استخدام المصفوفات الجزئية المنتهية لتشفير Hill للرسائل المرمزة بنظام ASCII

محمد نور شمه[1] و عبد الباسط الخطيب[2]

تاريخ الإيداع 2014/09/07
قبل للنشر في 2014/12/24

الملخص

قدّمت ورقة البحث هذه استخدام المصفوفات الجزئية المنتهية لتشفير الرسائل المرمزة بنظام ASCII معتمدين على طريقة هِلْ (Hill cipher) 1929م من خلال :

1. **تجزئة مصفوفة النص الأصلي إلى عدد محدود من المصفوفات الجزئية المنتهية لزيادة عدد مفاتيح التشفير داخل النص الواضح، بحيث نحصل على رسائل مشفرة بأكثر من مفتاح مما يجعلها صعبة الكسر، ويحافظ على أمن المعلومات داخل النصوص والرسائل المبثوثة.**
2. **الاعتماد على ترميز ASCII (Coding ASCII) المستخدم في حواسيبنا الحالية .**
3. **استخدام دالة هِلْ (Hill) $f(X)=(A.X+B)\bmod(n)$ إذْ (A,X,B) مصفوفات لها شروط خاصة لتشفير نص موضوعٍ داخل كل مصفوفة جزئية من مصفوفة النص الأصلي P.**
4. **قابلية تطبيق الطريقة حاسوبياً لتعطي نتائج سريعة وكبيرة.**

الكلمات المفتاحية: تشفير هِلْ، ترميز ASCII، طريقة المصفوفات المنتهية FMM، النص الواضح، النص المشفر، مفتاح التشفير.

[1] أستاذ، قسم العلوم الأساسية، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق، سورية.

[2] أستاذ، قسم الرياضيات، كلية العلوم، جامعة البعث، حمص، سورية.

Using Finite Matrices Method to Hill Encrypt Messages for ASCII Encoded System

M. N. Shamma[(1)] and A. Al-Khatib[(2)]

Received 07/09/2014
Accepted 24/12/2014

ABSTRACT

This paper presents the use of finite Matrices to encrypt messages encoded using ASCII system, dependent on the method (Hill cipher) 1929 by:

1. Using finite Matrices to divide the text into partial Matrices.
2. Depending on encoding ASCII (ASCII Coding).
3. Using the matrices A, X, B have special conditions to make Hill function ($f(X) = (A.X + B) \bmod(n)$) able to encrypt the text P that corresponding in the matrix. This matrix contains partial Matrices to get encryption messages with different keys to make it difficult to break, and save the security of information in the texts.
4. Method can be applied on the computer to give quick and great results.

Key words: Hill ciphers, ASCII Coding, Finite Matrices Method (FMM), Plaintext, Cipher text, Encryption Key.

(1) Professor, Department of Basic Sciences, Faculty of Mechanical and Electrical Engineering, Damascus University, Syria.
(2) Professor, Department of mathematics, Faculty of Sciences, Al-Baath University, Homs, Syria.

مقدمة

هدف "التشفير" الحفاظ على سرية الرسائل المبثوثة عبر قنوات الاتصال المختلفة كالراديو والهاتف والجوال والبريد الالكتروني والحكومات الالكترونية [3-1].

وهناك طرائق عديدة للتشفير نذكر منها التشفير بطريقة Hill التي قمنا بتطويرها لتصبح ملائمة للمتغيرات الحديثة. فبدلاً من الترميز بالحروف الانكليزية استخدمنا جميع المحارف المستخدمة في نظام ASCII التي (عددها 256 محرفاً)، كما استُخدمت مصفوفات $(A,\ X,\ B)$ لها شروط خاصة تجعل دالة هِلْ $f(X)=(A.X+B)\bmod(n)$ قادرة على تشفير نص P موضوع داخل مصفوفة تضم مصفوفات جزئية بحيث نحصل على رسائل مشفرة بأكثر من مفتاح؛ ممَّا يجعلها صعبة الكسر، ويحافظ على أمن المعلومات داخل النصوص والرسائل المبثوثة.

