التشفير وفك التشفير

Encryption & Decryption

أ. صلاح الهادي غبيقة*

مقدمة:

عُرف علم التشفير أو التعمية منذ ما يزيد عـن ألفـي عـام قبـل المـيلاد، واستخدمه الإنسان لحماية رسائله السرية، وبلغ هذا الاستخدام ذروتـه فـي فتـرات الحروب، حيث كانت الخطط الحربية وطرق الهجوم على العدو تُرسل عـن طريـق رسائل عادية مكتوبة بخط اليد في الأغلب ولكنها تُشفّر بإحدى الطرق خوفاً مـن أن تقع في أيدي العدو وبالتالي تفشل تلك الخطط. وقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة. وكذلك ذكر أن العرب كانت لهم محاولات قديمة في مجال التشفير. واستخدم الصينيون طرقاً عديدة في علم التـشفير والتعميـة لنقل الرسائل أثناء الحروب. وقد كان قصدهم من استخدام التشفير هو إخفاء الـشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه تصعب عليه فهمها. وأفضل طريقة استخدمت في القدم هي طريقة يوليوس قيصر، وهو أحد قياصرة الروم.

أما في عصرنا الحالي فقد باتت الحاجة ملحّة لاستخدام هذا العلـم "التـشفير" وذلك لارتباط العالم ببعضه عبر شبكات مفتوحة . حيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بـين المنظمـات الخاصـة والعامة، عسكرية كانت أم مدنية. وعليه فلابد من طرق تحفـظ سـرية المعلومـات.

*- عضو هيئة تدريس بقسم تحليل البيانات والحاسب الآلي بكلية الاقتصاد والتجارة زليتن، salah2525@yahoo.com

ولهذا بُذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات.

ولا يزال العمل والبحث في مجال علم التشفير مستمراً، وذلك بسبب التطوّر السريع للحاسبات، والتقدّم الكبير للشبكات وبخاصة الشبكة العالمية الانترنت.

علم التشفير أو التعمية (*Cryptography*):

مصطلح علم التشفير أو التعمية (*Cryptography*) هو عبارة عن كلمة يونانية الأصل مكونة من مقطعين هما: (kryptós) وتعني مخفي، (gráphien) وتعني كتابة. أي بمعنى الكتابة المخفية[1].

وهو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات. التشفير يُمكّنُك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة – مثل الإنترنت – وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل له، وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (***Cryptoanalysis***) هو علم لكسر وخرق الاتصالات الآمنة[2].

كما يمكن تعريف التشفير أو التعمية على أنه تحويل نص واضح مقروء إلى نص غير مفهوم باستخدام إحدى طرق التشفير والتي قد تكون غير سرية، ولكنها تستخدم مفتاحاً سرياً يمكّن من يمتلكه من أن يعيد النص المشفّر إلى النص الواضح[3].

1- علاء حسين الحمامي، مازن سمير الحكيم، التشفير والترميز حماية ضد القرصنة والتطفل، الدار العربية، بغداد، العراق، 1999، ص18.

2- علاء حسين الحمامي، مازن سمير الحكيم، المصدر السابق ص22.

3- علاء حسين الحمامي، سعد عبدالعزيز العاني، تكنولوجيا أمنية المعلومات وأنظمة الحماية، دار وائل للنشر والتوزيع، ط:1، 2007، عمان، الأردن ص31.

أما فك أو كسر التشفير فهو العملية العكسية للتشفير، أي محاولـــة معرفـــة المفتـــاح السري من النص المشفر، ومن ثم الحصول على النص الواضح.

بعض المصطلحات الهامة في علم التشفير[1]:

- النص الواضح : (Plaintext) الرسالة الأصلية.
- النص المشفر :(Ciphertext) الرسالة المشفرة.
- الشيفرة :(Cipher) خوارزمية لتحويل النص الواضح إلى نص مشفر.
- المفتاح :(Key) معلومة تستخدم في الشيفرة وتكون معروفة فقط للمرسل والمستقبل.
- التشفير :(encrypt) تحويل النص الواضح إلى نص مشفر.
- فك التشفير :(decrypt) إعادة النص المشفر إلى نص واضح.
- علم التشفير :(cryptography) دراسة مبادئ وطرائق التشفير.
- علم كسر التشفير :(cryptanalysis) دراسة مبادئ وطرائق فك تـــشفير الـــنص المشفر دون معرفة المفتاح.

أهمية علم التشفير والحاجة إليه:

اكتسب علم التشفير وتطبيقاته أهمية بالغة منذ مطلع القرن العشرين. إذ تبين أن الحربين العالميتين الأولى والثانية كانتا حربي تشفير وفك تشفير في المقام الأول، ومثال ذلك أن معارك روميل ومونتجمري الشهيرة، في صحراء شمال إفريقيا، كانت تخفي وراءها حقائق مذهلة في معارك التشفير وفك التشفير التي دارت بين الطـــرفين والتي كانت أهم بكثير مما جرى على أرض الصحراء، فقـــد ضـــحى البريطـــانيون بقاعدة كاملة من قواعدهم لئلا يعلم الألمان أنهم استطاعوا كسر شـــفرتهم، إذ قـــررت

1- Scott Wilson (2004), An Introduction to Cryptography. "Intro To Crypto.pdf", P8.

حكومة تشرشل ترك الألمان يدمرون القاعدة رغم معرفتهم بتفاصيل الخطة الألمانيـــة وتوقيتها عن طريق كسر شفرة الألمان وقراءة رسائلهم[1].

وأصبح الجميع الآن يدركون أهمية علم التشفير وازدياد الحاجة إليه خـــصوصاً في هذه الأيام مع الانتشار الواسع للانترنـــت وكثـــرة ســـرقة المعلومـــات والبيانـــات الشخصية، وكلمات السر، إذ تكمن أهميته بالحفاظ علـــى ســـرية المعلومـــات الهامـــة والحساسة، وعدم وصولها إلى الأشخاص غير المخولين بالإطلاع عليها، ويمكن عـــن طريق التشفير التقليل من حجم المعلومات أثناء انتقالهـــا ، وضـــمان هويـــة المـــصدر المرسل للرسالة، وأكبر دليل على أهمية التشفير أنه في وقتنا الحاضر تم إنشاء العديـــد من الشركات المختصة بأمن المعلومات عامةً وتشفير الرسائل والبيانات خاصةً.

ففي الولايات المتحدة الأمريكية، نجد وكالة الأمن القومي السرية الأمريكيـــة التي تختص بالتشفير، ترتبط مباشرة بالرئيس الأمريكي ويرتبط بها حـــوالي 80,000 موظف، وتزيد نفقاتها السنوية عن 15 مليار دولار، وتضم عدداً كبيراً من الحواسيب المتقدمة تقنياً[2].

ومنذ منتصف عقد السبعينيات من القرن الماضي، امتـــد اســـتعمال التـــشفير ليتعدى مجال الاتصالات والمراسلات العسكرية والدبلوماسية والأمنية، ويـــصل إلـــى عدة مجالات واستخدامات أُخرى منها[3]:

1- دلال صادق، حميد الفتال، أمن المعلومات، الفصل التاسع: الترميز والتشفير، دار اليازوري العلمية للنشر والتوزيع، ط:1، 2008، عمان، الأردن، ص211.

2- Erkay Savas (2002), DATA SECURITY & CRYPTOGRAPHY. Oregon State University & rTrust Technologies. "L1.pdf", P29.

3- رائد عبدالعزيز العريقي، تشفير وفك تشفير الصور الرقمية، رسالة ماجستير غير منشورة، بغداد، كلية علوم وهندسة الحاسب، 2007، ص34.

– **في الصناعة والتجارة:** للمحافظة على الأسرار التجارية والعلميـــة والاختراعـــات والتصاميم، والوضع المالي وغيرها.

– **في حقوق البث التلفزيوني:** حيث يتم تشفير بعض البرامج التلفزيونية، ومباريـــات كرة القدم، حتى لا يستطيع مشاهدتها إلا المشتركون الذين يدفعون اشـــتراكاً شـــهرياً مقابل المفتاح السري (الجهاز) الذي يسمح بفك الشفرة ومشاهدة البرامج.

