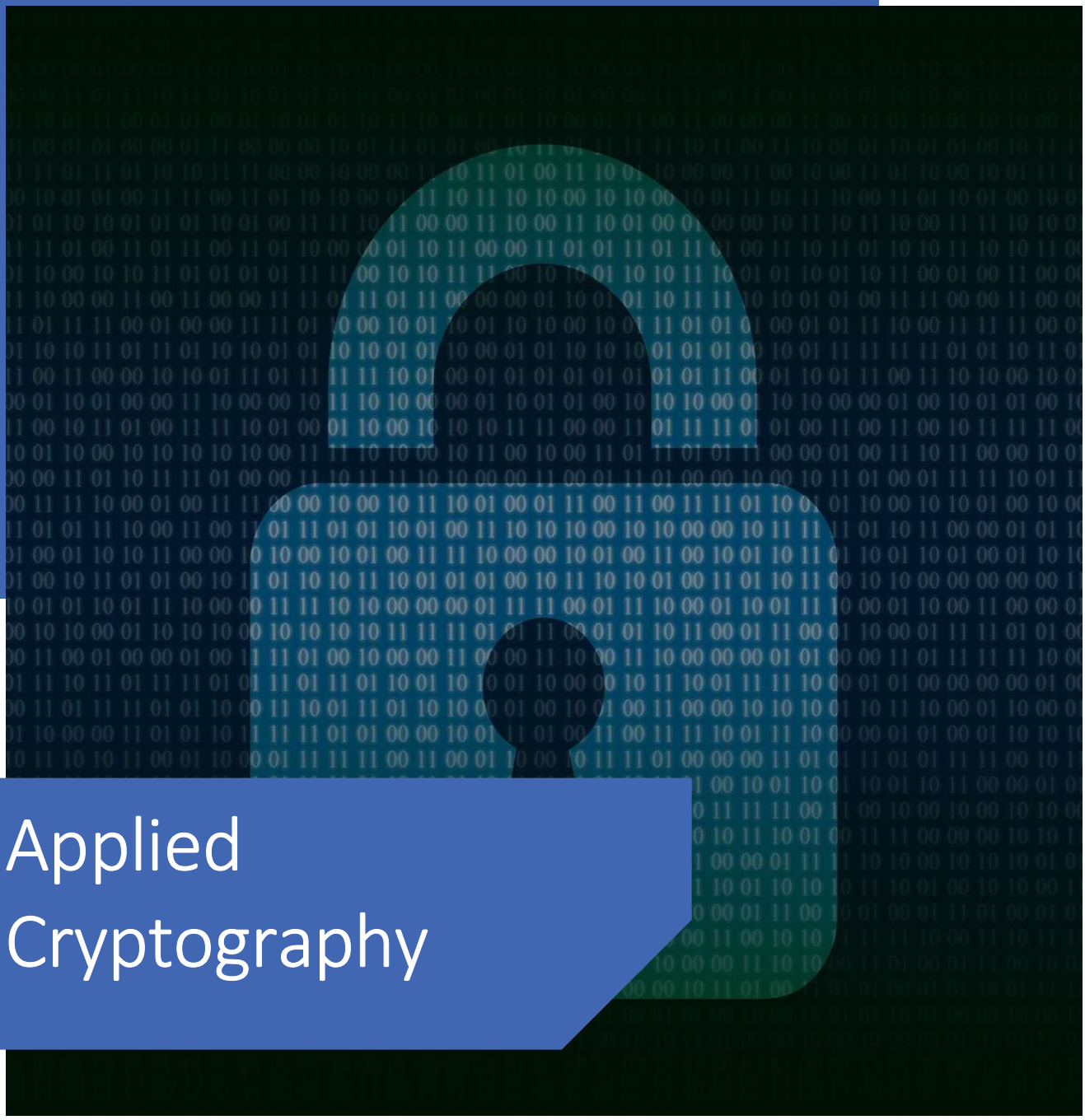


Applied Cryptography

التشفير التطبيقى

مدرب المادة: عبدالله الدحيلان

محتويات الملف

معلومات عن التشفير

• تعريف التشفير

هو علم إخفاء المعلومات، حيث يتم تحويل المعلومات إلى صيغة غير مفهومة بحيث لا يتمكن من إستعادتها إلا من يملك المفتاح الصحيح. يعتبر التشفير فرع من فروع الرياضيات.

• الأفكار الرئيسية في التشفير

- التشويش: Confusion
- الإستبدال: Substitution
- الخلط: Diffusion
- تبديل المواقع (إعادة الترتيب): transposition

المفتاح: هو العنصر السري الوحيد في عملية التشفير

• مصطلحات علم التشفير

- **(Encipher) Encryption**: التشفير
  تحويل العلومات المفهومة إلى صيغة غير مفهومة.
- **Plaintext**: النص الأصلي
  وهي المعلومات بصيغتها المفهومة.
- **Key**: مفتاح التشفير
- **Algorithm**: الخوارزمية
  وهي المعادلات الرياضيات المستخدمة.
- **Ciphertext**: النص المشفر
  وهي المعلومات بعد تشفيرها بحيث لا تكون مفهومة.
- **(Decipher) Decryption**: فك التشفير
  وهي تحويل المعلومات المشفرة إلى صيغة مفهومة.
- **Cryptography**: علم التشفير (التعمية)
- **Cryptanalysis**: عملية إسترجاع أو إيجاد المفتاح
- **Key Space**: العدد الأقصى للمفاتيح المحتملة

مبدأ كيرشوف:

ينص على أن قوة نظام التشفير يجب أن لا تعتمد على إخفاء خوارزمية التشفير أو ميكانيكة التشفير و إنما يجب أن يعتمد على إخفاء المفتاح. بينما إذا كانت مقاومة الخوارزمية للهجوم تعتمد على مفتاح التشفير فإنه يلزمك تغيير المفتاح (العنصر الوحيد السري في نظام التشفير هو المفتاح).

الخوارزمية الأولى: خوارزمية قيصر

عرفت في عهد جوليوس قيصر من آلاف السنين وتعتمد بشكل أساسي على الأحرف، كما لا تدعم الرموز والأرقام.

- مثال على الرموز والأرقام غير المدعومة:
  123@%$
- تعتمد على تبديل حرف بآخر.

• طريقة التشفير

```
X = (رقم الحرف) + (رقم المفتاح) (MOD 26)
```

X = النص المشفر و K = مفتاح التبديل

- على سبيل المثال، عند إستخدام الحرف m بـ مفتاح التبديل 3 سيكون
  X=m+3
- عند فك التشفير يتم إستخدام العملية المعاكسة (الطرح).

• لنفهم هذه القاعدة

كل رقم أقل من 26 سيعطي نفسه بينما الرقم الأكبر من 26 سيعطي الفرق بين الرقم 26 والرقم نفسه.

