مقدمة:

يعتبر البريد الالكتروني حاليا بديلا لإرسال الخطابات من خلال البريد العادي. و البريد الالكتروني وسيلة سريعة للتواصل لكن بطبيعة الحال لا توجد اظرف لحماية الرسائل بل ان ارسال رسالة بالبريد الالكتروني اشبه بإرسال رسالة عبر البريد العادي بدون ظرف لذلك من يرد ارسال رسالة سرية او شخصية عبر البريد الالكتروني سيحتاج طرق اخرى لحمايتها . تتمثل احدى هذه الطرق في التشفير حيث اذا تم اعتراض الرسالة من طرف شخص غير المستقبل المراد لن يستطيع معرفة المحتوى الحقيقي لهذه الرسالة و هناك عدة طرق لتشفير رسالة ما منها البسيط و منها المعقد (نتحدث هنا عن التشفير الكلاسيكي اما التشفير الحديث فله حديث اخر) وسوف تجد في الصفحات التالية بعضا من اهم طرق التشفير الكلاسيكي كما سنشدد باننا ذكرنا مبادئ عمل هذه الطرق فقط مع بعض الامثلة ليتمكن القارئ من اخذ فكرة عن التشفير الكلاسيكي على الاقل.

شفرة قيصر: تعتبر من ابسط طرق التشفير و ذلك لسهولة فكها. حيث يتم استبدال كل حرف من النص الاصلي بالحرف الثالث الذي يليه في الابجدية او ازاحة بمقدار ثلاثة احرف . وهذا يعني ان الحرف A يصبح D و الحرف B يصبح E و هكذا الى الاحرف X ، Y و Z حيث تصبح هذه الاحرف A ، B و C على الترتيب .

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

نشفر الكلمة ACT

الكلمة بعد التشفير تصبح DFW يمكن تشفير الكلمة بمفتاح اخر لكن لن تكون الشفرة المستعملة هي شفرة قيصر(يمكن استعمال المفاتيح او ازاحة من 1 الى 25)

- نشفر الكلمة BIG

الكلمة بعد التشفير ELJ

- لفك التشفير نقوم بالعملية العكسية

النص المشفر هو DFW و منه النص الاصلي هو ACT

بالنسبة للمثال الثاني النص المشفر هو ELJ و بنفس الطريقة النص الاصلي هو BIG

شفرة الاستبدال البسيط:

حيث يتم استبدال كل حرف من النص الاصلي بحرف اخر وفق جدول معين . وتكمن صعوبة استعمالها في حفظ جدول التشفير لان ترتيب الحروف يكون عشوائيا كما هو مبين في الجدول التالي

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k	u	f	s	o	c	q	a	p	x	w	e	m	v	g	b	d	y	t	z	n	j	h	l	i	r

نشفر الكلمة the cipher حيث نستبدل كل حرف منها بالحرف الذي يقابله في الجدول فيصبح لدينا zao fpbaoy . لفك التشفير نقوم بالعملية العكسية

لتسهيل استعمال هذه الطريقة نستعمل جملة التشفير

مثال : نستخدم جملة التشفير التالية

Cryptography itself can be divided into two branches

نقوم بترتيب احرف الجملة تحت احرف الابجدية و بدون تكرار . حيث ترتب الاحرف الباقية حسب الابجدية

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
c	r	y	p	t	o	g	a	h	i	s	e	l	f	n	b	d	v	w	j	k	m	q	u	x	z

الاحصاء اللغوي (التحليل الاحصائي) : عند تشفير نص ما بشفرة قيصر او الاستبدال البسيط يحل محل كل حرف من النص الاصلي حرف واحد و وحيد لهذا يكون معدل تكرار حرف التشفير هو نفس معدل تكرار حرف النص الاصلي . لذلك عندما يعترض احد ما الرسالة يمكنه استخدام الاحصاء اللغوي لمعرفة محتوى الرسالة بدون معرفة المفتاح لان كل لغة من اللغات تمتاز بحروف تتكرر اكثر من غيرها. تكمن الطريقة في حساب عدد المرات التي ظهر فيها كل حرف في النص المشفر ثم نلاحظ الحرف الاكثر تكرار في النص المشفر و نعتبره يمثل الحرف الاكثر تكرارا في اللغة المعنية و هكذا مع باقي الحروف

