إعداد وعرض: مدى وصل الله الطياري

التشفير أو التعمية

هو عملية الحفاظ على سرية المعلومات باستخدام برامج وخوارزميات لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مرخص لهم بذلك لا يستطيعون فهم أي شئ لأن ما يظهر لهم هو خليط من الرموز والأرقام و الحروف الغير مفهومة ومن ناحية أخرى، فإن فك التشفير هو عملية إعادة تحويل البيانات إلى صيغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك الشيفرة
ولقد شهدت أسواق هذه البرامج انتعاشا مذهلا بعد أن سمحت السلطات الأمريكية للشركات التجارية المتخصصة ببيع هذه التقنية للجمهور و عامة الناس بعدما كانت محصورة للاستخدامات العسكرية والحكومية لسنوات طويلة ولقد اتخذت الحكومة الأمريكية هذا القرار في سبيل دعم الجانب الأمني لمجال التجارة الإلكترونية علما بأنها وحتى وقت قريب جدا لم تسمح بتصدير هذه التكنولوجيا إلى خارج الولايات المتحدة، خاصة للتي تزيد قوة تشفيرها عن ٥٦ بت

هل أنت بحاجة لها؟

الجواب بالتأكيد نعم فلكل فرد و شركة أو هيئه تجارية خصوصيات و أسرار و معلومات هامة جدا لا يجب أن يطلع عليها أحد ، كما أنك اليوم لا تستطيع الاستغناء عن خدمات متوفرة في الإنترنت مثل البريد الإلكتروني و التسوق عبر مواقع التجارة الإلكترونية

نبذه تاريخية

استخدم الإنسان التشفير منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية، وبلغ هذا الاستخدام ذروته في فترات الحروب؛ خوفاً من وقوع الرسائل الحساسة في أيدي العدو.

و لكن التشفير كعلم مـ سس منظم يدين بولادته و نشأته للعلماء الرياضيين و اللغويين العرب إبان العصر الذهبي للحضارة العربية و أشهرهم الفراهيدي و الكندي ، و قدم هؤلاء العلماء مفاهيم رياضية متقدمة من أهمها التوافيق و التباديل.
و قد شاع في أيامنا استخدام مصطلح "تشفير "ليدل على إخفاء المعلومات و لكن كلمة التشفير وافدة من اللغات الأوربية و هذه بدورها جاءت أصلاً من اللغة العربية.
و من هنا تطور استخدام كلمة "Cipher" في جميع اللغات الأوربية تقريباً لتعني إخفاء المعلومات و قمنا - نحن العرب - بعد ستة قرون بإعادة بضاعتنا الأصلية و لكن بمعنى مختلف فتحنا كلمة غربية على اللغة العربية هي التشفير.

بعض الطرق المتبعة للتشفير:

طريقة **Caesar**

طريقة **Monoalphabetic**

طريقة هل

أولى الطرق : طريقةCaesar

مفهومها : هي من أبسط طرق التشفير و أقدمها و فكرتها تكمن في تبديل كل حرف بثالث حرف بعده.

سيصبح تبادل لأماكن الحروف يعني بدل (a) يكتب (d) و قس ذلك عل باقي الحروف..
لنأخذ مثال :
لو أرنا أن نشفر كلمة hayatech
ستصبح بعد التشفير kdbdwhfk :

و تسمى أيضاً هذه الطريقة بطريقة : البحث الشامل ، Brute force search.

الطريقة الثانية :طريقةMonoalphabetic

***فكرتها :**

فكرة هذه الطريقة أن يكون لدينا مفتاح key و نقوم بتبديل النص الأصلي بالمفتاح ، و هي أفضل من طريقة Caesarلأن المفتاح يكون هنا متغير.

لاحظنا في الطريقة الأولى أننا بدلنا بدل الحرف A بالحرف D و أكملنا تسلسل الأحرف ،، و هذه الطريقة سهلة و متوقعة عند أغلب قطاع الطرق!!
أما الطريقة الثانية تتشابه معها قليلاً لأننا مازلنا نقوم فقط بتبديل الأحرف ، لكن تبديل الأحرف هنا يكون بشكل عشوائي و بعد ترتيبه يطلق عليه (المفتاح) و يجب أن يكون المفتاح معلوم لدى كلاً من المستقبل و المرسل حتى يتم فك الشفرة..
في الطريقة السابقة لم نذكر كلمة مفتاح لأننا لم نحتاج إليه ،، فبمجرد معرفة كل من المرسل و المستقبل أن النص المشفر ، قدُشفر بطريقة Caesar فيكون معرفة فك التشفير أمر بديهي لهم..

