تشفير الرسائل النصية باستخدام المعادلات الخطية ودالة التولد العشوائي

أكرم سالم محمد[1] و سعدون حسين عبدالله[2]

[1] قسم علوم الرياضيات، كلية العلوم، جامعة تكريت، تكريت، جمهورية العراق

[2] قسم علوم الحياة، كلية العلوم، جامعة الموصل، الموصل، جمهورية العراق

الملخص:

تم في هذا البحث تشفير الرسائل النصية الصريحة Plain Text Massage ثم فك الرسالة المشفرة وذلك بأستخدام معادلتين خطيتين مع دالة التولد العشوائي(Random Function) وهي دالة تولد أرقام عشوائية غير محددة .

المقدمة :

إن الحاجة للحفاظ على سرية الرسائل المنقولة أو المخزونة نالت اهتمام العديد من الباحثين وهنالك عدة طرق للحفاظ على سرية الرسائل أو البيانات منها استخدام وسائط لإرسال البيانات التي تكون غير قابل للاعتراض وبأستخدام هذه الوسائط سوف تكون كل الرسائل ذات سرية تامة.لكن اغلب الطرق لا تحقق هذا الهدف إلا إذا كانت الطريقة المستخدمة قوية جدا يصعب فك شفرتها وهذا يعتمد على استخدام أنظمة التشفير المعقدة التي يستخدم طرق عديدة لتشفير الرسالة وفك التشفير وهذا العلم يسمى بعلم التشفير[2].

في هذا البحث تم وضع معادلة واحدة لتشفير الرسالة ومعادلة أخرى لفك التشفير مع استخدام دالة التولد العشوائي للأرقام الصحيحة وبحجم الرسالة(عدد الأحرف الرسالة) بالتعامل مع الأحرف والرموز بنظامASCII[1] .

(*American Standard for Code Information Interchange*) ومختصره ASCII ، هي مجموعة رموز ونظام ترميز مبني على الألفابيتا اللاتينية بالشكل الذي تستخدم به في الإنجليزية الحديثة ولغات غرب أوروبية أخرى. من أكثر الاستخدامات شيوعا للنصوص المكتوبة ASCII تشتمل على استخدامها في أنظمة الحاسوب، كما تستخدم في أجهزة الاتصالات وأنظمة التحكم التي تتعامل مع نصوص.

و يعرّف نظام ASCII القياسي الرموز القابلة للطباعة الآتية ، مرتبة حسب قيمة ASCII الخاصة بها

```
 !"#$%&'()*+,-
٠١٢٣٤٥٦٧٨٩:;<=>؟
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
`abcdefghijklmnopqrstuvwxyz{|}~.
```

ASCII هو نظام ترميز من ٧ بت ، بمعنى أنه يستخدم قيمة مكونة من سبعة أرقام ثنائية (تتراوح بين ٠ و ١٢٧) لتمثيل الحروف والرموز.

الجانب النظري:

إن أي جملة تتكون من الحروف الكبيرة ("A"…..."Z") والحروف الصغيرة ("a"…..."z") والأرقام ("0"…..."9") و الرموز ("*"…..."%") وان كل ما سبق لها ما يقابلها من الأرقام الثابتة والممثلة بالنظام الأمريكي ASCII كما في الجدول(١).

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
0	0	NUL	16	10	DLE	32	20	(space)	48	30	0
1	1	SOH	17	11	DC1	33	21	!	49	31	1
2	2	STX	18	12	DC2	34	22	"	50	32	2
3	3	ETX	19	13	DC3	35	23	#	51	33	3
4	4	EOT	20	14	DC4	36	24	$	52	34	4
5	5	ENQ	21	15	NAK	37	25	%	53	35	5
6	6	ACK	22	16	SYN	38	26	&	54	36	6
7	7	BEL	23	17	ETB	39	27	'	55	37	7
8	8	BS	24	18	CAN	40	28	(	56	38	8
9	9	TAB	25	19	EM	41	29	)	57	39	9
10	A	LF	26	1A	SUB	42	2A	*	58	3A	:
11	B	VT	27	1B	ESC	43	2B	+	59	3B	;
12	C	FF	28	1C	FS	44	2C	,	60	3C	<
13	D	CR	29	1D	GS	45	2D	-	61	3D	=
14	E	SO	30	1E	RS	46	2E	.	62	3E	>
15	F	SI	31	1F	US	47	2F	/	63	3F	?