في اللغة الانجليزية الحرف e هو الحرف الاكثر تكرارا من غيره ثم يليه الحرف t ثم a

ثم o ثم i ثم..... حسب الجدول التالي :

الحرف	% النسبة	الحرف	% النسبة
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.2	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.0
H	6.1	U	2.8
I	7.0	V	1.0
J	0.1	W	2.4
K	0.8	X	2.0
L	4.0	Y	0.1
M	2.4	Z	0.1

وبهذه الطريقة اصبحت شفرات الاستبدال البسيط لا فائدة منها تقريبا . لذلك نلجأ الى طرق اكثر تعقيدا منها :

الترميز المتناغم:

في هذا النوع من التشفير يتم اعطاء رقم واحد معين لكل حرف الا الحروف الستة الاكثر تكرارا حيث يتم التعبير عنها برقمين مختلفين كما يظهر الجدول التالي :

A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N
15	02	05	23	30	24	16	07	00	01	14	08	03	04	11	31

N	O	O	P	Q	R	R	S	T	T	U	V	W	X	Y	Z
09	10	13	20	22	19	18	17	06	12	29	25	28	21	26	27

نشفر الجملة التالية بالجدول السابق

GOOD BROOMS SWEEP CLEAN

00 10 13 30 05 19 13 13 11 17 17 28 24 16 20 23 04 24 02 09

لا يمكننا الاستفادة من التحليل الإحصائي (الاحصاء اللغوي). و هذا ما يصعب الامور الا انه مع الكثير من الجهد و الحظ يمكن ايجاد ثغرات في هذا النوع من التشفير و يمكن فكه اذا كان النص طويلا بما فيه الكفاية

يمكنك المحاولة في النص الاتي الموجود في كتاب علم التشفير لشون ميرفي :

24 29 25 00 20 01 12 27 10 01 12 06 29 07 08

31 29 05 07 14 20 26 01 04 26 20 06 28 29 28

05 04 31 28 18 30 01 31 21 26 25 24 26 12 29

04 26 31 18 23 15 21 25 26 31 28 26 30 10 01

21 07 31 18 16 12 12 28 18 13 05 08 21 24 30

20 21 25 24 21 30 10 18 17 19 31 28 18 05 12

31 05 24 09 21 08 26 05 08 14 12 17 27 07 04

18 20 08 12 05 25 04 13 27 31 12 28 18 19 05

24 31 12 28 05 12 12 28 18 08 31 01 12 21 08

31 21 24 08 05 23 18 19 10 01 12 12 26 23 15

26 05 25 08 21 31 21 08 07 29 12 08 29 26 05

08 14 12 17 21 04 26 25 12 21 19 14 31 28 18

30 17 30 27 10 01 20 10 26 31 12 26 20 08 21

25 12 28 18 30 10 05 21 07 12 18 16 31 30 01

12 21 18 25 24 26 01 07 04 10 27 24 09 05 23

26 13 29 31 28 11 18 20 14 21 15 30 29 20 12

01 07 31 19 17 23 12 28 26 24 23 14 30 12 01

07 01 10 14 08 12 21 25 19 01 24 31 13 20 18

05 09 21 07 00 24 21 30 28 26 20 08 27 08 27

05 10 10 14 21 07 11 29 10 11 18 08 01 15 21

16 31 27 23 26 17 19 08 24 21 18 25 12 21 19

21 24 20 18 01 08 17 07 21 25 00 05 25 04 21

07 08 30 21 20 18 04 00 27 26 08 08 06 17 23

09 21 07 12 28 21 08 24 17 25 31 18 16 31 06

26 25 17 12 18 31 28 01 12 31 28 26 24 20 14

30 12 17 00 20 01 30 28 21 24 12 18 05 15 18

15 30 10 29 14 18 04 01 31 13 10 26 12 24 28

10 26 14 30 05 23 09 21 07 24 10 27 04 26 04

30 26 17 30 10 26 06 21 12 28 05 07 01 30 31

21 31 27 04 18 19 17 23 24 20 17 08 08 06 17

20 04 30 27 03 03 10 26 08

التشفير متعدد الاحرف :

