استخدام قانون التحويل التنسوري في التشفير

الباحث الدكتور: باسل حمدو العرنوس

مدرّس في قسم الرياضيات – كليّة العلوم – جامعة البعث

الملخص

قمنا في هذا البحث باستخدام التّحليل التّنسوري في التشفير، وذكرنا التعاريف الأساسيّة اللازمة لذلك، وعرّفنا ترتيب مركّبات تنسور، وتطابق التّنسورات بالمقاس n.

أثبتنا أنّ تشفير كل نص واضح P (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n,p,q\right)$ يتم بشكلٍ وحيد. و أنّ فك التتشفير عن كل نص مشفّر C (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n,p,q\right)$ يتم بشكلٍ وحيد.

الكلمات المفتاحيّة:

تنسور – قانون التحويل التنسوري – مصفوفة هل – مفتاح التشفير – تشفير – النّص الواضح – النّص المشفّر.

Using The Law of Transformation Tensor in Cryptography

.Dr. Basel Hamdo Al-Arnous

Department Of Mathematics - Faculty of Sciences - Al- Baath University

Abstract

We used in this paper Tensor analysis in cryptography and mentioned some fundamental definitions as the order of tensor components and congruence of tensors mod n.

we proved that the cryptography of any clear text P from ASCII characters , using the law of tensor transformation by a key $C\left(C_n, p, q\right)$, is unique. we can decrypt any encrypted text C from ASCII characters using the law of tensor transformation by a key $C\left(C_n, p, q\right)$ in a unique manner.

Key Words:

Tensor - Law of Transformation Tensor – Hill matrix - The Cryptography key – Cryptography - Plaintext ,Ciphertext .

1.مقدّمة

يُقصد بالتّشفير هو ذلك العلم الذي يدرس تحويل الرّسائل والمعلومات إلى شكل، غير قابل للفهم من قبل جميع الأشخاص غير المصرّح لهم. وبالتّالي فهو عمليّة إخفاء المعلومات باستخدام الخوارزميّات ومفاتيح سريّة [3−1].

يتطوّر علم التّشفير باستمرار من حيث الآليّة المستخدمة في التّشفير، ودرجة التّعقيد التي تجعل الشّيفرة أكثر أماناً.

نقوم في هذا البحث على تطوير طريقة هيل [9],[1] في التّشفير بالاعتماد على جدول الـ$ASCII$، حيث تعتمد طريقة هيل على مفتاح وهو عبارة عن مصفوفة A من المرتبة $n \times n$ محدّدها أوّليّ نسبيّاً مع 256 (عدد عناصر جدول الـ$ASCII$). وتتلخّص الطّريقة بالخطوات الآتية.

- تُرتّب حروف ورموز النّص الأصلي في مصفوفة X من المرتبة $n \times k$.
- تُقابل الحروف والرّموز بما يقابلها من جدول $ASCII$.
- تُضرب المصفوفة النّاتجة بالمصفوفة A بالمقاس 256.
- تُرجع الأرقام إلى ما يُقابلها من حروف أو رموز في جدول $ASCII$ للحصول على النّص المشفّر.

قمنا باستبدال المصفوفة X بتنسور، وبدلاً من الضّرب بالمفتاح قمنا باستخدام قانون التّحويل التّنسوري من قاعدة إلى أخرى، وذلك من خلال مصفوفة الانتقال، ومن ثمّ الحصول على النّص المشفّر.

2. هدف البحث

يهدف البحث إلى استخدام قانون التّحويل التّنسوري في الحصول على النّص المشفّر، ودراسة قابليّة العكس بحيث نحصل على النّص الأصل من نص مشفّر.

3. أهميّة البحث:

تهدف كل طرق التّشفير إلى زيادة أمان الشّيفرة، وتغيير آليّة التّشفير، وتعمل على ذلك باستمرار. لذا فإنّ استخدام مركّبات تنسور ما في التّشفير يحقّق أماناً أعلى ممّا تحقّقه طريقة هيل، نظراً لصعوبة العمليّات الحسابيّة وتعدّد المفاتيح وكثرة الخيارات في اعتماد نوع التّنسور المستخدم.

4. المناقشة و النّتائج

4 – 1: تعاريف أساسيّة: [4,7]

تعريف1:

ليكن n عدداً طبيعيّاً وأكبر تماماً من 1، وليكن $1 \le a < n$ ، نقول عن العدد a إنه أولي نسبياً مع العدد n إذا كان: $\gcd(a,n) = 1$.

تعريف2:

ليكن n عدداً طبيعيّاً وأكبر تماماً من 1، نرمز بالرّمز M_n إلى مجموعة جميع الأعداد الأوّليّة نسبيّاً مع العدد n، أي أنّ:

$$M_n = \{a \in \mathbb{Z} ; 1 \le a < n \ , \ \gcd(a,n) = 1\}$$

تعريف3:

مصفوفة هيل: هي مصفوفة عدديّة مربّعة من المرتبة k $\left(k \in \mathbb{N}^{*}\right)$ نرمز لها بالرّمز C_k، وتحقّق:

$$\det\left(C_k\right) \in M_{256} \qquad (1)$$

مثال1:

إنّ المصفوفة $\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}$ هي مصفوفة هيل، بينما $\begin{pmatrix} 4 & 2 \\ 0 & 4 \end{pmatrix}$ ليست كذلك.

تعريف 4:[10]

لتكن $W, V_1, \ldots, V_s$ فضاءات متّجهيّة حقيقيّة ، نسمّي التطبيق :

$$F : V_1 \times \ldots \times V_s \to W$$

متعدّد الخطيّة إذا كان F خطيّاً بالنسبة لكل مركّبة.