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
64	40	@	80	50	P	96	60	`	112	70	p
65	41	A	81	51	Q	97	61	a	113	71	q
66	42	B	82	52	R	98	62	b	114	72	r
67	43	C	83	53	S	99	63	c	115	73	s
68	44	D	84	54	T	100	64	d	116	74	t
69	45	E	85	55	U	101	65	e	117	75	u
70	46	F	86	56	V	102	66	f	118	76	v
71	47	G	87	57	W	103	67	g	119	77	w
72	48	H	88	58	X	104	68	h	120	78	x
73	49	I	89	59	Y	105	69	i	121	79	y
74	4A	J	90	5A	Z	106	6A	j	122	7A	z
75	4B	K	91	5B	[	107	6B	k	123	7B	{
76	4C	L	92	5C	\	108	6C	l	124	7C	|
77	4D	M	93	5D	]	109	6D	m	125	7D	}
78	4E	N	94	5E	^	110	6E	n	126	7E	~□
79	4F	O	95	5F	_	111	6F	o	127	7F	

الجدول (١): ASCII codes table Format of standard characters

إن الجملة المرسلة بين الطرفين المرسل والمستلم تكون غير محدودة ، ممكن أن تتكون الجملة من ثلاث كلمات أو ألف كلمة أو أكثر من ذلك أو اقل ليكن لدينا الرسالة البسيطة.

Dear Sir Ahmed:

نرى إن هذه الجملة تحتوي على الحروف الكبيرة والصغيرة والرموز ، تدخل هذه الجملة أو الرسالة إلى المصفوفة سواء أكانت مربعة أو غير مربعة وهذا يتعلق باتفاق الطرفين (المخولين) لتكن المصفوفة التي تتعامل معها مربعة ((ASZ(i,j)) حيث أن (i) هو عدد الصفوف و (j) عدد الأعمدة .

D	e	a r
	S	i r
A	h	m
E	d	:

((ASZ(i,j))

مصفوفة النص الصريح

ملاحظة: إذا كانت عدد حروف الرسالة أو الجملة غير مكملة للمصفوفة المربعة فنكمل بفراغات (Space) ويكون ذلك باتفاق من قبل الطرفين.

ملاحظة: إعطاء فراغ واحد أو أكثر للرسالة لا يؤثر على سير عملية التشفير وفكها.

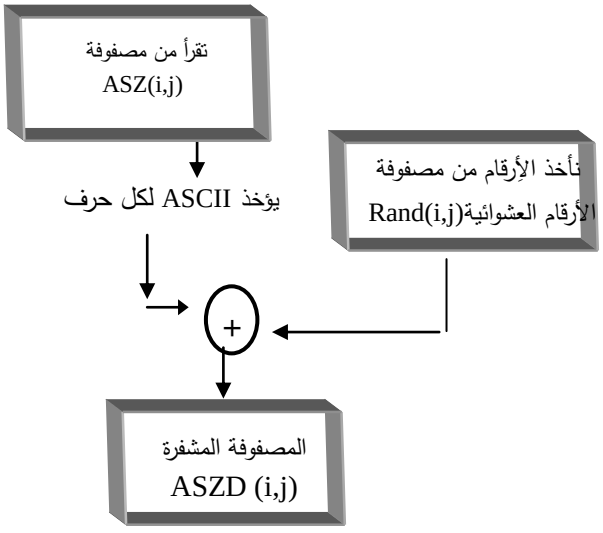
بالاعتماد على حجم (النص الصريح) يولد الدالة العشوائية أرقام عشوائية Rand(i,j) وأيضاً تكون هذه القيمة معلومة للطرفين المخولين (الشرعيين) ودالة التولد العشوائي يولد أرقام عشوائية غير محددة ولكنا نأخذ منها بقدر حجم المصفوفة (نص الصريح) وكذلك نفس الحالة مع المصفوفة المشفرة.بهذه الحالة نأخذ أول (16 رقم عشوائية) بحجم المصفوفة لتكن الدالة العشوائية ولدت الأرقام العشوائية الآتية:

5	11	3	9
2	3	8	10
4	1	0	3
19	0	45	83

Rand(i,j)

مصفوفة الأرقام العشوائية

فتكون معادلة تشفير الرسالة بالمخطط (١)



مخطط(١)

يكون ناتج جمع بين ASCII لحرف النص الصريح مع رقم التولد العشوائي ضمن حدود مجموع الأحرف الكبيرة والصغيرة والرموز ["127"…."0"].

نأخذ أول حرف من النص الصريح في المصفوفة ((ASZ(1,1)) (D) مع رقم أول رقم في مصفوفة التولد العشوائي(5) (Rand (1,1) وهكذا البقية…

إن معادلة التشفير يكون:

ASZD (i,j) = (ASCII (ASZ (i,j)) + Rand (i,j)) mod 127……(1)

فيكون معادلة تحويل حرف (D) من مصفوفة النص الصريح(ASZ (i,j

ASZD(1,1) = (ASCII (D) + Rand (1,1))

mod 127= (68 + 5) mod 127= (73) mod 127 = 73

نرى إن ناتج عملية التشفير (معادلة التشفير) أنتج رقم (73) وهذا ما يقابلها (J) في الجدول (ASCII) وهكذا يكون تشفير بقية الرسالة وبنفس الطريقة السابقة، فيكون ناتج المصفوفة المشفرة(ASZD(i,j بالشكل الآتي:

J	P	d	@
B	V	q	?
D	B	h	p
x	d	?	e

ASZD(i,j)

مصفوفة النص المشفرة

يقرأ المصفوفة فيكون الناتج: Jpd@BVq?DBhpxd?e

أما فك الشفرة إلى ما يقابلها من النص الصريح هذا يحدث في الطرف الأخر وهو يقوم بدوره بإدخال النص المشفر إلى مصفوفة بنفس الأبعاد ، أما دالة التولد العشوائي فيكون متفق عليه من الطرفين المخولين:

5	11	3	9
2	3	8	
10			
4	1	0	3

Rand(i,j)

مصفوفة الأرقام العشوائية

J	P	d	@
B	V	q	?
D	B	h	p
x	d	?	e

ASZD(i,j)

مصفوفة النص المشفرة

أما معادلة فك الشفرة:

ASZ(i,j) = (ASCII (ASZD (i,j) + 127) – Rand (i,j)) mod 127……(2)

نأخذ أول حرف من مصفوفة النص المشفر ((ASZD(1,1)) (J) مع أول رقم في مصفوفة دالة التولد العشوائي ((٥) Rand)

ASZ (1,1) = (ASCII (ASZD(1,1)) + 127) – Rand (1,1) mod 127 = (ASCII(J) + 127) – (5)) mod 127= (73 + 127) – 5) mod 127 = 195 mod127= (68) ="D"

وهكذا سوف يفك الشفرة بقية الرسالة ويظهر النص الصريح لدى الطرف الأخر:

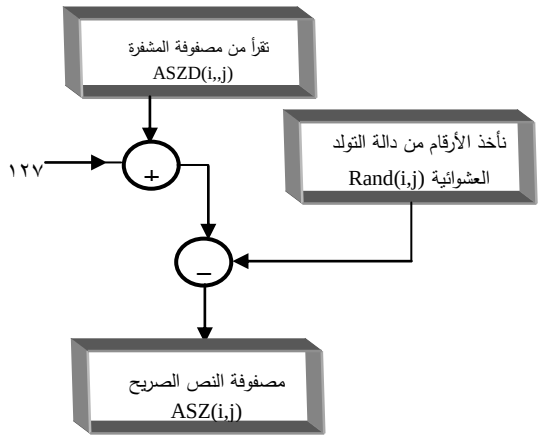
Dear Sir Ahmed:

D	e	a	r
	S	i	r
A	h	m	
e	d	:	

ASZ(i,j)

مصفوفة النص الصريح

فيكون معادلة فك الشفرة بالمخطط (٢).



