المحاضرة 05: **تحويل النص لشيفرة**

الشيفرة أو التعمية: Code point

تعدد تعريفات هذا المصطلح :

-طريقة للتشفير الملغز تعتمد على تشفير تسلسل الحروف والبيتات.

-كلمة سايفر أو **شيفرة** أصلها من الكلمة العربية للرقم «صفر». حيث إنها في الماضي كانت تستخدم **كلمة** سايفر على اعتبارها الرقم صفر العادي، إلا أنه يوجد عدة روايات عن سبب تحول استخدام **كلمة** سايفر من **معنى** الرقم صفر إلى **معنى** الشيفرة السرية وهذه الروايات **هي** :التعمية غالباً **ما** تتضمن استخدام الأرقام.

أنواع الشيفرات: يوجد الكثير من الشيفرات والبرامج المخصصة لتشفير النصوص أو فك التشفير وفي هذه المحاضرة، سأحاول التعامل ع نوعين من الشيفرة هما: شيفرة قيصر وشيفرة هيل.

شيفرة قيصر:

شفرة قيصر تعتبر في علم التعمية التقليدي بالإنجليزيةclassic cryptography : هي وسيلة لتشفير النصوص، هذه الشفرة شاع استخدامها قديما ويُعتقد أن يوليوس قيصر كان أول من استخدم هذه الوسيلة وكان ذلك بين 58 ق.[1][2][3]م حتى 51 ق.م، وخوارزمية التشفير كانت جدا بسيطة إذ انه كان يبدل الحرف المراد تشفيره بالحرف الثالث الذي يليه، أي لو أراد تشفير حرف «ا» كان يكتب مكانه حرف «ث» وهكذا. عندما أخذ زمام الأمور أغسطس كانت الإزاحة مقدار حرفين فقط!

حسب المعايير الحديثة هذا النوع من التشفير هو غير امن البتة إذ انه من النص المشفر يمكن استنباط النص الأصلي، وذلك لأن توزيع الحروف في النص لا يتغير وبالتالي حسب التوزيع الأصلي للغة الأصل يمكن استنباط النص الأصلي، هذا النوع من الهجمات يسمى: هجوم النص المشفر فقط.

جدول الحروف الخاص بالأبجدية الإنجليزية

Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

التشفير في شفرة قيصر:

يتم التشفير في شفرة قيصر من خلال اختيار المفتاح، ونأخذ على سبيل المثال: المفتاح: 3
والرسالة أو الكلمة التي سنقوم بتشفيرها هي كلمة الانجليزية: Hello

القاعدة في تشفير قيصر تقول:

C=(P+K) mod 26

C: هي اختصار لشيفرة قيصر.

P: هي اختصار لحرف الكلمة المراد تشفيرها

K: اختصار للمفتاح.

Mod 26: والمقصود بها بعد أن نجد النتيجة بعد كل عملية وتكون أكبر من 26 نقوم بعملية طرح 26 كل مرة، حتى نصل لرقم لا يمكن أن ننقص منه 26: مثال 78- 26= 52، وهذا يعني مزال فيه إمكانية للطرح 52-26=26، وهنا يتوقف الطرح؛ لأن الرقم 26 يساوي عدد الحروف في الأبجدية الانجليزية.

مثال لتشفير كلمة Hello:

القاعدة تقول: C=(P+K) mod 26

C=(h+3) mod26

بالتعويض :ترقيم حرف h في الجدول هو رقم 7

C=(7+3)mod26

C=(10)mod 26

- **لا يتم الطرح من العدد 10 ؛لأنه أقل من عدد حروف الأبجدية الإنجليزية.**
- **ما يقبل العدد 10 في الجدول هو الحرف .k**

فنقول H=7+3=10=K

نفس العملية على باقي الحروف المتبقية فنجد:

E= 4+3=7=H

L=11+3=14=O

L=11+3=14=O

O=14+3=17=R

وبهذا يكون التشفير لكلمة Hello هو KHOOR

C='KHOOR'

فك تشفير كلمة Hello:

لفك التشفير نقوم بالعملية العكسية: نتعامل مع الشفرة: KHOOR

وقاعدة فك التشفير: M=(P-K) mod 26

نقوم بالعملية السابقة ولكن بالطرح لنحصل على:

K=10-3=7=H

H=7-3=4=E

O=14-3=11=L

O=14-3=11=L

R=17-3=14=O

وهكذا نكون قدم قمنا بفك التشفير للكلمة الانجليزية انطلاقا من التشفير باستعمال عملية الطرح.