- على سبيل المثال، عند إستخدام الرقم 28
  2=26–28

- أرقام الأحرف تكون بحسب موقعه في ترتيب الأحرف إبتداءاً بـ 0 كالتالي:

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

عند إستخدام K = 3 يكون ترتيب الأحرف كالتالي:

```
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
```

• أمثلة

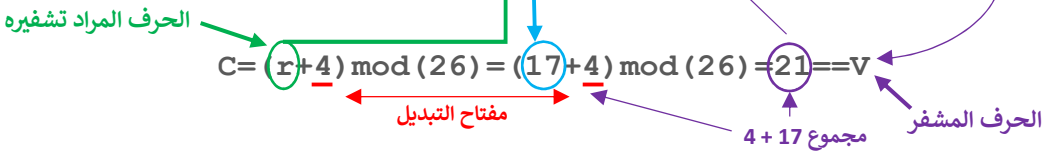
```
17 mod26 = 17
22 mod26 = 22
28 mod26 = 2
```

• تمرين

نريد تشفير الكلمة SECURITY ROOT بإستخدام مفتاح التبديل 4

لاحظ تشفير الحرف الأول ونقوم بتطبيق نفس الطريقة على بقية الحروف

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




```
C=(o+4)mod(26)=(14+4)mod(26)=18==S
C=(o+4)mod(26)=(14+4)mod(26)=18==S
C=(t+4)mod(26)=(19+4)mod(26)=23==X
C=(s+4)mod(26)=(18+4)mod(26)=22==W
   C=(e+4)mod(26)=(4+4)mod(26)=8==I
   C=(c+4)mod(26)=(2+4)mod(26)=6==G
C=(u+4)mod(26)=(20+4)mod(26)=24==Y
C=(r+4)mod(26)=(17+4)mod(26)=21==V
  C=(i+4)mod(26)=(8+4)mod(26)=12==M
C=(t+4)mod(26)=(19+4)mod(26)=23==X
C=(y+4)mod(26)=(24+4)mod(26)=28==C
```

النص المشفر : VSSX WIGYVMXC

الخوارمية الثانية: أعمدة السياج

تسمى بالإنجليزية Rail Fence أو ZigZag cipher وهي طريقة سهلة وسريعة ويمكن تنفيها يدوياً. إضافة إلى ذلك يمكن فك شفرتها بسهولة، كما تستخدم في التشفير البسيط.

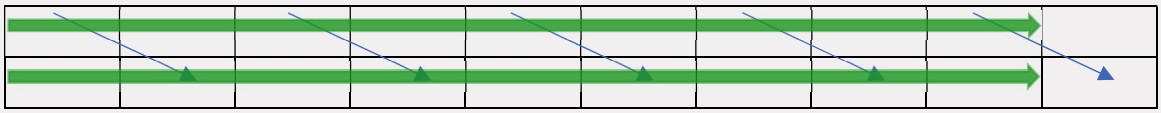
• طريقة التشفير

يكتب النص المراد تشفيره على عدد من الأسطر (محدد مسبقاً)، حيث يعتبر عدد الأسطر هو مفتاح التشفير.

- يتم كتابة النص بشكل قطري على الصفوف.
- يتم كتابة النص بحيث يوضع الحرف الأول في الصف الأول ثم الثاني في الصف الثاني.
- لا يتم إعتبار الفراغات في الكلمة (في الخوارزمية الأصلية) ولكن يمكن معالجتها.
- ينتج النص المشفر من خلال قراءة النص صفاً صفاً.

• لنفهم هذه القاعدة

مثال: خوارزمية من صفين:



• أمثلة

تشفير عبارة (إقرأ بأسم ربك) بإستخدام صفين (عدد الصفوف = 2)

		ك		ر		س		ب		ر		إ
			ب		م		أ		أ		ق	

ينتج النص المشفر: إربسركقأأمب

فك التشفير

يتم فك تشفير الكلمة بإتباع التالي (مع التطبيق على المثال السابق):

- نأخذ طول الكلمة المشفرة.
إربسركقاأمب = 11 حرف،

- نقسم طول الكلمة على عدد الصفوف (يعتبر ك مفتاح التشفير = 2)
11 ÷ 2 = 5.5

- نقسم الكلمة إلى جزئين (يكون الجزء الأول هو الأطول في حال وجود كسور)

الكلمة : إربسركقاأمب
طول الجزء الأول = 6
طول الجزء الثاني = 5

الجزء الأول = إربسرك
الجزء الثاني = قاأمب

- يستخرج النص المشفر عن طريق قراءة حرف من كل جزء على التوالي
(حرف من الجزء الأول وحرف من الجزء الثاني).

إقرأ بأسم ربك

تمرين

قم بتشفير العبارة (إقرأ بإسم ربك) بإستخدام ثلاثة صفوف (عدد الصفوف = 3)

	ب			س			أ			إ
ك			م			ب			ق	
		ر			أ			ر		

ينتج النص المشفر: إأسبقبمكررأر

تمرين

قم بتشفير العبارة CRYPTOGRAPHY بإستخدام ثلاثة صفوف (عدد الصفوف = 3)

C			P			G			P		
	R			T			R			H	
		Y			O			A			Y

ينتج النص المشفر: CPGPRTRHYOAY

الخوارمية الثالثة: MONO ALPHABETIC

تعتمد هذه الخوارزمية بشكل أساسي على إعادة ترتيب الأحرف بشكل عشوائي، على عكس خوارزمية قيصر التي يتم بها التشفير بإستخدام مفتاح على أساسه يتم تبديل الأحرف. بينما في هذه الخوارزمية نبدأ بالحرف على إحتمالية 1 من 26.

- 26 = A
- 25 = B
- 24 = C
- ...
- وهكذا بقية الأحرف إلى النهاية

• شرط هذه الخوارزمية

في حال إستخدمنا حرف في التشفير فلا تسمح لنا هذه الخوارزمية بإستخدام الحرف الذي يليه وذلك لتفادي التكرار أو التسلسل.

• مثال

- عند إستبدال الحرف A بالحرف B
  لا يسمح لنا بتبديل الحرف B بالحرف C

- عند إستبدال الحرف A بالحرف R
  لا يسمح لنا بتبديل الحرف B بالحرف S

تعتبر هذه الخوارزمية قوية لأنه في حال تم كشف أحد الأحرف فإن بقية الأحرف تبقى مشفرة، على عكس خوارزمية قيصر

• فك التشفير بدون جدول التشفير

عدد المحاولات لفك التشفير هي مضروب العدد 26 وهذا يعطينا رقم لا نستطيع قراءته وهو
403291653839397365733630 94

ويعتبر رقم ضخم جداً لا يوصف، ولكن رغم ضخامته فإننا سنشاهد بالدرس القادم كيف نقوم بـ فك التشفير بطريقة معقدة حيث أنها تحتاج إلى جهد.