لاحظنا في طرق التشفير السابقة انه يتم تمثيل كل حرف من النص الاصلي بحرف واحد فقط مما جعل هذه الطرق ضعيفة للغاية . الا ان في التشفير متعدد الاحرف يمكن ان يمثل حرف النص الاصلي بعدة حروف في النص المشفر، و من اشهر الطرق :

- شفرة فيجنر بكل انواعها
- شفرة بلايفير
- اسطوانة جيفيرسون
- شفرة هيل

1 - شفرة فيجنر البسيطة :

تتمثل في استعمال عدة مفاتيح مرتبة حيث يتم تشفير الحرف الاول من النص بالمفتاح الاول و الحرف الثاني بالمفتاح الثاني و هكذا الى نهاية النص الاصلي . اما بالنسبة للمفاتيح عندما تنتهي نعيدها مرة اخرى بنفس الترتيب . وسيتضح ذلك في المثال الاتي :

لدينا المفتاح التالي :

3 5 12 1

نريد تشفير الجملة التالية بهذا المفتاح

Every word has a vowel in it

الجدول التالي يمثل رقم كل حرف في الابجدية

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

الحرف الاول في الجملة يشفر بالرقم 3 و الثاني بالرقم 5 و الثالث بالرقم 12 و الرابع بالرقم 1 ثم نعود الى الرقم 3 ثم 5 ثم ..... حتى ينتهي النص الاصلي

E + 3 = h

V + 5 = 26 (mode 26) =a

(mode 26) تعني باقي القسمة على 26 و تستعمل عند الحصول على نتيجة اكبر من

25

e + 12 = q

وهكذا حتى ينتهي النص الاصلي حيث تكون النتيجة كما هو مبين في الجدول

النص الاصلي	e	v	e	r	y	w	o	r	d	h	a	s	a	v	o	w	e	l	i	n	i	t
المفتاح	3	5	12	1	3	5	12	1	3	5	12	1	3	5	12	1	3	5	12	1	3	5
النص المشفر	h	a	q	s	b	b	a	s	g	m	m	t	d	a	a	x	h	q	u	o	l	y

النص المشفر:

Haqs bbas gmmt daax hquo ly

لفك التشفير نقوم بعملية طرح المفاتيح بالترتيب كما فعلنا في عملية الجمع فنحصل على النص الاصلي

- بدل استعمال الارقام كمفاتيح نستعمل كلمات يسهل حفظها ثم نعوض كل حرف من هذه الكلمة بالرقم الذي يمثله

عندما نستعمل الكلمة التالية:

Code

يكون المفتاح هو:

2 14 3 4

2 – شفرة فيجنر الكاملة :

نختار كلمة المفتاح مثل شفرة فيجنر البسيطة الا اننا نستعمل جدول فيجنر للتشفير و تكون عملية التشفير بملاحظة حرف التقاطع بين حرف النص الاصلي و حرف كلمة المفتاح و سيتضح ذلك في المثال

نريد تشفير الجملة التالية

Meet me tonight

و نستعمل كلمة المفتاح

Four

قبل البدء في التشفير يجب وضع جدول فيجنر بالقرب منا و هو الجدول الموجود اسفله .

- نلاحظ تقاطع الحرف الاول من النص الاصلي مع الحرف الاول من كلمة المفتاح ثم الحرف الثاني من النص الاصلي مع الحرف الثاني من كلمة المفتاح و هكذا مع تكرار كلمة المفتاح كلما انتهت .

