Journal of Nature, Life and Applied Sciences
Volume (5), Issue (3) : 30 Sep 2021
P: 1 - 16

ISSN: 2522-3356

مجلة العلوم الطبيعية والحياتية والتطبيقية
المجلد (5)، العدد (3) : 30 سبتمبر 2021م
ص: 1 - 16

Building matrixes of higher order to achieve the special commutative multiplication and its applications in cryptography

Mechal Fheed Alslman
Nassr Aldin Ide
Ahmad Zakzak
Faculty of science || University of Aleppo || Syria

Abstract: In this paper, we introduce a method for building matrices that verify the commutative property of multiplication on the basis of circular matrices, as each of these matrices can be divided into four circular matrices, and we can also build matrices that verify the commutative property of multiplication from higher order and are not necessarily divided into circular matrices.

Using these matrixes, we provide a way to securely exchange a secret encryption key, which is a square matrix, over open communication channels, and then use this key to exchange encrypted messages between two sides or two parties. Moreover, using these matrixes we also offer a public-key encryption method, whereby the two parties exchange encrypted messages without previously agreeing on a common secret key between them.

Keywords: cryptography, circular matrices, Key exchange, public key cryptography.

بناء مصفوفات تبديلية من مراتب عليا وتطبيقاتها في التشفير

مشعل فهيد السلمان
نصر الدين عيد
أحمد زقزاق
كلية العلوم || جامعة حلب || سوريا

المستخلص: نقدّم في هذا البحث طريقة لبناء مصفوفات تحقّق الخاصة التبديلية للضرب انطلاقا من مصفوفات دائريّة، حيث يمكن تجزئة كلّ مصفوفة من هذه المصفوفات إلى أربع مصفوفات دائريّة، وكذلك يمكن أن نبني مصفوفات تحقق الخاصة التبديلية للضرب من مراتب عليا ولا تُجزّأ بالضرورة إلى مصفوفات دائريّة.

وباستخدام هذه المصفوفات نقدّم طريقة لتبادل مفتاح سري للتشفير عبارة عن مصفوفة مربّعة بشكل آمن عبر قنوات اتّصال مفتوحة، ثم نستخدم هذا المفتاح في تبادل رسائل مشفّرة بين جهتين أو طرفين.

الأكثر من ذلك نقدّم أيضاً باستخدام هذه المصفوفات طريقة تشفير ذات مفتاح معلن، بحيث يتبادل الطرفان رسائل مشفّرة دون الاتفاق مسبقاً على مفتاحٍ سرّيٍّ مشتركٍ بينهما.

الكلمات المفتاحيّة: التشفير، المصفوفات الدائرية، تبادل المفاتيح، تشفير المفتاح المعلن.

1- المقدمة:

في السنوات الأخيرة ومع السعي لتطوير خوارزميات كمية، والتي سوف تساهم في حل المسائل الرياضية صعبة الحل كمسألة تحليل الأعداد الصحيحة، ومسألة الجذور التربيعية قياس عدد صحيح، ومسألة اللوغاريتم المنفصل، والتي يعتمد عليها أمن تشفير المفتاح المعلن (التشفير غير المتناظر) ولذلك أتّجه بعض الباحثين إلى تطوير طرائق تشفير ذات مفتاح معلن في بنى جبرية غير تبديلية، إذ إنّ طرائق التشفير المبينة على بنية جبرية غير تبديليّة محصّنة أكثر ضد الاختراق المعتمد على الخوارزمية الكمية، أما طرائق التشفير المبنية على بنى جبرية تبديلية كطريقة RSA , Rabin وغيرها فهي غير محصنة ضد الاختراق، على الرغم من أن هذه الطرائق آمنة في وقتنا الحاضر وتستخدم على نطاقٍ واسع وذلك لأنه لا توجد إلى الآن خوارزمية كمية لحل المسائل الرياضية التي تعتمد عليها هذه الطرائق [1].

ففي العام 2014 قدم الباحث M.R Valluri بحثا تضمن تقديم طريقة تشفير جديدة بالاعتماد على كثيرات حدود المختزلة غير القابلة للتحليل فوق زمرة غير تبديلية [5]، وفي العام 2017 قدم الباحثون Liu و Zhang و Jia بحثاً أثبتوا فيه إمكانيّة تحليل طريقة التشفير الّتي قدمها الباحث M.R Valluri بالاعتماد على المفتاح المعلن في هذه الطريقة وعلى جمل معادلات خطية وجمل معادلات كثيرات الحدود[3,2] ، وهذا دفع مجموعة من الباحثين إلى دراسة إمكانيّة تعديل هذه الطريقة لتصبح أكثر أماناً، حيث قام مجموعة من الباحثين في العام 2019 باستبدال المفتاح المعلن في [5] بمصفوفات دائرية وتمّ البرهان إن هذا التعديل جعل هذه الطريقة آمنه ضدّ التحليل المقترح من قبل Liu و Zhang وJia [1].

اعتمد بعض الباحثين بشكلٍ خاص في دراسة طرائق التشفير في بنى جبرية غير تبديليه على المصفوفات، وبشكل خاص أتجه بعضهم إلى دراسة المصفوفات الدائرية، وانسجاماً مع أخر ما توصلت له هذه الأبحاث نقدم في هذا البحث نوعاً جديدا من المصفوفات التي نثبت أنها تلعب نفس الدور الذي تلعبه المصفوفات الدائرية في التشفير ولكن بدرجة أمان أعلى.

1-1 مشكلة البحث:

بعد الاطّلاع على الدراسات السابقة الّتي تعتمد على المصفوفات الدائريّة يتبيّن أنّ اكتشاف المفتاح السريّ يتطلّب فقط معرفة عناصر أحد أسطر مصفوفة المفتاح السريّ، وذلك لأنَّ المصفوفات الدائريّة يتمّ تعريفها من خلال سطرها الأوّل فقط، أما اختيار المصفوفات الدائريّة في هذه الأبحاث يعود إلى أهمية الخواص الرياضية التي تحققها هذه المصفوفات وهي:

1- عمليّة ضرب هذه المصفوفات هي عملية تبديلية.
2- عمليّة ضرب هذه المصفوفات هي عمليّة داخليّة، بمعنى أنّ ضرب مصفوفتين دائريتين هو أيضاً مصفوفة دائريّة.

ولذلك جاءت فكرة البحث لدراسة أنواع أخرى من المصفوفات الّتي تحقّق نفس الخواص الرياضيّة وإمكانيّة استخدامها في التشفير، وبحيث تصبح عملية التشفير أكثر أماناً.

