استخدام المصفوفات المتولدة من عنصر واحد مع المعادلات الخطية في تشفير الرسائل النصية

نزار خلف حسين[1] و أكرم سالم محمد[2] و صباح سلمان حمدي[2]

[1] رئاسة الجامعة، مركز الحاسبة والمعلومات، جامعة تكريت، تكريت، جمهورية العراق

[2] قسم الرياضيات، كلية العلوم، جامعة تكريت، تكريت، جمهورية العراق

الملخص:

تضمن هذا البحث طريقة تشفير تعتمد على مصفوفة التشفير السرية (Secret encrypt metrics) التي تكون متولدة من عنصر واحد وهو تاريخ إرسال الرسالة حيث يتم التشفير بواسطة معادلة التشفير (مفتاح التشفير) حيث أن هذه المعادلة تعتمد على مصفوفة التشفير السرية ومصفوفة النص الصريح و الترتيب (تسلسل الحرف في النص) الذي يمثله الحرف لنحصل على نص مشفر، كذلك تضمن البحث تقديم معادلة فك التشفير التي تعتمد على معادلة التشفير.

المقدمة:

في ظل التطور الحاصل في مجال الاتصالات وإرسال الرسائل كان لابد أن يصاحب هذا التطور الحاصل في مجال الاتصالات تطوراً في مجال حماية هذه الاتصالات والرسائل من المتطفلين الـ (Hakars) ، إلا انه كلما حصل تطور في مجال امن المعلومات فانه دائماً يصاحبه تطور في الضد أي في مجال التطفل مما يجعل مهمة امن المعلومات سواء كانت اتصالات أو رسائل نصية أو أية صيغة أخرى من المعلومات معرضة للكشف من المتطفلين فصار لازماً التفكير بأعداد منظومة حماية المعلومات من هكذا تطفل. ولذلك ظهر علم التشفير لحماية هذه المعلومات والتشفير هو عبارة عن تشفير النص الصريح للحصول على الكتابة المشفرة [٤] ورغم أن الدور المهم الذي لعبته تقنيات التشفير في منظومات امن الحاسوب إلا أن أدوات المستخدم لتشفير بيانات الملف أصبحت متعبة وثقيلة وبنفس الوقت مكتوبة وغير رصينة [1] .

١ – نظام ألاسكي:ASCII

إن نظام ألاسكي هو نظام يقوم بتحويل أبجدية السياق التعبيري من حروف ورموز سيطرة إلى قطع (Block) وبطول 7-bit وكلمة ASCII مشتقة من العبارة الآتية (American standard code for information Interchange) والتي تعني النظام القياسي الأمريكي لتبادل المعلومات [4] حيث أنه من الأنظمة المستخدمة في تحويل الرموز والتنقيط ورموز السيطرة إلى متتابعات من الأرقام[3].

كذلك نلاحظ في جداول الاسكي الموجودة في المصادر انه على الأغلب يكون عدد عناصر أبجدية السياق التعبيري لا تزيد عن 128وهذا العدد لم يأتي بصورة عشوائية وذلك أن $127 = 2^7$ أي أن احتمالية تكوين قطعة مكونة من سبعة رموز من {1 ، 0 } فقط هي 128 ولكن احد هذه الاحتمالات هو 0000000 وهو عدد يخلو من الواحد ولذلك سيستثنى من المجموع فتكون 127.

لأننا في هذا البحث اعتمدنا في تشفيرنا للنصوص على ما يقابلها من رموز في نظام الاسكي ، وندرج جدول أرقام الاسكي الأتي :-

وأيضاً يجب أن نشير وكما هو واضح في الجدول (١) أن منظومة التشفير التي تعمل لدينا سوف تكون على اللغة الانكليزية فقط .