– **في المصارف:** وذلك للمحافظة على حسابات المودعين، وحمايتها من التلاعـــب أو الاختلاس خصوصاً مع تطوّر الخدمات المصرفية الالكترونية.

– **في حماية الاتصالات السلكية واللاسلكية:** وذلك بالمحافظة عليها مـــن الاختـــراق والتصنت والاطلاع على أسرار الآخرين الشخصية.

– **في الكشف عن اللغات القديمة البائدة:** حيث كان لعلم تحليل التعمية وفك التـــشفير بالغ الأثر في الكشف عن رموز اللغة الهيروغليفية في مطلع القرن التاسع عشر، ولا يزال هذا العلم يستخدم في الكشف عن أسرار اللغات المسمارية القديمة.

على هذا الأساس تبرز أهمية تشفير البيانات أو تعميتها لضمان سريتها عنـــد تنقلها عبر الشبكة وللتأكد من هوية مرسل المعلومات ووصولها كاملة دون تغيير إلى الجهة التي يفترض أن تصلها .

إسهامات العلماء العرب في تطوّر علم التشفير:

التشفير أو التعمية كما كان يُطلق عليه عند العرب، كعلم مؤسس على قواعد ونظريات لم يبدأ إلا عندهم بعد بزوغ الحضارة العربية الإسلامية، ويقـــول المـــؤرخ الشهير لعلم التشفير (ديفيد كان) في كتابه المـــشهور (كاســـرو التعميـــات)، بعـــد أن استعرض استعمال التشفير أو التعمية من قبل كل الحضارات الـــسابقة حتـــى القـــرن السابع الميلادي ما نصه:

"لم نجد في أي من الكتابات التي نقبّنا عنها أي أثرٍ واضحٍ لعلـم اسـتخراج التعمية، وعلى الرغم من بعض الحالات المعزولة العرضية مثل: الرجال الأيرلنديين الأربعة، أو دانييل، أو أي مصريين يمكن أن يكونوا قد اسـتخرجوا بعـض كتابـات المقابر الهيروغليفية، فإنه لا يوجد شيء في علم تحليل التعمية. وبالتـالي فـإن علـم التعمية الذي يشمل علم وضع التعمية وعلم تحليلها لم يولد حتى هذا التاريخ (القـرن السابع الميلادي) في جميع الحضارات التي استعرضناها بما فيها الحضارة الغربيـة، ولقد وُلد عند العرب، فقد كانوا هم أول من اكتشف طرق تحليـل التعميـة وكتابتهـا وتدوينها. إن هذه الأمة التي انبثقت من الجزيرة العربية في القرن السابع المـيلادي، والتي انتشرت فوق مساحات شاسعة من العالم المعروف، أخرجت وبسرعة، إحـدى أرقى الحضارات التي عرفها التاريخ حتى ذلك الوقت. لقد ازدهر العلـم، فأصـبحت علوم الطب والرياضيات أفضل ما في العالم في ذلك الوقت"[1].

وقد لا نكون مبالغين إذا ذكرنا بأن كلمة (تشفير) في اللغات اللاتينيـة كلهـا وهي كلمة (Cipher) سايفر، قد جاءت من الكلمة العربية (شفرة)، وذهـب بعـضهم إلى القول بأنها مشتقة من كلمة (صفر).

ويدين علم التشفير أو التعمية للعرب في ولادته ونشأته كعلم مؤسس ومنظم. وأول العلماء العرب في التعمية هو الخليل بن أحمد الفراهيدي (718–786م) الـذي يُنسب إليه (كتاب المُعَمَّى) الذي يعتبر الكتاب الأول في هذا العلم. الخليل هـو عـالم اللغة العربية المشهور وواضع علم العروض وأول من كتب معجمًا للغـة العربيـة. ولكن أعظم العلماء المسلمون في هذا الميدان هو الفيلسوف العربي يعقوب بن إسحاق الكِنْدي (185–260هـ، 801–874م) الذي ضـمت مؤلفاتـه الكثيـرة أول كتـاب

1 –W. M. Farmer (2003), Overview of Cryptography. "cryptographyoverview.pdf", P21.

معروف في علم التعمية وهو (رسالة في استخراج المعمَّى) استقصى فيه قواعـد علـم التعمية وأسرار اللغة العربية، واستخدم لأول مرة في التاريخ مفاهيم الإحصاء في تحليل النصوص المعمّاة، وذلك قبل كتابات باسكَال وفيرما الأولية (1654م) التـي يعتبرهـا مؤرخو الرياضيات الغربيون بداية علم الإحصاء والاحتمالات بحوالي ثمانية قرون[1].

وازدهر علم التعمية عند العرب كذلك في القرن السابع الهجري (الثالث عشر الميلادي)، نتيجة لأسباب حضارية وعسكرية وسياسية برزت بعد اجتيـاح المغـول للعالم الإسلامي وقدوم الحملات الصليبية، وظهرت في تلك الفترة مؤلفات كثيرة فـي علم التعمية منها، كتاب ابن دنينيـر (583–627هـ، 1187–1229م) المعنـون: (مقاصد الفصول المترجمة عن الترجمة)، وكتـاب إبـن عـدلان (583–666هـ، 1187–1268م) المؤلف للملك الأشرف، وكتاب (مفتاح الكنوز في إيضاح المرموز) الذي كتبه علي بن الدريهم (712–762هـ، 1312– 1359م).

وقد عُثر على مخطوطات من هذه المؤلفات وحقّقها ونشرها المجمع اللغـوي في دمشق عام 1987م. ولكن النشاطات العلمية في ميدان التعمية اختفت مع انهيـار الحضارة الإسلامية. يقول (ديفيد كان) : "إن تعمية قيصر بقيت حيّة حتـى آخـر أيـام الروم، لأن أول محللي التعمية لم يظهروا إلا بعد عدة قرون لاحقة. إن العرب كانوا هم أول من اكتشف مبادئ تحليل التعمية، ولكن جهودهم تقلصت مع أفول حضارتهم"[2].

أهـداف التشفـير:

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي[3]:

1– دلال صادق، حميد الفتال، مصدر سابق، ص65.

2- W. M. Farmer (2003), Overview of Cryptography. "cryptographyoverview.pdf", P27.

3- Tal Malkin (2003), Introduction to Cryptography. "Summary1 What is Cryptography.pdf", P14.

1. السرية أو الخصوصية (*Privacy*): هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.
2. تكامل البيانات (*Integrity*): هي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.
3. التحقق وإثبات الهوية (*Authentication*): وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (للمصرح لهم).
4. عدم الإنكار (*Non-repudiation*): وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما.

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم.

كيفية عمل التشفير:

خوارزمية التشفير هي دالة رياضية تستخدم في عملية التشفير وفك التشفير، وهي تعمل بالاتحاد مع المفتاح أو كلمة السر أو الرقم أو العبارة، لتشفير النصوص المقروءة.

نفس النص المقروء يشفر إلى نصوص مشفرة مختلفة مع مفاتيح مختلفة، والأمن في البيانات المشفرة يعتمد على أمرين مهمين قوة خوارزمية التشفير وسرية المفتاح. والشكل التالي يوضح طريقة عمل التشفير.

شكل 1: طريقة عمل التشفير

أنواع التشفير:

حالياً يوجد نوعان من التشفير وهما كالتالي:

1- التشفير التقليدي ***Conventional Cryptography***.

2- التشفير بالمفتاح العام ***Public Key Cryptography***.

التشفير التقليدي:

يسمى أيضاً التشفير المتماثل أو المتناظر (*Cryptography Symmetric*)، وهو يستخدم مفتاحاً واحداً لعملية التشفير وفك التشفير للبيانات، وقد كان النوع الوحيد من التشفير المُستخدم قبل ظهور تشفير المفتاح العام في أواخر السبعينيات. وقد استخدم هذا التشفير من قِبل أشخاص ومجموعات عديدة بداية من يوليوس قيصر، والغواصات الألمانية، ومازال يُستخدم حتى الآن من قِبل البعثات الدبلوماسية، وفي المجال العسكري والتجاري من أجل سرية الاتصالات. ويبقى هذا النوع من التشفير الأكثر استخداماً مقارنة مع أنواع التشفير الأخرى[1].

ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدَم. حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات. مثال على ذلك؛ إذا أراد شخص ما إرسال رسالة مشفرة إلى شخص آخر، فعليه إيجاد طريقة آمنة لإرسال المفتاح إليه. فإذا حصل أي طرف ثالث على هذا المفتاح فإن بإمكانه قراءة جميع الرسائل المشفرة بين هذين الشخصين.

وللتشفير المتناظر خمسة مكونات هي[2]:

1- رعد مهجر، نهلة فليح، تشفير الملفات النصية باستعمال المفتاح المتناظر، مجلة كلية العلوم، جامعة البصرة، العدد 32، 2006، ص67.

2- المصدر السابق، ص69.

■ النص الصريح أو الواضح: وهو الرسالة الأصـلية أو المعطيـات التـي تُعطـى للخوارزمية كمدخل.

■ خوارزمية التشفير: هي مجموعة من الخطوات المرتبة بطريقة معينة لتؤدي هـدفاً معيناً، وتنجز خوارزمية التشفير العديد من عمليات النقل والاسـتبدال علـى الـنص الصريح.

■ المفتاح السري: المفتاح السري هو عبارة عن سلسلة مـن الرمـوز، وهـو أحـد مدخلات خوارزمية التشفير، وتعتمد الاستبدالات الدقيقة وعمليات النقل التي تنجزهـا الخوارزمية على المفتاح السري.

■ النص المُشفّر: وهو الرسالة المبعثرة التي تكون مخرج للخوارزمية وتعتمد علـى النص الصريح والمفتاح السري.

■ خوارزمية فك التشفير: وهي في الواقع خوارزمية تـشفير ولكـن تعمـل بـشكل معاكس، وتحتاج هذه الخوارزمية إلى النص المشفر والمفتاح السري لكي تنتج النص الصريح.

وفيما يلي رسم توضيحي يبين طريقة التشفير بالمفتاح الواحد.

شكل 2: يوضح طريقة التشفير باستخدام المفتاح الواحد

تشفير البيانات القياسي (DES):

طُوّر هذا النظام في نهاية السبعينيات من قبل وكالة الأمن القومي الأمريكية، وهذا النظام بات من الجدوى عدم استخدامه مع تطور أنظمة الحاسوب وزيادة سرعة معالجته للبيانات، حيث أنه صار بالإمكان كشف محتوى رسائل مشفرة به في وقت قصير. وتوجد أنظمة حديثة ومتطورة وأثبتت جدواها في عصرنا الحالي في مجال التشفير منها AES, IDEA, 3DES, blowfish[1].

غير أن كل ما ذكر من الأمثلة السابقة يعتمد على مبدأ المفتاح الواحد لعملية التشفير وفك التشفير.

التشفير بالمفتاح العام:

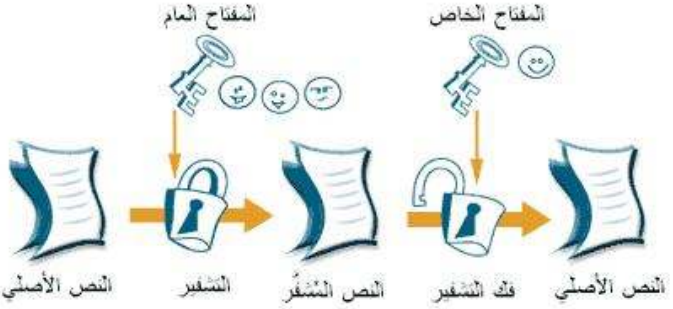
يُعرف أيضاً بالتشفير اللا متماثل (*Asymmetric Cryptography*). تم تطوير هذا النظام في السبعينيات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة. ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح العام *Public key*، والمفتاح الخاص *Privet key*، حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل[2].

المفتاح العام يُرسل لجميع الناس أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد. فمن يحتاج أن يرسل لك رسالة مشفرة فإنه يستخدم المفتاح العام

1- إبراهيم سليمان عبدالله، أمن المعلومات، دار المريخ للنشر والتوزيع والطباعة، المملكة العربية السعودية، ط:1، 2008، ص98.

2- محمد صالح، علاء العزاوي، التشفير والترميز-النظرية والتطبيق، دائرة التدريب، العراق، 2001، ص42.

لتشفيرها ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص. وفيما يلي رسم توضيحي يبين طريقة التشفير باستخدام المفتاح العام والمفتاح الخاص.



شكل3: يوضح طريقة التشفير باستخدام المفتاح العام والمفتاح الخاص

ويُدعى نظام التشفير الذي يستخدم المفاتيح العامة بنظام RSA، ورغم أنه أفضل وأكثر أمناً من نظام DES إلا إنه أبطأ؛ إذ إن جلسة التشفير وجلسة فك التشفير يجب أن تكونا متزامنتين تقريباً. وعلى كل حال، فإن نظام RSA ليس عصياً على الاختراق، إذ إن اختراقه أمر ممكن إذا توفَّر ما يلزم لذلك من وقت ومال. ولذلك، تمّ تطوير نظام PGP الذي يُعَدُّ نموذجاً محسَّناً ومطوَّراً من نظام .RSA ويستخدم PGP مفتاحاً بطول 128 بت، إضافة إلى استخدامه البصمة الإلكترونية للرسالة، ولا يزال هذا النظام منيعاً على الاختراق حتى يومنا هذا.

مزايا وعيوب التشفير التقليدي والتشفير باستخدام المفتاح العام:

التشفير التقليدي أسرع بكثير باستخدام أنظمة الحاسوب الحديثة، ولكنه يستخدم مفتاحاً واحداً فقط، ولذلك فهو أكثر عرضة للاختراقات. أما تشفير المفتاح العام فيستخدم مفتاحين في عملية التشفير وفك التشفير، وهو أقوى وأقل عرضة للاختراقات، ولكنه أبطأ من التشفير التقليدي.

ونتيجة لهذه المزايا والعيوب أصبحت الأنظمة الحديثة تستخدم كلا الطريقتين حيث أنها تستخدم الطريقة التقليدية للتشفير وأما تبادل المفتاح السري الواحد بين الأطراف المتراسلة تتم من خلال استخدام طريقة تشفير المفتاح العام.

قياس قوة التشفير:

التشفير قد يكون قوياً أو ضعيفاً، حيث أن مقياس القوة للتشفير هو الوقت اللازم والمصادر المطلوبة لعملية كشف النصوص غير المشفرة من النصوص المشفرة. نتيجة التشفير القوي هو نص مشفر يصعب كشفه مع الوقت أو توفر الأدوات اللازمة لذلك.

علم التشفير وعلم الإخفاء:

أولاً دعونا نلقي نظرة عامّة عن علم الإخفاء من حيث مفهومه وتاريخه وأهمية استخدامه، فمن الملاحظ أن كثيراً من المتخصصين في علم حماية وأمن المعلومات يخلط بين علم التشفير وعلم إخفاء المعلومات، معتقدين أن كلا المصطلحين يعطي المعنى نفسه، بينما في حقيقة الأمر كل مصطلح منهما يغطي علماً خاصاً من علوم أمن المعلومات.

تهدف تقنية إخفاء المعلومات إلى الإخفاء التام لوجود هذه المعلومات عن طريق إخفائها داخل معلومات أخرى ليست بتلك الأهمية مع الحرص التام على عدم تأثر المعلومات المستخدمة للإخفاء بحقيقة كونها حاملة للمعلومات المخفية، وذلك لتجنب احتمالية الكشف عن وجود المعلومات المُخفاة تحت هذه المعلومات. باستخدام هذه الطريقة تقل نسبة الكشف عن المعلومات والعبث بها بنسبة كبيرة؛ لأنه إن كان المهاجم لا يعلم بوجود هذه المعلومات أصلاً فكيف باستطاعته العبث بها والاستفادة منها؟

علم الإخفاء:

يأتي أصل مصطلح علم إخفاء المعلومات (Stenography) مـــن الكلمتـــين الإغريقيتين: steno والتي تعني السقف أو الغطاء و graphia والتي تعني الكتابـــة. ويُعرف علم إخفاء المعلومات على أنه إخفاء رسالة ما (بيانات) داخل رسالة أخـــرى (بيانات أخرى) بهدف إخفاء وجود الرسالة الأولـــى، لهـــدف محـــدد[1]. والبيانـــات المستخدمة في الإخفاء قد تكون عبارة عن ملفات الوسائط المتعـــددة (multimedia) كالنصوص، الصور، و ملفات الصوت أو الفيديو وغيرها. وقد تكون أيضاً عبارة عن ملفات تنفيذية للبرامج (executable files)، وفي عملية الإخفاء نحتاج إلـــى تـــوفر عنصرين مهمين لإتمام هذه العملية، الأول هو الرسالة التي نهدف إلى إخفائها والثاني هو الوعاء أو الغطاء (cover) المستخدم لإخفاء هذه الرسالة.