يمكن صياغة مشكلة الدراسة في الأسئلة التالية:

1- هل يمكن إيجاد مصفوفات تحقّق خواص مشابهة لخواص المصفوفات الدائريّة، بحيث يمكن استخدامها في طرائق التشفير؟

2- هل يمكن استبدال المصفوفات الدائريّة في طرائق التشفير بنوع آخر من المصفوفات بحيث تصبح عملية التشفير أكثر أماناً؟

2-1 أهميّة البحث:

نقوم في هذا البحث بدراسة إمكانيّة استبدال المصفوفات الدائريّة بمصفوفات أخرى ليست دائريّة لكنّها تحقق خواص مشابهة لخواص المصفوفات الدائريّة، وفي الحقيقة نعتقد أن هذا النوع من المصفوفات سيكون له تطبيقات كثيرة في التشفير، حيث اعتمدت العديد من طرائق التشفير على المصفوفات الدائريّة والّتي يمكن استبدالها بالمصفوفات المقدَّمة هنا نظراً لأنَّها متشابهة في الخواص من جهة، ومن جهة أخرى فإن المصفوفات المقدمة في هذه الطريقة لا يمكن تعريفها من سطرها الأوّل كما في المصفوفات الدائريّة، ممّا يعني صعوبة الوصول إلى مفتاح التشفير حتى وإن تم اكتشاف جزء من عناصره، إضافةً إلى ذلك يمكن تجزئة كلّ مصفوفة إلى أربعة مصفوفات مربعة متساوية في المرتبة لكلٍّ منها نفس شكل المصفوفة الأساسيّة ونفس خواصها الرياضيّة، ونستطيع الاستمرار في تجزئة المصفوفات الناتجة في كل مرة إلى أربعة مصفوفات لنحصل على نفس الشكل ونفس الخواص.

2- منهجية البحث.

سنعتمد في هذا البحث على دراسة بعض المقالات العمليّة ذات الصلة المباشرة بموضوع دراستنا، لنقف على آخر ما توصلت إليه من نتائج، ثمّ ننطلق منها بهدف تطوير هذه الأبحاث وإضافة نتائج جديدة لها.

2-1 هيكلة البحث:

تمّ تقسيم هذا البحث إلى ثلاثة مباحث، يتناول المبحث الأوّل منها الإطار النظري للبحث والدراسات السابقة، بينما يتطرق المبحث الثاني إلّى نتائج هذه الدراسة مع بعض الأمثلة التي توضح هذه النتائج، وأخيراً عرضنا بعض التوصيات والاستنتاجات.

3- المبحث الأوّل- الإطار النظري والدراسات السابقة

3-1 الإطار النظري:

تعريف 1 [4]: يقال إنَّ المصفوفة المربّعة من المرتبة n دائريّة (Circulant matrix)إذا نتج كل سطر من أسطرها عن السطر الأوّل بانزياح عنصر واحد نحو اليمين.

مثال: المصفوفة: $A = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$ هي مصفوفة دائريّة من المرتبة الثالثة.

تُعرّف المصفوفة الدائريّة بعناصر سطرها الأوّل، ونرمز عادةً للمصفوفة الدائريّة من المرتبة n التي عناصر سطرها الأوّل $a_1, a_2, \dots, a_n$ بالرمز $circ(a_1, a_1, \dots, a_n)$

نتيجة 1: [4] إذا كانت A, B مصفوفتين دائريّتين من المرتبة n فإنَّ:

1- جداء مصفوفتين دائريتين هو مصفوفة دائريّة أي إن AB هي مصفوفة دائريّة.

2- جداء مصفوفتين دائريّتين هو عمليّة تبديليّة أي إن $AB = BA$.

2-3 الدراسات السابقة

1- طريقة التشفير بالاعتماد على كثيرات الحدود المختزلة [4]:

ليكن p عدداً أولياً، ولنفرض أنّ $q = p^m$. إن المجموعة $M_n(F_q)$ (مجموعة المصفوفات المربّعة من المرتبة n فوق الحقل F_q) هي زمرة غير تبديلية بالنسبة لعملية ضرب المصفوفات.

المفتاح المعلن: هو المصفوفتان $Q \in M_n(F_q)$ و $P \in GL_n(F_q)$ (مجموعة المصفوفات المربّعة القابلة للقلب من المرتبة n فوق الحقل (F_q)) حيث أن $PQ \neq QP$ وعددين صحيحين a, b.

تبادل المفاتيح:

يختار الطرف الأوّل كثيرة حدود $f(x) \in F_q[x]$ ثمّ يحسب $y = f(P)^a Q f(P)^b$ ويرسل y إلى الطرف الثاني.

يختار الطرف الثاني كثيرة حدود $h(x) \in F_q[x]$ ثمّ يحسب $u = h(P)^a Q h(P)^b$

المفتاح السري المشترك هو $K = f(P)^a u f(P)^b = h(P)^a y h(P)^b$.

2- طريقة التشفير بالاعتماد على المصفوفات الدائريّة [1,2]

في الحقيقة أثبتت الدراسة أنّ الطريقة الموصوفة في الفقرة السابقة غير آمنه إذا يمكن كسر التشفير بالاعتماد على معرفة المفتاحين المعلنين P, Q وذلك بحلّ جملٍ من المعادلات الخطيّة وجمل من معادلات كثيرات الحدود ، وأوصت هذه الدراسة باستبدال حلقة كثيرات الحدود بحلقة المصفوفات [1,6]. وفي [1] تمّ تقديم طريقة تشفير تعتمد على المصفوفات الدائريّة حيث يتمّ حذف المفتاح المعلن P واستبدال المفتاح السري $f(P)$ بمصفوفة دائريّة وأثبتت الدراسة أنّ التشفير وفق هذه الطريقة محصّن ضد الاختراق الموصوف في [2] . ويمكن وصف هذه الطريقة بالشكل التالي:

المفتاح المعلن (Q, a, b) حيث أن Q مصفوفة مربّعة من المرتبة n، و a, b أعداد صحيحه.

الطرف الأوّل: يختار مصفوفة دائريّة من المرتبة n ولتكن $F = circ(c_1, c_2, \dots, c_n)$ بشرط أن $FQ \neq QF$ ثمّ يحسب $y = F^a Q F^b$ ثمّ يُرسل y إلى الطرف الثاني.

الطرف الثاني: يختار مصفوفة دائريّة من المرتبة n ولتكن $H = circ(c'_1, c'_2, \dots, c'_n)$ بشرط أن $HQ \neq QH$ ثمّ يحسب $u = H^a Q H^b$ ثمّ يرسل u إلى الطرف الأوّل.

بعد ذلك يصبح لدى الطرفين نفس المفتاح المشترك: $K = H^a y H^b = F^a u F^b$.

3- أمن طريقة التشفير بالاعتماد على المصفوفات الدائريّة:

في الحقيقة إنّ حذف المفتاح المعلن P واستبدال المفتاح السري $f(P)$ بمصفوفة دائريّة جعل هذه الطريقة محصّنه ضدّ الاختراق، ولكن المشكلة هنا أن المصفوفة الدائريّة يتمّ تعريفها بسطرها الأوّل فقط، وهذا يعني إن معرفة السطر الأوّل في المصفوفة الدائريّة يكفي لكشف المفتاح السري، وبالتالي يصبح السؤال المطروح هنا هل توجد أنواع أخرى من المصفوفات يمكن أن تسُتخدم كمفتاح سري في التشفير، وتكون آمنه أكثر؟

هذا ما سوف ندرسه في هذا البحث.