جدول(١): جدول الأسكي

Char	Dec	Hex
NUL	0	00
SOH	1	01
STX	2	02
ETX	3	03
EOT	4	04
ENQ	5	05
ACK	6	06
BEL	7	07
BS	8	08
HT	9	09
LF	10	0A
VT	11	0B
FF	12	0C
CR	13	0D
SO	14	0E
SI	15	0F
DLE	16	10
DC1	17	11
DC2	18	12
DC3	19	13
DC4	20	14
NAK	21	15
SYN	22	16
ETB	23	17
CAN	24	18
EM	25	19
SUB	26	1A
ESC	27	1B
FS	28	1C
GS	29	1D
RS	30	1E
US	31	1F

Char	Dec	Hex
space	32	20
!	33	21
"	34	22
#	35	23
$	36	24
%	37	25
&	38	26
'	39	27
(	40	28
)	41	29
*	42	2A
+	43	2B
,	44	2C
-	45	2D
.	46	2E
/	47	2F
0	48	30
1	49	31
2	50	32
3	51	33
4	52	34
5	53	35
6	54	36
7	55	37
8	56	38
9	57	39
:	58	3A
;	59	3B
<	60	3C
=	61	3D
>	62	3E
?	63	3F

Char	Dec	Hex
@	64	40
A	65	41
B	66	42
C	67	43
D	68	44
E	69	45
F	70	46
G	71	47
H	72	48
I	73	49
J	74	4A
K	75	4B
L	76	4C
M	77	4D
N	78	4E
O	79	4F
P	80	50
Q	81	51
R	82	52
S	83	53
T	84	54
U	85	55
V	86	56
W	87	57
X	88	58
Y	89	59
Z	90	5A
[	91	5B
\	92	5C
]	93	5D
^	94	5E
_	95	5F

Char	Dec	Hex
`	96	60
a	97	61
b	98	62
c	99	63
d	100	64
e	101	65
f	102	66
g	103	67
h	104	68
i	105	69
j	106	6A
k	107	6B
l	108	6C
m	109	6D
n	110	6E
o	111	6F
p	112	70
q	113	71
r	114	72
s	115	73
t	116	74
u	117	75
v	118	76
w	119	77
x	120	78
y	121	79
z	122	7A
{	123	7B
|	124	7C
}	125	7D
~	126	7E
DEL	127	7F

٢ – مصفوفة منظومة التشفير

كلما كان النص المشفر بعيداً جداً عن النص الصريح سواءً كان ذلك بالشكل أم بالمعنى فان ذلك يقوي منظومة التشفير ويجعلها أمنة من المتطفلين . لذلك ولتعقيد أو زيادة درجة التعقيد على المتطفل اقترحنا مصفوفة لكي تستخدمها في منظومة التشفير بالإضافة إلى مصفوفة النص الصريح .

٢-١ – مصفوفة النص الصريح Metrics of Plain Text

وهي مصفوفة تتحدد تبعاً للنص وحجم النص حيث أن عناصرها هي عبارة عن حروف النص ورموزه وما يحتويه النص فمثلاً إذا كان عدد مكونات النص (حروف، رموز، تنقيط) هي K بحيث أن K عدد صحيح غير سالب فان حجم المصفوفة سيكون n×n بحيث أن $K = n \times n$ وفي حالة كون العدد الصحيح K لا يملك جذر صحيح (عدد صحيح) فإننا نأخذ عدد $L > K$ بحيث أن $L = m \times m$ وفي هذه الحالة ستنتهي حروف النص دون أن تملا المصفوفة ولذلك سوف يكون هناك اتفاق بين الطرفين

(المرسل، المُستقبل) على أن تملا هذه الفراغات بحروف بحيث يحدد لكل يوم في الشهر حرف معين حسب الجدول الشهري للفراغات حيث يكون جدول متفق عليه وسوف نعتبر إن الجدول الآتي هو الجدول المطلوب وعلى شرط إن هذا الجدول يُغيّر كل شهر باتفاق الطرفين