	حروف النص الاصلي																								
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

الحروف الحمراء تمثل حروف النص الاصلي و الحروف الزرقاء تمثل حروف كلمة المفتاح و هذا للفهم فقط

تكون النتيجة النهائية كالتالي:

النص الاصلي	m	e	e	t	m	e	t	o	n	i	g	h	t
المفتاح	f	o	u	r	f	o	u	r	f	o	u	r	f
النص المشفر	r	s	y	k	r	s	n	f	s	w	a	y	y

النص المشفر:

Rsyk rsnf sway y

- كلما كانت كلمة المفتاح اطول كانت الشفرة اكثر امانا

3- شفرة فيجنر طويلة المفتاح :

في هذا النوع من شفرة فيجنر يكون المفتاح او جملة المفتاح اطول من النص الاصلي مما يجعلها صعبة التطبيق في حالة النصوص الطويلة

- نشفر الجملة السابقة

Meet me tonight

و لتكن جملة المفتاح

Codes and ciphers

نقوم بعملية الجمع مثل شفرة فيجنر البسيطة فينتج

النص الاصلي	m	e	e	t	m	e	t	o	n	i	g	h	t
المفتاح	c	o	d	e	s	a	n	d	c	i	p	h	e
النص المشفر	o	s	h	x	e	e	g	r	p	q	v	o	x

النص المشفر:

Oshx eegr pqvo x

4 – شفرة فيجنر تلقائية المفتاح :

نختار كلمة المفتاح ونقوم بنفس الطريقة في شفرة فيجنر البسيطة الا انه عند انتهاء كلمة المفتاح نقوم بإدخال النص الاصلي كمفتاح

- نريد تشفير هذه الجملة بهذه الطريقة

we can encode a simple message

و لتكن كلمة المفتاح هي

Luck

النص الاصلي	w	e	c	a	n	e	n	c	o	d	e	a	s	i	m	p	l	e	m	e	s	s	a	g	e
المفتاح	l	u	c	k	w	e	c	a	n	e	n	c	o	d	e	a	s	i	m	p	l	e	m	e	s
النص المشفر	h	y	e	k	j	i	p	c	b	h	r	c	g	l	q	p	d	m	y	t	d	w	m	k	w

النص المشفر

Hyek jipc bhrc glqp dmyt dwmk w

- عند فك التشفير نقوم بالعملية العكسية الا انه عند انتهاء كلمة المفتاح نقوم بفك ما بقي بالنص الاصلي الذي نتج و هكذا الى ان نصل الى نهاية النص

- تعد شفرة فيجنر بكل انواعها من اقوى طرق التشفير الكلاسيكي الا انه تم كسرها بواسطة (باباج و كاسيكي) في منتصف القرن التاسع عشر

5 – شفرة بلايفير :

نستعمل في هذه الشفرة جدولا يتكون من 25 خانة حيث يوضع في كل خانة حرف من حروف الابجدية الا الحرفين I و J في خانة واحدة كما هو مبين في الجدول

H	B	G	D	N
A	Q	I/J	W	R
E	U	C	L	O
M	V	P	X	S
Z	K	Y	T	F

قبل البدء في التشفير يجب علينا :

- استبدال كل حرف **I** بحرف **J** في النص الاصلي

- كتابة الرسالة في ازواج من الاحرف

- يدرج الحرف Z بين الاحرف المتطابقة

- اضافة الحرف Z في الاخير اذا كان عدد حروف النص فرديا

اما طريقة عمل الشفرة تحتاج الى التركيز و هي كالتالي :

- اذا وقع الحرفان في نفس السطر يحل محل كل حرف الحرف الذي الى يمينه

- اذا وقع الحرفان في نفس العمود يحل محل كل حرف الحرف الذي تحته مباشرة

- غير ذلك يحل محل الحرف الاول الحرف الذي ينتج من تقاطع سطر الحرف الاول و عمود الحرف الثاني و يحل محل الحرف الثاني الحرف الذي يقع في الركن الرابع من المستطيل الذي تشكل من الحروف الثلاثة السابقة

نشفر النص التالي بالجدول السابق

Gifford was still a youth

نقوم بكتابتها في ازواج و نحد بين الاحرف المتطابقة بالحرف Z

GJ FZ FO RD WA SZ ST JL LA YO UT HZ

H	B	G	D	N
A	Q	I/J	W	R
E	U	C	L	O
M	V	P	X	S
Z	K	Y	T	F

- نلاحظ ان G وJ يقعان في العمود نفسه لهذا يمثل الحرف G بالحرف الذي تحته وهو J و يمثل الحرف J بالحرف الذي تحته وهو C