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

(جدول 1.1) جدول الحروف ومقابلها من التشفير

• أمثلة

قم بتشفير كلمة ROOT SEC

من جدول التشفير

L = R
X = O
X = O
M = T
Z = S
W = E
F = C

تكون النتيجة:

R	O	O	T	S	E	C
L	X	X	M	Z	W	F

• فك التشفير

لكي نقوم بفك شيفرة MONO علينا أن نعرف جدول التشفير الأساسي والذي تم الإعتماد عليه في عملية التشفير، وبهذه الحالة يجب على الشخص الذي يريد فك التشفير إعادة ترتيب الأحرف بالإعتماد على صف توزيع الأحرف المشفرة.

ملاحظة:

لابد أن نحتفظ بالجدول الأساسي في حال وضع خوارزمية خاصة، وفي حال ضياع الجدول تصبح لدينا عملية فك التشفير شبه مستحيلة ولذلك بسبب أن الأحرف يتم توزيعها بشكل عشوائي وأشكال الجداول وطرق التشفير ضخمة جداً ويصعب الحصول عليها

- في حال كانت عملية التشفير عبارة عن مراسلة بين شخصين، فإن على الشخص الذي يقوم بالتشفير إعطاء الجدول للشخص الذي يريد أن يراسله ليتمكن من فك تشفير الرسالة.

- على الشخص الذي يريد فك التشفير الإعتماد على صف وتوزيع الأحرف المشفرة.

- يتم إنشاء جدول فك التشفير كما هو مبين أدناه.

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

(جدول 1.2) جدول فك التشفير المشتق من (جدول 1.1)

• ملاحظة

عدد المحاولات لـ فك التشفير بدون معرفة جدول التشفير تبلغ 4,032,900,000,000,000 محاولة. أي لو أستغرق كل شخص منا ثانية واحدة لقراءة كل جدول فإننا نحتاج إلى مليار ونصف ضعف عمر الأرض. لذلك يلجأ المحللين إلى طريقة تحليل النص.

• تحليل النص

وتعتمد على هذه الطريق بشكل أساسي على طريقتين:

- **Brute Force Attack:** وهي طريقة مكلفة وتستخدم على النطاق الدولي.

  - تعتمد هذه الطريقة على تجربة كل الجداول المحتملة للخوارزمية بهدف إرجاع النص الأصلي بالإعتماد على قوة المعالج (Processor) الخاص بالكمبيوتر أو بقدرتنا على العمل بشكل يدوي بسرعة كبيرة.

  - تستخدم الدول هذه الطريقة لأنها تعتمد على أجهزة كمبيوتر يطلق عليها إسم (Supercomputer) حيث أنها تعمل بسرعة كبيرة وتحتوي على المئات من المعالجات.

- **Crypto Analysis Attack**

يتم إستخدامها من قبل الأشخاص بشكل عام، وتعتمد في الخوارزميات التقليدية على خصائص اللغة.

مثال:
- تكرار بعض الأحرف في اللغة الإنجليزية حيث يتكرر الحرف (E) بنسبة 12% وحرف (I) بنسبة 6%.
- كذلك اللغة العربية حيث نرى حرف (أ) و (ل) تتكرر بنسبة 12%.

• محلل الشفرة

- يقوم محلل الشفرة بالإستفادة من هذه الحالة عن طريق إعادة بناء النص الأصلي، ثم القيام بتركيب الإحتمالات.

❖ يقوم محلل الشفرة بالبداية بـ عد مجموع الأحرف المشفرة المتكررة ضمن النص.
❖ ثم يقوم بمقارنة هذا النص مع العديد من الجداول المحتملة.
❖ ينتقل المحلل إلى مرحلة مقارنة بعض الأحرف التي تكون بشكل دائم متصلة.
❖ يعتمد المحلل على إحصائية تكرار الأحرف ليحصل في النهاية على فك التشفير.

يحصل المحلل في النهاية على أحد الأنواع التالية:

- شيفرة أحادية

أقوى من شفرة قيصر وهناك الكثير من الخوارزميات القوية التي سندرسها ونتعرف عليها لاحقا

الخوارمية الرابعة: PLAY FAIR

إخترعها العالم البريطاني Charles Wheatstone في عام 1854م، وقام بتسميتها بإسم صديقه Lord Playfair. تم إستخدام الخوارزمية في الحرب العالمية الأولى والثانية، كما إستخدمها الرئيس الأمريكي جون كينيدي. تعتمد هذه الخوارزمية في عملية تشفير الحرف بالإعتماد على إرتباطه بحرف آخر.

ملاحظة:

من الممكن أن يشفر الحرف R في المرة الأولى إلى G، ثم يشفر في المرة الثانية إلى S

المصفوفة الخماسية:

تعتمد هذه الخوارزمية على المصفوفة (Matrix) الخماسية التالية.

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

من خلال المصفوفة السابقة يلاحظ حذف الحرف J حتى نتمكن من إنشاء مصفوفة خماسية. ويتم إستبدال الحرف J عند وجوده في النص أو في مفتاح التشفير بالحرف I (الحرف I يمثل الحرفين I و J).

• خطوات التشفير

قم بتشفير كلمة INSTRUMENTS بإستخدام مفتاح التشفير MONARCHY

- يحتاج الشخص إلى تجهيز النص بحيث
  - لا يسمح بوجودين حرفين متتاليين متشابهين عند تقسيم الحروف إلى مجموعات من حرفين (يتم فصل الحرفين بإضافة الحرف X).
  - في حال لم تكن الأحرف زوجية يتم إضافة X آخر النص حتى نتمكن من تقسيم الأحرف لاحقاً.

مفتاح التشفير المستخدم: MONARCHY

الكلمة المراد تشفيرها: INSTRUMENTS

النص الجاهز للتشفير: INSTRUMENTSX

- نقوم بتقسيم النص بحيث يوضع كل حرفين مع بعضهم البعض.

النص الجاهز للتشفير: INSTRUMENTSX
النص المقسم إلى حرفين: IN ST RU ME NT SX

- نقوم ببناء مصفوفة التشفير بإستخدام مفتاح التشفير كالتالي.

نقوم بكتابة مفتاح التشفير في بداية المصفوفة، حيث تنطبق الشروط السابقة على مفتاح التشفير بحيث لا يكون هناك أي حرفين متتاليين، ثم نقوم بتوزيع بقية الأحرف

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

- يتم التشفير بإتباع القواعد التالية:

1) عند وجود الحرفين المراد تشفيرهما على عامود واحد.

