تحويل النص إلى شفرة

الأهداف:

من خلال هذا الدرس يصبح الطالب قادرا على اكتساب عدة مهارات والقيام بعدة عمليات من بينها:

- ✓ التعرف على طريقة عمل الحاسوب وكيفية تخزين البيانات.
- ✓ التعرف على مختلف الخوازميات المتداولة في عملية التشفير.
- ✓ إدراك أهمية التشفير في الحفاظ على أمن وسرية المعلومات والبيانات.
- ✓ القدرة على تشفير أي نص باستخدام خوارزميات الخاصة بالتشفير.
- ✓ القدرة على فك التشفير.

تمهيد:

كان الحاسوب أول ما تم اختراعه يقتصر على القيام بالعمليات الحسابية فقد كان يحسبها بسرعة فائقة إضافةً إلى قدرته على التعامل مع العمليات الحسابية المعقدة وذلك قبل أن يتم تطوير الحاسوب.

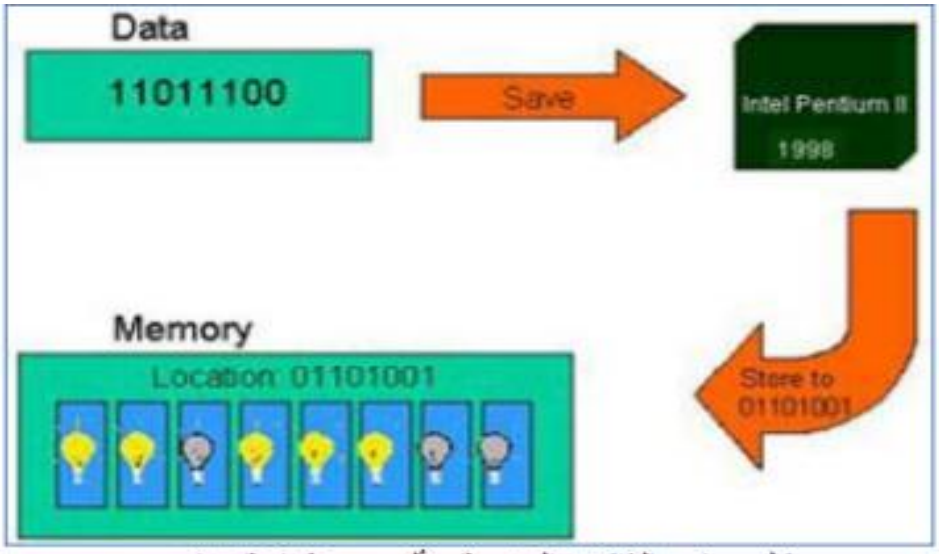
كيف يعمل الحاسوب

الحاسوب جهاز كهربائي، والكهرباء لها حالتان هي الفصل ويرمز لها بالرمز (0)، وحالة الوصل ويرمز لها بالرمز (1)، يعمل هذا الجهاز وفق ما يعرف بالنظام الثنائي؛ وهو أحد

أنظمة العد يتكون من رقمين اثنين هما الصفر والواحد، وهذا النظام الثنائي يستخدم

قطع	وصل	وصل	قطع	قطع	وصل	وصل	قطع
0	1	1	0	0	1	1	0
Byte1							

أيضا مع الأجهزة الإلكترونية مثل: الحاسوب.



كل موقع بالذاكرة الرئيسة يتألف من ثمانية مفاتيح.

مثال: تحويل الرقم 21 وفق النظام الثنائي

- تحويل أي رقم وفق النظام الثنائي تكون بقسمته على العدد (2)