- الحرفان F وZ في نفس السطر اذا الحرف F يمثل بالحرف الذي على يمينه و هو Z و الحرف Z يمثل بالحرف الذي على يمينه وهو K حيث تكون النتيجة النهائية

JC ZK NS WN RQ MF XF WC EW FC LK AH

عند فك التشفير نعكس الاتجاهات فقط حيث:

- اذا وقع الحرفان في نفس العمود الحرف الاصلي لكل حرف هو الحرف الذي فوقه

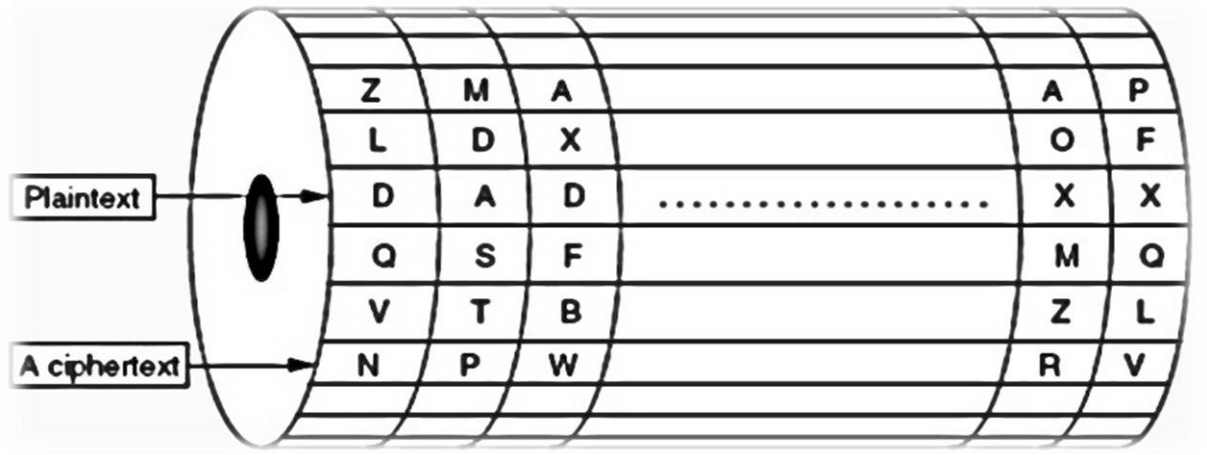
- اذا وقع الحرفان في نفس السطر الحرف الاصلي لكل حرف هو الحرف الذي على يساره

- غير ذلك بنفس الطريقة عند تشفير الحرفين

6- اسطوانة جيفرسون:

نسبة الى مخترعها (توماس جيفرسون) . تتكون هذه الاسطوانة من 36 عجلة بجانب بعضها البعض و في كل عجلة 26 حرف (حروف الابجدية الانجليزية) بالإجمال لدينا

26 سطر في كل سطر 36 حرف. و هذه صورة توضيحية لها :



صورة لأسطوانة جيفرسون في الواقع

- عندما نريد تشفير نص ما بهذا الجهاز نقوم بتحريك العجلات بحيث نكتب هذا النص في احد السطور مما يبقي 25 سطر للتشفير. نقوم بإرسال احد السطور ال25 الى المستقبل اما بالنسبة لفك التشفير نقوم بتحريك العجلات بحيث نكتب النص المشفر ثم ننظر الى السطور الاخرى لنجد النص الاصلي من بينها

7- شفرة هيل:

سميت بهذا الاسم نسبة الى مخترعها (لستر هيل). تعتمد هذه الشفرة على الجبر الخطي حيث يجب عليك معرفة اساسيات التعامل بالمصفوفات لكي تستطيع العمل بها.