شيفرة هيل:

تعتبر شيفرة هيل أول شيفرة تتعامل فيها مع 3 حروف في نفس الوقت[1]، ويمكنك التعامل مع عدد أكبر من الأحرف (أو أقل) وتعتبر من الشيفرات متعددة الأبجدية.[2] اخترعت سنة 1929 وسميت بهذا الاسم نسبة إلى مخترعها ليستر اس. هيلLester S. Hill [3] وهي تعتمد في عملها على الجبر الخطي.[4] ولكي تستطيع، التشفير بها يجب أن يكون لديك أساسيات التعامل مع المصفوفات) ضرب المصفوفات بالتحديد.

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 الإنجليزية25 .

ملاحظة: يشترط في شيفرة هيل أن تكون الكلمة ذات أحرف ثنائية.

جدول الحروف الخاص بالأبجدية الإنجليزية

Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

التشفير في شفرة هيل:

نختار أولا الكلمة المفتاحية ونحولها لمصفوفة أرقام على شكلn*n ، أي 2*2مثلا كلمة JECD.

تصير $K = \begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}$ وبعد ذلك نختار عدد أحرف النص الأولي على حسب مصفوفة الكلمة المفتاحية حيث أن أعمدة مصفوفة الكلمة المفتاحية يجب أن يساوي عدد صفوف مصفوفة أحرف النص الصريح، في هذه الحالة يجب أن يكون عدد الأحرف زوجيا مثلا لنختار كلمة Encryptionكنص أصلي ولنختر التشفير بحرفين:

- تصيرEn $\begin{pmatrix} 4 \\ 13 \end{pmatrix}$
- تصيرcr $\begin{pmatrix} 2 \\ 17 \end{pmatrix}$
- تصيرyp $\begin{pmatrix} 24 \\ 15 \end{pmatrix}$
- تصيرti $\begin{pmatrix} 19 \\ 8 \end{pmatrix}$
- تصيرon $\begin{pmatrix} 14 \\ 13 \end{pmatrix}$

.2نقوم بضرب المصفوفتين في بعضهما ويحتاج ذلك معرفة طريقة الضرب بعدها نعمل مود 26 لضرب المصفوفتين (مود 26 لأن عدد أحرف الأبجدية الإنجليزية 26 وهي الحروف المستخدمة في هاته الحالة).

$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 4 \\ 13 \end{pmatrix} = \begin{pmatrix} 88 \\ 47 \end{pmatrix}$$
$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 2 \\ 17 \end{pmatrix} = \begin{pmatrix} 86 \\ 55 \end{pmatrix}$$
$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 24 \\ 15 \end{pmatrix} = \begin{pmatrix} 276 \\ 93 \end{pmatrix}$$
$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 19 \\ 8 \end{pmatrix} = \begin{pmatrix} 203 \\ 62 \end{pmatrix}$$
$$\begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 14 \\ 13 \end{pmatrix} = \begin{pmatrix} 178 \\ 67 \end{pmatrix}$$

توضيح طريقة الحساب 47=13*3+4*2/.88=13*4+4*9

ونعمل مود 26 للأرقام التي تتخطى عدد حروف الأبجدية الإنجليزية.