أولاً تعاريف ومبرهنات ذات الصلة: [7] و[8]

تعريف 1 (مصفوفة النص الواضح):

ليكن لدينا **P** نصاً واضحاً (Plaintext) نشكل منه مصفوفة حروف مربعة من المرتبة k نرمز لها P_k إذْ نحصل عليها بتبديل الحروف بحسب الأعمدة فنضع الحرف الأول من النص مكان العنصر p_{11} ، والحرف الثاني من النص مكان العنصر p_{21} ، وهكذا حتى نصل إلى العنصر الأخير p_{kk} .

تعريف 2 (مصفوفة النص المشفر):

ليكن لدينا نصاً مشفراً C (Cipher text) نشكل منه مصفوفة عددية مربعة Y_k من المرتبة k إذْ $k\in N$ بحيث نحصل عليها بتبديل محارف ASCII بالمقابل العددي مرتبة كما وردت في النص المشفر. ندعو هذه المصفوفة بمصفوفة النص المشفر.

تعريف 3:

ليكن $1\le a<n$ نقول: إن العدد a أولي نسبياً مع العدد n إذا تحقق: $\gcd(a,n)=1$

تعريف 4:

نسمي M_n مجموعة جميع الأعداد الأولية نسبياً مع العدد n أي إن:

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

المحارف ومقابلاتها العددية:

نستطيع الحصول على المقابل العددي لبعض محارف ASCII عن طريق برنامج Excel2010 عبر تعليمة CODE(.) وتعليمة CHAR(.)، وهي موضّحة في الجدول (1).

الجدول (1)

Decimals	***ASCII***	***Decimals***	***ASCII***	***Decimals***	***ASCII***
34	*"*	*63*	***?***	*92*	\
35	*#*	*64*	*@*	*93*	*]*
36	*$*	*65*	*A*	*94*	^
37	*%*	*66*	*B*	*95*	_
38	*&*	*67*	*C*	*96*	`
39	*'*	*68*	*D*	*97*	*A*
40	*(*	*69*	*E*	*98*	*B*
41	*)*	*70*	*F*	*99*	*C*
42	*	*71*	*G*	*100*	*D*
43	+	*72*	*H*	*101*	*E*
44	,	*73*	*I*	*102*	*F*
45	-	*74*	*J*	*103*	*G*
46	.	*75*	*K*	*104*	*H*
47	/	*76*	*L*	*105*	*I*
49	*1*	*78*	*N*	*107*	*K*
50	*2*	*79*	*O*	*108*	*L*
51	*3*	*80*	*P*	*109*	*M*
52	*4*	*81*	*Q*	*110*	*N*
53	*5*	*82*	*R*	*111*	*O*
54	*6*	*83*	*S*	*112*	*P*
55	***7***	*84*	***T***	*113*	***Q***
56	***8***	*85*	***U***	*114*	***R***
57	***9***	*86*	***V***	*115*	***S***
58	***:***	*87*	***W***	*116*	***T***
59	***;***	*88*	***X***	*117*	***U***
60	<	*89*	***Y***	*118*	***V***
61	=	*90*	***Z***	*119*	***W***
62	>				

ملاحظة (1):

1) لا تظهر حروفٍ مقابلة لعناصر المجموعة جميعها {0,1,..255} فهي حروف محجوبة عن الظهور علماً أنها موجودة.

2) إذا أردنا استبدال رقم k بمحرف غير ظاهر في الجدول (1) فإننا نضع الــرقم بــين إشارتي تنصيص "k".

تعريف 5:

نقول: إن العدد $1 \le b < n$ هو النظير الضربي للعدد $1 \le a < n$ بالمقاس n إذا تحقق: $a.b \equiv 1 \bmod(n)$

مبرهنة (1):

يوجد نظير ضربي وحيد للعدد a بالمقاس $n \in \mathbb{N}$ إذا وفقط إذا كان: $\gcd(a,n) = 1$.

تعريف 6 دالة التشفير (Encryption Key):

هي الدالة المصفوفية $f(X) = (A.X + B) \bmod(n)$ التي عناصرها (A, X, B) يمكن تطبيقها على مصفوفات لها شروط خاصة تُستخدم في وصف عملية التشفير وتعطينا النص المشفر.