جدول (٢): الجدول الشهري للفراغات

ت	تاريخ الإرسال	الحرف البديل	ت	تاريخ الإرسال	الحرف البديل
1	٢٠٠٧/١/١	r	16	٢٠٠٧/١/١٦	g
2	٢٠٠٧/١/٢	s	17	٢٠٠٧/١/١٧	h
3	٢٠٠٧/١/٣	t	18	٢٠٠٧/١/١٨	i
4	٢٠٠٧/١/٤	u	19	٢٠٠٧/١/١٩	j
5	٢٠٠٧/١/٥	v	20	٢٠٠٧/١/٢٠	k
6	٢٠٠٧/١/٦	w	21	٢٠٠٧/١/٢١	l
7	٢٠٠٧/١/٧	x	22	٢٠٠٧/١/٢٢	m
8	٢٠٠٧/١/٨	y	23	٢٠٠٧/١/٢٣	n
9	٢٠٠٧/١/٩	z	24	٢٠٠٧/١/٢٤	o
10	٢٠٠٧/١/١٠	a	25	٢٠٠٧/١/٢٥	p
11	٢٠٠٧/١/١١	b	26	٢٠٠٧/١/٢٦	q
12	٢٠٠٧/١/١٢	C	27	٢٠٠٧/١/٢٧	r
13	٢٠٠٧/١/١٣	d	28	٢٠٠٧/١/٢٨	s
14	٢٠٠٧/١/١٤	e	29	٢٠٠٧/١/٢٩	t
15	٢٠٠٧/١/١٥	f	٣٠	٢٠٠٧/١/٣٠	u

فلو كان لدينا النص الأتي :Computer Cryptography

وعندما نحسب حروف هذا النص لوجدناها 22ولكن ليس هناك جذر صحيح للعدد 22 وهذا فإننا نأخذ العدد 22 < 25 و 25= 5×5 وعندها تكون مصفوفة النص الصريح بحجم 5 ×5 على فرض إن النص كان من المقرر أن يرسل في يوم ٢٠٠٧/١/٥ فإننا سوف نرمز لمصفوفة النص الصريح بالرمز PTM وكما موضحة في أدناه وايضاً سوف نرمز للفراغ Space بالرمز ψ ونضع هذا الفراغ للفصل بين الكلمات للدلالة على نهاية الكلمة

$$PTM=\begin{bmatrix} C & o & m & p & u \\ t & e & r & \psi & C \\ r & y & p & t & o \\ g & r & a & p & h \\ y & v & v & v & v \end{bmatrix}$$

٢-٢- المصفوفة السرية لمنظومة التشفير Secret Matrices of Encrypt System

بعد أن أعطينا مصفوفة النص الصريح فإننا نحتاج إلى مصفوفة التشفير. حجم المصفوفة التي تستخدم يكون بنفس حجم مصفوفة النص الصريح وتتولد من عنصر واحد فقط وهو تاريخ إرسال الرسالة وسيكون رمزها SEM وكما يأتي :-

$$SEM=\begin{bmatrix} S(1,1) & S(1,2)=S(1,1)+1 & S(1,3)=S(1,1)+2 & \cdots & S(1,n)=S(1,1)+(n-1) \\ S(2,1)=2S(1,1) & S(2,2)=2S(1,2) & S(2,3)=2S(1,3) & \cdots & S(2,n)=2S(1,n) \\ \vdots & \vdots & \vdots & & \vdots \\ S(n,1)=nS(1,1) & S(n,2)=nS(1,2) & S(n,3)=nS(1,3) & \cdots & S(n,n)=nS(1,n) \end{bmatrix}$$