يتم تبديل كل حرف بالحرف الموجود أسفله (وفي كان الحرف الحالي هو آخر حرف في العامود يتم إستبداله بأول حرف في العامود).

مثال: في مصفوفة الشفير أعلاه نجد في تشفير ME

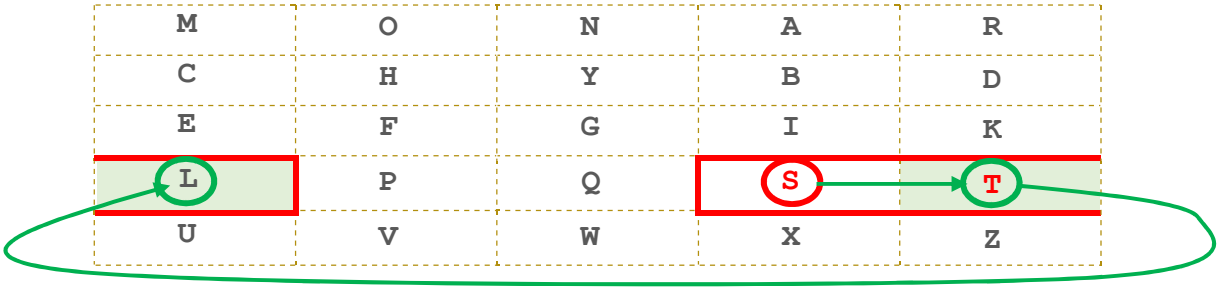
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

بناءاً عليه يكون النص المشفر للحرفين ME هو CL

2) عند وجود الحرفين المراد تشفيرهما على صف واحد.

يتم تبديل كل حرف بالحرف الموجود على يمينه (وفي كان الحرف الحالي هو آخر حرف في الصف من جهة اليمين يتم إستبداله بأول حرف في الصف من جهة اليسار).

مثال: في مصفوفة الشفير أعلاه نجد في تشفير ST



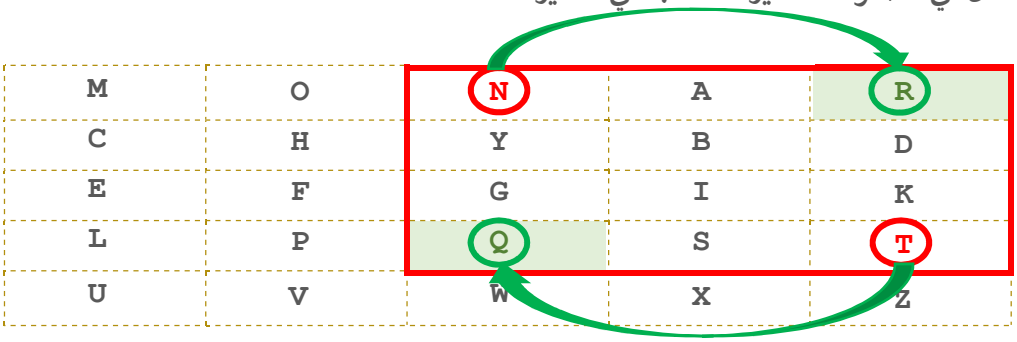
بناءاً عليه يكون النص المشفر للحرفين ST هو TL حيث تم إستبدال

- الحرف S بالحرف T الموجود على يمينه.
- الحرف T بالحرف L (لأن الحرف T هو آخر حرف من جهة اليمين في الصف).

3) إذا لم يكن الحرفين على نفس الصف ولا على نفس العامود.

يتم رسم مستطيل بحيث يكون كل حرف من الحرفين في أحدى زوايا المستطيل، ثم يتم إستبدال كل حرف من الحرفين بالحرف الموجود في الزاوية المقابلة من نفس الصف.

مثال: في مصفوفة الشفير أعلاه نجد في تشفير NT



بناءاً عليه يكون النص المشفر للحرفين NT هو RQ

- **نتيجة التشفير:**

من خلال إتباع قواعد التشفير المذكورة أعلاه ينتج لدينا الجدول التالي

I	N	S	T	R	U	M	E	N	T	S	X
G	A	T	L	M	Z	C	L	R	Q	X	A

وبذلك يكون:

- مفتاح التشفير: MONARCHY
- النص المراد تشفيره: INSTRUMENTS
- النص بعد التصحيح: INSTRUMENTSX
- النص المشفر: GATLMZCLRQXA

تمرين

- قم بتشفير كلمة BOOK بإستخدام مفتاح التشفير ROOT

مصفوفة التشفير

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

النص المراد تشفيره: BO OK

بإستخدام مصفوفة التشفير أعلاه ينتج لدينا النص المشفر: RTTI

ملاحظة:

لم يتم فصل الحرفين OO في كلمة BOOK بسبب أنهما ليسا في نفس المقطع عند تقطيع الكلمة إلى قطع من حرفين.

• فك التشفير

يتم فك التشفير من خلال القيام بعكس عملية التشفير وذلك من خلال (مع الأخذ بعين الإعتبار المثال المستخدم في التشفير أعلاه). مع الأخذ بعين الإعتبار النص المشفر: GATLMZCLRQXA

1) عند وجود الحرفين المراد تشفيرهما على عامود واحد.

يتم تبديل كل حرف بالحرف الموجود أعلاه (وفي كان الحرف الحالي هو أول حرف في العامود يتم إستبداله بآخر حرف في العامود).

مثال: في مصفوفة الشفير أعلاه نجد في فك تشفير CL

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

بناءاً عليه يكون النص المشفر للحرفين CL هو ME

2) عند وجود الحرفين المراد تشفيرهما على صف واحد.

يتم تبديل كل حرف بالحرف الموجود على يساره (وفي كان الحرف الحالي هو أول حرف في الصف من جهة اليسار يتم إستبداله بآخر حرف في الصف من جهة اليمين).

مثال: في مصفوفة الشفير أعلاه نجد في فك تشفير TL

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

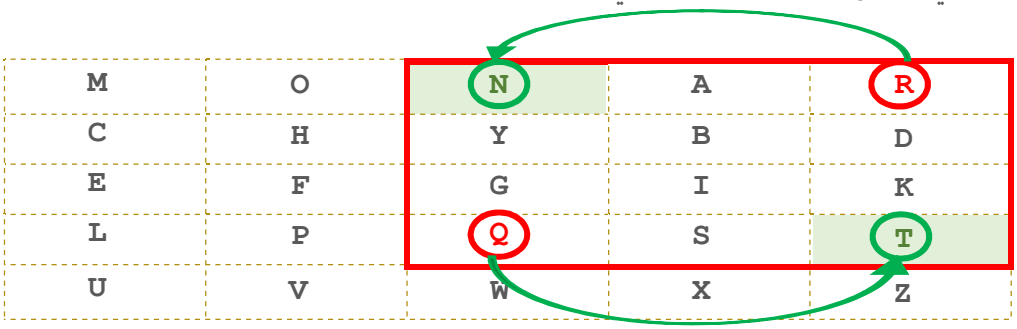
بناءاً عليه يكون النص المشفر للحرفين TL هو ST حيث تم إستبدال

- الحرف T بالحرف S الموجود على يساره.
- الحرف L بالحرف T (لأن الحرف L هو أول حرف من جهة اليسار في الصف).