مخطط(٢)

الجانب التطبيقي (العملي):

لكي نتعمق في شرح البحث بشكل عملي وبشكل أدق ليكن الرسالة(النص الصريح) من الطرف الأول هي:

Monitor: (Known as Video Display Unit VDU) Used for outputting information in an Understandable format for human's It is Similar to television's screen but in sharper Picture It display the work being by CPU.

يدخل النص الصريح إلى مصفوفة مربعة وعلى ضوء حجم المصفوفة يولد دالة التولد العشوائي عدد الأرقام أو حجم المصفوفة ((Rand (i,j).

نأخذ على سبيل المثال أول سطر من الرسالة:

Monitor: (Known as Video Display Unit VDU)

M	o	n	i	t	e	r
:	(	K	n	o	w	n
▼	a	s		V	i	d
e	o	▼	D	i	s	p
l	a	y	▼	U	n	i
t	▼	V	D	U	)	↵
▼	▼	▼	▼	▼	▼	▼

((ASZ(i,j))

حيث أن المصفوفة تكون (7*7) لان عدد حروف أو مجموع الأحرف في السطر الأول من النص الصريح هو (42) فاقرب مربع للمصفوفة (7*7) أما الباقي فيكمل بالفراغات (▼) حسب الأتفاق.

أما كيف نعرف عدد حروف الرسالة فهذا يعتمد على عداد (Pointer)(P)أخر حرف في الرسالة حيث انه عداد يعد من بداية الرسالة إلى أخر حرف من الرسالة ويبن حجم الرسالة المرسلة.

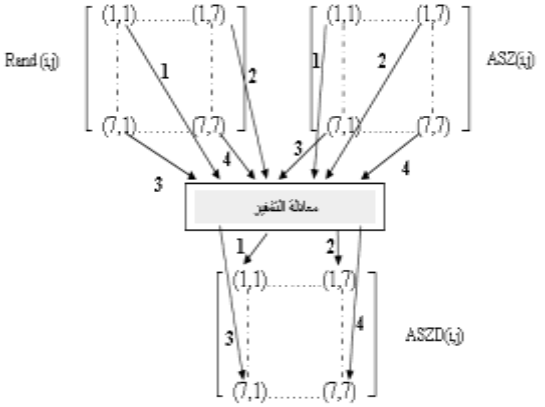
10	1	3	7	5	11	12
10	13	15	12	0	3	22
17	15	0	1	30	4	5
8	4	2	1	0	7	7
0	3	0	4	4	4	4
2	0	7	7	0	3	8
3	9	7	16	29	32	14

Rand (i,j)

وعلى غرار العداد (P) تكون المصفوفة مصفوفة النص الصريح وكذلك نفس العملية تحدث في الطرف الأخر (المستلم).

في المثال السابق كان (P=42) فاخترنا مصفوفة (7*7 = 49) لتكوين مصفوفة النص المشفر وتم تكملة المصفوفة بالفراغات (Space) لتكوين مصفوفة مربعة وان إعطاء (Space) لا يؤثر على سير عمل العملية وبالمقابل هذا اتفاق بين الطرفي المخولين.

في هذه الحالة نأخذ الحرف الأول من المصفوفة ((ASZ(1,1)) مع أول رقم عشوائي مولد في مصفوفة التولد العشوائي ((Rand (1,1)) يدخل إلى معادلة التشفير ويشفر ويضاف إلى بداية مصفوفة التشفير ((ASZD(1,1)) وهكذا ((ASZ(1,2)) مع ((Rand(1,2)) ويضاف إلى ((ASZD(1,2)) وهكذا أخر حرف ((ASZ(7,7)) مع أخر رقم مولد عشوائياً ((7,7)) Rand) ويضاف إلى ((ASZD(7,7)).كما في المخطط(٣).