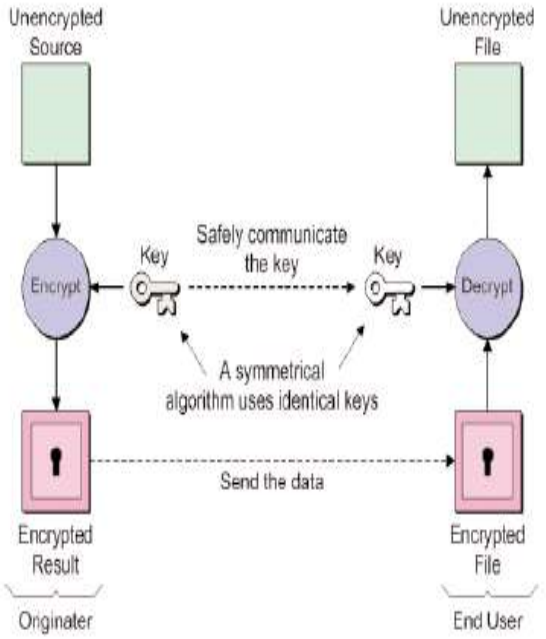
حيث أن الصف الأول للمصفوفة يتكون من إضافة واحد إلى العنصر S(1,1) لتكوين S(1,2) وإضافة ٢ إلى S(1,1) لتكوين S(1,3) وهكذا نصل إلى S(1,N) الذي يتكون من إضافة (N-1) إلى S(1,1) وبعدها نكون الصفوف الأخرى حيث يتكون الصف الثاني بضرب الصف الأول في 2 والصف الثالث يتكون من ضرب الصف الأول في 3 وهكذا إلى إن نصل إلى الصف n الذي يتكون من ضرب الصف الأول في n

٢-٣- معادلة منظومة التشفير ومعادلة فك التشفير Equation of Encryption System and Equation of Decryption

بعد إن أعطينا مصفوفتي النص الصريح والتشفير فإننا نعطي الآن المعادلة التي من خلالها يتم التشفير والتي نرمز لها بالرمز ESE وبعدها معادلة فك التشفير والتي نرمز لها بالرمز DSE .

٢-٤- معادلة منظومة التشفير

إن المعادلة التي سوف نقترحها هي معادلة تأخذ ما يقابل الحرف أو الرموز أو التنقيط في النص الصريح ليتم معاملته مع ما يقابله في مصفوفة منظومة التشفير السرية SEM مع ترتيب كل حرف ورمز وتنقيط في النص الصريح وبحيث إن ناتج المعادلة يجب أن لا يتجاوز (127) ولا يقل عن 1 ولذلك فإننا يجب أن نجعل ناتج المعادلة (127)Mod لكي يكون الناتج ضمن الجدول (١)، وهذا الإجراء هو لأجل أن يكون الناتج هو احد رموز الاسكي ، أي إما حرف أو رمز أو تنقيط لان هذا سوف يساعدنا في عملية فك شفرة هذا النص عندما نريد ذلك حيث أن معادلة منظومة التشفير مفتاح التشفير ومعادلة فك التشفير تمثل مفتاح فك الشفرة حيث انه في السابق كان المفتاح نفسه يستخدم للتشفير ولفك الشفرة كما أشار إلى ذلك Andrew Dauman [2] وكما في الشكل(١).



الشكل (١): منظومة تشفير

٢-٤-١- معادلة منظومة التشفير ESE

AESE(i,j)=[APTM(i,j)+order (PTM(i,j))+SEM(i,j)]mod127

حيث أن order(i,j) هو تسلسل أو ترتيب الحرف أو الرمز أو التنقيط ضمن النص الصريح . وان APTM هي المصفوفة التي تحوي على رموز الاسكي التي تقابل رموز النص الصريح . وسيأتي شرحها لاحقاً .

٢-٤-٢- معادلة فك التشفير DSE

ADSE(i,j)=[(AESE(i,j)+127)-(order(ESE(i,j))+SEM(i,j))]mod 127

وحيث أن AESE تمثل مصفوفة رموز الاسكي المقابلة لمصفوفة النص المشفر ESE وكذلك order [ESE(i,j)] هو تسلسل الحرف أو الرمز أو التنقيط ضمن النص المُشفر.