***ميزتها:**

أن في طريقة Caesar لو علم تحويل حرف واحد فقط سوف يتمكن من حل الشفرة بالكامل
أما في طريقة لو فك حرف واحد فقط لن يتمكن من فك البقية لآن الترتيب هنا يكون عشوائي و بشكل متباعد..

*المفتاح: Key

سنقوم بتبديل الأحرف بشكل عشوائي و لا يعتبر هذا المفتاح ثابت كما في الطريقة الأولى ،،لكنا قمنا بذلك للتدريب على هذه الطريقة و حتى يكون هذا المفتاح بيننـي و بينكم..

- مثال على ذلك :
  الكلمة المراد تشفيرها hayatech :
  تصبح بعد التشفير jdzdufvj

الطريقة الثالثة : طريقة هِلْ

تعمد هذه الطريقة على استخدام المصفوفات كتحويلات خطية.

وتقوم أولا بترقيم حروف اللغة العربية كما يلي:

أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص
١	٢	٣	٤	٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤
ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي
١٥	١٦	١٧	١٨	١٩	٢٠	٢١	٢٢	٢٣	٢٤	٢٥	٢٦	٢٧	٠

ونلاحظ أننا أعطينا الحرف ي الرقم صفر لأننا سنعمل داخل الحلقة

التي فيها : $28 \equiv 0 (\mathrm{mod}\ 28)$

مثال:

استخدم المصفوفة $A=\begin{bmatrix}2&5\\1&4\end{bmatrix}$ لتعمية الرسالة: الهجوم غدا.

الحل:

أولا: نحول الرسالة إلى متتالية من الأعداد فنحصل على

١، ٢٣، ٢٦، ٥، ٢٧، ٢٤، ١٩، ١،٨ على التوالي.

ثانيا: لتكوين المصفوفة من الدرجة ٢ X ٢ فإننا نجمع كل عددين متتالين في متجه كما يلي:

$$\begin{bmatrix}1\\1\end{bmatrix}،\begin{bmatrix}19\\8\end{bmatrix}،\begin{bmatrix}27\\24\end{bmatrix}،\begin{bmatrix}26\\5\end{bmatrix}،\begin{bmatrix}1\\23\end{bmatrix} \qquad (١)$$

لا حظ أننا كررنا العددين في المتجه الأخير لكون عدد حروف الرسالة فرديا.

ثالثا: نقوم بتعمية الرسالة كما يلي: $A\begin{bmatrix}x\\y\end{bmatrix}=\begin{bmatrix}x_1\\y_1\end{bmatrix}$ حيث $\begin{bmatrix}x\\y\end{bmatrix}$ هو أحد المتجهات الواردة في (١) فنحصل على:

$$\begin{bmatrix}2&5\\1&4\end{bmatrix}\begin{bmatrix}1\\23\end{bmatrix}=\begin{bmatrix}5\\9\end{bmatrix}$$
$$\begin{bmatrix}2&5\\1&4\end{bmatrix}\begin{bmatrix}26\\5\end{bmatrix}=\begin{bmatrix}21\\18\end{bmatrix}$$
$$\begin{bmatrix}2&5\\1&4\end{bmatrix}\begin{bmatrix}27\\24\end{bmatrix}=\begin{bmatrix}6\\11\end{bmatrix}$$
$$\begin{bmatrix}2&5\\1&4\end{bmatrix}\begin{bmatrix}19\\8\end{bmatrix}=\begin{bmatrix}22\\23\end{bmatrix}$$
$$\begin{bmatrix}2&5\\1&4\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}=\begin{bmatrix}7\\5\end{bmatrix}$$

لا حظ أننا قمنا بعملية الضرب والجمع قياس العدد (٢٨). أي أننا نعمل في الحلقة Z_{28} .

رابعا: نقوم بتحويل الرسالة إلى حروف فنحصل على الرسالة المشفرة:

ج ذ ق ع ح ز ك ل خ ج.

لا حظ أن عدد حروف الرسالة المشفرة هو عشرة وذلك نتيجة لتكرار الحرف الأخير من الواضح كما ذكرنا في ثانيا.

أنواع تكنولوجيا التشفير :

هنالك نوعين من التكنولوجيا المستخدمة في التشفير وهي :