ملاحظة 1:

سنتعامل مع ترميز آينشتاين للتّنسورات، وهو ترميز يهدف إلى تبسيط التّعبير عن مجموع، حيث نقوم بالاستغناء عن الرّمز Σ . وعلى سبيل المثال:

$$x^i e_i = \sum_{i=1}^{n} x^i e_i$$

تعريف 5: [10]

ليكن V_n فضاءً متّجهيّاً حقيقيّاً ، و V_n^{*} فضاءه الثنوي، و ليكن p,q عددين صحيحين موجبين، بحيث $(p,q) \neq (0,0)$ ، نسمّي تنسوراً من النوع $\begin{pmatrix} p \\ q \end{pmatrix}$ فوق

الفضاء V_n ، أيّة متعدّد الخطيّة:

$$T : (V_n)^p \times (V_n{}^*)^q = V_n \times ... \times V_n \times V_n{}^* \times ... \times V_n{}^* \to \square$$

معرّفة بالشكل:

$$\begin{aligned} T(x_1,...,x_p,\xi^1,...,\xi^q) &= T(x_1{}^{j_1}e_{j_1},...,x_p{}^{j_p}e_{j_p},\xi^1_{i_1}e^{i_1},...,\xi^q_{i_q}e^{i_q}) \\ &= T(e_{j_1},...,e_{j_p},e^{i_1},...,e^{i_q})x_1{}^{j_1}...x_p{}^{j_p}.\xi^1_{i_1}..\xi^q_{i_q} \\ &= T^{i_1...i_p}_{j_1...j_q}x^{j_1}...x^{j_p}\xi_{i_1}...\xi_{i_q} \end{aligned} \qquad (2)$$

حيث $\left(i = \overline{1,p}\right) x_i = x_i{}^{j_1}e_{j_1}$ متجهات من V_n و $\left(j = \overline{1,q}\right)$ $\xi^j = \xi^j_{j_1}e^{j_1}$ أشكال خطية من $V_n{}^*$ شريطة أن تكون الدالة T خطيّة في كل متغير.

نسمي الأعداد $T^{i_1...i_p}_{j_1...j_q}$ مركبات التنسور T بالنسبة للقاعدة (e_i) ، وكما هو واضح أنَّ عددها n^{p+q}.

نسمي العدد p مرتبة مخالف التغير ، والعدد q مرتبة موافق التغير.

4 – 2: قانون التّحويل التّنسوري: [10]

ليكن T تنسوراً من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n، مرّكّباته من الشّكل: $T^{i_1...i_p}_{j_1...j_q}$ في القاعدة (e_i)، ولتكن $(e_{i'})$ قاعدة جديدة للفضاء المذكور، بحيث تكون المصفوفة C^i_j : مصفوفة الانتقال من القاعدة (e_i) إلى القاعدة $(e_{i'})$. عندئذٍ تكون مركّبات التّنسور T بالنّسبة للقاعدة الجديدة، هي من الشّكل:

$$T'^{\,k_1...k_p}_{\,l_1...l_q} = T^{i_1...i_p}_{j_1...j_q}C^{j_1}_{l_1}...C^{j_q}_{l_q}.B^{k_1}_{i_1}...B^{k_p}_{i_p} \qquad (3)$$

حيث B^i_j هي مصفوفة الانتقال من القاعدة $(e_{i'})$ إلى القاعدة (e_i)، إنّ:

$$B_j^i = \left(C_j^i\right)^{-1}$$

نسمي العلاقة **(3)** ، قانون التحويل التنسوريّ وهي تحدّد العلاقة بين مركّبات تنسور بالنسبة لقاعدتين مختلفتين.

إنّ مركبات التنسور $T\begin{pmatrix} p \\ q \end{pmatrix}$ بالنسبة للقاعدة (e_i) هي:

$$T'^{\,i_1\ldots i_p}_{\;j_1\ldots j_q} = T^{\,k_1\ldots k_p}_{\;l_1\ldots l_q}\, B^{\,l_1}_{\;j_1}\ldots B^{\,l_q}_{\;j_q}\, C^{\,i_1}_{\;k_1}\ldots C^{\,i_p}_{\;k_p} \qquad (4)$$

ملاحظة 2:

يتّضح من العلاقة **(3)** أنّه إذا كانت مركبات تنسور معدومة بالنسبة لقاعدة ما ، فإنّها تكون كذلك بالنسبة لأيّة قاعدة أخرى في الفضاء V_n نفسه.

مبرهنة 1: [8]

من أجل أي عددين صحيحين موجبين p,q يوجد في الفضاء V_n ذي القاعدة (e_i) تنسوراً من النوع $\begin{pmatrix} p \\ q \end{pmatrix}$ بالنسبة لهذه القاعدة.

4 – 3: التّطابق

تعريف 6: $[10]$

نقول عن تنسورين T,S إنّهما متساويان، ونكتب اختصاراً $T = S$ ، إذا كانا من النّوع ذاته $\begin{pmatrix} p \\ q \end{pmatrix}$ ومركّباتهما متطابقة بالنّسبة لأي قاعدة مفروضة، فإذا كانت مركّباتهما بالنسبة للقاعدة (e_i) هي على الترتيب: $T^{\,i_1\ldots i_p}_{\;j_1\ldots j_q}$ ، $S^{\,i_1\ldots i_p}_{\;j_1\ldots j_q}$ فنقول إنّهما متطابقان إذا كانت:

$$S_{j_1\dots j_q}^{i_1\dots i_p} = T_{j_1\dots j_q}^{i_1\dots i_p} \qquad (5)$$

لكل $i_1,\dots,i_p, j_1,\dots,j_q$ حيث:

$$1 \le i_k \le n,\ k = 1,\dots,p \quad , \quad 1 \le j_l \le n \quad , \ l = 1,\dots,q$$

نتيجة 1:

نستنتج من العلاقة **(3)** أنَّ خواص تطابق التنسورين المشار إليهما بالتعريف السابق لا تتغير بالانتقال من قاعدة ما إلى أي قاعدة أخرى.

تعريف 7:

ليكن m عدداً طبيعيّاً يحقّق: $m > 1$، وليكن T, S تنسورين من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n ، ولنفرض أنّ:

$$S_{j_1\dots j_q}^{i_1\dots i_p}, T_{j_1\dots j_q}^{i_1\dots i_p} \in \square \ ; \ i_1,\dots,i_p, j_1,\dots,j_q \in \{1,\dots,n\}$$

نقول عن التّنسورين T, S إنّهما متطابقان بالمقاس m، ونكتب اختصاراً $T \equiv S \pmod m$ ، إذا كانت مركّباتهما متطابقة بالمقاس m بالنّسبة لأي قاعدة مفروضة، فإذا كانت مركّباتهما بالنسبة للقاعدة (e_i) هي على الترتيب: $T_{j_1\dots j_q}^{i_1\dots i_p}$ ، $S_{j_1\dots j_q}^{i_1\dots i_p}$ فنقول إنّهما متطابقان بالمقاس m، إذا كانت:

$$S_{j_1\dots j_q}^{i_1\dots i_p} \equiv T_{j_1\dots j_q}^{i_1\dots i_p} \pmod m \ ; \quad ; \ i_1,\dots,i_p, j_1,\dots,j_q \in \{1,\dots,n\} \qquad (6)$$

تعريف 8:

ليكن m عدداً طبيعيّاً يحقّق: $m > 1$، وليكن T تنسوراً من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n ، ولنفرض أنّ:

$$T_{j_1\dots j_q}^{i_1\dots i_p} \in \square \;\; ; \; i_1,\dots,i_p, j_1,\dots, j_q \in \{1,\dots,n\}$$

نعرّف **تنسور الممثّلات الرّئيسيّة للتّنسور** T **بالمقاس** m **ونرمز له بالرّمز** $^{(m)}T$ بأنّه تنسور من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ ويحقّق:

$$\begin{aligned} &1) \quad {}^{(m)}T_{j_1\dots j_q}^{i_1\dots i_p} \in \square_m \;\; ; \; i_1,\dots,i_p, j_1,\dots, j_q \in \{1,\dots,n\} \\ &2) \quad {}^{(m)}T \equiv T \pmod m \end{aligned} \qquad (7)$$

مثال2:

ليكن T تنسوراً من النّوع $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ في الفضاء $\square^2$، حيث:

$$T_1^{\,1} = -312 \;,\; T_1^{\,2} = 425 \;,\; T_2^{\,1} = 211 \;,\; T_2^{\,2} = 1012$$

إنّ تنسور الممثّلات الرّئيسيّة لهذا التّنسور بالمقاس 256 هو التّنسور $^{(256)}T$ من النّوع $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$، ومركّباته:

$$^{(256)}T_1^{\,1} = 200 \;,\; {}^{(256)}T_1^{\,2} = 169 \;,\; {}^{(256)}T_2^{\,1} = 211 \;,\; {}^{(256)}T_2^{\,2} = 244$$

4 – 4: الترتيب

لسهولة العمل بإجراء تقابل بين المحارف ومركّبات تنسور ما، نعتمد طريقة لترتيب مركّبات التّنسور.

تعريف 9:

لتكن $a_1,\dots,a_n,b_1,\dots,b_n$ أعداداً حقيقيّة، نقول إنّ الترتيبة $(a_1,\dots,a_n)$ تأتي بعد الترتيبة $(b_1,\dots,b_n)$، إذا تحقّق أحد الشّرطين الآتيين:

- إذا كان $a_1 > b_1$.
- إذا كان $a_i > b_i$ و $a_j = b_j$ لكل $j < i$ حيث $1 < i \le n$.

مثال3 :

الترتيبة $(2,1,3,4)$ تأتي بعد الترتيبة $(1,5,2,4)$، والترتيبة $(2,1,3,4)$ تأتي بعد الترتيبة $(2,1,2,4)$.

تعريف 10:

ليكن T تنسوراً من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n، نقول إنّ المركّبة $T^{i_1 \dots i_p}_{j_1 \dots j_q}$ تأتي بعد المركّبة $T^{r_1 \dots r_p}_{s_1 \dots s_q}$، إذا كانت الترتيبة $(i_1,\dots,i_p,j_1,\dots,j_q)$تأتي بعد التّرتيبة: $(r_1,\dots,r_p,s_1,\dots,s_q)$

مثال 4:

ليكن T تنسوراً من النّوع $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ في الفضاء $\mathbb{R}^3$، إنّ ترتيب مركّباته هو كالآتي:

$$T^1_{11},T^1_{12},T^1_{13},T^1_{21},T^1_{22},T^1_{23},T^1_{31},T^1_{32},T^1_{33},T^2_{11},T^2_{12},T^2_{13},T^2_{21},T^2_{22},T^2_{23},T^2_{31},T^2_{32},T^2_{33}$$

$$T^3_{11},T^3_{12},T^3_{13},T^3_{21},T^3_{22},T^3_{23},T^3_{31},T^3_{32},T^3_{33}$$

4 – 5: التّنسور المقابل للنّص

4 – 5 – 1 تنسور النّص الواضح:

ليكن لدينا P النص الواضح (Plaintext) المكوّن من α محرفاً، نختار نوع التّنسور T وفقاً لعدد المحارف ولنوع مصفوفة هيل. ثمّ نأخذ المقابل العددي لكل محرف في

النّص من جدول $ASCII$، ونسند هذه الأعداد إلى مركّبات التّنسور المختار بنفس ترتيب المحارف، فنحصل على تنسور النّص الواضح.

4 – 5 – 2 تنسور النّص المشفّر:

ليكن لدينا C النص المشفّر(Ciphertext) المكوّن من α محرفاً، نتّبع نفس الطريقة السّابقة لنحصل على تنسور النّص المشفّر R.

4 – 5 – 3 اختيار نوع التّنسور:

إنّ عدد مركّبات تنسور T من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ في الفضاء V_n، هو: n^{p+q}. ليكن P النّص الواضح وعدد محارفه α، ولتكن m هي مرتبة مصفوفة هيل. نختار من بين قوى العدد m أوّل قوّة أكبر أو تساوي α ولتكن m^{β}. عندئذٍ نختار تنسور في الفضاء الذي بُعده m ومن النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$ حيث $p+q=\beta$.

مثال 5:

ليكن لدينا النّص الواضح P هو: $Law-of-Transformation$ ولتكن مصفوفة هيل من المرتبة الثّالثة. واضح أنّ عدد المحارف هو 21 وأوّل قوّة لـ3 أكبر أو تساوي 21 هو القوّة 3^3.

وبالتّالي نأخذ تنسوراً في الفضاء $\square^3$ من أحد الأنواع الآتية:

$$\begin{pmatrix} 0 \\ 3 \end{pmatrix},\begin{pmatrix} 1 \\ 2 \end{pmatrix},\begin{pmatrix} 2 \\ 1 \end{pmatrix},\begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

4 – 6: التشفير باستخدام قانون التّحويل التنسوري

استخدام قانون التّحويل التنسوري

هي إبدال كل حرف ASCII في الرسالة المبثوثة بحرف آخر من ASCII من خلال استخدام قانون التّحويل التّنسوري على تنسور النّص الواضح.

نعتمد في هذه الطّريقة على مصفوفة هيل واعتمادها كمصفوفة انتقال من قاعدة إلى أخرى على تنسور النّص الواضح. لذا يلزمنا من أجل استخدام هذه الطّريقة:

- مصفوفة هيل من المرتبة n .
- نوع التّنسور المستخدم وليكن $\begin{pmatrix} p \\ q \end{pmatrix}$.

فإذا كان عدد حروف النص الأصلي أقل من n^{p+q} نملئ أماكن الحروف الناقصة بالمحرف $(-)$.