٢-٤-٣- خوارزمية التشفير

١- إبدأ.

٢- نكتب النص الصريح بشكل مصفوفة مربعة بحيث أن المصفوفة يجب أن تكون مربعة أي أن عدد حروف النص يجب أن يكون عدد n له جذر صحيح وبعكسه فأننا نختار عدد m بحيث أن m اكبر أو يساوي n وأن العدد m له جذر صحيح وفي هذه الحالة فأننا نملا الفراغات الباقية في المصفوفة برمز متفق عليه.

٣- نأخذ المصفوفة المقابلة لمصفوفة النص الصريح وهي المصفوفة التي تكون عناصرها عبارة عن أعداد عشرية وهي الأعداد المقابلة لحروف النص الصريح وحسب نظام الاسكي.

٤- نكوّن مصفوفة التشفير السرية.

٥- نستخدم معادلة التشفير لتشفير النص الصريح.

٦- نأخذ المصفوفة المقابلة لمصفوفة النص الناتج لأن معادلة التشفير سوف تنتج مصفوفة فيها أعداد عشرية.

٧- نكتب النص الناتج اعتماداً على مصفوفة النص الناتج وحسب الترتيب ونفصل بين كل رمز وأخر بفراغ.

٨- سوف يكون النص الناتج هو النص المشفر.

٩- انتهى.

٢-٤-٤- خوارزمية فك التشفير

١- إبدأ.

٢- نكتب النص المشفر بشكل مصفوفة مربعة بحيث أن المصفوفة يجب أن تكون مربعة.

٣- نأخذ المصفوفة المقابلة لمصفوفة النص المشفر وهي المصفوفة التي تكون عناصرها عبارة عن أعداد عشرية وهي الأعداد المقابلة لحروف النص الصريح وحسب نظام الاسكي.

٤- نكوّن مصفوفة التشفير السرية.

٥- نستخدم معادلة فك التشفير وذلك لفك شفرة النص المشفر.

٦- نأخذ المصفوفة المقابلة لمصفوفة النص الناتج لأن معادلة فك التشفير سوف تنتج مصفوفة فيها أعداد عشرية.

٧- نكتب النص الناتج اعتماداً على مصفوفة النص الناتج وحسب الترتيب وحسب المعنى ايضاً.

٨-سوف يكون النص الناتج هو النص الصريح.

٩-انتهى.

٣- مثال تطبيقي

إذا كان لدينا النص الآتي :

Computer Cryptography:

فلو حسبنا حروف ورموز وتنقيط هذا النص لوجدناها 22 وكما أسلفنا فإننا نحتاج أن يكون العدد الصحيح له جذر صحيح وبما أن 22 ليس لها جذر صحيح فإننا نأخذ عدد مثل 22>25 , 5×5 =25 أي انه له جذر صحيح ولهذا فان مصفوفة النص الصريح ستكون بسعة 5×5 وعلى فرض أن الرسالة سوف ترسل في ٢٠٠٧/١/١ فانه وحسب الجدول (2) فان الباقي من المصفوفة يملأ بالحرف r .

$$PTM=\begin{bmatrix} C & o & m & p & u \\ t & e & r & \psi & C \\ r & y & p & t & o \\ g & r & a & p & h \\ y & : & r & r & r \end{bmatrix}$$

$$APTM=\begin{bmatrix} 67 & 111 & 109 & 112 & 117 \\ 118 & 101 & 114 & 32 & 67 \\ 114 & 121 & 112 & 118 & 111 \\ 103 & 114 & 97 & 112 & 104 \\ 121 & 58 & 114 & 114 & 114 \end{bmatrix}$$

بعدها يتم تولد مصفوفة منظومة التشفير السرية SEM وبما أن الإرسال يتم في اليوم الأول من الشهر فان المصفوفة تكون كالآتي :

$$SEM=\begin{bmatrix}1&2&3&4&5\\2&4&6&8&10\\3&6&9&12&15\\4&8&12&16&20\\5&10&15&20&25\end{bmatrix}$$

وبعد أن أعطينا مصفوفة النص الصريح وما يقابلها من مصفوفة رموز الاسكي وكذلك مصفوفة منظومة التشفير السرية فإننا نطبق معادلة التشفير

.