يوجد عدة انواع من هذه الشفرة

2-HILL CIPHER تكون مصفوفة المفتاح 2*2

3-HILL CIPHER تكون مصفوفة المفتاح 3*3

n-HILL CIPHER بصفة عامة حيث تكون مصفوفة المفتاح n*n

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

نختار مصفوفة المفتاح و لتكن:

$$\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$$

نريد تشفير الكلمة التالية بهذه المصفوفة

GOOD

يتم تحويلها الى مصفوفة

$$\begin{bmatrix} G & O \\ O & D \end{bmatrix}$$

ثم نعوض كل حرف بالرقم الذي يقابله في الجدول فتصبح لدينا المصفوفة التالية

$$\begin{bmatrix} 6 & 14 \\ 14 & 3 \end{bmatrix}$$

ثم نضرب مصفوفة المفتاح في مصفوفة النص الاصلي

$$\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}\begin{bmatrix} 6 & 14 \\ 14 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 5 \\ 20 & 22 \end{bmatrix} mode\ 26$$

نعوض كل رقم بالحرف الذي يقابله في الجدول فينتج النص المشفر التالي

AUFW

لفك التشفير نقوم بإيجاد معكوس مصفوفة المفتاح و ضربها في مصفوفة النص المشفر

- بما ان :

$$det\begin{bmatrix}2 & 1\\3 & 2\end{bmatrix} = 2 * 2 - 1 * 3 = 1$$

فان المصفوفة لها معكوس و بالطبع هي كذلك. لأنه في حالة مصفوفة ليس لها معكوس لن يستطيع المستقبل معرفة محتوى الرسالة

ايجاد معكوس المصفوفة 2*2 ليس صعبا و هذا ما قصدنا به معرفة أساسيات التعامل بالمصفوفات

معكوس مصفوفة المفتاح هو:

$$\begin{bmatrix}2 & -1\\-3 & 2\end{bmatrix}$$

نقوم بضربها في مصفوفة النص المشفر

$$\begin{bmatrix}2 & -1\\-3 & 2\end{bmatrix}\begin{bmatrix}0 & 5\\20 & 22\end{bmatrix} = \begin{bmatrix}6 & 14\\14 & 3\end{bmatrix} mode\ 26$$

فتنتج مصفوفة النص الاصلي

$$\begin{bmatrix}G & O\\O & D\end{bmatrix}$$

نأخذ العمود الاول ثم الثاني لينتج النص :

GOOD

- لاحظنا في الطرق السابقة انه يحل محل الحرف في النص الاصلي حرف واحد او اكثر الا انه هناك طرق اخرى يتم فيها تبديل مواقع الحروف بطريقة معينة مما يجعل النص غير مفهوم و هو ما يسمى بالتشفير التبادلي

التشفير التبادلي:

هناك عدة طرق نذكر الاشهر منها :

الطريقة 1 : (the rail fence cipher)

في هذه الطريقة نقوم بكتابة النص الاصلي في خطوط متعرجة حيث كل خط يحتوي على حرفين او ثلاثة احرف ثم نقوم بكتابة الخطوط المستقيمة فنحصل على نص مشفر و سيتضح ذلك في المثال

نشفر العبارة التالية :

GO HOME NOW Z

اضفنا الحرف الاخير ليصبح عدد الحروف زوجيا

نقوم بكتابتها في خطوط متعرجة حيث كل خط يحتوي على حرفين

G H M N W

O O E O Z

نقوم الان بكتابة السطر الاول ثم الثاني لينتج النص المشفر التالي

GHMN WOOE OZ

لفك التشفير نقوم بقسمة النص المشفر الى نصفين

GHMNW OOEOZ

نأخذ الحرف الاول من الجهة اليسرى ثم الحرف الاول من الجهة اليمنى ثم الثاني من اليسرى ثم الثاني من اليمنى و هكذا حتى ينتهي النص

GO HOME NOW Z

الطريقة الثانية : (المسار الملتوي) (the twisted path cipher) :

نقوم بكتابة النص الاصلي في جدول به اربعة اسطر و خمسة اعمدة بعدها نأخذ العمود الاخير من الاسفل الى الاعلى ثم الذي بعده من الاعلى الى الاسفل و هكذا

- نشفر النص التالي بهذه الطريقة :