3) إذا لم يكن الحرفين على نفس الصف ولا على نفس العامود.

يتم رسم مستطيل بحيث يكون كل حرف من الحرفين في أحدى زوايا المستطيل، ثم يتم إستبدال كل حرف من الحرفين بالحرف الموجود في الزاوية المقابلة من نفس الصف.

مثال: في مصفوفة الشفير أعلاه نجد في فك تشفير RQ



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

بناءاً عليه يكون النص المشفر للحرفين RQ هو NT

فيديو:

يمكنك مشاهدة فيديو توضيحي عن التشفير بهذه الخوارزمية من خلال الضغط هنا.

أو يمكنك زيارة الرابط: https://youtu.be/zI585IT9NCs

علم إخفاء البيانات: STEGANOGRAPHY

هناك طرق عديدة وكثيرة تلعب دوراً مهمًا فيما يتعلق بأمن المعلومات، ومنها الطريقة الأكثر شيوعاً والمعروفة بالتشفير (Cryptography) وهو تغيير/إخفاء البيانات الأساسية وفق أسلوب معين لتصبح غير مقروءة.

هناك فن آخر يهدف إلى إخفاء البيانات كليًا للتواصل مابين جهتين بشكل غير ظاهر لجهة ثالثة، وهذا مايعرف بإخفاء المعلومات(Steganography) ، فهي طريقة أو تقنية لحجب و إخفاء البيانات داخل وسيط رقمي، حتى يتم إخفاء أن هناك إتصال أوتبادل معلومات يتم في الخفاء، ولا يكون على علم بهذا الإتصال إلا الأشخاص المعنيين.

• أساس علم إخفاء البيانات

كلمة Steganography في الأساس مشتقة من كلمة يونانية تعني "الكتابة المخفية".

موضوع إرسال رسالة مخفية عن طريق حجب أن هناك شيء مرسل من الأساس هي طريقة (وفكرة) قديمة. ولها قصة تاريخية بدأت أيام الإمبراطورية اليونانية القديمة عندما كانت تكتب الرسائل على رؤوس العبيد آنذاك بعد حلق شعر العبد، حيث يكتب على رأسه رسالة سرية معينة، وعندما يعود شعره للنمو مرة أخرى تختبئ الرسالة السرية تحت شعره الكثيف، وعندها، يتم إرساله للطرف الثاني يقوم بدوره بحلق رأس العبد مرة أخرى حتى يستطيع قرأة الرسالة، وهكذا كانت بدايات استخدام هذة الطريقة لإخفاء رسالة أو معلومة ما تحت غطاء أو شيء ما حتى لا يكون هناك علم أن أي إتصال سري يتم مابين إثنين أو أكثر.

• أساس علم إخفاء البيانات

ربما سمعت سابقًا بمصطلح التشفير (Encryption أو Cryptography) وهو – باختصار – تشفير المعلومة لتصبح غير مفهومة وغير قابلة للقرآة إلا من قبل الشخص الذي يمتلك مفتاح التشفير لفك الشفرة وكل من يحصل على هذا المفتاح. التشفير يكون دائمًا لغرض حماية وأمن المعلومات وأسباب تشفير المعلومات كثيرة، منها: تبادل بيانات سرية بين شركات معينة، بين دوائر حكومية معينة، وغيرها. في المقابل، عند الرغبة في إخفاء المعلومات (Steganography) فإننا نقوم بتضمين المعلومات داخل وسيط ما وتحت غطاء معين بحيث لا تظهر هذه الرسالة لمن يستعرض الوسيط الأساسي (سواءً كان صورة أو فيديو) لأنها مخفية تمامًا داخله، وهذا أشبه ما يكون بالتواصل من وراء الكواليس.

بالتالي، نستطيع القول أن الفرق الأساسي بين التشفير وإخفاء المعلومات هو أنه عند تشفير (Encryption أو Cryptography) معلومة ما، يستطيع الطرف الثالث معرفة أن هناك إتصال يتم مابين طرفين (شخصين أو جهتين) لكنه لا يستطيع فهم المعلومات لأنها مشفرة. أما في حالة إخفاء المعلومات (Steganography)، لا يعلم الطرف الثالث بأن هناك شيء مخفي في الخفاء أو أن هناك إتصال بين إثنين يتم من وراء الكواليس لأنه تم استخدام وسيط ما لإخفاء هذا الإتصال تمامًا.

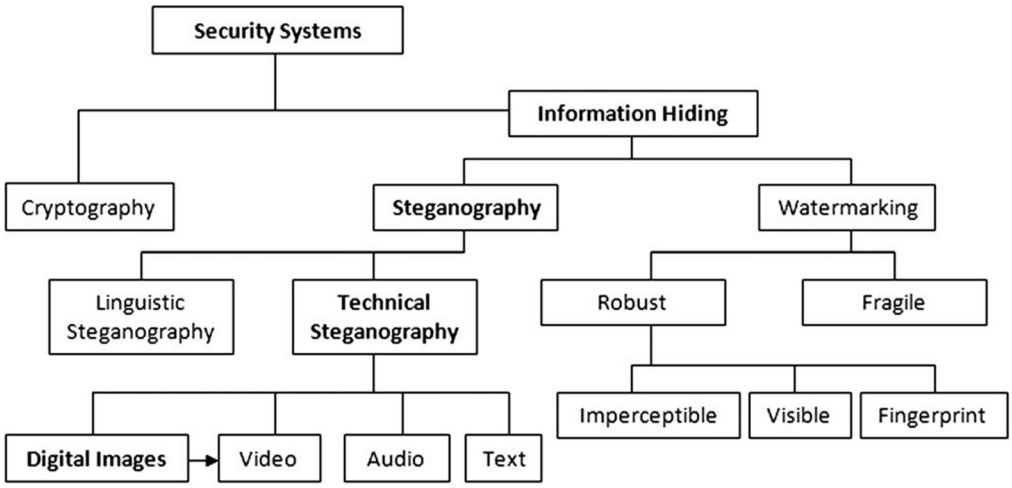
الوسائط المستخدمة في إخفاء البيانات

أبرز الوسائط التي تستخدم في إخفاء المعلومات هي:

- الملفات النصية
- الصور
- الملفات الصوتية
- مقاطع الفيديو

أنواع وطرق حجب البيانات

الشكل التالي يوضح عدة أنواع وطرق لحجب البيانات والتي من بينها التشفير (Encryption أو Cryptography) و إخفاء البيانات (Steganography)، وكما هو موضّح، هنالك أقسام فرعية تحت كل نوع.