تعريف 11:

مفتاح التشفير: نرمز بالرّمز $C(C_n, p, q)$ إلى التشفير باستخدام المصفوفة C_n كمصفوفة انتقال على تنسور النّص الواضح T والذي هو من النّوع $\begin{pmatrix} p \\ q \end{pmatrix}$. ويبقى المفتاح ذاته في العمليّة المعاكسة.

إذا كان T هو تنسور النّص الواضح فإنّ الرّمز $F(T)$ يدل على استخدام قانون التّحويل التّنسوري على التّنسور T للحصول على التّنسور R تنسور النّص المشفّر.

خوارزمية التشفير باستخدام التّحليل التّنسوري:

إذا كان لدينا نص واضح P والمراد تشفيره باستخدام المفتاح $C(C_n, p, q)$:

- نكتب مركّبات تنسور النّص الواضح T مرتّبةً كما بيّنا في التعريف 10، ونسند إليها الأعداد المقابلة لمحارف النّص الواضح في جدول ASCII.
- نستخدم قانون التّحويل التّنسوري على التّنسور T فنحصل على:

$$R = F(T)$$

- نوجد تنسور الممثّلات الرّئيسيّة للتّنسور R بالمقاس 256، أي: نوجد التّنسور $^{(256)}R$.
- نكتب مركّبات التّنسور $^{(256)}R$ بشكل مرتّب.
- نستبدل مركّبات التّنسور $^{(256)}R$ بالحروف المقابلة لها في جدول ال $ASCII$ فنحصل على النص المشفر **C** المطلوب .

مبرهنة 2 :

إن تشفير كل نص واضح P (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C(C_n, p, q)$ يتم بشكلٍ وحيد.

الإثبات :

لتكن P, P' رسالتين مختلفتين من الحروف ASCII وليكن T, T' هما تنسوري النّصّين P, P' على التّرتيب، $R = F(T), R' = F(T')$ ولنثبت أن :

$$^{(256)}R' \neq ^{(256)}R .$$

بما أنّ $P_1 \neq P_2$ فإنّه حسب جدول الحروف ومقابلاتها العددية:

$$T' \neq T$$

وباستخدام قانون التّحويل التّنسوري على التّنسورين T', T وحيث إنّ تطبيق التّحويل التّنسوري على تنسور يُعطي تنسوراً وحيداً، فإنّ:

$$F(T') \neq F(T)$$

وبالتّالي:

$$R' \neq R$$

نفرض جدلاً أنّ : $R \overset{(256)}{=} R'$، أي أنّ:

$$R' \pmod{256} \equiv R \pmod{256}$$

وبالتّالي يكون:

$$R'^{k_1 \ldots k_p}_{l_1 \ldots l_q} \equiv R^{k_1 \ldots k_p}_{l_1 \ldots l_q} \bmod(256) \; ; \; k_1, \ldots, k_p, l_1, \ldots, l_q \in \{1, \ldots, n\}$$

وبالتالي :

$$T'^{i_1 \ldots i_p}_{j_1 \ldots j_q} C^{j_1}_{l_1} \ldots C^{j_q}_{l_q} . B^{k_1}_{i_1} \ldots B^{k_p}_{i_p} \equiv T^{i_1 \ldots i_p}_{j_1 \ldots j_q} C^{j_1}_{l_1} \ldots C^{j_q}_{l_q} . B^{k_1}_{i_1} \ldots B^{k_p}_{i_p} \pmod{256}$$

لننظر إلى خواص التّطابقات، ولا سيّما إلى الخاصّتين الآتيتين:

- إذا كان $a \equiv b \pmod{m}$ و $k \in \mathbb{Z}$ فإنّ: $k.a \equiv k.b \pmod{m}$.
- إذا كان $a \equiv b \pmod{m}$ و $k \in \mathbb{Z}$ فإنّ: $k + a \equiv k + b \pmod{m}$.

وبالنّظر إلى بنية قانون التّحليل التّنسوري، فإنّه بتطبيق قانون التّحويل العكسيّ نجد:

$$T'^{i_1 \ldots i_p}_{j_1 \ldots j_q} \equiv T^{i_1 \ldots i_p}_{j_1 \ldots j_q} \pmod{256} \; ; \; i_1, \ldots, i_p, j_1, \ldots, j_q \in \{1, \ldots, n\}$$

وبالتّالي:

$$T' \equiv T \pmod{256}$$

وبالتّالي يكون:

$$T' = T$$

وهذا مخالف للفرض ، إذاً $R \overset{(256)}{\neq} R'$ وبالتالي ، تشفير كل رسالة باستخدام قانون التّحويل التّنسوري يتم بشكلٍ وحيد .

مبرهنة3:

إن فك التتشفير عن كل نص مشفّر C (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n, p, q\right)$ يتم بشكلٍ وحيد.

الإثبات :

يتمّ الإثبات بطريقة مماثلة للإثبات السّابق.

مثال 6:

لنحوّل الجملة الآتية: " $Basel\ Alarnous$ " إلى شيفرة باستخدام التّحليل التّنسوري مستخدمين المفتاح $C\left(C_4, 1, 1\right)$، حيث:

$$C = \begin{pmatrix} 6 & 0 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -2 & 3 & 2 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

بما أنّ المصفوفة C من المرتبة الرّابعة فسنستخدم تنسور من النّوع $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ في الفضاء الرّباعي. سننظّم الجدول الآتي:

الحرف	B	a	s	e	l	_	A	l

ASCII	66	97	115	101	108	95	65	108
مركّبة التّنسور	$T_1^{\,1}$	$T_2^{\,1}$	$T_3^{\,1}$	$T_4^{\,1}$	$T_1^{\,2}$	$T_2^{\,2}$	$T_3^{\,2}$	$T_4^{\,2}$
الحرف	*a*	*r*	*n*	*o*	*u*	*s*	–	–
ASCII	97	114	110	111	117	115	95	95
مركّبة التّنسور	$T_1^{\,3}$	$T_2^{\,3}$	$T_3^{\,3}$	$T_4^{\,3}$	$T_1^{\,4}$	$T_2^{\,4}$	$T_3^{\,3}$	$T_4^{\,4}$

سنستخدم مصفوفة الانتقال للحصول على الشيفرة.