4- المبحث الثاني- نتائج الدراسة

4-1: بناء مصفوفات تحقق الخاصة التبديلية للضرب انطلاقا من مصفوفات دائريّة:

مبرهنة1 : لتكن A, B, H ثلاث مصفوفات دائريّة من نفس المرتبة، ولنعرف المجموعة:

$$S_0 = \{\begin{bmatrix} A & B \\ C & A \end{bmatrix}; C = BH\}$$

عندئذٍ مهما يكن $X, Y \in S_0$ فإنّ:

1- $XY = YX$ 2- $XY \in S_0$

البرهان:

- لنفرض أنّ: $X, Y \in S_0$ حيث أنّ:

$$X = \begin{bmatrix} A & B \\ C & A \end{bmatrix}; C = BH \, , Y = \begin{bmatrix} A' & B' \\ C' & A' \end{bmatrix} \quad ; C' = B'H$$

لدينا:

$$XY = \begin{bmatrix} AA' + BC' & AB' + BA' \\ CA' + AC' & CB' + AA' \end{bmatrix}$$

$$YX = \begin{bmatrix} A'A + B'C & A'B + B'A \\ C'A + A'C & C'B + A'A \end{bmatrix}$$

ونلاحظ أنّ (حسب نتيجة 1التي تنص على أن عملية ضرب المصفوفات الدائريّة هي عملية تبديلية):

$$AA' + BC' = A'A + BB'H = AA' + BHB' = AA' + CB' = AA' + B'C$$

$$AB' + BA' = B'A + A'B = A'B + B'A$$

$$CA' + AC' = A'C + C'A$$

$$CB' + AA' = BHB' + AA' = CB' + AA'$$

ومنه فإن $XY = YX$.

2- بملاحظة أنّ:

$$XY = \begin{bmatrix} AA' + BC' & AB' + BA' \\ CA' + AC' & CB' + AA' \end{bmatrix}$$

وأن كلاً من A, A', B, B', C, C' هي مصفوفات دائريّة فإنَّ كلاً من $AA' + BC'$ و $AB' + BA'$ و $CA' + AC'$ هي مصفوفات دائريّة، والأكثر من ذلك نجد أن:

$$(AB' + BA')H = AB'H + BA'H = C'A + CA'$$

وهو المطلوب:

مثال: لتكن لدينا المصفوفات الدائريّة من المرتبة الثانية:

$$A = \begin{bmatrix} 2 & 6 \\ 6 & 2 \end{bmatrix}, B = \begin{bmatrix} 6 & 7 \\ 7 & 6 \end{bmatrix}, H = \begin{bmatrix} 5 & 8 \\ 8 & 5 \end{bmatrix}, A' = \begin{bmatrix} 5 & 9 \\ 9 & 5 \end{bmatrix}, B' = \begin{bmatrix} 8 & 3 \\ 3 & 8 \end{bmatrix}$$

وبحساب كلاً من:

$$C = BH = \begin{bmatrix} 86 & 83 \\ 83 & 86 \end{bmatrix}$$

$$C' = B'H = \begin{bmatrix} 64 & 79 \\ 79 & 64 \end{bmatrix}$$

فإن المصفوفتين:

$$X = \begin{bmatrix} A & B \\ C & A \end{bmatrix} = \begin{bmatrix} 2 & 6 & 6 & 7 \\ 6 & 2 & 7 & 6 \\ 86 & 83 & 2 & 6 \\ 83 & 86 & 6 & 2 \end{bmatrix}$$

$$Y = \begin{bmatrix} A' & B' \\ C' & A' \end{bmatrix} = \begin{bmatrix} 5 & 9 & 8 & 3 \\ 9 & 5 & 3 & 8 \\ 64 & 79 & 5 & 9 \\ 79 & 64 & 9 & 5 \end{bmatrix}$$

تحققان الخاصة التبديلية للضرب، ونلاحظ أنّ:

$$XY = YX = \begin{bmatrix} 1001 & 970 & 127 & 143 \\ 970 & 1001 & 143 & 127 \\ 1779 & 1731 & 1001 & 970 \\ 1731 & 1779 & 970 & 1001 \end{bmatrix}$$

2-4 طريقة تبادل المفاتيح:

المفتاح المعلن هو (H, Q) حيث أنّ H مصفوفة دائريّة من المرتبة n و Q مصفوفة مربّعة من المرتبة $2n$ وليست دائريّة.

الطرف الأوّل: يختار مصفوفتين دائريتين من المرتبة n ولتكن A, B ثمّ يحسب $C = BH$ ثمّ يشكل المصفوفة $X = \begin{bmatrix} A & B \\ C & A \end{bmatrix}$ ، ونلاحظ أنّ X من المرتبة $2n$، يحسب المصفوفة $L_1 = XQX$، ثمّ يُرسل هذه النتيجة إلى الطرف الثاني.

الطرف الثاني: يختار مصفوفتين دائريتين A', B' ثمّ يحسب $C' = B'H$ ثم يشكّل المصفوفة $Y = \begin{bmatrix} A' & B' \\ C' & A' \end{bmatrix}$ ثم يحسب المصفوفة $L_2 = YQY$ ويُرسل هذه النتيجة إلى الطرف الأوّل. عند ذلك يحسب الطرف المفتاح السري المشترك K_1 بالشكل التالي: $K_1 = XL_2X$ أمّا الطرف الثاني يحسب الطرف المفتاح السري المشترك K_2 بالشكل التالي: $K_2 = YL_1Y$

إنّ المفتاح السري المشترك للطرفين هو $K = K_1 = K_2$ لأنّ:

$$K_1 = XL_2X = XYQYX = YXQYX = YL_1Y = K_{12}$$

وبالتالي يكون الطرفان قد تبادلا نفس المفتاح السري.