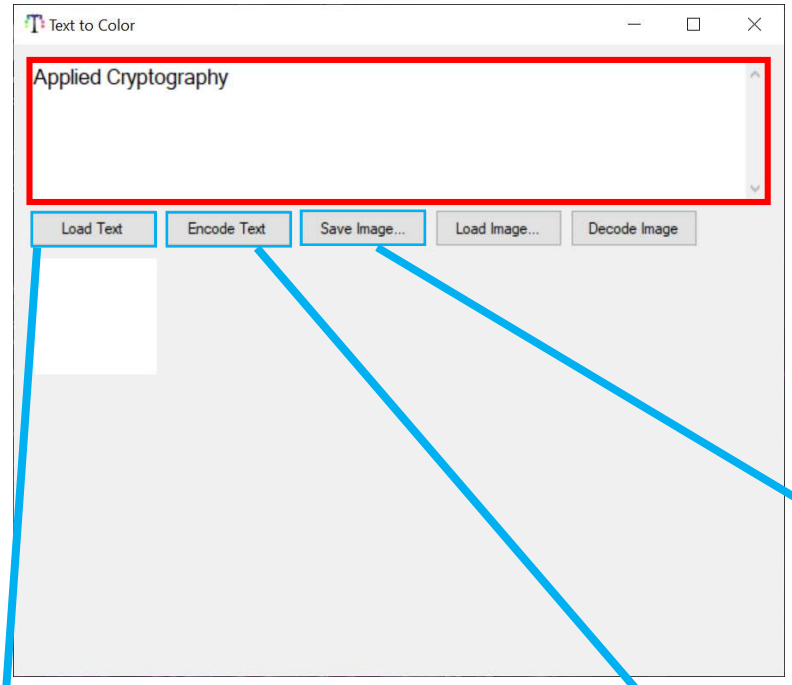
معلومات إضافية:

يمكنك الحصول على معلومات إضافية من خلال زيارة الرابط التالي:

https://educad.me/67189/%D8%A5%D8%AE%D9%81%D8%A7%D8%A1-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D9%85%D9%82%D8%AF%D9%85%D8%A9/

• برنامج Text to Color

قم بتشفير الجملة Applied Cryptography وذلك من خلال وضعها في صورة.



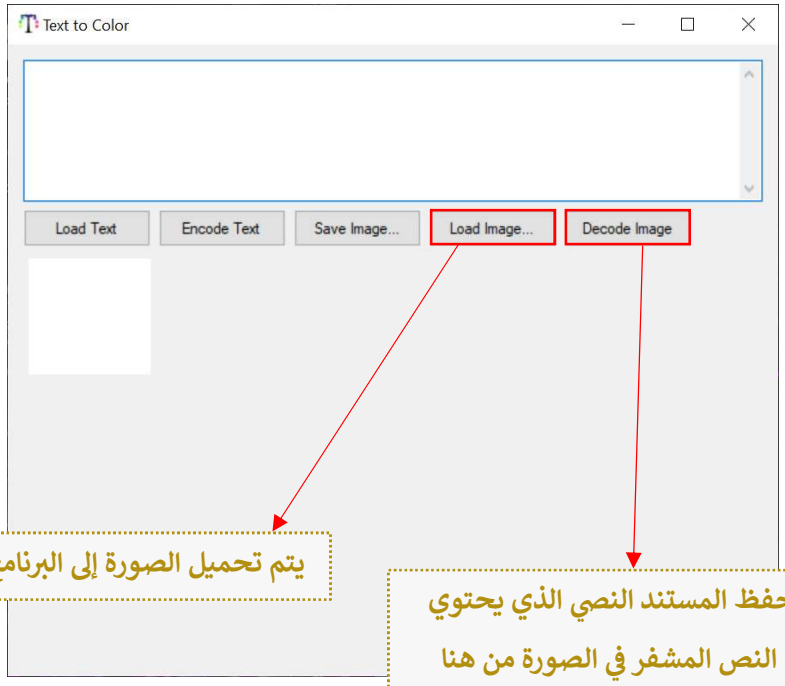
عند الرغبة في تشفير كلمة أو عبارة، يتم وضع العبارة في مربع النص الموجود (تم تحديده بالأحمر في الصورة)، ثم الضغط على زر Encode Text وذلك حتى يعرض لنا الصورة في الأسفل.

يتم حفظ صورة النص المشفر من خلال الضغط هنا

يمكن إختيار مستند نصي من هنا وذلك لتحميله إلى البرنامج وتشفير محتواه إلى صورة

بعد كتابة النص، أو تحميل المستند النصي المراد تشفيره يتم الضغط هنا ليتم التشفير إلى صورة

عند الرغبة في فك تشفير الملف يتم الضغط على Load Image وإختيار الصورة من الجهاز ثم الضغط على Decode Image والذي سيقوم بالطلب منك وضع أسم الملف وموقعه وذلك لحفظ النص في مستند txt



يتم تحميل الصورة إلى البرنامج من هنا

يتم حفظ المستند النصي الذي يحتوي على النص المشفر في الصورة من هنا

الخوارمية الخامسة: HILL CIPHER

تعتبر شيفرة هيل أول شيفرة تتعامل فيها مع 3 حروف في نفس الوقت، ويمكنك التعامل مع عدد أكبر من الأحرف (أو أقل) وتعتبر من الشيفرات متعددة الأبجدية. اخترعت سنة 1929 وسميت بهذا الاسم نسبة إلى مخترعها Lester S. Hill وهي تعتمد في عملها على الجبر الخطي. ولكي تستطيع، التشفير بها يجب أن يكون لديك أساسيات التعامل مع المصفوفات (ضرب المصفوفات بالذات).

تحتاج شيفرة Hill إلى كلمة مفتاحية (Key Word) وهي عبارة عن كلمة يتم تحويل أحرفها إلى أرقام حسب تسلسل كل حرف في الأبجدية حيث يبدأ التسلسل ب 0 ليأخذ Z مثلا في الأبجدية الإنجليزية 25.