تعطى قاعدة التحويل التّنسوري لتنسور من النّوع $\begin{pmatrix}1\\1\end{pmatrix}$ في الفضاء الرّباعي من خلال العلاقة:

$$R_{\beta}^{\alpha}=T_{j}^{i}C_{\beta}^{j}B_{i}^{\alpha}\quad;\ \alpha,\beta,i,j=\overline{1,4}$$

حيث:

$$C=\begin{pmatrix}1&-4&-2&1\\-2&9&4&-1\\-3&14&7&-3\\2&-10&-5&3\end{pmatrix}=\begin{pmatrix}C_1^1&C_2^1&C_3^1&C_4^1\\C_1^2&C_1^2&C_1^2&C_1^2\\C_1^3&C_2^3&C_3^3&C_4^3\\C_1^4&C_2^4&C_3^4&C_4^4\end{pmatrix}$$

$$B=C^{-1}=\begin{pmatrix}6&0&1&-1\\1&1&-1&-1\\1&-2&3&2\\1&0&1&1\end{pmatrix}=\begin{pmatrix}B_1^1&B_2^1&B_3^1&B_4^1\\B_1^2&B_1^2&B_1^2&B_1^2\\B_1^3&B_2^3&B_3^3&B_4^3\\B_1^4&B_2^4&B_3^4&B_4^4\end{pmatrix}$$

نقوم بحساب مركّبات التّنسور $R\begin{pmatrix}1\\1\end{pmatrix}$.

$$R_1^1 = T_j^{\,i} C_1^{\,j} B_i^1 = T_j^{\,1} C_1^{\,j} B_1^1 + T_j^{\,2} C_1^{\,j} B_2^1 + T_j^{\,3} C_1^{\,j} B_3^1 + T_j^{\,4} C_1^{\,j} B_4^1$$
$$= \left(T_1^{\,1} C_1^{\,1} + T_2^{\,1} C_1^{\,2} + T_3^{\,1} C_1^{\,3} + T_4^{\,1} C_1^{\,4}\right) B_1^1 +$$
$$+ \left(T_1^{\,2} C_1^{\,1} + T_2^{\,2} C_1^{\,2} + T_3^{\,2} C_1^{\,3} + T_4^{\,2} C_1^{\,4}\right) B_2^1 +$$
$$+ \left(T_1^{\,3} C_1^{\,1} + T_2^{\,3} C_1^{\,2} + T_3^{\,3} C_1^{\,3} + T_4^{\,3} C_1^{\,4}\right) B_3^1 +$$
$$+ \left(T_1^{\,4} C_1^{\,1} + T_2^{\,4} C_1^{\,2} + T_3^{\,4} C_1^{\,3} + T_4^{\,4} C_1^{\,4}\right) B_4^1$$
$$= -1657$$

$$R_2^1 = T_j^{\,i} C_2^{\,j} B_i^1 = T_j^{\,1} C_2^{\,j} B_1^1 + T_j^{\,2} C_2^{\,j} B_2^1 + T_j^{\,3} C_{12}^{\,j} B_3^1 + T_j^{\,4} C_2^{\,j} B_4^1$$
$$= \left(T_1^{\,1} C_2^{\,1} + T_2^{\,1} C_2^{\,2} + T_3^{\,1} C_2^{\,3} + T_4^{\,1} C_2^{\,4}\right) B_1^1 +$$
$$+ \left(T_1^{\,2} C_2^{\,1} + T_2^{\,2} C_2^{\,2} + T_3^{\,2} C_2^{\,3} + T_4^{\,2} C_2^{\,4}\right) B_2^1 +$$
$$+ \left(T_1^{\,3} C_2^{\,1} + T_2^{\,3} C_2^{\,2} + T_3^{\,3} C_2^{\,3} + T_4^{\,3} C_2^{\,4}\right) B_3^1 +$$
$$+ \left(T_1^{\,4} C_2^{\,1} + T_2^{\,4} C_2^{\,2} + T_3^{\,4} C_2^{\,3} + T_4^{\,4} C_2^{\,4}\right) B_4^1$$
$$= 7375$$

قمنا بصياغة برنامج بلغة التربو باسكال لحساب باقي القيم (البرنامج 1) فوجدنا :

$$R_1^1 = -1657 \quad R_2^1 = 7375 \quad R_3^1 = 3397 \quad R_4^1 = -454$$
$$R_1^2 = 115 \quad R_2^2 = -553 \quad R_3^2 = -258 \quad R_4^2 = 81$$
$$R_1^3 = -1282 \quad R_2^3 = 5801 \quad R_3^3 = 2661 \quad R_4^3 = -395$$
$$R_1^4 = -718 \quad R_2^4 = 3224 \quad R_3^4 = 1449 \quad R_4^4 = -85$$

نوجد تنسور الممثّلات الرّئيسيّة للتنسور R بالمقاس 256.

$$^{(256)}R_1^1 = 135 \quad ^{(256)}R_2^1 = 207 \quad ^{(256)}R_3^1 = 69 \quad ^{(256)}R_4^1 = 58$$
$$^{(256)}R_1^2 = 115 \quad ^{(256)}R_2^2 = 215 \quad ^{(256)}R_3^2 = 254 \quad ^{(256)}R_4^2 = 81$$
$$^{(256)}R_1^3 = 254 \quad ^{(256)}R_2^3 = 169 \quad ^{(256)}R_3^3 = 101 \quad ^{(256)}R_4^3 = 117$$
$$^{(256)}R_1^4 = 50 \quad ^{(256)}R_2^4 = 152 \quad ^{(256)}R_3^4 = 169 \quad ^{(256)}R_4^4 = 171$$

وبالتالي نستطيع تنظيم الجدول الآتي:

مركبة التنسور	$^{(256)}R_1^1$	$^{(256)}R_2^1$	$^{(256)}R_3^1$	$^{(256)}R_4^1$	$^{(256)}R_1^2$	$^{(256)}R_2^2$	$^{(256)}R_3^2$	$^{(256)}R_4^2$
ASCII	135	207	69	58	115	215	254	81
الحرف	‡	د	*E*	:	*s*	×		*Q*
مركبة التنسور	$^{(256)}R_1^3$	$^{(256)}R_2^3$	$^{(256)}R_3^3$	$^{(256)}R_4^3$	$^{(256)}R_1^4$	$^{(256)}R_2^4$	$^{(256)}R_3^4$	$^{(256)}R_4^4$
ASCII	254	169	101	117	50	152	169	171
الحرف		©	e	u	2	ک	©	«

فيكون النّص بعد التشفير هو:

‡دE:s× Q ©eu2ک©«

وبالعكس لنقوم بفك تشفير النّص المشفّر الذي حصلنا عليه:

ننتقل من التّنسور $R\begin{pmatrix}1\\1\end{pmatrix}$ إلى التّنسور $T\begin{pmatrix}1\\1\end{pmatrix}$