تعريف 7 دالة التشفير العكسية (Decryption Key)

هي الدالة $X = A^{-1}(F(X) - B) \bmod(n)$ التي ترد النص المشفر إلى النص الواضح، إذْ إن $|A| = a \in M_n$ لكي يكون التشفير وحيداً [1]

المصفوفات الجزئية المنتهية (FMM):

يقصد بالمصفوفات الجزئية المنتهية (FMM) أن نضع النص الواضح في مصفوفة X مربعة الشكل، ثم نقوم بتقسيم هذه المصفوفة إلى عدد محدود من المصفوفات الجزئية X_i : $\mathbf{U}_i X_i = X$, $\mathbf{I}_i X_i = f$; $i = 1,2..,m$

ونقوم بتطبيق الدوال $f_k(X_i) = (A_i X_i + B_i) \bmod(n)$; $i = 1,2..,m$ على المصفوفات الجزئية X_i . من الآن فصاعداً نعدُّ $n = 256$، ونذكّر بالمبرهنتين الآتيتين: [4] و[6]

مبرهنة (2):

إنّ كل نص واضح P (من الحروف ASCII) يشفر من خلال دالة هل المصفوفية من الشكل: $F(X) = (A.X + B) \bmod(n)$ بشكلٍ وحيد.

مبرهنة (3):

إنّ فك التشفير عن كل نص مشفر C (من الحروف ASCII) من خلال الدالة المصفوفية من الشكل: $X = A^{-1}(F(X) - B)\bmod(n)$ يتم بشكلٍ وحيد.

ثانياً أهم نتائج البحث:

طرائق استخدام المصفوفات الجزئية المنتهية:

مبرهنة (4):

ليكن لدينا مصفوفة مربعة من المرتبة $m \times m$، وليكن $m = m_1.m_2$، عندها نقسم المصفوفة المربعة إلى $m_1^{\,2}$ من المصفوفات المربعة، وكل منها يحوي $m_2^{\,2}$ عنصراً.

الإثبات:

إذا كان $m = m_1.m_2$ فإن $m^2 = m_1^{\,2}.m_2^{\,2}$ هذا يعني أن المصفوفة المربعة يمكن أن تقسم إلى $m_1^{\,2}$ مصفوفات مربعة، وكل منها يحوي $m_2^{\,2}$ عنصراً؛ وذلك $\forall m_1, m_2 \in N^*$.

نتيجة (1):

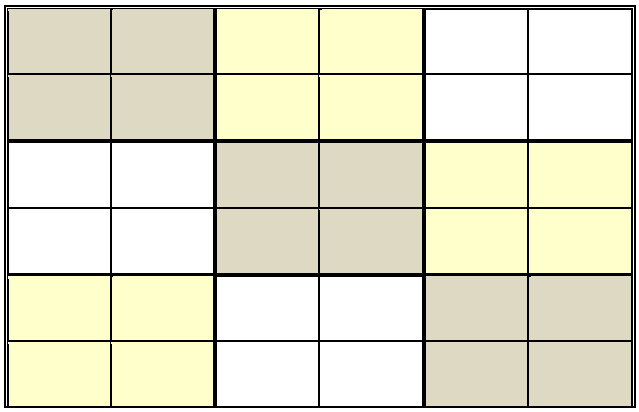
ليكن لدينا مصفوفة مربعة من المرتبة $m \times m$، وليكن $m = m_1.m_2$ ، واعتماداً على المبرهنة (4) نستطيع تجزئة المصفوفة إلى $m_2^{\,2}$ من المصفوفات المربعة، وكل منها يحوي $m_1^{\,2}$ عنصراً.

ملاحظة (2):

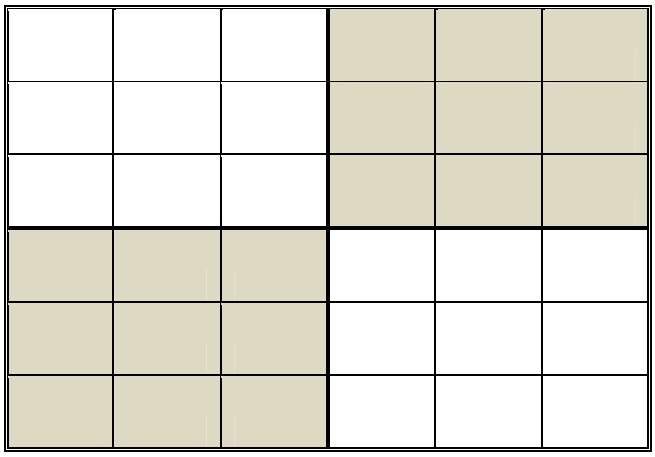
إن استخدام المصفوفات الجزئية المنتهية في التشفير يعني زيادة عدد المفاتيح المتعلقة بتجزئة المجموعات إلى أشكال (FMM)، أي زيادة فاعلية التشفير وزيادة فرص حماية المعلومات.