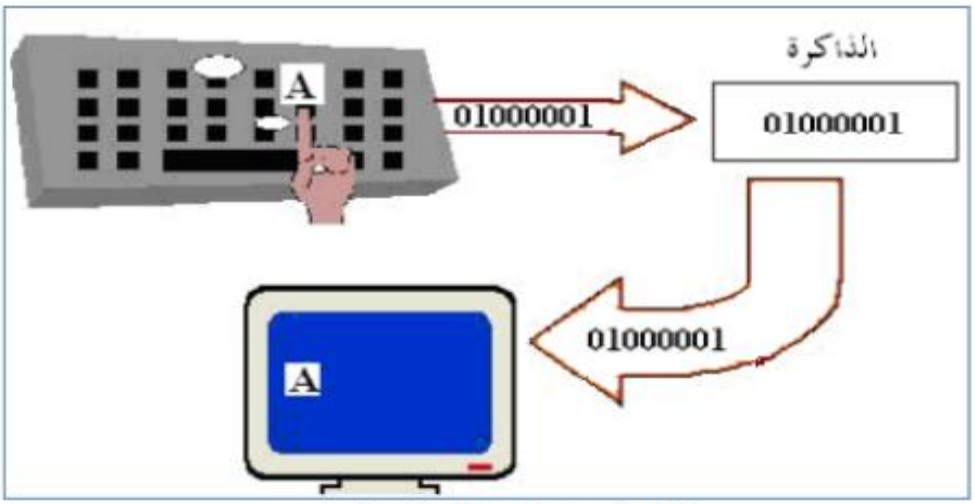
القاسم	المقسوم	باقي القسمة
21	**2**	**1**
10	**2**	**0**
5	**2**	**1**
2	**2**	**0**
1	**2**	**1**

- كما هو موضح في الجدول أعلاه نقوم بتحصيل باقي القسمة في كل مرة وبعد إكمال عملية القسمة بشكل تام ، بواقي القسمة هي الترميز الثنائي الخاص بكل عدد كما هو واضح في تحويل الرقم 21 وفق النظام الثنائي:(10101).

أما بالنسبة للحروف هناك العديد من الشفرات المستخدمة لتمثيل البيانات في الحاسب مثل:

- **شفرة آسكي (ASCII)** الشفرة الأمريكية النمطية لتبادل المعلومات
- **الشفرة الموحدة (Unicode)**معظم نظم التشغيل تستخدم الشفرة الموحدة(Unicode) وهي تدعم اللغة العربية، أي لكل حرف قيمة ثنائية تقابله

Character	Bit pattern	Byte number		Character	Bit pattern	Byte number
A	01000001	65		¼	10111100	188
B	01000010	66		.	00101110	46
C	01000011	67		:	00111010	58
a	01100001	97		$	00100100	36
b	01100010	98		\	01011100	92
o	01101111	111		~	01111110	126
p	01110000	112		1	00110001	49
q	01110001	113		2	00110010	50
r	01110010	114		9	00111001	57
x	01111000	120		©	10101001	169
y	01111001	121		>	00111110	62
z	01111010	122		‰	10001001	137



تمثيل الحرف A داخل ذاكرة الحاسب.

والنظام الثنائي مثله مثل بقية الأنظمة المعتمدة في الحياة اليومية مثل:

- ✓ النظام العشري(0.1.2.3.4.5.6.7.8.9) أساسه (10)
- ✓ النظام الثماني (0.1.2.3.4.5.6.7) أساسه (8)

✓ النظام الخماسي (0.1.2.3.4) أساسه (5)

ملاحظة:

- ❖ **كل الأرقام والحروف والرموز الموجودة في لوحة المفاتيح تكون وفق النظام الثنائي (0.1)**
- ❖ **البيت (Bit): أصغر وحدة تخزين البيانات تخزن وحدة أساسية فقط إما الصفر (0)، وإما الواحد (1).**
- ❖ **البايت (Byte): وحدة التخزين الأساسية**

1بايت = 8 بيت =1حرف = 1رقم =1 رمز

مثال: جملة "الصف السادس" = 11 حرف ×1بايت = 11بايت؛ أي تخزن في 11 بايت

تحويل نص إلى شفرة

أولا: مفهوم التشفير

التشفير عبارة عن ممارسة حماية مختلف المعلومات والبيانات والنصوص باستخدام الخوارزميات، وهذه المعلومات قد تكون:

- ✓ غير نشطة (مثل ملف على القرص الصلب)،
- ✓ متنقلة (مثل الاتصالات الإلكترونية المتبادلة بين طرفين أو أكثر)،
- ✓ قيد الاستخدام (أثناء الحوسبة على البيانات).