AESE(1,1)=[APTM(1,1)+order
(PTM(1,1))+SEM(1,1)]mod127
=[67+1+1]=[69]mod 127 =69
AESE(1,2)=114,AESE(1,3)=115,
AESE(1,4)=120,AESE(1,5)=127
AESE(2,1)=126,AESE(2,2)=112,
AESE(2,3)=1, AESE (2,4)=49,
AESE(2,5)=87, AESE(3,1)=1,
AESE(3,2)=12 AESE,(3,3)=7, AESE(3,4)=17,
AESE(3,5)=14 AESE(4,1)=123,
AESE(4,2)=12, AESE(4,3)=127,
AESE(4,4)=20,AESE(4,5)=17,AESE(5,1)=20,AESE(5,2
)=90,AESE(5,3)=25,AESE(5,4)=31,AESE(5,5)=37,

وهكذا فأن مصفوفة النص المشفرESE هي

$$ESE=\begin{bmatrix}E&S&S&X&DEL\\\neg&P&SOH&1&W\\SOH&FF&BEL&DC1&SO\\\{&FF&DEL&DC1&DC1\\DC4&Z&EM&US&\%\end{bmatrix}$$

ومصفوفة AESE هي

$$AESE=\begin{bmatrix}69&115&115&120&127\\126&112&1&5&87\\1&12&7&17&14\\123&12&127&20&17\\20&90&25&31&37\end{bmatrix}$$

ومن مصفوفة النص المشفر فان النص المشفر يكون كالأتي :

E s s x DEL ¬ P SOH 1 W SOH FF BEL DC1 SO { FF DEL DC1 DC1 DC4 Z EM US %

وبالتأكيد وكما هو واضح فان هذا النص هو غير مفهوم وفيه درجة تعقيد عالية جداً بحيث يصعب على المتطفل التعرف على مقصده .

بعد ذلك يأخذ الطرف الثاني النص المشفر ويجعله في مصفوفة مربعة وبعدها يأخذ المصفوفة المقابلة لها برموز الاسكي وهي كالأتي :-

$$ESE=\begin{bmatrix}E&S&S&X&DEL\\\neg&P&SOH&<&W\\SOH&FF&BEL&DC1&SO\\\{&FF&DEL&DC1&DC1\\DC4&Z&EM&US&\%\end{bmatrix}$$

$$AESE=\begin{bmatrix}69&115&115&120&127\\126&112&1&49&87\\1&12&7&17&14\\123&12&127&20&17\\20&90&25&31&37\end{bmatrix}$$

الان نطبق معادلة فك التشفير DSE

ADSE(i,j)=[(AESE(i,j)+127)-(order(ESE(i,j))+SEM(i,j)]
mod 127
ADSE(1,1)=[(AESE(1,1)+127)-
(order(ESE(1,1))+SEM(1,1)]]mod 127
=[(69+127)-(1+1)]mod 127
=[196-2]mod 127=194mod 127=67