هناك عدة تعريفات أخرى لعلم الإخفاء من أبرزها تعريف العالمين جونـــسن وجوجوديا على أنه: "فن إخفاء المعلومات بطريقة لا تسمح باكتشافها"[2].

تاريخ علم الإخفاء:

علم الإخفاء لا يُعد من العلوم المستحدثة، فلقد كان أول ظهور لهذا العلم فـــي العصر الإغريقي، حيث قام أحد قياصرة ذلك العصر بالتواصل مع الملوك الآخـــرين، عن طريق حلق شعر رؤوس عبيده ثم وشم الرسائل على رؤوسهم، بعد ذلـــك يقـــوم بانتظار نمو شعر رأسهم ثم إرسالهم إلى الشخص الذي يهدف إلى التواصل معه. ثـــم جاء بعده العديد من الأشخاص الذين استخدموا الناس والحيوانات والخشب المغطـــى بالشمع كوسيلة للتواصل مع الناس بطريقة خفية. واستمر تطور هـــذا العلـــم، حتـــى

1- مرام عبدالرحمن مكاوي، علم الإخفاء، مجلة المعرفة، العدد 147، 2010، ص212.

2- Tom St Denis (2004), Cryptanalysis in Society. "Cryptanalysis in Society.pdf", P6.

توصل العالم إلى اختراع الحبر السري إبان الحرب العالمية الثانية، والذي ساهم كثيراً في التواصل بين أطراف الحرب بطريقة بعيدة عن الشبهات وسالمة من التعقب وكشف الأسرار. وقد تطور علم الإخفاء في الوقت الحالي كثيراً، فأصبح يستخدم المعلومات الرقمية والحواسيب كوسيلة لنقل البيانات.

أهمية علم الإخفاء:

لإخفاء المعلومات أهمية كبيرة وذلك لأن عدم ظهور المعلومات سواء مشفرة أو غير مشفرة للعيان عاملاً مساعداً على إضفاء المزيد من الأمن والحماية على هذه المعلومات. يستخدم هذا الفن في عدد من المجالات إلا أن المجال الذي يبرز فيه هذا الفن هو التجارة الإلكترونية التي تزداد تطبيقاتها، والاهتمام بها يومًا بعد يوم، ومن تطبيقات هذا العلم، العلامات المائية (Watermarks) والتي تستخدم في عمليات حفظ الحقوق للمنتجات الرقمية، والحد من عمليات القرصنة. وبالرغم من أن المشتري أو مستخدم هذه البرامج قد يعلم بوجود مثل هذه العلامات، إلا أن اكتشاف أماكنها داخل البرنامج من الصعوبة بمكان. وعلى افتراض أن المستخدم قد تعرف على مكان وجود هذه العلامة، فسيظهر أمامه تحدٍ آخر، وهو معرفة البرنامج المستخدم في الإخفاء وكلمة السر ومفتاح التشفير، وكلاً من هذه الأشياء قد يستغرق اكتشافه وقتاً زمنياً طويلاً.

الفرق بين علم التشفير وعلم الإخفاء[1]:

لاكتشاف أهم فرق بين علم التشفير وعلم الإخفاء نكتفي بعرض تعريف لكليهما. فعلم التشفير هو العلم الذي يهدف إلى دراسة طرق إرسال الرسالة بصورة أخرى لا يستطيع فك رموزها إلا المرسل والمستقبل. بينما علم الإخفاء هو العلم الذي يهدف إلى إخفاء وجود الرسالة. إذن الفرق الأساسي هو أن التشفير يغير من هيئة

1- مرام عبدالرحمن مكاوي، مصدر سابق، ص215.

محتوى الرسالة بحيث لا يستطيع أحد قراءتها سوى الأطراف المعنية بهـا، لكنـه لا يخفي وجودها. أما علم الإخفاء فيخفي محتوى الرسالة في المقام الأول. وفيمـا يلـي مقارنة بينهما في النواحي الأخرى:

النـــوع / وجه المقـارنة	علم التشفـير	عـلم الإخفـــاء
من حيث العلم بوجود الرسالة	يعلم بوجود الرسالة	لا يعلم بوجود الرسالة
من حيث الاتصال	يمنع الأطراف الآخرين من معرفة محتوى الاتصال	يمنع الأطراف الآخرين من معرفة وجود الاتصال
من حيث الشيوع والانتشار	تقنية شائعة	تقنية غير شائعة

جدول1: مقارنة بين علم التشفير وعلم الإخفاء

علم التشفير وعلم الإخفاء هما طريقتان لحماية المعلومـات مـن عرضـها والعبث بها من قبل الأشخاص غير المخولين، لكن كلا من الطريقتين لو اسـتخدمت لوحدها، قد لا تعتبر وسيلة حماية كافية وكاملة. بالنسبة لإخفاء المعلومات مثلا، حالما يكتشف أو يشك أحد المهاجمين بوجود معلومات مخفية في مكان ما، فإن الهدف مـن عملية الإخفاء يصبح بلا قيمة! لذا فإنه ولزيادة حماية المعلومات المخفاة يجب علينـا استخدام كلاً من تقنيات حماية المعلومات، التشفير والإخفاء.

وخلاصة القول بأنه بالرغم من الأهمية الكبيرة والفوائد الجليلة التي يقـدمها هذا العلم إلا أن انتشاره حتى هذه اللحظة لا يقارن بانتشار علم التشفير. وكما ذكرنـا آنفاً بأن القوة التي ينتجها اتحاد هذان العلمان قد تكون قوة لا يُستهان بهـا حيـث أن اجتماعهما مع بعضهما البعض يؤدي إلى حصولنا على رسائل سرية صعبة في فـك التشفير وصعبة في إدراك وجودها.

طرق التشفير:

التشفير له طرق وأساليب متعددة سيتم التركيز على الطرق التقليديـــة منهـــا، ويقصد بالتقليدية هي الطرق القديمة التي استخدمت قبل اختراع الحاسب الآلـــي. أمـــا الآن فقد تطور علم التشفير وطرقه مع مرور الوقت وتم التوصل إلى طـــرق تـــشفير حديثة ذات كفاءة وفعالية عالية، لكنّها في أساسها تعتمد على أساسيات وخوارزميـــات طرق التشفير التقليدية[1].

أهم طرق التشفير التقليدية:

من المهم أن نوضح قبل البدء في شرح طرق التشفير التقليدية، أن جميـــع هـــذه الطرق تعتمد نظام التشفير المتماثل أو المتناظر، وأهم ما يميز هذا النوع من التشفير هـــو أن عمليتي التشفير وفك التشفير تكونان باستخدام مفتاح واحد يملكه المرسل والمستقبل.

وينقسم التشفير التقليدي إلى نوعين رئيسيين هما[2]:

التشفير بالإحلال *Substitution* :

التشفير بهذه الطريقة يكون عن طريق استبدال حرف أو رقـــم مـــن الـــنص الأصلي بحرف أو رقم آخر يحل محله في النص المشفر. عملية الإحلال هذه تكـــون عن طريق جمع مفتاح ما إلى الحرف من النص الأصلي.

التشفير بالإبدال *Transposition* :

في هذا النوع من التشفير يتم تغيير أماكن حروف النص الأصلي، أي مجرد تبديل في المواقع.