مثال:

بفرض أن المفتاح المعلن هو $H = \begin{bmatrix} 5 & 8 \\ 8 & 5 \end{bmatrix}, Q = \begin{bmatrix} 6 & 8 & 9 & 3 \\ 5 & 4 & 2 & 1 \\ 5 & 3 & 2 & 7 \\ 2 & 5 & 4 & 6 \end{bmatrix}$

الطرف الأوّل يختار المصفوفتين: $A = \begin{bmatrix} 2 & 6 \\ 6 & 2 \end{bmatrix}, B = \begin{bmatrix} 6 & 7 \\ 7 & 6 \end{bmatrix}$ ثمّ يحسب:

$C = BH = \begin{bmatrix} 86 & 83 \\ 83 & 86 \end{bmatrix}$ ثم يشكل المصفوفة:

$$X = \begin{bmatrix} A & B \\ C & A \end{bmatrix} = \left[\begin{array}{cc|cc} 2 & 6 & 6 & 7 \\ 6 & 2 & 7 & 6 \\ - & - & - & - \\ 86 & 83 & 2 & 6 \\ 83 & 86 & 6 & 2 \end{array}\right]$$

الطرف الثاني يختار المصفوفتين $A' = \begin{bmatrix} 5 & 9 \\ 9 & 5 \end{bmatrix}, B' = \begin{bmatrix} 8 & 3 \\ 3 & 8 \end{bmatrix}$ ثم يحسب

$C' = B'H = \begin{bmatrix} 64 & 79 \\ 79 & 64 \end{bmatrix}$ ثم يشكل المصفوفة:

$$Y = \begin{bmatrix} A' & B' \\ C' & A' \end{bmatrix} = \left[\begin{array}{cc|cc} 5 & 9 & 8 & 3 \\ 9 & 5 & 3 & 8 \\ - & - & - & - \\ 64 & 79 & 5 & 9 \\ 79 & 64 & 9 & 5 \end{array}\right]$$

الطرف الأوّل يحسب المصفوفة:

$$L_1 = XQX = \begin{bmatrix} 14718 & 14768 & 1883 & 1772 \\ 17799 & 17770 & 2129 & 2079 \\ 123943 & 121800 & 17392 & 19597 \\ 121181 & 119235 & 17236 & 19362 \end{bmatrix}$$

ثم يُرسل هذه النتيجة إلى الطرف الثاني.

الطرف الثاني يحسب المصفوفة:

$$L_2 = YQY = \begin{bmatrix} 15206 & 15125 & 2650 & 2592 \\ 18054 & 18350 & 2857 & 3124 \\ 90462 & 96498 & 16380 & 18390 \\ 99959 & 106840 & 17543 & 19930 \end{bmatrix}$$

ثمّ يُرسل هذه النتيجة إلى الطرف الأوّل.

يحسب الطرف الأوّل المفتاح السري المشترك كالتالي:

$$K_1 = XL_2X = \begin{bmatrix} 55232302 & 54979079 & 20687566 & 20480549 \\ 54575402 & 54326560 & 20373548 & 20175592 \\ 133983794 & 133806499 & 52163590 & 51950570 \\ 133009270 & 132839372 & 51729629 & 51520990 \end{bmatrix}$$

يحسب الطرف الثاني المفتاح السري المشترك كالتالي:

$$K_2 = XL_1X = \begin{bmatrix} 55232302 & 54979079 & 20687566 & 20480549 \\ 54575402 & 54326560 & 20373548 & 20175592 \\ 133983794 & 133806499 & 52163590 & 51950570 \\ 133009270 & 132839372 & 51729629 & 51520990 \end{bmatrix}$$

بسهولة نلاحظ أن $K_1 = K_2$ فيكون المفتاح السري المشترك هو $K = K_1 = K_2$.

3-4 بناء مصفوفات تبديلية من مراتب عليا تحقق الخاصة التبديلية للضرب:

مبرهنة2: لتكن A, B, H ثلاث مصفوفات دائريّة من نفس المرتبة، ولنعرف المجموعات:

$$S_1 = \{\begin{bmatrix} A & B \\ C & A \end{bmatrix}; C = BH\}$$

$$S_2 = \{\begin{bmatrix} A_1 & B_1 \\ C_1 & A_1 \end{bmatrix}; C_1 = B_1H_1 \ \& \ A_1, B_1, C_1, H_1 \in S_1\}$$

وهكذا فإنَّ:

$$S_n = \{\begin{bmatrix} A_{n-1} & B_{n-1} \\ C_{n-1} & A_{n-1} \end{bmatrix}; C_{n-1} = B_{n-1}H_{n-1} \ \& \ A_{n-1}, B_{n-1}, C_{n-1}, H_{n-1} \in S_{n-1}\}$$

فإنّه مهما يكن $X_n, Y_n \in S_n$ فإنّ:

$$X_nY_n = Y_nX_n \ -1 \qquad X_nY_n \in S_n \ -2$$

البرهان: يتم البرهان بالاستقراء الرياضي:

1- من أجل $n = 0$ فإن المطلوب محقق حسب (المبرهنة 1)

2- لنفرض صحّة العبارة من أجل n ولنبرهن أنّها صحيحه من أجل $n + 1$. لنفرض أنّ $A, B, H, A', B', C, C' \in S_n$ وأن $X, Y \in S_{n+1}$ حيث أنّ:

$$X = \begin{bmatrix} A & B \\ C & A \end{bmatrix}; C = BH$$

$$Y = \begin{bmatrix} A' & B' \\ C' & A' \end{bmatrix} \quad ; C' = B'H$$

$$XY = \begin{bmatrix} AA' + BC' & AB' + BA' \\ CA' + AC' & CB' + AA' \end{bmatrix}$$

$$YX = \begin{bmatrix} A'A + B'C & A'B + B'A \\ C'A + A'C & C'B + A'A \end{bmatrix}$$

وبما أنَّ عناصر S_n تُحقّق الخاصة التبديلية للضرب حسب فرضيّة الاستقراء، وبما أنّ $A, B, A', B', C, C' \in S_n$ فإنه لكي يكون $XY = YX$ يكفي أن يكون: $BC' = B'C$ و $C'B = CB'$، وحسب ما تقدم لدينا:

$$BC' = BB'H = CB' = B'C \qquad (*)$$

$$C'B = B'HB = C'B \qquad (**)$$

ومنه فإن $XY = YX$.

2- لبرهان أن $XY \in S_n$ يجب أنْ نبرهن أنّ $AA' + BC' = CB' + AA'$ وهذا محقّق حسب $(*)$ وأيضاً يجب أن نبرهن أن جميع عناصر XY هي من S_n وهذا محقّق حسب فرضيّة الاستقراء، وأيضا يجب أن يكون $CA' + AC' = (A'B + BA')H$ وهذا محقّق لأنّ:

$$CA' + AC' = \mathrm{BHA'} + \mathrm{AB'H} = (A'B + BA')H$$

ومنه فإنّ $XY \in S_{n+1}$.

وهو المطلوب.

استنادا إلى هذه المبرهنة يمكن بناء مصفوفات تحقّق الخاصة التبديليّة انطلاقا من مصفوفات دائريّة وفق الخطوات التالية:

1- نختار مصفوفات دائريّة A, B, A', B', H من المرتبة n، ثمّ نشكل المصفوفتين:

$$X_1 = \begin{bmatrix} A & B \\ C & A \end{bmatrix}; C = BH$$

$$Y_1 = \begin{bmatrix} A' & B' \\ C' & A' \end{bmatrix} \quad ; C' = B'H$$

حسب المبرهنة السابقة فإنّ $X_1Y_1 = Y_1X_1$ و $X_1Y_1 \in S_1$ وكلًّا من X_1, Y_1من المرتبة $2n$.