وهكذا نجد البقية

ADSE(1,2)=[(115+127)-(2+2)]mod127 =238
mod127=111
=ADSE(1,3)=109,ADSE(1,4)=112,
ADSE(1,5)=117,ADSE(2,1)=118,
ADSE(2,2)=101,ADSE(2,3)=114,
ADSE(2,4)=32,ADSE(2,5)=67,
ADSE(3,1)=114,ADSE(3,2)121,
ADSE(3,3)=112,ADSE(3,4)=118,
ADSE(3,5)=111,ADSE(4,1)=103,
ADSE(4,2)=114,ADSE(4,3)=97,
ADSE(4,4)=112,ADSE(4,5)=104,
ADSE(5,1)=121,ADSE(5,2)=58,
ADSE(5,3)=114,ADSE(5,4)=114, ADSE(5,5)=114

$$ADSE=\begin{bmatrix}67&111&109&112&117\\118&101&114&43&67\\114&121&112&118&111\\103&114&97&112&104\\121&58&114&114&114\end{bmatrix}$$

$$\Rightarrow DSE=\begin{bmatrix}C&O&m&p&u\\t&e&r&t&c\\r&y&p&t&o\\g&r&p&t&o\\y&:&r&r&r\end{bmatrix}$$

∴النص هو :- Computer cryptography:

مناقشة نتائج المثال التطبيقي:- بعد أن تم تشفير النص Computer cryptography: والذي يعتبر النص الصريح وتشفيره بواسطة معادلة منظومة التشفير ESE، وملاحظة النص المشفر والناتج من عملية

التشفير، يتبين لنا وبسهولة أن عملية التشفير أمنة بحيث لايمكن فك تلك الشفرة بسهولة. وكذلك سهولة ويسر ارجاع النص المشفر الى النص الصريح بواسطة منظومة فك التشفير DSE.

البرنامج

التشفير

```
A=[ 1 2 3 4 5;6 7 8 9 10;11 12 13 14 15;16 17 18 19 20;21 22 23 24 25];
APTM=[67 111 109 112 117;118 101 114 43 67; 114 121 112 118 111;103 114 97 112 104;121 58 114 114 114];
SEM=[1 2 3 4 5;2 4 6 8 10;4 6 9 12 15;4 8 12 16 20;5 10 15 20 25];
AESE=APTM+A+SEM;
B=rem(AESE,127)
```

فك التشفير

```
A=[ 1 2 3 4 5;6 7 8 9 10;11 12 13 14 15;16 17 18 19 20;21 22 23 24 25];
AESE=[69 115 115 120 127;126 112 1 5 87;1 12 7 17 14;123 12 127 20 17;20 90 25 31 37];
SEM=[1 2 3 4 5;2 4 6 8 10;4 6 9 12 15;4 8 12 16 20;5 10 15 20 25];
ADSE=(AESE+127*ones(5))-(A+SEM);
C=rem(ADSE,127)
```

References

1. Blaze,M. "A cryptographic File System for Unix,ACM conference on communications and computer security" (1993).
2. Dauman.A. "An open IP encryption flow permits industry-wide interoperability", California Ave (2006).
3. Lind,D. and Marcus,B. "An Introduction To Symbolic Dynamics and Coding", Cambridge University Pres(1995).

٤. بروس بوزورث، ترجمة الدبوني، ميثم محمد زكري. سليمان، أديب حمدون. سدخان، ستار بدر/ الدار العربية للطباعة/ بغداد/ الرموز والشفرات والحاسبات مقدمة إلى أمن المعلومات (١٩٨٩).

The use of Matrices that are generated from one component with the linear equations in order to encrypt the text messages

Nazar K. Hussain [1], Akram S. Mohamed[2] and Sabah S. Hamdi[3]

[1] College of Computer Sciences and Mathematics, University of Tikrit, Tikrit, Iraq
[2] Department of Mathematics, College of Computer Sciences and Mathematics, University of Tikrit, Tikrit, Iraq

Abstract:

This search includes a method of encryption relies on matrix secret encryption (Secret encrypt metrics) to be generated by one element which is the date of sending the message that, where encryption is by equation encryption (encryption key) is that the equation depend on the matrix of confidentiality and encryption matrix explicit text and arrangement (in the sequence of trades text), which represents trades to get the encrypted text, as well as the research includes to present equation decryption, which is also depend on the foregoing equation decryption .