- $\begin{pmatrix} 88 \\ 47 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 21 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 86 \\ 55 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 3 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 276 \\ 93 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 15 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 203 \\ 62 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 10 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 178 \\ 67 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 15 \end{pmatrix} \pmod{26}$

21=26-46/10=26-36=26-62=26-88

ونغير كل حرف بالعدد المقابل في الجدول ليصير النص الأولي بعد التشفير **بشيفرة هيل**:

kvidqpvkwp

فك التشفير في شيفرة هيل:

قانون فك التشفير: مثال للتعامل مع المفتاح $K = \begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}$ الذي هو كلمة: JECD

det(k)=(a*d)-(b*c) mod26

= (9*3)-(4*2) mod26=(27)-(8)=19 =11

D	1	3	5	7	9	11	15	17	19	21	23	25
D^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

المصفوفة المصاحبة للمفتاح.

الخطوات [عدل]

1. نحدد أولا محدد المصفوفة وفي حالتنا $det(K) = 19$، وهو غير منعدم.
2. نقوم بتحديد مود 26 المحدد $19 = 19 \pmod{26}$ إذن $Detmod = 19$، ويجب أن يكون $gcd(26, Detmod) = 1$ لذلك يجب أن يكون مخالفا ل13 وفرديا.
3. نقوم بتحديد x حيث أن $detmod * x = 1 \pmod{26}$ في حالتنا لدينا $11 * 19 - 1 = 208$ و $208 = 26 * 8$ إذن **x=11**
4. نحسب adjx حيث أن adjx = x * adj .
$$adjx = 11\begin{pmatrix} 3 & -4 \\ -2 & 9 \end{pmatrix} = \begin{pmatrix} 33 & -44 \\ -22 & 99 \end{pmatrix}$$
5. نعمل مود 26 لadjx
$$\begin{pmatrix} 33 & -44 \\ -22 & 99 \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 4 & 21 \end{pmatrix} \pmod{26}$$

إذن المصفوفة المعكوسة لمصفوفة المفتاح هي $\begin{pmatrix} 7 & 8 \\ 4 & 21 \end{pmatrix}$

بعد الحصول على المصفوفة المعكوسة [عدل]

نأخذ النص المشفر ونقسمه إلى ثنائيات أو حسب المتفق عليه في حالتنا kv id qp vk wp. نحولها إلى مصفوفات ونضرب المصفوفة المعاكسة فيها:

$$\begin{pmatrix} 7 & 8 \\ 4 & 21 \end{pmatrix}\begin{pmatrix} 10 \\ 21 \end{pmatrix} = \begin{pmatrix} 238 \\ 481 \end{pmatrix}$$
$$\begin{pmatrix} 7 & 8 \\ 4 & 21 \end{pmatrix}\begin{pmatrix} 8 \\ 3 \end{pmatrix} = \begin{pmatrix} 80 \\ 95 \end{pmatrix}$$
$$\begin{pmatrix} 7 & 8 \\ 4 & 21 \end{pmatrix}\begin{pmatrix} 16 \\ 15 \end{pmatrix} = \begin{pmatrix} 232 \\ 379 \end{pmatrix}$$
$$\begin{pmatrix} 7 & 8 \\ 4 & 21 \end{pmatrix}\begin{pmatrix} 21 \\ 10 \end{pmatrix} = \begin{pmatrix} 227 \\ 294 \end{pmatrix}$$
$$\begin{pmatrix} 7 & 8 \\ 4 & 21 \end{pmatrix}\begin{pmatrix} 22 \\ 15 \end{pmatrix} = \begin{pmatrix} 274 \\ 403 \end{pmatrix}$$

ونعمل مود 26

- $\begin{pmatrix} 238 \\ 481 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 13 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 80 \\ 95 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 17 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 232 \\ 379 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 15 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 227 \\ 294 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 8 \end{pmatrix} \pmod{26}$
- $\begin{pmatrix} 274 \\ 403 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 13 \end{pmatrix} \pmod{26}$

وبالتالي تصبح كلمة kvidqpvkwp كلمة encryption .

التطبيق:نماذج تطبيقية على نصوص.