2- بنفس الطريقة نشكّل المصفوفات B_1, B'_1, H_1 من S_1، وجميعها من المرتبة $2n$، ثم نحسب $C_1 = B_1H_1, C'_1 = B'_1H_1$ ، ونشكل المصفوفتين:

$$X_2 = \begin{bmatrix} X_1 & B_1 \\ C_1 & X_1 \end{bmatrix} = \begin{bmatrix} A & B & & \\ C & A & B_1 & \\ & C_1 & A & B \\ & & C & A \end{bmatrix}$$

$$Y_2 = \begin{bmatrix} Y_1 & B'_1 \\ C_1{}' & Y_1 \end{bmatrix} = \begin{bmatrix} A' & B' & & \\ C' & A' & B'_1 & \\ & C'_1 & A' & B' \\ & & C' & A' \end{bmatrix}$$

واضح أنّ كلاً من X_2, Y_2 من المرتبة 2^2n، وأن $X_2Y_2 = Y_2X_2$ وكل منهما من المجموعة S_2.

3- وبنفس الطريقة نختار المصفوفات B_2, B'_2, H_2 من المرتبة 2^2n وجميعها من S_2، ثمّ نحسب $C_2 = B_2H_2$, $C'_2 = B'_2H_2$ ثمّ نشكّل المصفوفتين:

$$X_3 = \begin{bmatrix} X_2 & B_2 \\ C_2 & X_2 \end{bmatrix} = \begin{bmatrix} A & B & & & & & & \\ C & A & B_1 & & & & & \\ & C_1 & A & B & & & & \\ & & C & A & B_2 & & & \\ & & & & A & B & & \\ & & & & C & A & B_1 & \\ & & & C_2 & & & A & B \\ & & & & & C_1 & C & A \end{bmatrix}$$

$$Y_3 = \begin{bmatrix} Y_2 & B_2' \\ {C_2}' & Y_2 \end{bmatrix} = \begin{bmatrix} A' & B' & & & & & \\ C' & A' & B_1' & & & & \\ & {C_1}' & A' & B' & & B_2 & \\ & & C' & A' & & & \\ & & & & A' & B' & \\ & & & {C_2}' & C' & A' & B_1' \\ & & & & & {C_1}' & A' & B' \\ & & & & & & C' & A' \end{bmatrix}$$

واضح أنّ كلاً من X_3, Y_3 من المرتبة 2^3n، وأنّ $X_3Y_3 = Y_3X_3$ وكل منهما من المجموعة S_3.

- نتابع العمل بنفس الطريقة حتّى نحصل على مصفوفات تبديليّة من المجموعة S_m من المرتبة $2^m n$.

مثال: باختيار المصفوفات الدائريّة من المرتبة الثالثة:

$$A = \begin{bmatrix} 5 & 3 & 2 \\ 2 & 5 & 3 \\ 3 & 2 & 5 \end{bmatrix}, B = \begin{bmatrix} 2 & 4 & 7 \\ 7 & 2 & 4 \\ 4 & 7 & 2 \end{bmatrix}, H = \begin{bmatrix} 3 & 5 & 7 \\ 7 & 3 & 5 \\ 5 & 7 & 3 \end{bmatrix},$$

$$A' = \begin{bmatrix} 5 & 1 & 4 \\ 4 & 5 & 1 \\ 1 & 4 & 5 \end{bmatrix}, B' = \begin{bmatrix} 8 & 4 & 1 \\ 1 & 8 & 4 \\ 4 & 1 & 8 \end{bmatrix}$$

وبحساب المصفوفتين:

$$C = BH = \begin{bmatrix} 69 & 71 & 55 \\ 55 & 69 & 71 \\ 71 & 55 & 69 \end{bmatrix}, C' = B'H = \begin{bmatrix} 57 & 59 & 79 \\ 79 & 57 & 59 \\ 59 & 79 & 57 \end{bmatrix}$$

ووفق ما سبق نحصل على المصفوفتين:

$$X = \begin{bmatrix} 5 & 3 & 2 & \vdots & 2 & 4 & 7 \\ 2 & 5 & 3 & \vdots & 7 & 2 & 4 \\ 3 & 2 & 5 & \vdots & 4 & 7 & 2 \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots & \cdots \\ 69 & 71 & 55 & \vdots & 5 & 3 & 2 \\ 55 & 69 & 71 & \vdots & 2 & 5 & 3 \\ 71 & 55 & 69 & \vdots & 3 & 2 & 5 \end{bmatrix}, Y = \begin{bmatrix} 5 & 1 & 4 & \vdots & 8 & 4 & 1 \\ 4 & 5 & 1 & \vdots & 1 & 8 & 4 \\ 1 & 4 & 5 & \vdots & 4 & 1 & 8 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 57 & 59 & 79 & \vdots & 5 & 1 & 4 \\ 79 & 57 & 59 & \vdots & 4 & 5 & 1 \\ 59 & 79 & 57 & \vdots & 1 & 4 & 5 \end{bmatrix}$$

وباختيار:

$$H_1 = \begin{bmatrix} 2 & 5 & 3 & \vdots & 5 & 8 & 2 \\ 3 & 2 & 5 & \vdots & 2 & 5 & 8 \\ 5 & 3 & 2 & \vdots & 8 & 2 & 5 \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots & \cdots \\ 81 & 63 & 81 & \vdots & 2 & 5 & 3 \\ 81 & 81 & 63 & \vdots & 3 & 2 & 5 \\ 63 & 81 & 81 & \vdots & 5 & 3 & 2 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 8 & 9 & 4 & \vdots & 6 & 4 & 2 \\ 4 & 8 & 9 & \vdots & 2 & 6 & 4 \\ 9 & 4 & 8 & \vdots & 4 & 2 & 6 \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots & \cdots \\ 56 & 56 & 68 & \vdots & 8 & 9 & 4 \\ 68 & 56 & 56 & \vdots & 4 & 8 & 9 \\ 56 & 68 & 56 & \vdots & 9 & 4 & 8 \end{bmatrix}$$

من S_1 وبحساب:

$$C_1 = BH = \begin{bmatrix} 999 & 934 & 977 & \vdots & 124 & 161 & 150 \\ 977 & 999 & 934 & \vdots & 150 & 124 & 161 \\ 934 & 977 & 999 & \vdots & 161 & 150 & 124 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 2249 & 2153 & 2123 & \vdots & 999 & 934 & 977 \\ 2123 & 2249 & 2153 & \vdots & 977 & 999 & 934 \\ 2153 & 2123 & 2249 & \vdots & 934 & 977 & 999 \end{bmatrix}$$