MEET ME THURSDAY NIGHT

M	E	E	T	M
E	T	H	U	R
S	D	A	Y	N
I	G	H	T	X

اضفنا الحرف X ليكتمل الجدول و نبدأ منه صعودا ثم نزولا ثم ..... فينتج النص المشفر التالي :

XNRM TUYT HAHE ETDG ISEM

- يمكن ايضا اتباع مسار حلزوني ابتداء من الحرف H ثم U ثم Y ثم ..... لينتج النص المشفر التالي :

HUYA DTEE TMRN XTHG ISEM

الطريقة الثالثة: (التشفير باستعمال المفتاح)

نختار المفتاح 5 لتشفير النص السابق حيث نقوم بتقسيم النص السابق الى 4 اسطر كل سطر يحتوي على 5 احرف ثم نقوم بكتابة العمود الاول ثم الثاني ثم .....

M	E	E	T	M
E	T	H	U	R
S	D	A	Y	N
I	G	H	T	X

النص المشفر :

MESI ETDG EHAH TUYT MRNX

- يمكننا اضافة مفتاح يتكون من 5 ارقام لتحديد ترتيب الاعمدة

نستخدم المفتاح 25143

2	5	1	4	3
M	E	E	T	M
E	T	H	U	R
S	D	A	Y	N
I	G	H	T	X

اذن نبدأ بالعمود الثالث ثم الاول ثم .... فينتج النص المشفر التالي :

EHAH MESI MRNX TUYT ETDG

بالنسبة لفك التشفير نقوم بقسمة عدد احرف النص المشفر على المفتاح في مثالنا يكون الناتج 4 اذن نكتب النص المشفر في جدول له 4 اعمدة حيث ينتج الجدول التالي

M	E	S	I
E	T	D	G
E	H	A	H
T	U	Y	T
M	R	N	X

- نقوم بقراءة الاعمدة التي تمثل النص الاصلي

عند استعمال مفتاح الترتيب نقوم بوضع الجزء الاول من النص المشفر في العمود الذي يحتوي على الرقم 1 ثم الجزء الثاني في العمود الذي يحتوي على الرقم 2 و هكذا

- لدينا النص المشفر بنفس المفتاح السابق و نريد معرفة محتوى الرسالة

OKEX GUTS LNEX DITX OCHT

2	5	1	4	3
G	O	O	D	L
U	C	K	I	N
T	H	E	T	E
S	T	X	X	X

اذن النص الاصلي هو :

GOOD LUCK IN THE TEST

- يمكنك محاولة معرفة محتوى الرسالة التالية حيث: المفتاح هو 3 و مفتاح الترتيب 312

HIEE PRTC H

التشفير المركب (المعقد):

هو عملية دمج بين التشفير التبادلي و تشفير الإحلال مما ينتج شفرة اقوى من الاثنين .
كمثال بسيط سنقوم بتشفير النص السابق بشفرة قيصر ثم بأحد طرق التشفير التبادلي

النص الاصلي :

GOOD LUCK IN THE TEST

نشفره بشفرة قيصر فيصبح :

JRRG OXFN LQ WKH WHVW

ثم نقوم بتشفيره بالمفتاح السابق

RNHX JXWV OQHX GLWX RFKW

- نلاحظ ان الشفرة الناتجة اقوى من الشفرتين المستعملتين

- طريقة اخرى لإيضاح الدمج بين شفرتين او اكثر حيث نستعمل في هذه الشفرة الجدول التالي :

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I/J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

- عندما نريد تشفير نص ما بهذه الطريقة نقوم بتعويض كل حرف من حروف النص الاصلي بالحرفين اللذان يمثلانه في الجدول ثم نقوم بتقسيم النتيجة الى نصفين و نأخذ

الحرف الاول من النصف الاول مع الحرف الاول من النصف الثاني و نلاحظ اين يتقاطعان و هكذا بالنسبة لباقي الحروف

- نريد تشفير هذا النص بهذه الطريقة

ENCRYPTION

- التعويض :