تعطى قاعدة التحويل التّنسوري لتنسور من النّوع $\begin{pmatrix}1\\1\end{pmatrix}$ في الفضاء الرّباعي من خلال العلاقة:

$$T_{\beta}^{\alpha} = R_j^i B_{\beta}^j C_i^{\alpha} \quad ; \quad \alpha,\beta,i,j = \overline{1,4}$$

وبالحساب كما السابق، نحصل على:

$$T_1^{\,1}=-6846 \quad T_2^{\,1}=1121 \quad T_3^{\,1}=-3213 \quad T_4^{\,1}=-667$$
$$T_1^{\,2}=15724 \quad T_2^{\,2}=-2721 \quad T_3^{\,2}=7745 \quad T_4^{\,2}=1900$$
$$T_1^{\,3}=24929 \quad T_2^{\,3}=-3982 \quad T_3^{\,3}=11630 \quad T_4^{\,3}=2415$$
$$T_1^{\,4}=-17291 \quad T_2^{\,4}=2675 \quad T_3^{\,4}=-7841 \quad T_4^{\,4}=-1441$$

نوجد تنسور الممثّلات الرّئيسيّة للتنسور T بالمقاس 256.

$$^{(256)}T_1^{\,1}=66 \quad ^{(256)}T_2^{\,1}=97 \quad ^{(256)}T_3^{\,1}=115 \quad ^{(256)}T_4^{\,1}=101$$
$$^{(256)}T_1^{\,2}=108 \quad ^{(256)}T_2^{\,2}=95 \quad ^{(256)}T_3^{\,2}=65 \quad ^{(256)}T_4^{\,2}=108$$
$$^{(256)}T_1^{\,3}=97 \quad ^{(256)}T_2^{\,3}=114 \quad ^{(256)}T_3^{\,3}=110 \quad ^{(256)}T_4^{\,3}=111$$
$$^{(256)}T_1^{\,4}=117 \quad ^{(256)}T_2^{\,4}=115 \quad ^{(256)}T_3^{\,4}=95 \quad ^{(256)}T_4^{\,4}=95$$

وبالتالي نستطيع تنظيم الجدول الآتي:

مركبة التنسور	$^{(256)}T_1^{\,1}$	$^{(256)}T_2^{\,1}$	$^{(256)}T_3^{\,1}$	$^{(256)}T_4^{\,1}$	$^{(256)}T_1^{\,2}$	$^{(256)}T_2^{\,2}$	$^{(256)}T_3^{\,2}$	$^{(256)}T_4^{\,2}$
ASCII	66	97	115	101	108	95	65	108
الحرف	*B*	*a*	*s*	*e*	*l*	–	*A*	*l*
مركبة التنسور	$^{(256)}T_1^{\,3}$	$^{(256)}T_2^{\,3}$	$^{(256)}T_3^{\,3}$	$^{(256)}T_4^{\,3}$	$^{(256)}T_1^{\,4}$	$^{(256)}T_2^{\,4}$	$^{(256)}T_3^{\,4}$	$^{(256)}T_4^{\,4}$
ASCII	97	114	110	111	117	115	95	95
الحرف	*a*	*r*	*n*	*o*	*u*	*s*	–	–

فيكون النّص الأصلي هو:

$$Basel-Alarnous--$$

نستطيع استخدام طريقة أخرى وذلك وفقاً لقاعدة التّحويل التّنسوري المُعطاة. يتّضح ذلك من خلال المثال الآتي:

لنحوّل الجملة الآتية: " $Basel\ Alarnous$ " إلى شيفرة باستخدام التّحليل التّنسوري مستخدمين المفتاح $C\,(C_2,2,2)$، حيث:

$$C = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

سننظّم الجدول الآتي:

الحرف	B	a	s	e	l	–	A	l
$ASCII$	66	97	115	101	108	95	65	108
مركّبة التّنسور	T_{11}^{11}	T_{12}^{11}	T_{21}^{11}	T_{22}^{11}	T_{11}^{12}	T_{12}^{12}	T_{21}^{12}	T_{22}^{12}
الحرف	a	r	n	o	u	s	–	–
$ASCII$	97	114	110	111	117	115	95	95
مركّبة التّنسور	T_{11}^{21}	T_{12}^{21}	T_{21}^{21}	T_{22}^{21}	T_{11}^{22}	T_{12}^{22}	T_{21}^{22}	T_{22}^{22}

سنستخدم مصفوفة الانتقال للحصول على الشيفرة.

تعطى قاعدة التحويل التّنسوري لتنسور من النّوع $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$ في الفضاء الثّنائي من خلال

العلاقة:

$$R_{\gamma\delta}^{\alpha\beta} = T_{kl}^{ij} C_{\gamma}^{k} C_{\delta}^{l} B_{i}^{\alpha} B_{j}^{\beta} \quad ; \quad \alpha,\beta,\gamma,\delta,i,j,k,l = \overline{1,2}$$

حيث:

$$C = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} C_1^1 & C_2^1 \\ C_1^2 & C_2^2 \end{pmatrix}$$

$$B = C^{-1} = \begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} B_1^1 & B_2^1 \\ B_1^2 & B_2^2 \end{pmatrix}$$

نقوم بحساب مركّبات التّنسور $R\begin{pmatrix}2\\2\end{pmatrix}$.