1- خالد العامري، عبدالحميد عبدالعاطي، حيل وأساليب الهاكرز وطرق الوقاية منها، الفصل العاشر: عناصر التشفير، دار الفاروق للنشر والتوزيع، القاهرة، مصر، ط:2، 2005، ص77.

2- وجدي عصام عبدالرحيم، مقدمة في التشفير بالطرق التقليدية، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، ط:2، 2007، ص51.

وفيما يلي نسرد أمثلة لأهم الشفرات التقليدية التي استخدمت قـديماً، والتـي بُنيت على أساسها معظم الشفرات الحديثة المتداولة في عالمنا اليوم.

شفرة قيصر *The Caesar Cipher*:

سُميت شفرة قيصر نسبة إلى يوليوس قيـصر الـذي يُقـال بأنـه أول مـن استخدمها. وفيها يتم استبدال كل حرف بحرف آخر يكون تسلسله ثابـت بعـده فـي ترتيب الحروف الأبجدية.

فمثلاً إذا استخدمنا إزاحة مقدارها **(5)** خانات، فإن ترتيب الحروف سـيكون على النحو التالي:

ترتيب الحروف الأبجدية	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
إزاحة قدرها 5 خانات	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

ولنأخذ مثالاً يتم من خلاله تشفير نص واضح مثل[1]:

Smoking is bad to health

باستخدام الجدول أعلاه سنضع (x) بدلاً من (s)، ونضع (r) بدلاً مـن (m)، وهكذا بالنسبة لبقية الأحرف مع الحفاظ على المسافات بينها، سيظهر لنا النص المشفّر التالي:

xrtpnsl nx gfi yt mjfqym

أما فك التشفير باستخدام هذه الطريقة فهو سهل وبسيط ولا يـستلزم سـوى معرفة مقدار الإزاحة، فمـثلاً إذا كـان لـدينا الـنص المـشفّر: rd gwtymjw xtrjynrjx mjqux rj ويُراد التعرّف على النص الواضح باستخدام شفرة قيـصر

1- Ke CHEN (2005), Cryptography. School of Informatics, The University of Manchester. "lec03.pdf", P32.

وإزاحة مقدارها (5) خانات فإنه باستخدام الجدول السابق أيضاً سنحصل على الـــنص الواضح والذي هو عبارة عن:

My brother sometimes helps me

وبالتأكيد لن يقف الأمر عند مقدار الإزاحة **(5)** حيث يمكننا استخدام مقـــادير أخرى أصغر أو أكبر، فمثلاً لو أردنا أن نستخدم مقدار الإزاحة **(10)** عندها ســـيتغير الجدول السابق ليكون على النحو التالي:

ترتيب الحروف الأبجدية	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
إزاحة قدرها 10 خانات	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

فإذا كان لدينا النص الواضح: My country is Libya، وأردنا تـــشفيره باستخدام الجدول السابق حيث الإزاحة مقدارها (10) خانات فإن النص النـــاتج عـــن عملية التشفير سيكون كالتالي:

Wi myexdbi sc vslik

والأمر يكون بصورة عكسية عند فك التشفير، فمثلاً إذا كـــان لـــدينا الـــنص المشفّر التالي:

dbszyvs sc mkzsdkv yp vslik

وأردنا التعرّف على النص الواضح باستخدام شفرة قيصر وإزاحة مقـــدارها (10) فإننا سنحصل على النص الواضح التالي:

Tripoli is the capital of Libya

مما سبق نلاحظ أن شفرة قيصر هي شفرة بسيطة، وذلك لأن الحروف هـــي نفسها عند استخدام نفس مقدار الإزاحة فمثلاً عندما استخدمنا مقدار الإزاحة (10) في المثالين السابقين لاحظنا بأن:

vslik = Libya ،sc = is

وهذا ما يجعل هذه الشفرة ضعيفة، والسبب الرئيسي في ضعفها هو إمكانية توقع النموذج المستخدم بكامله، فما على من يريد فك التشفير إلا عدد (25) محاولة فقط للوصول إلى النموذج المستخدم وبالتالي فك الشفرة.

ولهذا تم استخدام شفرة أخرى أكثر تعقيداً هي شفرة فيرنام.

شفرة فيرنام *Vernam Cipher*:

ابتكرها العالم جلبيرت فيرنام (*Gilbert Vernam*) وهي تعتبر شفرة مقاومة لأكثر الهجمات التحليلية، ومن الأشياء التي شجعت على استخدام هذه الشفرة هي سهول تنفيذها.

سنستخدم في هذه الشفرة مقياس 26 ، وهو ناتج باقي القسمة على 26 مع ملاحظة أن العدد إذا كان أصغر من 26 فإن الناتج في هذه الحالة هو العدد نفسه، فمثلاً: 30 بمقياس 26 يساوي 4، 45 بمقياس 26 يساوي 19، 60 بمقياس 26 يساوي 8.

أما 12 بمقياس 26 فيساوي 12، وكذلك 25 بمقياس 26 يساوي 25 ... وهكذا، وسنحتاج إلى تحويل الحروف إلى ما يقابلها من أعداد كما يلي:

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

وأخيراً سنحتاج إلى سلسلة من الأرقام العشوائية لدمجها مع الأعداد المناظرة للحروف الأبجدية، ومن خلال تسميتها بالعشوائية فمعنى ذلك أنه يشترط فيها أن لا تتبع أي نظام ترتيب مُحدد كأن تكون سلسلة من الأعداد الفردية أو الزوجية أو

الأعداد التي تقبل القسمة على 3 بدون باق. بل لابد أن تكون مكونـــة مـــن الأعـــداد العشوائية التي يستحيل توقعها، ولبيان هذه الطريقة نأخذ المثال التالي:

سنقوم بتشفير النص الواضح We live in Zliten مـــستخدمين شـــفرة فيرنام وسلسلة الأرقام العشوائية التالية:

72 44 12 85 40 02 51 13 60 04 46 90 32 87 55

06 36 65 وذلك باستخدام الخطوات الموضّحة في الجدول التالي:

النـــص الواضـــح	W	E	L	I	V	E	I	N	Z	L	I	T	E	N
ترتيب الحـــروف	22	4	11	8	21	4	8	13	25	11	8	19	4	13
الأرقـــام العشوائية	72	44	12	85	40	02	51	13	60	04	46	90	32	87
المجمـــــوع	94	48	23	93	61	06	59	26	85	15	54	109	36	100
مقيـــاس 26	16	22	23	15	09	06	07	0	07	15	02	05	10	22
النـــص المشفّـــر	Q	W	X	P	J	G	H	A	H	P	C	F	K	W

وعليه فإن النص المشفّر الذي حصلنا عليه باستخدام هذه الطريقة هو:

QW XPJG HA HPCFKW

لاحظ أن:

حرف E تحوّل في المرة الأولى إلى W وفي المرة الثانية إلـــى G وفـــي المرة الثالثة إلى K.

كذلك حرف I تحوّل في المرة الأولى إلى P وفي المرة الثانية إلى H وفي المرة الثالثة إلى C.

حرف L تحوّل في المرة الأولى إلى X وفي المرة الثانية إلى P .

حرف N تحوّل في المرة الأولى إلى A وفي المرة الثانية إلى W .

وهذا ما يعكس قوة هذه الشفرة مما جعلها الشفرة المعتمدة فـــي المراســـلات العسكرية لسنوات طويلة.

وبالمثل يمكننا استخدام هذه الشفرة بنفس الأرقام العـشوائية لتـشفير الـنص الواضح We are friends وسنحصل في نهاية الأمر على النص المشفّر QW MYS HQVMRXE

التشفير الضربي *Multiplicative Cipher*:

هو طريقة تشفير تستخدم مقياس 26 (MOD 26) ومفتـاح للتـشفير (K) بحيث يكون القاسم المشترك الأكبر بين المفتاح الذي نختاره والعـدد 26 يـساوي 1 وهذه الطريقة تتبع القانون التالي:

$$C = (K * M) \text{ MOD } 26$$

حيث K هو مفتاح التشفير، M حرف من النص الواضح، C يمثـل نـاتج المعادلة وهو الحرف المشفّر.

(ملاحظة: القاسم المشترك الأكبر لعددين هو أكبر عدد صحيح يقبل القـسمة على العددين).