مخطط (٣)

في المخطط (٣) تم توضيح الجوانب الأربعة للمصفوفة

ASZ (1,1) & Rand (1,1) ⟹ (معادلة١) = (ASZD(1,1))

ASZ (1,7) & Rand (1,7) ⟹ (معادلة ١) = (ASZD(1,7))

ASZ (7,1) & Rand (7,1) ⟹ (معادلة١) = (ASZD(7,1))

ASZ (7,7) & Rand (7,7) ⟹ (معادلة١) = (ASZD(7,7))

ASZD (i,j) := (ASCII(ASZ(i,j))+ Rand(i,j)) mod 127….(١)

ASZ (1,1) = M , Rand (1,1) = 10

ASZD(1,1) = (ASCII (ASZ(1,1) + Rand (1,1) mod 127= (77 + 10) mod 127= 87 = "W"

ASZD(1,7) = (ASCII (ASZ(1,7))+ Rand (1,7) mod 127= (ASCII (r) + (١٢)) mod 127= (114 + ١٢)mod 127=126

mod 127 =126 = "~" = (ASCII (Space) + (6) mod 127

ASZD(7,1)= (ASCII (ASZ(7,1))+ Rand (7,1) mod 127= (32 + 3) mod 127 = 35 = "#"

ASZD(7,7) = (ASCII (ASZ(7,7)) + Rand (7,7) mod 127= (ASCII (Space) + (91) mod 127 = (32 + 14) = 46="."

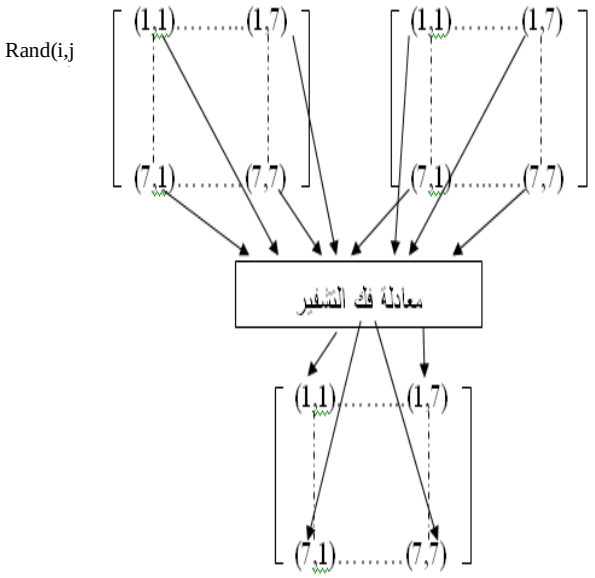
W	p	q	p	y	p	~
D	S	Z	z	o	z	1
P	s	!	t	m	i	m
S	"	E	i	z	w	I
d	y	$	Y	r	w	v
a	-	]	K	U	,	)
#	(	'	0	=	@	.

ASZ(i,j)

فيكون الرسالة المشفرة للسطر الأول من الرسالة:

Wpqpyp~DSZzoz1ps!tmimS"EizwIdy$Yrwva-]KU,)#('0=@.

أما الطرف الأخر يفك الشفرة باستخدام معادلة الشفرة(١) ، وبنفس عملية التشفير يكون عملية فك الشفرة فيؤخذ الحرف الأول من مصفوفة النص المشفرة ((ASZD(1,1) مع أول رقم عشوائي مولد في مصفوفة التولد العشوائي ((Rand (1,1) (وهي نفس الدالة التي استخدمت في عملية التشفير) يدخل الى معادلة فك الشفرة(٢) ويسترجع إلى بداية المصفوفة النص الصريح ASZ(1,1) وهكذا ASZD(1,2) مع ((Rand (1,2) .. وهكذا أخر حرف يفك الشفرة ASZD(7,7) مع أخر رقم مولد عشوائياً ((Rand (7,7) ويضاف إلى مصفوفة النص الصريح ASZ(7,7) كما في المخطط (٤).