مثال (1):

بفرض لدينا مصفوفة مربعة من المرتبة 6×6، إذْ $n = 3 \times 2$، عندها نجزئ المصفوفة إلى 9 مربعات، وكل مربع يحوي 4 عناصر.



أو نجزئ المصفوفة إلى 4 مربعات، وكل مربع يحوي 9 عناصر .



مثال (2):

بفرض $n = 8 = 4 \times 2$ عندها نجزّئ المصفوفة إلى (16) مربعاً، وكل مربع يحوي 4 عناصر. أو نجزّئ المصفوفة إلى 4 مربعات، وكل مربع يحوي 16 عنصراً.

مبرهنة (5):

كل نص واضح P (من الحروف ASCII) مجزأ وفق المربعات من خلال الدالة المصفوفية $F_k(X) = (A_k X + B_k) \bmod(n)$, $k = 1,2..m$ يشفر بشكلٍ وحيد.

الإثبات:

لتكن P_1 , P_2 رسالتين مختلفتين من الحروف ASCII ولتكن X_1 , X_2 المصفوفتين العدديتين المقابلتين لهما في الجدول (2) أو مكملاته ولنثبت أن:

$$F_k(X_1) \bmod(256) \neq F_k(X_2) \bmod(256) .$$

نظراً إلى أنّ $P_1 \neq P_2$ فإنه بحسب جدول الحروف ومقابلاتها العددية

$$X_1 \neq X_2 \Rightarrow X_{1i} \neq X_{2i} \; ; i = 1,2..,m$$

لتكن X_{1i} , X_{2i} مصفوفتين جزئيتين متقابلتين من X_1 , X_2 نفرض جدلاً أنّ:

$$F_k(X_{1i}) \bmod(256) \equiv F_k(X_{2i}) \bmod(256)$$
$$\Rightarrow F_k(X_{1i}) - F_k(X_{2i}) \equiv O \bmod(256)$$

إذْ إنّ O هي المصفوفة الصفرية، ومن ثمَّ:

$$[(A_k(X_{1i}) + B) - (A_k(X_{2i}) + B] = A_k(X_{1i} - X_{2i}) \equiv O \bmod(256)$$

ونظراً إلى أنّ محدد المصفوفة A_k ، يحقق: $|A_k| = a \in M_{256}$ إذاً بحسب مبرهنة (1) فإن A_k لها مقلوب A_k^{-1} ومن ثمَّ:

$$(X_{1i} - X_{2i}) \equiv A_n^{-1}.O \bmod(256)$$
$$\Rightarrow (X_{1i} - X_{2i}) \equiv O \bmod(256)$$
$$\Rightarrow X_{1i} = X_{2i}$$

وهذا مخالف للفرض، إذاً $F_k(X_{1i}) \bmod(256) \neq F_k(X_{2i}) \bmod(256)$ ، ومن ثمَّ تشفير كل رسالة من خلال الدالة: $F_k(X) = (A_k X + B_k) \bmod(n)$ يتم بشكلٍ وحيد.

مبرهنة (6):

كل نص مشفر C (من الحروف ASCII) مقسم وفق المربعات من خلال دالة مصفوفية خطية $X = A_k^{-1}(F(X) - B_k) \bmod(n)$ يفك تشفيره بشكلٍ وحيد.

الإثبات:

يتم بطريقة معاكسة لطريقة إثبات مبرهنة (5).

لتكن C_1 , C_2 رسالتين مختلفتين من الحروف ASCII ولتكن Y_1 , Y_2 المصفوفتان العدديتان المقابلتان لهما في الجدول (1) أو مكملاته ولنثبت أن: $X_1 \neq X_2$

نفرض جدلاً أنّ: $X_1 \equiv X_2$

$$\Rightarrow A_k^{-1}(F(X_1)-B_k)\bmod(n)=A_k^{-1}(F(X_2)-B_k)\bmod(n)$$

$$\Rightarrow A_k^{-1}.F(X_1)-F(X_2)\equiv O\bmod(256)$$

إذْ إنّ O هي المصفوفة الصفرية.