وسنحتاج في هذه الطريقة أيضاً إلى تحويل الحروف إلى ما يقابلها من أعداد كما مرّ بنا من قبل .

ولتوضيح هذه الطريقة نأخذ المثال التالي[1]:

نود تشفير كلمة NETWORK باستخدام طريقة التشفير الضربي، والمفتاح (K=5).

نقوم بإتباع القانون أعلاه كما يلي:

$C_1 = 5 * 13 = 65 \text{ MOD } 26 = 13 \leftrightarrow N$

$C_2 = 5 * 4 = 20 \text{ MOD } 26 = 20 \leftrightarrow U$

1- Ke CHEN (2005), Cryptography. School of Informatics, The University of Manchester. "lec03.pdf", P44.

$C_3 = 5 * 19 = 95 \ MOD\ 26 = 17 \leftrightarrow R$

$C_4 = 5 * 22 = 110 \ MOD\ 26 = 6 \leftrightarrow G$

$C_5 = 5 * 14 = 70 \ MOD\ 26 = 18 \leftrightarrow S$

$C_6 = 5 * 17 = 85 \ MOD\ 26 = 7 \leftrightarrow H$

$C_7 = 5 * 10 = 50 \ MOD\ 26 = 24 \leftrightarrow Y$

وبهذا نرى بأن كلمة NETWORK قد تحولت إلى الكلمة المشفّرة NURGSHY بعد تشفيرها بهذه الطريقة وباستخدام المفتاح (K=5).

أما عند استخدامنا لمفتاح آخر فإن النتيجة ستختلف بالتأكيد، فمثلاً عند قيامنا بتشفير نفس الكلمة السابقة (NETWORK) بنفس الطريقة السابقة (طريقة التشفير الضربي) مع اختلاف المفتاح هذه المرة وليكن (K=7) فإننا سنحصل على النتيجة التالية:

$C_1 = 7 * 13 = 91 \ MOD\ 26 = 13 \leftrightarrow N$

$C_2 = 7 * 4 = 28 \ MOD\ 26 = 2 \leftrightarrow C$

$C_3 = 7 * 19 = 133 \ MOD\ 26 = 3 \leftrightarrow D$

$C_4 = 7 * 22 = 154 \ MOD\ 26 = 24 \leftrightarrow Y$

$C_5 = 7 * 14 = 98 \ MOD\ 26 = 20 \leftrightarrow U$

$C_6 = 7 * 17 = 119 \ MOD\ 26 = 15 \leftrightarrow P$

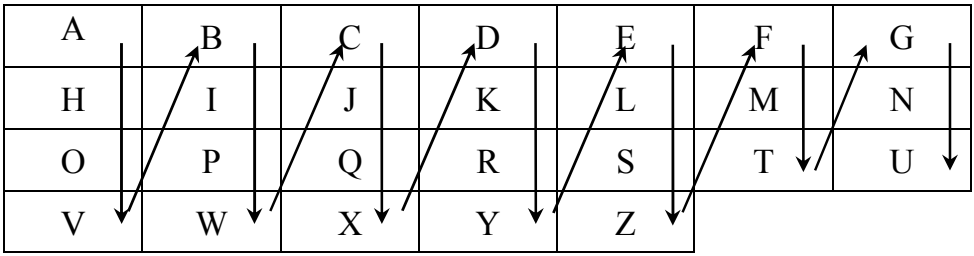
$C_7 = 7 * 10 = 70 \ MOD\ 26 = 18 \leftrightarrow S$

وسيكون الناتج هو الكلمة المشفّرة NCDYUPS وهو مختلف عما حصلنا عليه في المرة السابقة.

طريقة Zig-Zag:

تعتمد هذه الطريقة على استخدام نموذج معين في ترتيب الحروف الأبجدية كأن تُرتب مثلاً بحيث تكون كل **7** حروف في سطر، كذلك تعتمد على العمق المستخدم في الانتقال بين الحروف خلال النموذج.

فمثلاً لتشفير كلمة TEACHER باستخدام هذه الطريقة بعمق (4) ونموذج الحروف الهجائية بتنسيق 7 حروف في كل سطر، نحصل على ما يلي[1]:



عند انتقال حرف (T) بواقع 4 خانات فإنه يتحول إلى الحرف (A)، وكذلك إذا انتقل حرف (E) 4 خانات فإنه سيتحول إلى الحرف (F) ... وهكذا لبقية حروف كلمة TEACHER وسنحصل في النهاية على الكلمة المشفّرة AFBDIFS.

أما بالنسبة لفك التشفير بهذه الطريقة فهو سهل للغاية، وكل ما علينا فعله هو عكس المسار بالرجوع للخلف حسب العمق المستخدم، ولنأخذ المثال التالي لتوضيح ذلك:

إذا طُلب منا فك تشفير الكلمة MDYBPA باستخدام هذه الطريقة بعمق (8)، ونموذج الحروف الهجائية بتنسيق 5 حروف في كل سطر.

1- وجدي عصام عبدالرحيم، مقدمة في التشفير بالطرق التقليدية، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، ط:2، 2007، ص62.

أول ما نقوم به هو كتابة الحروف الأبجديـــة وفقـــاً للنمـــوذج المطلـــوب (5 حروف في كل سطر) كما يلي:

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				

وباستخدام هذا النموذج، وعند رجوعنا للخلف بكل حـــرف بمقـــدار العمـــق المطلوب وهو 8 خانات، نلاحظ التغييرات التالية:

حرف (M) تحوّل إلى حرف (Z)

حرف (D) تحوّل إلى حرف (L)

حرف (Y) تحوّل إلى حرف (I)

حرف (B) تحوّل إلى حرف (T)

حرف (P) تحوّل إلى حرف (E)

حرف (A) تحوّل إلى حرف (N)

وبهذا نكون قد استطعنا فك تشفير الكلمة (MDYBPA) والوصـــول إلـــى الكلمة الأصلية وهي (ZLITEN).

ملاحظة: لعلنا أصبحنا نُدرك الآن بأن العمق المستخدم مهما كان كبيراً فإنه لن يشكّل عائقاً، لأنه باستخدام مفهوم مقياس 26 الذي مرّ بنا من قبل أصبح جليـــاً بأنـــه علـــى سبيل المثال: عمق (2) هو نفسه عمق (80)، كذلك عمق (6) هو نفسه عمق (110)، وعمق (12) كذلك نفسه عمق (792) .... وهكذا.

طريقة المربع الكامل:

طريقة التشفير:

تتلخص هذه الطريقة فيما يلي:

1- يُحدد عدد الأعمدة للمربع بنفس طول المفتاح المُستخدم.

2- تُكتب الرسالة الواضحة بالترتيب تحت أحرف المفتاح.

3- إذا بقيت مربعات فارغة فيتم إكمالها بأحرف تُستخدم بكثرة مثل حرف (e) في اللغة الانجليزية.

4- نقوم بإعطاء أرقام لحروف المفتاح، وذلك حسب تسلسل ترتيبها في الحروف الأبجدية.

5- نبدأ بكتابة النص المُشفّر ابتداءً من العمود الأول ثم العمود الثاني، وهكذا إلى بقية الأعمدة، وذلك حسب ترتيب حروف المفتاح.

ملاحظة: يجب الحرص على اختيار مفتاح تشفير بحيث يكون كلمة جميع حروفها مختلفة عن بعضها ولا يوجد حرفان متشابهان، لأن ذلك سيوقعنا في أخطاء عند التشفير وفك التشفير.

ولتوضيح آلية التشفير باستخدام طريقة المربع الكامل نأخذ المثال التالي[1]:

إذا كان لدينا النص الواضح: There is nothing new under the sun ويُراد تشفيره باستخدام طريقة المربع الكامل، والمفتاح (ENGLISH).

فإن أولى خطوات الحل تبدأ بإنشاء جدول عدد أعمدته بطول المفتاح (أي عدد أحرف المفتاح)، وفي هذه الحالة 7 أحرف أي جدول مكوّن من 7 أعمدة، أما

1- Ke CHEN (2005), Cryptography. School of Informatics, The University of Manchester. "lec03.pdf", P59.