$$
\begin{aligned}
R_{11}^{11} &= T_{kl}^{ij}C_1^kC_1^lB_i^1B_j^1 = T_{kl}^{i1}C_1^kC_1^lB_i^1B_1^1 + T_{kl}^{i2}C_1^kC_1^lB_i^1B_2^1 \\
&= T_{kl}^{11}C_1^kC_1^lB_1^1B_1^1 + T_{kl}^{21}C_1^kC_1^lB_2^1B_1^1 + T_{kl}^{12}C_1^kC_1^lB_1^1B_2^1 + \\
&\quad + T_{kl}^{22}C_1^kC_1^lB_2^1B_2^1 \\
&= T_{k1}^{11}C_1^kC_1^1B_1^1B_1^1 + T_{k2}^{11}C_1^kC_1^2B_1^1B_1^1 + T_{k1}^{21}C_1^kC_1^1B_2^1B_1^1 + \\
&\quad + T_{k2}^{21}C_1^kC_1^2B_2^1B_1^1 + T_{k1}^{12}C_1^kC_1^1B_1^1B_2^1 + T_{k2}^{12}C_1^kC_1^2B_1^1B_2^1 + \\
&\quad + T_{k1}^{22}C_1^kC_1^1B_2^1B_2^1 + T_{k2}^{22}C_1^kC_1^2B_2^1B_2^1 \\
&= T_{11}^{11}C_1^1C_1^1B_1^1B_1^1 + T_{21}^{11}C_1^2C_1^1B_1^1B_1^1 + T_{12}^{11}C_1^1C_1^2B_1^1B_1^1 + \\
&\quad + T_{22}^{11}C_1^2C_1^2B_1^1B_1^1 + T_{11}^{21}C_1^1C_1^1B_2^1B_1^1 + T_{21}^{21}C_1^2C_1^1B_2^1B_1^1 + \\
&\quad + T_{12}^{21}C_1^1C_1^2B_2^1B_1^1 + T_{22}^{21}C_1^2C_1^2B_2^1B_1^1 + T_{11}^{12}C_1^1C_1^1B_1^1B_2^1 + \\
&\quad + \left(+T_{21}^{12}C_1^2C_1^1B_1^1B_2^1\right) + T_{12}^{12}C_1^1C_1^2B_1^1B_2^1 + T_{22}^{12}C_1^2C_1^2B_1^1B_2^1 + \\
&\quad + T_{11}^{22}C_1^1C_1^1B_2^1B_2^1 + T_{21}^{22}C_1^2C_1^1B_2^1B_2^1 + T_{12}^{22}C_1^1C_1^2B_2^1B_2^1 + \\
&\quad + T_{22}^{22}C_1^2C_1^2B_2^1B_2^1 = 251
\end{aligned}
$$

(نلاحظ هنا تعقيد العمليّات الحسابيّة ، ممّا يُعطي أماناً أكثر لعمليّة التّشفير)

وباستخدام لغة التربو باسكال (البرنامج 2) نتمكن من حساب باقي المركّبات، فنجد أنّ:

$$
\begin{array}{cccc}
R_{11}^{11}=251 & R_{12}^{11}=556 & R_{21}^{11}=842 & R_{22}^{11}=1767 \\
R_{11}^{12}=11 & R_{12}^{12}=67 & R_{21}^{12}=-45 & R_{22}^{12}=53 \\
R_{11}^{21}=67 & R_{12}^{21}=201 & R_{21}^{21}=115 & R_{22}^{21}=420 \\
R_{11}^{22}=-7 & R_{12}^{22}=-34 & R_{21}^{22}=-2 & R_{22}^{22}=-67
\end{array}
$$

نوجد تنسور الممثّلات الرّئيسيّة للتنسور R بالمقاس 256.

$$^{(256)}R_{11}^{11}=251 \quad ^{(256)}R_{12}^{11}=44 \quad ^{(256)}R_{21}^{11}=74 \quad ^{(256)}R_{22}^{11}=231$$
$$^{(256)}R_{11}^{12}=11 \quad ^{(256)}R_{12}^{12}=67 \quad ^{(256)}R_{21}^{12}=211 \quad ^{(256)}R_{22}^{12}=53$$
$$^{(256)}R_{11}^{21}=67 \quad ^{(256)}R_{12}^{21}=201 \quad ^{(256)}R_{21}^{21}=115 \quad ^{(256)}R_{22}^{21}=164$$
$$^{(256)}R_{11}^{22}=249 \quad ^{(256)}R_{12}^{22}=222 \quad ^{(256)}R_{21}^{22}=254 \quad ^{(256)}R_{22}^{22}=189$$

وبالتالي نستطيع تنظيم الجدول الآتي:

مركبة التنسور	$^{(256)}R_{11}^{11}$	$^{(256)}R_{12}^{11}$	$^{(256)}R_{21}^{11}$	$^{(256)}R_{22}^{11}$	$^{(256)}R_{11}^{12}$	$^{(256)}R_{12}^{12}$	$^{(256)}R_{21}^{12}$	$^{(256)}R_{22}^{12}$
ASCII	251	44	74	231	11	67	211	53
الحرف	û	′	J	ç		C	س	5
مركبة التنسور	$^{(256)}R_{11}^{21}$	$^{(256)}R_{12}^{21}$	$^{(256)}R_{21}^{21}$	$^{(256)}R_{22}^{21}$	$^{(256)}R_{11}^{22}$	$^{(256)}R_{12}^{22}$	$^{(256)}R_{21}^{22}$	$^{(256)}R_{22}^{22}$
ASCII	67	201	115	164	249	222	254	189
الحرف	C	ة	s	¤	ù	ق		½

فيكون النّص بعد التشفير هو:

Û'Jç Cس5Cةs¤ùق ½

وبالعكس لنقوم بفك تشفير النّص المشفّر الذي حصلنا عليه:

ننتقل من التّنسور $R\begin{pmatrix}2\\2\end{pmatrix}$ إلى التّنسور $T\begin{pmatrix}2\\2\end{pmatrix}$

تعطى قاعدة التحويل التّنسوري لتنسور من النّوع $\begin{pmatrix}2\\2\end{pmatrix}$ في الفضاء الرّباعي من خلال العلاقة:

$$T_{\gamma\delta}^{\alpha\beta}=R_{kl}^{ij}B_{\gamma}^{k}B_{\delta}^{l}C_{i}^{\alpha}C_{j}^{\beta} \quad ; \quad \alpha,\beta,\gamma,\delta,i,j,k,l=\overline{1,2}$$

وبالحساب كما السابق، نحصل على:

$$T_{11}^{11}=4418 \quad T_{12}^{11}=-1951 \quad T_{21}^{11}=-1677 \quad T_{22}^{11}=613$$
$$T_{11}^{12}=5740 \quad T_{12}^{12}=-2465 \quad T_{21}^{12}=-1983 \quad T_{22}^{12}=620$$
$$T_{11}^{21}=6241 \quad T_{12}^{21}=-2702 \quad T_{21}^{21}=-2450 \quad T_{22}^{21}=879$$
$$T_{11}^{22}=8565 \quad T_{12}^{22}=-3725 \quad T_{21}^{22}=-3233 \quad T_{22}^{22}=119$$

نوجد تنسور الممثّلات الرّئيسيّة للتّنسور T بالمقاس 256.

$$^{(256)}T_{11}^{11}=66 \quad ^{(256)}T_{12}^{11}=97 \quad ^{(256)}T_{21}^{11}=115 \quad ^{(256)}T_{22}^{11}=101$$
$$^{(256)}T_{11}^{12}=108 \quad ^{(256)}T_{12}^{12}=95 \quad ^{(256)}T_{21}^{12}=65 \quad ^{(256)}T_{22}^{12}=108$$
$$^{(256)}T_{11}^{21}=97 \quad ^{(256)}T_{12}^{21}=114 \quad ^{(256)}T_{21}^{21}=110 \quad ^{(256)}T_{22}^{21}=111$$
$$^{(256)}T_{11}^{22}=117 \quad ^{(256)}T_{12}^{22}=115 \quad ^{(256)}T_{21}^{22}=95 \quad ^{(256)}T_{22}^{22}=95$$