ونظراً إلى أنّ محدد المصفوفة A_k يحقق: $|A_k| = a \in M_{256}$ ، إذاً بحسب مبرهنة (1) A_k لها مقلوب A_k^{-1} ومن ثمَّ:

$$F(X_1)-F(X_2)\equiv A_n.O\bmod(256)$$

$$\Rightarrow F(X_1)-F(X_2)\equiv O\bmod(256)$$

$$\Rightarrow F(X_1)=F(X_2)$$

وهذا مخالف للفرض، إذاً $F(X_1)\neq F(X_2)\bmod(256)$ ومن ثمَّ، فك التشفير عن كل رسالة من خلال الدالة: $X = A_k^{-1}(F(X)-B_k)\bmod(n)$ يتم بشكلٍ وحيد.

خوارزمية التشفير:

ليكن لدينا نص واضح P ونريد تشفيره وفق الدوال المصفوفية $F_k(X)=(A_kX+B_k)\bmod(n)$, $k=1,2..m$ عندئذٍ نقوم بما يأتي:

1. نرتب حروف النص الواضح في المصفوفة P_k .
2. نجزئ المصفوفة المربعة إلى ${m_1}^2$ مربعاً، وكل مربع يحوي ${m_2}^2$ عنصراً، ثم نستبدل المصفوفة P_k بمصفوفة الأرقام X الموافقة.
3. نضرب المصفوفة A_k بالمصفوفة الرقمية X ونضيف إلى الناتج المصفوفة B_k فنحصل على المصفوفة العددية $F_k(X)=(A_kX+B_k)\bmod(n)$, $k=1,2..m$.
4. نعوض القيم العددية بمحارف ASCII الموافقة فنحصل على النص المشفر C المطلوب.

مثال (3):

نقوم بتشفير النص P ={Natural Sciences} بطريقة المصفوفات الجزئية المنتهية مقسمين النص إلى أربع مصفوفات مربعة، مشفرين مصفوفتي القطر الرئيسي بالدالة $F_1(X) = (A_1\ X + B_1) \bmod(n)$ ، ومصفوفتي القطر الثانوي بالدالة $F_2(X) = (A_2\ X + B_2) \bmod(n)$ ، إذْ إن:

$$A_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ B_1 = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}\ A_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ B_2 = \begin{bmatrix} 0 & 5 \\ 1 & 2 \end{bmatrix}$$

الحـــــل:

1.نضع الحروف الناتجة عن النص المراد تشفيره جميعها في مصفوفة واحدة مرتبتها (4) أي إنَّ:

$$P = \begin{bmatrix} N & r & S & n \\ a & a & c & c \\ t & l & i & e \\ u & \_ & e & s \end{bmatrix}$$

2.نبدل الحروف بالأرقام المقابلة لها في جدول (1) فنحصل على الرسالة الرقمية في المصفوفة كما يأتي:

$$X = \begin{bmatrix} 78 & 114 & 83 & 110 \\ 97 & 97 & 99 & 99 \\ 116 & 108 & 105 & 101 \\ 117 & 95 & 101 & 115 \end{bmatrix}$$

إذْ:

$$X = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 78 & 114 \\ 97 & 97 \end{bmatrix} & \begin{bmatrix} 83 & 110 \\ 99 & 99 \end{bmatrix} \\ \begin{bmatrix} 116 & 108 \\ 117 & 95 \end{bmatrix} & \begin{bmatrix} 105 & 101 \\ 101 & 115 \end{bmatrix} \end{bmatrix}$$

3.نطبق دالتي التشفير $F_1(X)$, $F_2(X)$ كما يأتي:

$$F(X)=\begin{bmatrix} F_1(X_1) & F_2(X_2) \\ F_2(X_3) & F_1(X_4) \end{bmatrix}$$

بالإصلاح نجد:

$$F(X)=\begin{bmatrix} \begin{bmatrix} 176 & 212 \\ 97 & 98 \end{bmatrix} & \begin{bmatrix} 249 & 335 \\ 100 & 11 \end{bmatrix} \\ \begin{bmatrix} 349 & 329 \\ 118 & 97 \end{bmatrix} & \begin{bmatrix} 207 & 217 \\ 101 & 116 \end{bmatrix} \end{bmatrix}$$