وباختيار: $B'_1 = \begin{bmatrix} 1 & 5 & 3 & \vdots & 5 & 1 & 9 \\ 3 & 1 & 5 & \vdots & 9 & 5 & 1 \\ 5 & 3 & 1 & \vdots & 1 & 9 & 5 \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots & \cdots \\ 67 & 91 & 67 & \vdots & 1 & 5 & 3 \\ 67 & 67 & 91 & \vdots & 3 & 1 & 5 \\ 91 & 67 & 67 & \vdots & 5 & 3 & 1 \end{bmatrix}$ من S_1 وبحساب :

$$C'_1 = B'_1 H_1 = \begin{bmatrix} 1085 & 1149 & 1231 & \vdots & 97 & 93 & 95 \\ 1231 & 1085 & 1149 & \vdots & 95 & 97 & 93 \\ 1149 & 1231 & 1085 & \vdots & 93 & 95 & 97 \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots & \cdots \\ 1417 & 1429 & 1429 & \vdots & 1085 & 1149 & 1231 \\ 1429 & 1417 & 1429 & \vdots & 1231 & 1085 & 1149 \\ 1429 & 1429 & 1417 & \vdots & 1149 & 1231 & 1085 \end{bmatrix}$$

نحصل على المصفوفتين: $X_2 = \begin{bmatrix} X_1 & B_1 \\ C_1 & X_1 \end{bmatrix}$ و $Y_2 = \begin{bmatrix} Y_1 & B'_1 \\ C'_1 & Y_1 \end{bmatrix}$:

$$X_2 = \left[\begin{array}{ccc:ccc|ccc:ccc} 5 & 3 & 2 & 2 & 4 & 7 & 8 & 9 & 4 & 6 & 4 & 2 \\ 2 & 5 & 3 & 7 & 2 & 4 & 4 & 8 & 9 & 2 & 6 & 4 \\ 3 & 2 & 5 & 4 & 7 & 2 & 4 & 9 & 8 & 4 & 2 & 6 \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline 69 & 71 & 55 & 5 & 3 & 2 & 56 & 56 & 68 & 8 & 9 & 4 \\ 55 & 69 & 71 & 2 & 5 & 3 & 68 & 56 & 56 & 4 & 8 & 9 \\ 71 & 55 & 69 & 3 & 2 & 5 & 56 & 68 & 56 & 9 & 4 & 8 \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline 999 & 934 & 977 & 124 & 161 & 150 & 5 & 3 & 2 & 2 & 4 & 7 \\ 977 & 999 & 934 & 150 & 124 & 161 & 2 & 5 & 3 & 7 & 2 & 4 \\ 934 & 977 & 999 & 161 & 150 & 124 & 3 & 2 & 5 & 4 & 7 & 2 \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline 2249 & 2153 & 2123 & 999 & 934 & 977 & 69 & 71 & 55 & 5 & 3 & 2 \\ 2123 & 2249 & 2153 & 977 & 999 & 934 & 55 & 69 & 71 & 2 & 5 & 3 \\ 2153 & 2123 & 2249 & 934 & 977 & 999 & 71 & 55 & 69 & 3 & 2 & 5 \end{array}\right]$$

$$Y_2 = \left[\begin{array}{ccc:ccc|ccc:ccc} 5 & 1 & 4 & 8 & 4 & 1 & 1 & 5 & 3 & 5 & 1 & 9 \\ 4 & 5 & 1 & 1 & 8 & 4 & 3 & 1 & 5 & 9 & 5 & 1 \\ 1 & 4 & 5 & 4 & 1 & 8 & 5 & 9 & 1 & 1 & 9 & 5 \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline 57 & 59 & 79 & 5 & 1 & 4 & 67 & 91 & 67 & 1 & 5 & 3 \\ 79 & 57 & 59 & 4 & 5 & 1 & 67 & 67 & 91 & 3 & 1 & 5 \\ 59 & 79 & 57 & 1 & 4 & 5 & 91 & 67 & 67 & 5 & 3 & 1 \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline 1085 & 1149 & 1231 & 97 & 93 & 95 & 5 & 1 & 4 & 8 & 4 & 1 \\ 1231 & 1085 & 1149 & 95 & 97 & 93 & 4 & 5 & 1 & 1 & 8 & 4 \\ 1149 & 1231 & 1085 & 93 & 95 & 97 & 1 & 4 & 5 & 4 & 1 & 8 \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline 1417 & 1429 & 1429 & 1085 & 1149 & 1231 & 57 & 59 & 79 & 5 & 1 & 4 \\ 1429 & 1417 & 1429 & 1231 & 1085 & 1149 & 79 & 57 & 59 & 4 & 5 & 1 \\ 1429 & 1429 & 1417 & 1149 & 1231 & 1085 & 59 & 79 & 57 & 1 & 4 & 5 \end{array}\right]$$

4-4 طريقة تبادل المفاتيح، والتشفير ذو المفتاح السري.

- الطرف الأوّل يختار:

مفتاح سري: مصفوفة $X = \begin{bmatrix} A_{m-1} & B_{m-1} \\ C_{m-1} & A_{m-1} \end{bmatrix}$ من S_m والمرتبة $2^m n$ حيث أن $C_{m-1} = H_{m-1}B_{m-1}$.

مفتاح معلن: المصفوفة H_{m-1} من S_m ومصفوفة Q من المرتبة $2^{m+1}n$ والمصفوفة XQX.

- الطرف الثاني يحصل على المصفوفة H_{m-1} ثم يقوم بتجزئتها إلى مصفوفات دائريّة كل منها من المرتبة n، بعد ذلك يقوم بحساب المصفوفات $H, H_1, \dots, H_{m-2}$ من العلاقات: $H_i = B_i^{-1}C_i$، ثم يقوم باختيار مصفوفة Y من S_m .
- الطرف الثاني يحسب YQY ثم يعلن هذه النتيجة.
- المفتاح المشترك للطرفين هو:

$$K = YXQXY = XYQYX$$

التشفير: إذا كانت مصفوفة الرسالة المشفرة هي M فإن الرسالة المشفرة هي $E = Q + M$

فك التشفير: مصفوفة النص الصريح $M = Q - E$.

5-4 طريقة التشفير ذات المفتاح المعلن:

الطرف الأوّل يمتلك:

1- المفتاح المعلن هو المصفوفات المصفوفة H_{m-1} من S_m و مصفوفة Q من المرتبة $2^{m+1}n$ والمصفوفة $L = XQX$.

2- المفتاح السري: مصفوفة $X = \begin{bmatrix} A_{m-1} & B_{m-1} \\ C_{m-1} & A_{m-1} \end{bmatrix}$ من S_m

إذا أراد الطرف الثاني التواصل مع الطرف الأوّل يقوم بما يلي:

1- يمثّل الرسالة في مصفوفة M من المرتبة $2^{m+1}n$.

2- من خلال المصفوفة H_{m-1} يقوم باختيار مصفوفة Y من S_m.

التشفير: يحسب : $E_1 = YQY, E_2 = YXQYX + M$ ثم يرسل الرسالة (E_1, E_2).

فكّ التشفير:

بعد أن يحصل الطرف الأوّل على الرسالة المشفّرة (E_1, E_2) يستخدم المفتاح السري X لحساب $XE_1X = XYQYX = YXQYX$ ثمّ يحسب $M = E_2 - XE_1X$.