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

(جدول 1.3) الخاص بالأبجدية الإنجليزية

• خطوات التشفير

قم بتشفير كلمة ENCRYPTION بإستخدام مفتاح التشفير JECD

- نقوم أولاً ببناء مصفوفة مفتاح التشفير

حيث تصبح مصفوفة التشفير (بالإعتماد على جدول 1.3 أعلاه) كالتالي

$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}$ = JECD حيث أن J = 9 و E = 4 و C = 2 و D = 3

- نقوم بحساب عدد أعمدة مصفوفة مفتاح التشفير أعلاه، وبناءاً عليه يتم تقسيم الأحرف حتى ينتج لنا (عدد أعمدة مصفوفة مفتاح التشفير = عدد صفوف مصفوفات النص المراد تشفيرة)

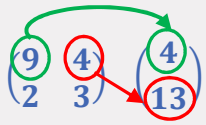
بما أن لدينا عدد أعمدة مصفوفة مفتاح التشفير = 2، يتم تقسيم الكلمة إلى مجموعات من حرفين وإنشاء مصفوفة لكل حرفين (بناءاً على الرقم المقابل لكل حرف في الجدول 1.3)

EN	CR	YP	TI	ON
$\begin{pmatrix} 4 \\ 13 \end{pmatrix}$	$\begin{pmatrix} 2 \\ 17 \end{pmatrix}$	$\begin{pmatrix} 24 \\ 15 \end{pmatrix}$	$\begin{pmatrix} 19 \\ 8 \end{pmatrix}$	$\begin{pmatrix} 14 \\ 13 \end{pmatrix}$

- نقوم بضرب كل مصفوفة من المصفوفات المنشأة في الخطوة السابقة في مصفوفة التشفير وتكون عملية الضرب كالتالي

طريقة ضرب مصفوفتين:

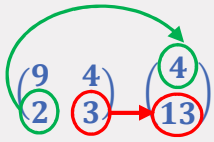
1- يتم ضرب الصف الأول من مصفوفة مفتاح التشفير بالمصفوفة المنشأة



$$= (9 \times 4) + (4 \times 13) = 88$$

حيث يتم ضرب العنصر الأول من الصف الأول في مصفوفة التشفير مع العنصر الأول من مصفوفة النص المراد تشفيره و العنصر الثاني من الصف الأول في مصفوفة التشفير مع العنصر الثاني من المصفوفة المراد تشفيرها ثم نقوم بـ جمع حاصل ضرب الرقمين

2- يتم ضرب الصف الثاني من مصفوفة مفتاح التشفير بالمصفوفة المنشأة



$$= (2 \times 4) + (3 \times 13) = 47$$

حيث يتم ضرب العنصر الأول من الصف الثاني في مصفوفة التشفير مع العنصر الأول من مصفوفة النص المراد تشفيره و العنصر الثاني من الصف الثاني في مصفوفة التشفير مع العنصر الثاني من المصفوفة المراد تشفيرها ثم نقوم بـ جمع حاصل ضرب الرقمين

3- يتم تكوين مصفوفة النص المشفر من خلال وضع ناتج الخطوة الأولى في الأعلى وناتج الخطوة الثانية في الأسفل كالتالي:

$$\begin{pmatrix} 88 \\ 47 \end{pmatrix}$$

بناءاً على طريقة ضرب المصفوفتين، والتس تم تطبيقها على المصفوفة الأولى لـ EN نقوم الآن بضرب بقية المصفوفات بنفس الطريقة كالتالي:

$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 2 \\ 17 \end{pmatrix} = \begin{pmatrix} 86 \\ 55 \end{pmatrix}$$

$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 24 \\ 15 \end{pmatrix} = \begin{pmatrix} 276 \\ 93 \end{pmatrix}$$

$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 203 \\ 62 \end{pmatrix}$$

$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 14 \\ 13 \end{pmatrix} = \begin{pmatrix} 178 \\ 67 \end{pmatrix}$$

- الآن نقوم بإخراج باقي القسمة على 26 من جميع عناصر المصفوفات المشفرة وذلك حتى تكون الأرقام في نطاق العدد 26.

$$\begin{pmatrix}88\\47\end{pmatrix} mod26 \equiv \begin{pmatrix}10\\21\end{pmatrix}$$
$$\begin{pmatrix}86\\55\end{pmatrix} mod26 \equiv \begin{pmatrix}8\\3\end{pmatrix}$$
$$\begin{pmatrix}276\\93\end{pmatrix} mod26 \equiv \begin{pmatrix}16\\15\end{pmatrix}$$
$$\begin{pmatrix}203\\62\end{pmatrix} mod26 \equiv \begin{pmatrix}21\\10\end{pmatrix}$$
$$\begin{pmatrix}178\\67\end{pmatrix} mod26 \equiv \begin{pmatrix}22\\15\end{pmatrix}$$

مثال (إستخراج باقي القسمة):

$$26\overline{)\,88}\quad 3,\ 78,\ 10$$

ولا نستطيع قسمة 10 على 26 بدون كسور، عندها يكون 10 هو باقي القسمة

- ثم نقوم بتغيير كل رقم بالحرف المقابل له من (الجدول 1.3) لـ ينتج لدينا النص المشفر

$\begin{pmatrix}10\\21\end{pmatrix}$	$\begin{pmatrix}8\\3\end{pmatrix}$	$\begin{pmatrix}16\\15\end{pmatrix}$	$\begin{pmatrix}21\\10\end{pmatrix}$	$\begin{pmatrix}22\\15\end{pmatrix}$
KV	ID	QP	VK	WP

ينتج النص المشفر : KVIDQPVKWP

تمرين

نريد تشفير الكلمة MATH بإستخدام المصفوفة المربعة 2 X 2 وهي $\begin{pmatrix}3 & 1\\6 & 5\end{pmatrix}$

- نقوم بتحديد كل حرف ومقابله من (الجدول 1.3) أعلاه.

M	A	T	H
12	0	19	7

- ثم نقوم ببناء المصفوفتين الخاصة بكل حرفين من الكلمة كالتالي

$$\begin{pmatrix}12\\0\end{pmatrix} = \begin{matrix}M\\A\end{matrix}$$
$$\begin{pmatrix}19\\7\end{pmatrix} = \begin{matrix}T\\H\end{matrix}$$

- ثم نقوم بضرب كل مصفوفة من المصفوفتين المنشأتين في مصفوفة التشفير

$$\begin{pmatrix}3 & 1\\6 & 5\end{pmatrix}\begin{pmatrix}12\\0\end{pmatrix} = \begin{pmatrix}36\\72\end{pmatrix}$$
$$\begin{pmatrix}3 & 1\\6 & 5\end{pmatrix}\begin{pmatrix}19\\7\end{pmatrix} = \begin{pmatrix}64\\149\end{pmatrix}$$

- بعد ذلك نقوم بإخراج باقي القسمة على 26

$$\begin{pmatrix}36\\72\end{pmatrix} mod26 \equiv \begin{pmatrix}10\\20\end{pmatrix}$$
$$\begin{pmatrix}64\\149\end{pmatrix} mod26 \equiv \begin{pmatrix}12\\19\end{pmatrix}$$