ثانيا: الغاية من التشفير

- ✓ السرية حيث تكون المعلومات متاحة للمستخدمين المصرح لهم فقط.
- ✓ النزاهة حيث يضمن لنا التشفير ضمان عدم التلاعب أو مساس بالمعلومات.
- ✓ المصادقة - تأكيد صحة المعلومات أو هوية المستخدم-.

ثالثا: استخدامات التشفير

تعود بدايات التشفير إلى إرسال معلومات حساسة بين الشخصيات العسكرية والسياسية. ويمكن تشفير الرسائل بحيث تبدو وكأنها نص عشوائي لأي شخص باستثناء المستلم المقصود. لكن في الوقت الحالي، جرى فك تقنيات التشفير الأصلية بالكامل ، حقق

هذا المجال تقدمًا كبيرًا في ناحية الأمن، وتعتمد الخوارزميات المستخدمة اليوم على التحليل الدقيق والرياضيات لضمان أمنها.

ومع تطور الأمن، توسع مجال التشفير ليشمل نطاقًا أكبر من أهداف الأمان. ومن هذه الأهداف مصادقة الرسائل وتكامل البيانات والحساب الآمن وغيرها الكثير.

يُعد التشفير أساس المجتمع الحديث، وهو أساس لعدد لا يحصى من تطبيقات الإنترنت من خلال برتوكول النقل الآمن للنصوص التشعبية(HTTPS) ، والاتصالات النصية والصوتية الآمنة، وحتى العملات الرقمية.

رابعا: مفهوم الخوارزميات

الخوارزمية هي مجموعة من الخطوات الرياضية والمنطقية والمتسلسلة اللازمة لحل مسألة ما. وسميت الخوارزمية بهذا الاسم نسبة إلى العالم أبو جعفر محمد بن موسى الخوارزمي الذي ابتكرها في القرن التاسع الميلادي. الكلمة المنتشرة في اللغات اللاتينية والأوروبية هي «algorithm» وفي الأصل كان معناها يقتصر على خوارزمية لتراكيب ثلاثة فقط وهي :التسلسل والاختيار والتكرار.

- التسلسل: تكون الخوارزمية عبارة عن مجموعة من التعليمات المتسلسلة، هذه التعليمات قد تكون إما بسيطة أو من النوعين التاليين.
- الاختيار: بعض المسائل لا يمكن حلها بتسلسل بسيط للتعليمات، وقد تحتاج إلى اختبار بعض الشروط وتنظر إلى نتيجة الاختبار، إذا كانت النتيجة صحيحة تتبع مسار يحوي تعليمات متسلسلة، وإذا كانت خاطئة تتبع مسار آخر مختلف من التعليمات. هذه الطريقة هي ما تسمى اتخاذ القرار أو الاختيار.
- التكرار: عند حل بعض المسائل لا بد من إعادة نفس تسلسل الخطوات عدد من المرات. وهذا ما يطلق عليه التكرار.

خامسا: نموذج خوارزمية هيل في التشفير النصوص

ويُصطلح عليها **تعمية هيل** أو **تشفير هيل** أول طريقة تعمية تتعامل فيها مع 3 حروف في نفس الوقت، ويمكنك التعامل مع عدد أكبر من الأحرف (أو أقل) وتعتبر من التعميات المتعددة الألفبائيات.[2] اخترعت سنة 1929 وسميت بهذا الاسم نسبة إلى مخترعها ليستر اس. هيل (Lester S. Hill) وهي تعتمد في عملها على الجبر الخطي ولكي تستطيع، التعمية بها يجب أن يكون لديك أساسيات التعامل مع (المصفوفات) ضرب المصفوفات بالتحديد.

صورة (Lester S. Hill)

لاستخدام تشفير هيل نحتاج 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 على نحو ما هو موضح في الجدول أسفله

جدول الحروف الخاص بالأبجدية الإنجليزية

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

1- كيفية التشفير

يلزم أولاً اختيار الكلمة المفتاحية وتحويلها لمصفوفة أرقام على شكلn*n ، مثلا كلمة JECD تصير:

$$K = \begin{pmatrix} 9 & 4 \\ 2 & 3 \end{pmatrix}$$

بعد ذلك يختار 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

ملاحظة: للتعرف على بقية العمليات الخاصة بكيفية التشفير ينظر الفيديو رقم 1