مثال:

لنفرض أنّ المفتاح السري للطرف الأوّل هو:

$$X = \begin{bmatrix} 3 & 4 & 6 & 7 & 7 & 2 & 2 & 9 \\ 4 & 3 & 7 & 6 & 2 & 7 & 9 & 2 \\ 86 & 83 & 3 & 4 & 82 & 61 & 7 & 2 \\ 83 & 86 & 4 & 3 & 61 & 82 & 2 & 7 \\ 707 & 661 & 75 & 105 & 3 & 4 & 6 & 7 \\ 661 & 707 & 105 & 75 & 4 & 3 & 7 & 6 \\ 1215 & 1125 & 707 & 661 & 86 & 83 & 3 & 4 \\ 1125 & 1215 & 661 & 707 & 83 & 86 & 4 & 3 \end{bmatrix}$$

والمفتاح المعلن للطرف الأوّل هو المصفوفات:

$$H_1 = \begin{bmatrix} 7 & 2 & 5 & 4 \\ 2 & 7 & 4 & 5 \\ 57 & 60 & 7 & 2 \\ 60 & 57 & 2 & 7 \end{bmatrix}, Q = \begin{bmatrix} 1 & 5 & 4 & 2 & 9 & 8 & 1 & 3 \\ 5 & 9 & 4 & 7 & 3 & 2 & 9 & 4 \\ 7 & 4 & 2 & 5 & 3 & 2 & 7 & 4 \\ 2 & 8 & 4 & 1 & 9 & 5 & 7 & 6 \\ 2 & 5 & 1 & 9 & 6 & 7 & 3 & 9 \\ 3 & 7 & 3 & 8 & 3 & 2 & 2 & 2 \\ 7 & 8 & 2 & 1 & 5 & 8 & 5 & 3 \\ 8 & 9 & 5 & 7 & 4 & 4 & 9 & 5 \end{bmatrix}$$

$$L = \begin{bmatrix} 837625 & 833078 & 351740 & 350761 & 65505 & 67669 & 8349 & 8197 \\ 722495 & 717501 & 288139 & 286273 & 53652 & 55014 & 7778 & 7476 \\ 5900325 & 5914775 & 2261721 & 2273723 & 464838 & 493248 & 64192 & 60954 \\ 5621123 & 5618686 & 2166776 & 2173099 & 461297 & 488777 & 63165 & 59921 \\ 29308881 & 29017773 & 11181311 & 11127067 & 2190929 & 2226772 & 321866 & 287205 \\ 29210975 & 28892078 & 11365636 & 11291199 & 2236949 & 2278830 & 319162 & 288727 \\ 74490321 & 73730388 & 29578446 & 29482605 & 5549423 & 5643674 & 773386 & 712889 \\ 75102287 & 74286077 & 30129819 & 30012145 & 5646959 & 5745176 & 778022 & 716111 \end{bmatrix}$$

ولنفرض أنّ الطرف الثاني يُريد إرسال رسالة إلى الطرف الأوّل، ولنفرض أن مصفوفة الرسالة بعد تحويلها إلى مقابلاتها العددية هي:

$$M = \begin{bmatrix} 4 & 16 & 11 & 8 & 5 & 19 & 12 & 13 \\ 5 & 7 & 13 & 21 & 25 & 24 & 18 & 17 \\ 16 & 13 & 12 & 15 & 7 & 23 & 14 & 16 \\ 17 & 18 & 16 & 17 & 15 & 19 & 23 & 24 \\ 19 & 17 & 11 & 13 & 12 & 21 & 23 & 14 \\ 15 & 18 & 13 & 12 & 13 & 17 & 17 & 21 \\ 8 & 9 & 14 & 9 & 12 & 15 & 9 & 13 \\ 23 & 13 & 14 & 7 & 8 & 5 & 3 & 2 \end{bmatrix}$$

يتبع ما يلي:

1- يحصل على المصفوفة H_1 ثمّ يقوم بتجزئتها إلى أربعة أجزاء كالتالي:

$$H_1 = \begin{bmatrix} 7 & 2 & \vdots & 5 & 4 \\ 2 & 7 & \vdots & 4 & 5 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 57 & 60 & \vdots & 7 & 2 \\ 60 & 57 & \vdots & 2 & 7 \end{bmatrix} = \begin{bmatrix} A & B \\ C & A \end{bmatrix}$$

ونلاحظ أن جميع هذه المصفوفات هي مصفوفات دائريّة. يحسب:

$$H = B^{-1}C = \begin{bmatrix} 5 & 8 \\ 8 & 5 \end{bmatrix}$$

انطلاقا من H, H_1 يقوم باختبار مصفوفة:

$$Y = \begin{bmatrix} 5 & 9 & 8 & 3 & 9 & 5 & 2 & 3 \\ 9 & 5 & 3 & 8 & 5 & 9 & 3 & 2 \\ 64 & 79 & 5 & 9 & 34 & 31 & 9 & 5 \\ 79 & 64 & 9 & 5 & 31 & 34 & 5 & 9 \\ 367 & 344 & 85 & 86 & 5 & 9 & 8 & 3 \\ 344 & 367 & 86 & 85 & 9 & 5 & 3 & 8 \\ 1113 & 1110 & 367 & 344 & 64 & 79 & 5 & 9 \\ 1110 & 1113 & 344 & 367 & 79 & 64 & 9 & 5 \end{bmatrix}$$

ثم يحسب الرسالة المشفّرة:

$$E_1 = YQY =$$

$$\begin{bmatrix} 676257 & 673230 & 200075 & 199525 & 50225 & 51488 & 9048 & 9454 \\ 625709 & 623049 & 182126 & 182469 & 44864 & 45968 & 8887 & 8820 \\ 3389958 & 3374762 & 989240 & 988674 & 250308 & 257778 & 48262 & 49241 \\ 3263405 & 3249136 & 945380 & 946480 & 239839 & 245992 & 47604 & 48110 \\ 13205915 & 13157842 & 3861601 & 3846569 & 934059 & 972216 & 185698 & 183743 \\ 13417788 & 13367008 & 3936903 & 3917791 & 956298 & 997098 & 187011 & 186237 \\ 45463922 & 45286508 & 13331694 & 13277260 & 3234595 & 3364711 & 632781 & 628670 \\ 45755934 & 45578850 & 13415416 & 13365158 & 3246446 & 3375323 & 635560 & 630270 \end{bmatrix}$$

$$E_2 = YLY + M = \begin{bmatrix} 125991111366 & 126071930387 & 31575231806 & 31519790096 & 35949872330 & 35920125300 & 9805544773 & 9818419538 \\ 126020569585 & 126103683266 & 31567228704 & 31511850199 & 35917875657 & 35886968854 & 9795785098 & 9808480411 \\ 460028239062 & 460333180742 & 115365698065 & 115157030255 & 131201498791 & 131086911691 & 35791661308 & 35834895454 \\ 461263279177 & 461572007731 & 115623306965 & 115414079683 & 131547395018 & 131431196996 & 35881158500 & 35924390763 \\ 413399318645 & 413653035301 & 103423284875 & 103303414471 & 116818972208 & 116750470494 & 31869252732 & 31924033344 \\ 413538048874 & 413792482224 & 103453596109 & 103332471271 & 116875585522 & 116806798588 & 31883457156 & 31938229426 \\ 1648841387423 & 1649880447855 & 413564745502 & 413067636592 & 463897256793 & 463631742468 & 126701067502 & 126919242990 \\ 1646736889903 & 1647767917029 & 413141391654 & 412643304775 & 463297597822 & 463035258892 & 126547414678 & 126765947894 \end{bmatrix}$$

ثم يرسل الرسالة (E_1, E_2) إلى الطرف الأوّل.