AE CC AC DB ED CE DD BD CD CC

- نأخذ الحرف الاول من النصف الاول مع الحرف الاول من النصف الثاني و هكذا فينتج

AC EE CD CD AB CD DC BD EC DC

- نلاحظ اين يتقاطع كل حرفين فينتج النص المشفر التالي :

CZOO BOSI XS

لفهم كيفية فك التشفير نقوم بفك النص المشفر التالي:

TQKL BXDN ORE

اولا نعوض كل حرف بالأحرف التي تمثله في الجدول

DD DA BE CA AB EC AD CC CD DB AE

نأخذ الاحرف الحمراء كأزواج و عندما تنتهي نبدأ في الاحرف الباقية

DD BC AE AC CD AD AE AB CD CD BE

نلاحظ الان تقاطع كل حرفين فينتج النص الاصلي التالي :

THE CODE BOOK

يمكنك محاولة فك هذه الكلمة: DGG

- مهما تبدو الشفرات المذكورة معقدة الا انه تم كسرها وذلك بسبب وجود خوارزميات حيث تضمن هذه الخوارزميات وجود نظام محدد للتشفير وبإيجاد ثغرات في هذه الانظمة يمكن كسر الشفرات . الا انه توجد طريقة واحدة لم و ربما لن يستطيع احد كسرها و هي ما تدعى بالشفرة الامنة (one time pad)

- الشفرة الامنة :(one time pad)

يتم استخدام كتاب تحتوي صفحاته على ارقام (مفاتيح) عشوائية و لا تتكرر ابدا. و يجب ان يكون الكتاب لدى كل من المرسل و المستقبل

- عندما نريد تشفير نص ما نقوم باختيار صفحة من الكتاب و نستعمل المفاتيح التي فيها ثم نتخلص من هذه الصفحة (تستعمل المفاتيح كإزاحة لأحرف النص الاصلي) حيث يتم قطعها من الكتاب و لا يتم استعمالها مرة اخرى

- عندما يستلم المستقبل رقم الصفحة و الرسالة يقوم بطرح المفاتيح من النص المشفر فيحصل على النص الاصلي و يتخلص هو ايضا من الصفحة . بما انه لا يوجد نظام محدد تعمل به الشفرة فلا يمكن كسرها اعتمادا على دراسة النص المشفر و الطريقة الوحيدة لمعرفة محتوى النص المشفر هي الحصول على الكتاب.

خاتمة:

قد تكون الطرق المذكورة اعلاه مثالية لتشفير نص قصير الا انه في حالة النصوص الطويلة لا يمكن الاعتماد عليها و ذلك لأنه كلما كان النص اطول كلما ظهرت الثغرات في الطريقة المستعملة و مما يزيد ضعف هذه الطرق انها تعتمد على اللغة او البناء اللغوي

اما بالنسبة لطرق التشفير الحديثة فكل شيء يمثل بالأعداد و هناك فكرتين اساسيتين هما الاعداد الثنائية و المقياس الحسابي . يمكن القول بان هذه الطرق افضل من الطرق الاولى لكن لا يمكن الجزم بانه لا يمكن كسرها فهي تعمل وفق نظام محدد و لابد ان يتم كسر هذا النظام في يوم ما.

الفهرس:

المراجع:

- كتاب علم التشفير (شون ميرفي و فريد بايبر)

- كتاب الشفرة (the code book) لسيمون سينج

- كتاب فاكو الشفرات(the codebreakers) لدايفيد كان

- كتاب مقدمة في التشفير بالطرق الكلاسيكية (وجدي عصام عبد الرحيم)

- codes - ciphers - and secret writing (martin gardner)

- codes and ciphers (Robert churchhouse)

- hill cipher and modular linear algebra (Morray eisenberg)

- شفرة هيل (محمد ضيف الله الزيداني)

- hill cipher (jonaki B ghosh)

- introduction to hill cipher

- DATA ENCRYPTION AND DECRYPTION BY USING HILL CIPHER TECHNIQUE AND SELF REPETITIVE MATRIX (AMOGH MAHAPATRA And RAJBALLAV DASH)

WROTE BY H.Z

2019/03/26