عدد صفوفه فيعتمد على طول النص المُراد تشفيره، ثم نقوم بإعطاء أرقام لحـــروف المفتاح وذلك حسب تسلسل ترتيبها في الحروف الأبجدية كما يلي:

E	N	G	L	I	S	H
1	6	2	5	4	7	3
T	H	E	R	E	I	S
N	O	T	H	I	N	G
N	E	W	U	N	D	E
R	T	H	E	S	U	N

الآن نبدأ بكتابة النص المُشفّر ابتداءً من العمود الذي يحمل الرقم 1 ثم العمود الذي يحمل الرقم 2 وهكذا حتى العمود رقم 7 لنحصل على النص المـــشفر التـــالي، والذي هو عبارة عن تشفير للعبارة المذكورة أعلاه.

TNNR ETWH SGEN EINS RHUE HOET INDU

طريقة فك التشفير:

لفك التشفير نستخدم نفس طريقة التشفير، ولكن بصورة معكوسة كما يلي:

1- إنشاء جدول عدد أعمدته يساوي طول المفتاح.

2- نكتب المفتاح في الصف الأول من هذا الجدول.

3- نقوم بإعطاء أرقام لحروف المفتاح وذلك حسب تسلسل ترتيبهـــا فـــي الحـــروف الأبجدية.

4- نكتب النص المشفر عموداً عموداً في الجدول مع مراعاة الترتيب.

5- يُقرأ النص الصريح على هيئة صفوف من الجدول.

ولنأخذ المثال التالي لتوضيح طريقة فك التشفير.

إذا كـــان لـــدينا الـــنص المـــشفر: IUUR EECT LOOR WKRN، والمطلوب هو فك تشفير هذا النص وتحويله إلى نص واضـــح باســـتخدام الطريقـــة السابقة ومفتاح التشفير (TIME).

أولاً نقوم بإعطاء أرقام لمقاطع هذا النص بالترتيب كما يلي:

IUUY EECT LOOR WKRN

1 2 3 4

ثم نقوم بإنشاء جدول عدد أعمدته بطول المفتاح (أي عدد أحرف المفتـــاح)، وفي هذه الحالة 4 أحرف أي جدول مكوّن من 4 أعمدة، ثـــم نقـــوم بإعطـــاء أرقـــام لحروف المفتاح وذلك حسب تسلسل ترتيبها في الحروف الأبجدية ثم نكتـــب الـــنص المشفر عموداً عموداً في الجدول مع مراعاة الترتيب كما يلي:

T	I	M	E
4	2	3	1
W	E	L	I
K	E	O	U
R	C	O	U
N	T	R	Y

ومن خلال هذا الجدول نقوم بقراءة النص الصريح عبر الصفوف من الصف الأول إلى الصف الأخير ليظهر لنا النص التالي:

WELIKEOURCOUNTRY

وبإجراء قليل من التعديلات على هذا النص نحصل على النص الصريح في صورته النهائية والذي يمثل العبارة:

WE LIKE OUR COUNTRY

طريقة الإبدال العمودي:

وفيها يتم اختيار مفتاح رقمي بطول (d) ويكون المفتاح عبارة عـــن أرقـــام متسلسلة تم إعادة ترتيبها بشكل معين. يتم توزيع النص الصريح بالتسلسل على جدول يكون عدد أعمدته يساوي طول المفتاح، وعدد الصفوف يعتمد علـــى طـــول الـــنص الواضح.

عند التشفير يتم قراءة الأعمدة اعتماداً على المفتاح المستخدم، وكمثال علـــى هذه الطريقة دعونا نقوم بتشفير كلمة CRYPTOGRAPHY حيث D = 4 (تمثـــل طول المفتاح وعدد الأعمدة)، ومفتاح التشفير هو K=3142[1] .

وعندها سيكون لدينا الجدول:

1	2	3	4
C	R	Y	P
T	O	G	R
A	P	H	Y

اعتماداً على المفتاح (K=3142) سيتم قراءة الأعمدة بالشكل التالي والـــذي يمثل النص المشفر:

النص المشفر = YGH CTA PRY ROP

أما فك التشفير في هذه الطريقة فيعتبر سهلاً، وذلك بإتباع المنطق المعـــاكس لطريقة التشفير.

1- Alistair Donaldson (2001), Strategy for cryptographic support services in the NHS. "Strategy for cryptographic support services in the NHS crypstra.pdf", P46.

طريقة عكس الرسالة:

الطريقة بسيطة للغاية، وفيها نأخذ النص الواضح ونعكس كتابة حروفه لنحصل على النص المشفر كما يلي:

النص الواضح = Smoking is bad to health

النص المشفر = htlaeh ot dab si gnikoms

وبعد تقسيمها إلى كتل (من 5 حروف مثلاً) يصبح لدينا:

htlae hotda bsign ikoms

كما يمكن تقسيمها إلى كتل من 4 حروف أيضاً لتكون على الشكل:

htla ehot dabs igni koms

الدمج بين طريقتي الإبدال والإحلال:

شفرة ADFGVX :

وهي شفرة ألمانية استخدمها هتلر أثناء الحرب العالمية الثانية، وقد استعصت هذه الشفرة على الفك والكسر لفترة من الزمن، ولكنها كُسرت في نهاية المطاف على يد عالم فرنسي بعد أن استغرقت منه الكثير من الوقت والجهد في المحاولات[1].

وطريقة عمل هذه الشفرة تتلخص في ثلاث خطوات رئيسية، ولتوضيحها نأخذ المثال التالي[2]:

الخطوة الأولى: ليكن لدينا الجدول التالي، الذي سنستخدمه في التشفير مرتين:

1- Kirk Job-Sluder (2002), Cryptography: A guide to protecting your files for consultants, educators and researchers. Indiana University. "IST_Conf_2002_sluder.pdf", P86.

2- Claire Topping, (2003). General Cryptographic Knowledge. White Paper "general_cryptographic_knowledge3.pdf", P112.

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

(لاحظ أن الحرفان Q، Z معاً داخل خانة واحدة، وذلك مـــن أجـــل اكتمـــال الجدول ليكون مصفوفة 5*5).

الآن وعلى سبيل المثال أريد أن أشفّر الحرف A، الناتج هو الحرف الذي في أول الصف، والحرف الذي في أول العمود. أي أن A يتم تشفيره إلى الحـــرفين AA (أي بأخذ الصف والعمود الذي يقع فيه الحرف المراد تشفيره).

وهكذا بالنسبة لبقية الحروف، فمثلاً:

الحرف B يتم تشفيره إلى الحرفين AB

الحرف C يتم تشفيره إلى الحرفين AC

الحرف Q يتم تشفيره إلى الحرفين DB

الحرف Y يتم تشفيره إلى الحرفين EE

الحرف Z يتم تشفيره إلى الحرفين DB

مثال: ليكن لدي العبارة التالية (النص الأصـــلي): TAKE ME TO YOUR LEADER

نبدأ الآن بالتشفير، الحرف T يتم تشفيره إلى DE، الحرف الثـــاني A يـــتم تشفيره إلى AA، وهكذا لتنتج لدي الشفرة:

DE AA CA AE CC AE DE CE EE CE EA DC CB AE AA AD AE DC

انتهت الخطوة الأولى التي تمّ فيها تشفير الحرف الواحد في النص الأصـــلي إلى حرفين.

الخطوة الثانية: نقوم بتقسيم النص المشفّر إلى قسمين (صفين)، وأخذ الحـــرف الأول من الصف الأول والحرف الأول من الصف الثاني، وأخذ الحرف الثاني من الـــصف الأول وأخذ الحرف الثاني من الصف الثاني، وهكذا ...

النص المشّفر هو:

DE AA CA AE CC AE DE CE EE CE EA DC CB AE AA AD AE DC

بعد تقسيمه إلى صفين ينتج لدينا:

DE AA CA AE CC AE DE CE EE
CE EA DC CB AE AA AD AE DC

الآن نأخذ الحرفين D ، C ليكونا الكتلة الأولى، والحرفـــان E ، E ليكونـــا الكتلة الثانية، وهكذا لينتج لدينا:

DC EE AE AA CD AC AC EB CA CE AA EA DA ED CA EE ED EC

الخطوة الثالثة: نقوم بالرجوع إلى الجدول السابق، الذي ذكرنا أننا سنستخدمه مرتين، ونقوم بتشفير كل كتلة على حده:

الكتلة الأولى DC حرفاها يتقاطعان في الجدول عند الحرف R .