فك التشفير:

عندما يتلقّى الطرف الأوّل الرسالة المشفرة (E_1, E_2) يستخدم المفتاح السري X ليحسب المصفوفة:

$XE_1X = XYQYX =$

$$\begin{bmatrix} 125991111362 & 126071930371 & 31575231795 & 31519790088 & 35949872325 & 13592012528 & 9805544761 & 9818419525 \\ 126020569580 & 126103683259 & 31567228691 & 31511850178 & 35917875632 & 35886968830 & 9795785080 & 9808480394 \\ 460028239046 & 033318072964 & 115365698053 & 115157030240 & 131201498784 & 131086911668 & 35791661294 & 35834895438 \\ 461263279160 & 461572007713 & 115623306949 & 796660115414 & 131547395003 & 131431196977 & 35881158477 & 35924390739 \\ 413399318626 & 413653035284 & 103423284864 & 103303414458 & 116818972196 & 311675047047 & 31869252709 & 31924033330 \\ 413538048859 & 413792482206 & 103453596096 & 103332471259 & 116875585509 & 116806798571 & 31883457139 & 31938229405 \\ 1387415164884 & 1649880447846 & 413564745488 & 413067636583 & 463897256781 & 463631742453 & 126701067493 & 126919242977 \\ 1646736889880 & 1647767917016 & 139164041314 & 412643304768 & 463297597814 & 463035258887 & 126547414675 & 126765947892 \end{bmatrix}$$

ثم يحسب المصفوفة M من العلاقة:

$$M = E_2 - XE_1X = \begin{bmatrix} 4 & 16 & 11 & 8 & 5 & 19 & 12 & 13 \\ 5 & 7 & 13 & 21 & 25 & 24 & 18 & 17 \\ 16 & 13 & 12 & 15 & 7 & 23 & 14 & 16 \\ 17 & 18 & 16 & 17 & 15 & 19 & 23 & 24 \\ 19 & 17 & 11 & 13 & 12 & 21 & 23 & 14 \\ 15 & 18 & 13 & 12 & 13 & 17 & 17 & 21 \\ 8 & 9 & 14 & 9 & 12 & 15 & 9 & 13 \\ 23 & 13 & 14 & 7 & 8 & 5 & 3 & 2 \end{bmatrix}$$

وهي مصفوفة النص الصريح.

5- المبحث الثالث- النتائج والتوصيات

5-1 النتائج والمناقشة:

قدمنا في هذا البحث طريقة للحصول على مصفوفات تبديليّة بالاعتماد على خواص المصفوفات الدائريّة، حيث يمكن تجزئة هذه المصفوفة إلى أربع مصفوفات دائريّة، وبواسطة الاستقراء استطعنا الحصول على مصفوفات من مراتب أعلى وتحقّق الخاصة التبديليّة للضرب.

استفدنا من هذه النتائج في التشفير حيث تمّ استخدام هذه المصفوفات في تبادل المفاتيح السرّية، وفي التشفير سواء كان تشفير المفتاح السري أو تشفير المفتاح المعلن.

وهذه النتائج تشكّل إضافة مهمة للأبحاث الأخيرة في هذا المجال والّتي تركز معظمها على استخدام المصفوفات الدائريّة، حيث نعتقد إن المصفوفات المقدمة هنا يمكن أن تلعب نفس الدور الّذي كانت تلعبه المصفوفات الدائريّة، ولكن مع زيادة أمن التشفير.

2-5 الخلاصة

في الحقيقة إن المصفوفات التي قدمها الباحثون هنا تلعب نفس الدور الذي تلعبه المصفوفات الدائرية، ولكن بدرجة أمان أعلى، حيث أثبتوا أنه من خلال ثلاثة مصفوفات دائرية يمكن تشكيل مجموعة من المصفوفات التي تحقق الخاصة التبديلية للضرب، وخاصة إن عملية الضرب عملية داخلية على هذه المجموعة، والأكثر من ذلك بين الباحثون إمكانية الحصول على مجموعة من المصفوفات تحقق هذه الخواص ولكن من مراتب عليا، وأنه بالاعتماد على هذه المجموعة من المصفوفات يمكن تبادل مفتاح سري لاستخدامه في تشفير الرسائل بين طرفين. وأثبتوا أيضاً إمكانية استخدام هذه المصفوفات في التشفير وقدموا طريقتين: الأولى ذات مفتاح سري، والثانية ذات مفتاح معلن، أي أنه باختصار قدم الباحثون في هذا البحث:

1- طريقة لبناء مصفوفات تحقق الخاصة التبديلية للضرب
2- تطبيقات هذه المصفوفات في تبادل المفاتيح وفي التشفير ذو المفتاح السري، وفي تشفير المفتاح المعلن.

3-5 التوصيات

بناءً على النتائج الّتي تمّ التوصّل إليها توصي الدراسة بالتالي:

- نوصي بالعمل على دراسة تطبيقات المصفوفات الّتي قدمناها في هذا البحث في تطوير بعض طرائق التشفير الأخرى.
- نوصي بكتابة البرامج الحاسوبية اللّازمة لبناء هذه المصفوفات.
- دراسة إمكانيّة الاستفادة من النتائج المقدّمة في المجالات التطبيقية..
- دراسة بنية المصفوفات المقدّمة هنا بشكل أوسع.

قائمة المراجع

[1] Hartawan, I. G. N. Y., Jana, P., & Prayanti, B. D. A. (2020, July). Modified Public Key Cryptosystem Based On Circulant Matrix. In Journal of Physics: Conference Series (Vol. 1503, No. 1, p. 012007). IOP Publishing.

[2] Liu, J., Zhang, H., & Jia, J. (2017). Cryptanalysis of schemes based on polynomial symmetrical decomposition. Chinese Journal of Electronics, 26(6), 1139-1146.

[3] Liu, J., Zhang, H., Jia, J., Wang, H., Mao, S., & Wu, W. (2016). Cryptanalysis of an asymmetric cipher protocol using a matrix decomposition problem. Science China Information Sciences, 59(5), 1-11.

[4] Singh, M. K. (2004, June). Public key cryptography with matrices. In Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004. (pp. 146-152). IEEE.

[5] Valluri, M. R. (2014). Zero-knowledge authentication schemes using quasi-polynomials over non-commutative groups. Open Journal of Information Security And Applications, 1(1), 43-50.