4 . نجعل $F(x)$ ، بالمقاس 256 فنحصل على النص المشفر رقمياً:

$$\mathrm{mod}(F,256)=\begin{bmatrix} 176 & 212 & 249 & 79 \\ 97 & 98 & 100 & 101 \\ 93 & 73 & 207 & 217 \\ 118 & 97 & 101 & 116 \end{bmatrix}$$

5. نعوض عن الأرقام بمحارف ASCII الموافقة فنحصل على الــنص المــشفر C الآتي:

ش	ù	O	S
B	d	E	S
I	د	ظ	I
A	e	T	O

خوارزمية فك التشفير: تتم بشكلٍ معاكسٍ لعملية التشفير.

مثال (4):

نقوم بفك التشفير عن النص المشفر في المصفوفة الآتية:

â	ا	ة	ة	ا	ا
!	N	Ù	!	,	W
ت	ب	-	™	{	ئ
ة	ض	د	ة	و	ب
ï	2	µ	S	*	چ
-	ع	`	C	™	C

بطريقة المصفوفات الجزئية المنتهية مقسماً إلى أربع مــصفوفات مربعــة، مــشفراً مصفوفتي العمود الأول الرقمية بالدالة $F_1(X)=(A_1 X+B_1)\bmod(n)$ ، ومصفوفتي العمود الثاني بالدالة $F_2(X)=(A_2 X+B_2)\bmod(n)$ إذ:

$$A_1=\begin{bmatrix}1&0&0\\0&3&1\\0&0&1\end{bmatrix},\ B_1=\begin{bmatrix}1&0&0\\2&3&1\\0&0&1\end{bmatrix}\ A_2=\begin{bmatrix}1&0&0\\0&3&1\\0&0&7\end{bmatrix},\ B_2=\begin{bmatrix}1&0&0\\31&34&1\\0&0&1\end{bmatrix}$$

الحل:

1 . إن النص المشفر يقابل مصفوفة عددية مربعة من المرتبة السادسة، وهي:

$$F=\begin{bmatrix}266&199&201&201&199&199\\33&110&249&33&44&119\\202&200&220&153&123&198\\201&214&207&201&230&200\\237&50&181&115&42&141\\95&218&96&67&153&67\end{bmatrix}$$

2.نقسم المصفوفة إلى أربع مصفوفات كما يأتي:

$$F=\begin{bmatrix}\begin{bmatrix}266&199&201\\33&110&249\\202&200&220\end{bmatrix}&\begin{bmatrix}201&199&199\\33&44&119\\153&123&198\end{bmatrix}\\\begin{bmatrix}201&214&207\\237&50&181\\95&218&96\end{bmatrix}&\begin{bmatrix}201&230&200\\115&42&181\\67&153&67\end{bmatrix}\end{bmatrix}=\begin{bmatrix}F_1&F_3\\F_2&F_4\end{bmatrix}$$

3.نطبق دالة فك التشفير على المصفوفة السابقة:

$$X=\begin{bmatrix}A_1^{-1}(F_1-B_1)&A_2^{-1}(F_3-B_2)\\A_1^{-1}(F_2-B_1)&A_2^{-1}(F_4-B_2)\end{bmatrix}=\begin{bmatrix}\begin{bmatrix}225&199&201\\199&225&95\\202&200&219\end{bmatrix}&\begin{bmatrix}200&199&199\\225&95&225\\95&237&211\end{bmatrix}\\\begin{bmatrix}200&214&207\\218&199&199\\95&218&95\end{bmatrix}&\begin{bmatrix}200&230&200\\218&227&202\\229&95&46\end{bmatrix}\end{bmatrix}$$

4. نضع المصفوفات في مصفوفة واحدة:

$$\begin{bmatrix} 225 & 199 & 201 & 200 & 199 & 199 \\ 199 & 225 & 95 & 225 & 95 & 225 \\ 202 & 200 & 219 & 95 & 237 & 211 \\ 200 & 214 & 207 & 200 & 230 & 200 \\ 218 & 199 & 199 & 218 & 227 & 202 \\ 95 & 218 & 95 & 229 & 95 & 46 \end{bmatrix}$$

5. فتكون مصفوفة النص الواضح المقابلة للمصفوفة الرقمية هي:

ل	ا	ة	ب	ا	ا
ا	ل	-	ل	-	ل
ت	ب	غ	-	ي	س
ب	ض	د	ب	و	ب
ع	ا	أ	ع	م	ت
-	ع	-	هـ	-	.