مخطط(٤)

ASZD (1,1) & Rand (1,1) ⟹ (معادلة٢) = (ASZ (1,1))

ASZD (1,7) & Rand (1,7) ⟹ (معادلة٢) = (ASZ (1,7))

ASZD (7,1) & Rand (7,1) ⟹ (معادلة٢) = (ASZ (7,1))

ASZD (7,7) & Rand (7,7) ⟹ (معادلة٢) = (ASZ (7,7))

ASZ (i,j):=(ASCII(ASZD(i,j)+127) – Rand(i,j)) mod 127…… (٢)

ASZD (1,1) = W , Rand (1,1) = 10

ASZ (1,1) = (ASCII (ASZD(1,1) + 127) – Rand (1,1)) mod 127 (ASCII (w) + 127) – 10) mod 127= (87 + 127)-10 = 77 = "M"

ASZ (1,7) = (ASCII (ASZD(1,7) + 127) – Rand (1,7)) mod 127 = (ASCII (~) + 127) - 12) mod 127 = (126 + 127) – 12) mod 127 =(241) mod 127 = 114 = "r"

ASZ (7,1) = (ASCII (ASZD(7,1)+127) – Rand (7,1)) mod 127 = (ASCII (#) + 127) – 3) mod 127

= (35 + 127) – 3) mod 127 = 32 = Space(▼)

ASZ (7,7) = (ASCII (ASZD(7,7)+ 127) – Rand (7,7) mod 127

ASZ (7,7) = (ASCII (ASZD(7,7)+ 127) – Rand (7,7) mod 127

= (ASCII (.) + 127) – 14) mod 127= (46 + 127) –14) mod 127 =32 = Space(▼)

وهكذا بقية فك الرسالة المشفرة فتظهر الرسالة الصريحة:

Monitor: (Known as Video Display Unit VDU)

البرنامج:

لكي نكتب برنامج بلغة Mat lab لتشفير الرسالة وبرنامج لفك الرسالة المشفرة سنرمز لاسم الموصوفة التي وضعنا فيها النص الصريح والتي سمنينا ها ASZ بـ M وسنرمز لمصفوفة الأرقام العشوائية والتي سميناها Rand بـ N وسنرمز للمصفوفة التي توضع فيها الرسالة المشفرة والتي سميناها ASZD بـ D .

برنامج تشفير الرسالة:

يؤخذ ASCII للمفصوفة (M) = [ ] ASCII (M)

نولد المصفوفة عشوائياً [ ] = N

D = (ASCII (M) + N) mod 127

Z = D'

L = Z(:)

Q = L'

برنامج فك شفرة الرسالة:

يؤخذ ASCII للمفصوفة (D) = [ ] ASCII (D)

نولد المصفوفة عشوائياً [ ] = N

M = (ASCII (P) + 127) – N) mod 127

X = M'

Y = X(:)

W = Y'

الهدف من البحث:

الهدف من هذا البحث هو نقل المعلومات بين الأطراف المخولة بسرية تامة وصعوبة كسر شفرة هذه المعلومات من قبل الطرف الثالث(المتطفلين) الطرف غير المخول.

المحاسن والمساوئ:

من محاسن هذه الطريقة هي:

١. صعوبة إيجاد مصفوفة الأرقام العشوائية من قبل المتطفلين مما يصعب ذلك فك شفرة الرسالة المرسلة.

٢. يجب على المتطفلين معرفة معادلة التشفير(١) ومعادلة فك الشفرة(٢).

٣. يجب على المتطفلين معرفة سعة المصفوفة المستخدمة.

ومن مساوئها صعوبة تذكر المصفوفة العشوائية.

المصادر :

1. W.Stalling, Network Security Essentials, 2000.
2. W.Hamadani, Encryption system, 1997 .
3. D.E.R.Dening, Cryptography and Data Security, Purdue University,1982.
4. Hoffmam L.J,Modern for computer security .1977.
5. Liu.L.,"On linear Queries in statistical Data base ",1980.

Encryption Text Massage by used Linear Equation and Random function

Akram salim Mohammed[1] and Sadoon Hussein Abdullah[2]

[1] Department of Mathematic, Collage of Secince, University of Tikrit, Tikrit, Iraq
[2] Department of Biology, Collage of Secince, University of Mousl, Mousl, Iraq

Abstract:

The plain text massage encryption by used linear equation and random function ,which the text massage input to matrices and by used quation as a key with random function, we another linear equation with the same random function as a key deciphering process we go back plain text massage.