أمن وحماية النظام

المعلومة:-

هي كل ما يعرفه الإنسان عن قضية ما أو عن حادث أو هي الأخبار والتحقيقات أو هي كل ما يؤدي إلي كشف الحقائق الموصلة لرسالة تستخدم لتمثيل حقيقة أو مفهوم باستخدام البيانات أو هي عملية توصيل حقائق أو مفاهيم من أجل زيادة المعرفة أو هي شي غير محدد المعالم . وقد تكون مصادر المعلومة عدة أشكال كالصورة أو الخريطة أو غيرها تحملها أوعية تدرجت في تطورها عبر الزمن.

مصادر المعلومات :

المكاتبات والالتزامات المرتبطة بحقوق الأفراد والهيئات وهي تجاوزا أوعية الإداريات أو أوعية القراءات والبحوث ولكل من تلك المصادر طريقة خاصة في الإنتاج والاختزان.

مؤسسات إستخدام المعلومات:

بعد أن كانت المعلومات حكرا علي فئة معينة تستأثر بها أصبحت متطورة ونشأت في مراحل وتطورت المؤسسات الإستخدامية لكل أنماط القراء والباحثين في المجتمعات العصرية. وعرفت هذه المؤسسات بتسميات مختلفة مثلاً :

بيت الحكمة، دار الحكمة ، خزانة الكتب ثم المكتبة بأنواعها قومية – خاصة – مدرسية – عامة – متخصصة. كما عرفت دور الوثائق ومراكز المعلومات وبنوك المعلومات والمراصد.

أمن المعلومات والوثائق:-

يمكن عن طريق المعلومات والوثائق بناء الكثير من الخطط وتعتبر سرية وأمن المعلومات من المقومات الأساسية للمكاتبات التي تسهم في المحافظة علي المعلومات. فهناك معلومات أو مكاتبات ذات طابع سري كالمشروعات في مرحلة الدراسة أو بداية التطبيق أو المشروعات ذات الطابع التنافسي أو التي لها علاقة بالأمن العام وهذه ينبغي حفظها وعدم الاطلاع عليها عاد المسئولين في المرفق أو المؤسسة.

المعلومات هي هدف للعدو لذلك يجب الحفاظ علي سريتها وأمنها مثلا:-

المكاتبات والأوراق السرية التي تتضمن معلومات خاصة بالأفراد أو موضوعات تعتبر سرية في مجال العمل.

المعلومات والمكاتبات السرية جدا وتشمل ما هو متعلق بمجال المرفق أو المنشأة أو المؤسسة.

المكاتبات السرية للغاية والتي تتعلق بأمن المرفق أو المؤسسة ومشروعاتها.

المكاتبات التي يحظر الاطلاع عليها ولها صلة بخطط المرفق أو المؤسسة أو نظامها الذي أنفقت الأموال من أجله فقط.

المحافظة علي سرية المراسلات والأوراق عن طريق:-

ختم المراسلات والمظاريف ذات الطابع السري بختم السرية

لا يسمح بفتح المكاتبات والمظاريف السرية إلا للشخص المسموح له بذلك.

تحفظ المكاتبات داخل ظروف سميكة لا تمكن من الاطلاع عليها من خلال المظروف.

عدم نقل المعلومات السرية من مكان لآخر إلا في حالة توصيلها للشخص المسموح له بالاطلاع عليها.

حفظ الأوراق التي تزول سريتها بعد التأكد من ذلك في ملفات الحفظ العادي أو التخلص منها بالطريقة الصحيحة.

<u>قواعد يجب مراعاتها وإتباعها :</u>

الاحتفاظ بالمكاتبات المهمة في مكان مأمون وبعيدا عن الأيدي العابثة

الاحتفاظ بالمكاتبات المهمة في خزن حديدية مخصصة لذلك

حرق المسودات وإتلافها ضمانا لعدم تسرب المعلومات التي تحويها.

الاحتفاظ بصورة لكل مكاتبة حتي يمكن الرجوع إليها عند حدوث أي تلف أو ضياع للوثيقة وتوفير شروط الأمان للصور مثل الأصل.

تداول الوثائق بنظام ثابت لتحديد مسئولية الاحتفاظ بها.

عدم السماح لمن ليس له حق الاطلاع علي الوثيقة ولو لمجرد المعرفة فقط ضمانا لسرية المعلومة بها.

أن يكون الأفراد الذين يتداولون الوثائق من الموثوق بهم.

يجب وضع تعليمات مقيدة لعملية النسخ والتصوير لتلك الوثائق.