- ينتج الآن بإستخراج النص المشفر من المصفوفة

10	20	12	19
K	U	M	T

ينتج النص المشفر : KUMT

• فك التشفير

يتم فك التشفير بإستخدام المعادلة $(P = K^{-1} C \ mod\ 26)$

قم بفك تشفير النص المشفر FURSFZDSDENZ بإستخدام مفتاح التشفير TVTC

- نقوم أولاً ببناء مصفوفة مفتاح التشفير (كما تم سابقاً في طريقة التشفير)

حيث تصبح مصفوفة التشفير (بالإعتماد على جدول 1.3 أعلاه) كالتالي

$$\begin{pmatrix}19 & 21\\19 & 2\end{pmatrix} = \text{TVTC}$$ حيث أن T = 19 و V = 21 و T = 19 و C = 2

- نقوم بإيجاد محددة det (K) من مصفوفة التشفير

حيث أن قيمة المحددة تستخرج بضرب قطري مصفوفة التشفير وطرح الناتج منها كالتالي

$$det(K) = \begin{pmatrix} 19 & 21 \\ 19 & 2 \end{pmatrix} = (19 \times 2) - (19 \times 21) = -361$$

القطر الهابط (النازل) — القطر الصاعد

- ثم نقوم بإخراج المقابل للمحددة من خلال الجدول التالي

Determinant	1	3	5	7	9	11	15	17	19	21	23	25
Reciprocal Modulo 26	1	9	21	15	3	19	7	23	11	5	17	25

وفي حال لم يكن كان الرقم لدينا أكبر من 25 نقوم بإيجاد باقي القسمة على 26
يمكن إجراء ذلك بطريقة سريعة كالتالي

$\frac{-361}{26}$ = ... -13.8846

نأخذ الرقم الصحيح 13- ونضربه في 26 ونجمع هذا الناتج (بما أنه بالسالب) من الرقم الأساسي

$$26 \times 13 = 338$$
$$-361 + 338 = -23$$

بما أن 23- ليست موجودة في الجدول ف نوجد باقي القسمة على 26 وهو 3

وبناءاً عليه (وبالإستناد للجدول) يكون مقابل المحددة هو 9

- ثم نقوم بتبديل محتوى القطر النازل لمصفوفة التشفير وعكس الإشارة للقطر الصاعد مع الضرب في ناتج الخطوة السابقة

$$\begin{pmatrix} 2 & -21 \\ -19 & 19 \end{pmatrix}$$

- ثم نقوم بإيجاد باقي القسمة للمصفوفة في الخطوة السابقة على 26 ونضرب لمصفوفة الناتجة في الرقم المقابل للمحددة

$$\begin{pmatrix} 2 & 5 \\ 7 & 19 \end{pmatrix} = \begin{pmatrix} 2\ mod\ 26 = 2 & -21\ mod\ 26 = 5 \\ -19\ mod\ 26 = 7 & 19\ mod\ 26 = 19 \end{pmatrix}$$

$$9 \times \begin{pmatrix} 2 & 5 \\ 7 & 19 \end{pmatrix} = \begin{pmatrix} 18 & 45 \\ 63 & 171 \end{pmatrix}$$

- في حال وجود أرقام في المصفوفة أعلى من 26 نقوم بإيجاد باقي القسمة للمصفوفة المستخرجة في الخطوة السابقة

$$\begin{pmatrix} 18 & 45 \\ 63 & 171 \end{pmatrix} mod26 \equiv \begin{pmatrix} 18 & 19 \\ 11 & 15 \end{pmatrix}$$

وتسمى هذه المصفوفة بـ مصفوفة فك التشفير

- ثم نقوم بحساب عدد أعمدة مصفوفة مفتاح التشفير أعلاه، وبناءاً عليه يتم تقسيم الأحرف حتى ينتج لنا (عدد أعمدة مصفوفة مفتاح التشفير = عدد صفوف مصفوفات النص المراد فك تشفيره)

بما أن لدينا عدد أعمدة مصفوفة مفتاح التشفير = 2، يتم تقسيم الكلمة إلى مجموعات من حرفين وإنشاء مصفوفة لكل حرفين (بناءاً على الرقم المقابل لكل حرف في الجدول 1.3)

FU	RS	FZ	DS	DE	NZ
$\begin{pmatrix} 5 \\ 20 \end{pmatrix}$	$\begin{pmatrix} 17 \\ 18 \end{pmatrix}$	$\begin{pmatrix} 5 \\ 25 \end{pmatrix}$	$\begin{pmatrix} 3 \\ 18 \end{pmatrix}$	$\begin{pmatrix} 3 \\ 4 \end{pmatrix}$	$\begin{pmatrix} 13 \\ 25 \end{pmatrix}$

- ثم نقوم بضرب كل مصفوفة من مصفوفات النص المشفر أعلاه بـ مصفوفة فك التشفير وعند وجود أرقام 26 فما فوق يتم إيجاد باقي قسمة المصفوفة على 26

$$\begin{pmatrix} 18 & 19 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 5 \\ 20 \end{pmatrix} = \begin{pmatrix} 470 \\ 355 \end{pmatrix} mod26 \equiv \begin{pmatrix} 2 \\ 17 \end{pmatrix}$$
$$\begin{pmatrix} 18 & 19 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 17 \\ 18 \end{pmatrix} = \begin{pmatrix} 648 \\ 457 \end{pmatrix} mod26 \equiv \begin{pmatrix} 24 \\ 15 \end{pmatrix}$$
$$\begin{pmatrix} 18 & 19 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 5 \\ 25 \end{pmatrix} = \begin{pmatrix} 565 \\ 430 \end{pmatrix} mod26 \equiv \begin{pmatrix} 19 \\ 14 \end{pmatrix}$$
$$\begin{pmatrix} 18 & 19 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 3 \\ 18 \end{pmatrix} = \begin{pmatrix} 396 \\ 303 \end{pmatrix} mod26 \equiv \begin{pmatrix} 6 \\ 17 \end{pmatrix}$$
$$\begin{pmatrix} 18 & 19 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 130 \\ 93 \end{pmatrix} mod26 \equiv \begin{pmatrix} 0 \\ 15 \end{pmatrix}$$
$$\begin{pmatrix} 18 & 19 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 13 \\ 25 \end{pmatrix} = \begin{pmatrix} 709 \\ 518 \end{pmatrix} mod26 \equiv \begin{pmatrix} 7 \\ 24 \end{pmatrix}$$

- ثم نقوم بإيجاد مقابل الأعداد الموجودة في المصفوفات النهائية (في جدول 1.3)

2	17	24	15	19	14	6	17	0	15	7	24
C	R	Y	P	T	O	G	R	A	P	H	Y

النص بعد فك التشفير: **CRYPTOGRAPHY**