجيد حميد، دراسة حول الفضـاء الصـفري للمربعات السـحرية المركبة،رسالة ماجستير، الأردن، ٢٠٠٨.

٣- الحمـداني، وسـيم عبـدالامير، أنظمـة التشـفير، الجامعـة التكنولوجيـة، ١٩٩٧.

٤- بيرنـارد، كولمـان، مقدمـة فـي الجبـر الخطـي مـع تطبيقـات، ترجمـة د.عادل غسان، باسل عطا الهاشمي، جامعة الموصل، ١٩٩٠.

٥- ليبشتز، سيمور، الجبر الخطي، سلسلة شوم، ط٨، مصر، ٢٠٠٦.

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


| | | | | |
|---|---|---|---|---|
| 23 | 5 | 7 | 14 | 16 |
| 4 | 6 | 13 | 20 | 22 |
| 10 | 12 | 19 | 21 | 3 |
| 11 | 18 | 25 | 2 | 9 |

حيث ان الثابت السحري للصفوف والاعمدة والاقطار الرئيسية يساوي ٦٥

نقوم بضرب متجه النص الواضح في المصفوفة:

[15,11,0,13,4].

نقوم بتحويلها الى ما يقابلها من الحروف الابجدية

فنحصل على النص الواضح : PLANE

**الاستنتاجات والتوصيات :**

**الاستنتاجات:**

١- باستخدام المصفوفات السحرية الفردية تكون خيارات المفاتيح المتولدة كبيرة جدا" ولا تعيد نفسها حيث يصعب كسرها .

٢- تمت الاستفادة من خاصية المصفوفات السحرية الفردية لوجود معكوس لها وسهولة توليدها يدويا وحاسوبيا.

٣- قوة التشفير في هذا البحث تعتمد على عشوائية المفتاح واستخدامه لمرة واحدة ( one time) .

**التوصيات:**

١- نوصي باستخدام المصفوفات الشبه سحرية[٢] ( مصفوفات مدخلاتها اعداد صحيحة موجبة ويكون ناتج جمع الصفوف والاعمدة مساوية للثابت السحري) لان المصفوفات الشبه سحرية ستزيد من عشوائية توليد المفتاح حيث يتم حذف شرط الاقطار الرئيسية.

٢-مكننة الخوارزمية اعلاه لصنع جهاز يقوم بعملية التشفير والحل .

# Ciphering by Using Linear Transformation of odd Magic Matrices

( Received 9 / 6 / 2009 , Accepted 23 / 5 / 2010 )

**Abstract**

We study Magic Matrices, and it uses to Linear Transformation for Plain text to cipher text for its Properties of non repeated and have inverse, by using Matlab programming.