١-التشفير المتناظر

٢-التشفير الغير متناظر

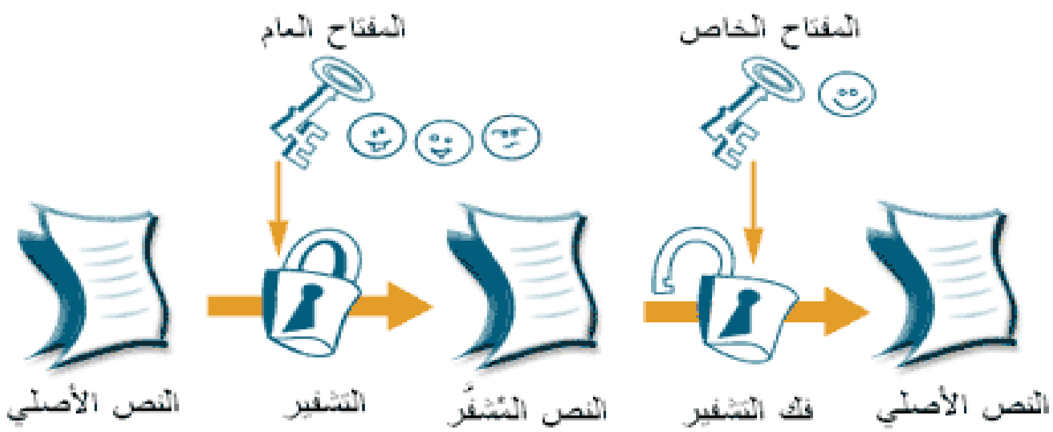
و الفرق بينهم بسيط جدا ولكنه مهم جدا في مستوى ودرجة الأمن حيث أن التشفير المتناظر يتم بتشفير الرسالة أو المعلومات باستخدام الرقم العام وكذلك في نفس الوقت يتم فك الشفرة و ترجمة المعلومات إلى وضعها الأصلي باستخدام نفس الرقم العام. ولذلك لو حصل و أن شخص آخر يعرف هذا الرقم فإنه قادر على فك الشفرة و قراءة تلك الرسالة أو المعلومة

أما إذا ما تم تشفير المعلومات بأسلوب (الغير متناظر) فإن المعلومات يتم تشفيرها بالرقم العام ولكن لا يمكن فك الشفرة و الوصول إلى تلك المعلومات إلا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تم على أساسه عملية التشفير.

فمثلا تخيل بأنك تقوم بالاتصال هاتفيا بأحد أصدقاؤك وعندما تدخل رقم هاتفه (الرقم العام) ويبدأ هاتفه بالرنين ولكن ذلك الصديق لا يرد على مكالمتك فيرد عليك جهاز إجابة و تترك له رسالة صوتية في ذلك الجهاز . و الان لنتخيل بأنك قمت بحماية (تشفير) تلك الرسالة برقم سري و لا يستطيع أحد الاستماع إلى تلك الرسالة إلا بإدخال ذلك الرقم السري. فإن كان صديقك هذا قد اتفق معك على اختيار الرقم السري هو نفس رقم هاتفك العام فهذا ما يسمى بطريقة التشفير المتناظر لأن المفتاح العام = الرقم السري أما لو قام ذلك الصديق ببرمجة التشفير لطلب

الرقم السري الخاص بك (رقم آخر لا يعرفه أحد غيرك) فهذا ما يعرف بالتشفير الغير متناظر لأن المفتاح العام لا يساوي الرقم السري

....



قوة التشفير

تعتمد على عدد الخانات المكونة لكل رقم و تقاس ب البت فمثلا اذا كان الرقم مكون من ٤٠ خانة فإن القوة ستكون ٤٠ بت إذا كان الرقم عبارة عن ٥٦ خانة تكون قوة التشفير ٥٦ بت وهكذا. علما بأن التكنولوجيا المتوفرة في هذا المجال يمكن أن توفر قوة تشفير تصل إلى أكثر من ٣٠٠٠ بت ولكن لم تسمح الحكومة الأمريكية حتى الان بتداول قوة تشفير أكثر من ١٢٨ بت لأنه كاف جدا لحماية التجارة الإلكترونية و جدير بالذكر أن الوقت اللازم ليتمكن أحد لصوص الإنترنت لفك شفرة بقوة ٥٦ بت هو ٢٢ ساعة و خمسة عشر دقيقة ، أما الوقت اللازم لفك شفرة بقوة ١٢٨ بت باستخدام التكنولوجيا الحالية لفك الشفرات فهو سنتان!! لأن اللص في حالة ٥٦ بت بحاجة لتجربة ٧٢ من الاحتمالات (يعني رقم و أمامه ١٥ صفر) أما في قوة ١٢٨ فإن الاحتمالات المطلوبة للتجربة تصل إلى عدد فلكي وهو ٣٤٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠٠احتمال (يعني رقم وأمامه ٣٦ صفر) ولذلك لم نسمع أبدا بأن معلومة تم تشفيرها بهذه القوة قد تم فكها من قبل هؤلاء اللصوص المحترفين و نحن لا نعتقد بأن أحد يمكنه فعل ذلك على الأقل في المستقبل القريب أو المنظور **ولذلك تسوق على شبكة الإنترنت وأنت مطمئن البال بشرط التأكد من قوة التشفير المستخدمة من قبل الموقع الذي تود الشراء منه و كذلك التأكد من قوة التشفير في متصفحك...**