وبالتالي نستطيع تنظيم الجدول الآتي:

مركبة التنسور	$^{(256)}T_{11}^{11}$	$^{(256)}T_{12}^{11}$	$^{(256)}T_{21}^{11}$	$^{(256)}T_{22}^{11}$	$^{(256)}T_{11}^{12}$	$^{(256)}T_{12}^{12}$	$^{(256)}T_{21}^{12}$	$^{(256)}T_{22}^{12}$
ASCII	66	97	115	101	108	95	65	108
الحرف	*B*	*a*	*s*	*e*	*l*	–	*A*	*l*
مركبة التنسور	$^{(256)}T_{11}^{21}$	$^{(256)}T_{12}^{21}$	$^{(256)}T_{21}^{21}$	$^{(256)}T_{22}^{21}$	$^{(256)}T_{11}^{22}$	$^{(256)}T_{12}^{22}$	$^{(256)}T_{21}^{22}$	$^{(256)}T_{22}^{22}$
ASCII	97	114	110	111	117	115	95	95
الحرف	*a*	*r*	*n*	*o*	*u*	*s*	–	–

فيكون النّص الأصلي هو:

$$Basel-Alarnous--$$

5. النتائج:

تمّ تعميم طريقة هيل في التشفير و إدخال التّنسورات عوضاً عن المصفوفات في التشفير، من خلال اعتماد قانون التّحويل التّنسوري، وتمّ التوصّل إلى إثبات صحّة المبرهنتين:

مبرهنة2:

إن تشفير كل نص واضح P (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n, p, q\right)$ يتم بشكلٍ وحيد.

مبرهنة 3:

إن فك التتشفير عن كل نص مشفّر C (من الحروف ASCII) من خلال استخدام قانون التّحويل التّنسوري بالمفتاح $C\left(C_n, p, q\right)$ يتم بشكلٍ وحيد.

6. المقترحات والتّوصيات:

إنّ التعميم باستخدام التّنسورات في التشفير يفتح آفاقاً جديدة لتطوير التشفير وزيادة أمانه، وذلك بتحميل محارف النص الواضح على مركّبات تنسور، لذلك يمكن العمل في المرحلة اللاحقة على استبدال مصفوفة هيل بتنسور يحقّق شروطاً تجعل عمليّة التشفير العكسيّة عمليّة ممكنة.

7. الملحقات:

7 – 1 برنامج رقم 1

```
Program Basel1;
Uses crt;
var
T,B,C,B: array [1..2,1..2] of integer;
I,j,k,l:integer;
Begin
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('C[',i,j,']=');readln(C[i,j]);
end;
readln;
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('B[',i,j,']=');readln(B[i,j]);
end;
readln;
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('T[',i,j,']=');readln(T[i,j]);
```

```
end;
readln;
for k:=1 to 4 do
for l:=1 to 4 do
begin
R[k,l]:=0
for i:=1 to 2 do
for j:=1 to 2 do
R[k,l]:= R[k,l]+T[i,j]*C[j,l] *B[k,i];
End;
for i:=1 to 2 do
for j:=1 to 2 do
write('R[',i,j,']=',R[i,j]);
readln;
end.
```

7 – 2 برنامج رقم 2

```
Program Basel2;
Uses crt;
var
T,R: array [1..2,1..2,1..2,1..2] of integer;
C,B: array [1..2,1..2] of integer;
lup,jup,kdown,ldown,l,j,k,l:integer;
Begin
```

```
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('C[',i,j,']='); readln(C[i,j]);
end;
readln;
for i:=1 to 2 do
for j:=1 to 2 do
begin
write('B[',i,j,']=');readln(B[i,j]);
end;
readln;
for i:=1 to 2 do
for j:=1 to 2 do
for k:=1 to 2 do
for l:=1 to 2 do
begin
write('T[',i,j,k,l,']=');readln(T[i,j,k,l]);
end;
readln;
for iup:=1 to 2 do
for jup:=1 to 2 do
for kdown:=1 to 2 do
for ldown:=1 to 2 do
```

```
begin
R[iup,jup,kdown,ldown]:=0
for i:=1 to 2 do
for j:=1 to 2 do
for k:=1 to 2 do
for l:=1 to 2 do
R[iup,jup,kdown,ldown]:=
R[iup,jup,kdown,ldown]+T[l,j,k,l]*C[k,kdown]*C[l,ldown]*B[iup,
i]*B[jup,j];
End;
for i:=1 to 2 do
for j:=1 to 2 do
for k:=1 to 2 do
for l:=1 to 2 do
write('R[',i,j,k,l,']=',R[i,j,k,l]);
readln;
end.
```

8. المراجع:

1. Lester S. Hill public son article "Cryptography in an Algebraic Alphabet", dans American Mathematical Monthly, 36, pp. 306-312, 1929
2. H.S.A. Rose, Course in number theory. Oxford Sciences Publication. (Clarendon), 1988.
3. B. Schneier , Applied cryptography. Second edition, protocols, algorithms and source coding C(John Wiley\& Sons), 1996.
4. M. I. Sowalle, Introduction to cryptology, Dist. Center, (Arabic version)Riyadh, 1996.
5. D. Welsh, Codes and Cryptography, Oxford Science publications ,1988.
6. F. A. Zoukair, and A. Samhan, Introduction to number theory , Pub. Dist. Center, Riyadh, (Arabic version), 2001
7. Swapan Kumar Sarkar ,A Text book of Discrete mathematics S.CHAND & COMPANY LTD, A TEXTBOOK OF DISCRETE MATHEMATICS RAMNAGAR,NEW DELHI-110055, 2008.
8. Moravitz Martin, Tensor Decompositions Workshop Discussion. University of Cornell (2004).

9. د. عبد الباسط الخطيب ، د. محمدنور شمه ، 2008 ، **التشفير العربي المطور "التشفير المطورة"**، مجلة جامعة البعث للعلوم الهندسية ، مجلد 30، العدد 17.

10.باسل العرنوس، 2015 ، التطبيقات الجيوديزيّة بين فضاءات ريمان ، رسالة ماجستير ، جامعة البعث.