فالنص الواضح هو: (***لا تبع البضاعة غداً بل بعها يوم السبت.***)

ملاحظة (3):

إذا لم نحصل على مصفوفة مربعة من النص P فإننا نقوم بتجزئة النص P إلـــى اثنين أو أكثر بحيث يشكل كل نص مصفوفة مربعة ، كما في المبرهنة الآتية:

مبرهنة (7):

من أجل $K \in N^*$ فإنه يوجد $0 \le K_n \le 3$; $K > m_1 > m_2 > .. > m_n > K_n$

بحيث نكتب $K = m_1^2 + m_2^2 + .. + m_n^2 + K_n$; $0 \le K_n \le 3$

الإثبات:

بفرض أن $m_1^2 \le K < (m_1 + 1)^2$ ، فإن (3) $m_2^2 \le K_1 < m_1^2$; $K = m_1^2 + K_1$ ، ثم نكتب $K_1 = m_2^2 + K_2$, $m_3^2 \le K_2 < m_2^2$ وهكذا تستمر عملية التقسيم حتى نصل إلى الباقي الأخير $m_n^2 \le K_n \le 3$, $K_{n-1} = m_n^2 + K_n$ وبتعويض قيم $K_1, K_2 .., K_{n-1}$ من العلاقات السابقة في العلاقة (3) نحصل على المطلوب.

مثال (5):

اعتماداً على المبرهنة (7) نستطيع كتابة الأعداد الآتية $N(P) = 29 , 117 , 119$ كما يأتي:

1. $N(P)=29=5^2+2^2$ فإننا نقسمه إلى نصين مرتبين على التتـــالي P_1 , P_2 يقابلان مصفوفتين مربعتين من المرتبتين (2×2 , 5×5)

2. كذلك $N(P)=117=10^2+4^2+1^2$ نقسمه إلى مصفوفات مربعة من المراتب (1×1 , 4×4 , 10×10) إذْ إن: $N(P_3)=1$, $N(P_2)=16$, $N(P_1)=100$ وكل نص منهما يشكل مصفوفة مربعة .

3. أمّا $N(P)=119=10^2+4^2+1^2+1^2+1^2$ منقسمة إلى خمـــس مـــصفوفات مربعة من المراتب (1×1 , 1×1 , 1×1 , 4×4 , 10×10) إذْ إن:

$N(P_5)=1$, $N(P_4)=1$, $N(P_3)=1$, $N(P_2)=16$, $N(P_1)=100$ وكل نص منهما يشكل مصفوفة مربعة.

ملاحظات (4):

1. نستطيع تشفير نص أكبر حجماً بالاعتماد على برامج رياضية جاهزة الـــدوال مثـــل برنامج MATHCAD2001 أو MATHEMATICA.
2. يمكننا استبدال نظام ASCII بنظام UNICODE، عنـــدها ســـيتغير المقـــاس مـــن $n=256$ إلى المقاس $n=65536$ (عدد محارف UNICODE)، وسيتغير معهـــا الأولية نسبياً مع كل مقاس وستبقى المبرهنتان (4) و(5) صحيحتين.

References

[1] Christof Paar, Jan Pelzl, 2010. Understanding Cryptography, © Springer-Verlag Berlin Heidelberg.
[2] Garrett, P., 2007. Making, Breaking Codes. An Introduction to Cryptology. Prentice–Hall.
[3] Goldreich, O., 2009. Foundations of Cryptography. Basic Applications. Cambridge University Press .
[4] Katz, J., Lindell, Y., 2008. Introduction to Modern Cryptography. Chapman & Hall/CRC.
[5] Keijo Ruohonen, 2014. Mathematical Cryptology,Translation by Jussi Kangas and Paul Coughlan.
[6] M. N. Shamma, A. Al-Khatib, 2009. On the modern cryptology method of Hill for encoded letters with ASCII system, Far East Journal of Mathematical Education FJME Volume 3 No. 2, June, pp. 183 – 193.
[7] Rosen, K. H., 2010. Elementary Number Theory. Longman .
[8 Rosen, K. H, 2012. Discrete mathematics and its applications. 7th ed., The McGraw-Hill Companies .