الكتلة الثانية EE حرفاها يتقاطعان في الجدول عند الحرف Y .

ونستمر بنفس الطريقة لينتج لدينا:

R Y E A N C C V K O A U P X K Y X W

الآن نقوم بوضع الناتج على شكل كتل، كل كتلة تتكون من 5 حروف:

RYEAN CCVKO AUPXK YXW

وبهذا نكون قد أنهينا عملية التشفير، معقدة قليلاً، ولكنها جيدة إلى حد ما.

ولفك التشفير، نقوم بالعملية العكسية، لنفك الشفرة الناتجة من عملية التشفير السابقة:

RYEAN CCVKO AUPXK YXW

نبدأ بأخذ الحرف الأول، ثم ننظر إلى الجدول ونأخذ الحرفين اللـــذين نقطـــة تقاطعهما الحرف المُراد، ونضع الحرف الأول في الصف الأول، والحـــرف الثـــاني نضعه في الصف الثاني، وهنا أول حرف في الشفرة هو R ، ننظر إلـــى الجـــدول، نلاحظ أن الحرفين D ، C نقطة تقاطعهما هو R ، لذلك نضع الحرف الأول D فـــي الصف الأول، والحرف الثاني C في الصف الثاني، ونستمر بهذه الطريقـــة إلـــى أن نُكمل حروف الشفرة، والناتج هو:

DE AA CA AE CC AE DE CE EE
CE EA DC CB AE AA AD AE DC

الآن نبدأ بفك التشفير من الصف الأول، ونأخذ كتلة تلو الأخرى من الـــصف الأول، وعندما ينتهي نبدأ بالصف الثاني:

الكتلة DE تتحول إلى الحرف T

الكتلة AA تتحول إلى الحرف A

الكتلة CA تتحول إلى الحرف K

وهكذا لينتج لدينا النص الأصلي: TAKEMETOYOURLEADER

قم بترتيبه بحيث يكون قابلاً للقراءة، لينتج:

TAKE ME TO YOUR LEADER

خـــاتمـــــة:

حملت لنا الإنترنت التي تضم مجموعة كبيرة من الشبكات حول العالم فوائـد جمة، وأصبحت وسيلة سهلة وممتعة تُتيح لملايين البشر الوصول إلى كم هائـل مـن المعلومات، إضافةً إلى التواصُل وتبادُل المعلومات والرسائل فيما بينهم. ولكن بعـض العوامل مثل الطبيعة المفتوحة لهذه الشبكة، وعدم وجود أي جهة يمكنها الادعاء بأنها تمتلكها أو تسيطر عليها، وعدم وجود قوانين مركزية رادعة، أدَّت إلى انتشار العديـد من الجرائم مثل التجسس على الحسابات البنكية وبطاقات الائتمان، وكـذلك تخريـب أجهزة الحاسوب وملفاتها، وَشَنّ هجوم الفيروسات على البريد الإلكتروني، إضافة إلى عمليات التصنت والخداع وغيرها[1].

وبالرغم أن الإنترنت ليست البيئة الوحيدة التي تحدُث فيها الجرائم والمخالفات القانونية، إذ أن الجريمة ظاهرة موجودة في مجتمعات عديدة، إلا أن المشكلة الرئيسية تكمن في عدم وجود قوانين حازمة ورادعة تحمي مستخدمي الإنترنت.

ومما سبق نجد أن أمن المعلومات والإنترنت أصبح شأناً مهماً لا بد مـن حـل مشاكله، نظرا لأهمية هذا الأمن في عمليات تبادُل المعلومات الشخصية ومعلومات العمل، وتشكل قضايا الأمن والتهديدات الناتجة عنها العائق الأكبر أمـام اكتـساب ثقـة النـاس ومشاركتهم في تقدم الإنترنت، وتبقى مسألة الحفاظ على أمن الإنترنت باعتمـاد وسـائل سهلة واقتصادية من أكثر المسائل التي تشكِّل حالياً تحدياً كبيراً لهذه التقنية، ومـع غيـاب هذه القوانين والتشريعات التي تحمي رواد هذه الشبكة فقد باتت الحاجـة ملحـة لابتكـار طرق تشفير قوية لأن التطور السريع للحاسبات يضعف من قوة التشفير؛ وذلك لان زيادة سرعة الحاسوب تعني اختصار الوقت الذي يحتاجه لفك أو كسر مفتاح تشفير معين.

1- خالد الغثبر، محمد القحطاني، أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، المملكة العربية السعودية، ط:2، 2009، ص261.

المراجـع

أولاً: المراجع العربية:

1- علاء حسين الحمامي، سعد عبدالعزيز العاني، تكنولوجيا أمنية المعلومات وأنظمة الحماية، دار وائل للنشر والتوزيع، ط:1، 2007، عمان، الأردن.

2- علاء حسين الحمامي، مازن سمير الحكيم، التشفير والترميز حماية ضد القرصنة والتطفل، الدار العربية، بغداد، العراق، 1999.

3- دلال صادق، حميد الفتال، أمن المعلومات، الفصل التاسع: الترميز والتشفير، دار اليازوري العلمية للنشر والتوزيع، ط:1، 2008، عمان، الأردن.

4- مرام عبدالرحمن مكاوي، علم الإخفاء، مجلة المعرفة، العدد 147، 2010.

5- خالد العامري، عبدالحميد عبدالعاطي، حيل وأساليب الهاكرز وطرق الوقاية منها، الفصل العاشر: عناصر التشفير، دار الفاروق للنشر والتوزيع، القاهرة، مصر، ط:2، 2005.

6- وجدي عصام عبدالرحيم، مقدمة في التشفير بالطرق التقليدية، دار المسيرة للنشر والتوزيع والطباعة، عمان، الأردن، ط:2، 2007.

7- محمد صالح، علاء العزاوي، التشفير والترميز- النظرية والتطبيق، دائرة التدريب، العراق، 2001.

8- رعد مهجر، نهلة فليح، تشفير الملفات النصية باستعمال المفتاح المتناظر، مجلة كلية العلوم، جامعة البصرة، العدد 32، 2006.

9- رائد عبدالعزيز العريقي، تشفير وفك تشفير الصور الرقمية، رسالة ماجستير غير منشورة، بغداد، كلية علوم وهندسة الحاسب، 2007.

10- إبراهيم سليمان عبدالله، أمن المعلومات، دار المريخ للنشر والتوزيع والطباعة، المملكة العربية السعودية، ط:1، 2008.

11- خالد الغثبر، محمد القحطاني، أمن المعلومات بلغة ميسرة، مركز التميز لأمـــن المعلومات، جامعة الملك سعود، الرياض، المملكة العربية السعودية، ط:2، 2009.

ثانياً: المراجع الأجنبية:

1- Ke CHEN (2005), Cryptography. School of Informatics, The University of Manchester. "lec03.pdf".

2- Erkay Savas (2002), DATA SECURITY & CRYPTOGRAPHY. Oregon State University & rTrust Technologies. "L1.pdf".

3- Tal Malkin (2003), Introduction to Cryptography. "Summary1 What is Cryptography.pdf".

4- Tom St Denis (2004), Cryptanalysis in Society. "Cryptanalysis in Society.pdf".

5- Alistair Donaldson (2001), Strategy for cryptographic support services in the NHS. "Strategy for cryptographic support services in the NHS crypstra.pdf".

6- Claire Topping, (2003). General Cryptographic Knowledge. White Paper "general_cryptographic_knowledge3.pdf".

7- Scott Wilson (2004), An Introduction to Cryptography. "Intro To Crypto.pdf".

8- Kirk Job-Sluder (2002), Cryptography: A guide to protecting your files for consultants, educators and researchers. Indiana University."IST_Conf_2002_sluder.pdf".

9- W. M. Farmer (2003), Overview of Cryptography. "cryptographyoverview.pdf".