المعلومات المستهدفة تتعلق بالاتي:-

معلومات عسكرية عن الأفراد والسلاح والتدريب والخطط

معلومات اقتصادية عن المصانع والكفاءات الإنتاجية.

القدرة الصناعية للدولة ومدي كفاءتها لاحتياجات البلاد وقت السلم والحرب.

الحالة التموينية للدولة وخططها في حالة السلم والحرب

إجراءات الدفاع المدني.

إجراءات الأمن بالدولة ومدي تعاون أجهزة الأمن المختلفة.

حالة المستشفيات ومدي استعدادها بمخزونها من الأدوية والكفاءات في حالة المرضي والمصابين.

مدي التعاون بين الأجهزة التنفيذية في الدولة.

أجهزة الشرطة وإمكانياتها وتدريبها بتسليحها وخطط مواجهة الجريمة والإرهاب.

أمن الاتصالات والنظام الإلكتروني :

يجب مراعاة الآتي :-

التفتيش الدائم عن الخطوط والأجهزة والتأكد من عدم التنصت.

وضع الحراسة علي الكابلات والتأكد من تمام قفلها أو فتحها.

يراعي أن يكون الأفراد العاملين علي الأجهزة من الأفراد الموثوق بهم وذوي خبرة في المجال.

لابد من وجود عدد من الفنيين للقيام بأعمال الإصلاح السريع للأجهزة ويستحسن أن يكونوا من ذوي الكفاءة العالية.

الإختراقات للنظم والفيروسات :

تفتقر نظم المعلومات مع التطور الكبير في أجهزة الحاسب ، وأنظمة المعلومات، و مع التوسع في شبكات المعلومات والسرعة الكبيرة التي يمكن أن تنتشر بها المعلومات ، إلي وجود نظم حماية تمنع المخترقين الذين يعرفون [الهاكرز] من الدخول إلى شبكات المعلومات واختراقها لأسباب تخريبية أو بغرض سرقة معلومات مالية وسرية ، وصاحب التطور في استخدام المعلومات الإلكترونية ازدياد مشاكل أمن المعلومات كالاختراقات والفيروسات وغيرها مما شكل خطراً كبيراً على البنيات الأساسية للمنشات الحكومية والخاصة يحتاج ألها كرز إلى منفذ يستطيع به الدخول اى شبكات المعلومات أو المواقع الالكترونية التي تتميز بأهمية المعلومات مما يجعل المخترقين يحتاجون إلى برمجة فيروس وفي الغالب نجد إن هذا الفيروس لا يضر بنظام الحاسوب كثيرا فوظيفته هي التجسس علي محتوى البيانات المهمة لكي يستفيد منها المخترق ومن أشهر أنواع هذه الفيروسات ما يعرف بالتروجان لذلك تمثل برامج حماية الحاسوب من الاختراق شيئا مهما وتحتاج إلي تحديث دوري خاصة إذا كان المستخدم متصلا بشبكة الانترنت.

وقد أصبحت التجارة الالكترونية هدفاً مفضلاً لمحترفي اختراق شبكات المعلومات نشرت مؤخراً دراسة أجريت في سنغافورة أن مواقع التجارة الإلكترونية أصبحت هدفا مفضلا لقراصنة الإنترنت ومحترفي اختراق شبكات المعلومات المعروفين بالها كرز.

وذكرت الدراسة التي أجرتها شركة سيمانتك المتخصصة في تأمين شبكات المعلومات أن[16%] من هجمات مخترقي اختراق الشبكات علي مواقع التجارة الإلكترونية كانت متعمدة وبزيادة نسبتها [12%] عن النصف الثاني من العام الماضي .

وفي دراسة وجد أنه قد كانت هناك أكثر من [250.000] محاولة اختراق لأجهزة الحكومة الأمريكية في العام 1995. ويقدر أن هذا العدد يتضاعف كل عام كما يقدر أن [64%] من هذه المحاولات نجحت في اختراق أجهزة الحكومة الأمريكية .

في الأيام الماضية أدرك الرئيس الأمريكي باراك أوباما خطورة هذا الأمر مما جعله يتخذ خطوات جادة لتحصين شبكات المعلومات الأمريكية وإتباع إجراءات لتحصين أمن شبكات المعلومات الأمريكية من هجمات القراصنة والمتسللين وأتخذ قرارا بوجود مكتب تابع للبيت الأبيض مهمته الأشراف علي أمن الشبكات بعد إجراء التقييم الذي يتطلب [60] يوما وأشرفت علي تقييم أمن شبكات البلاد ميليسا هاثواي مستشارة الأمن المعلوماتي في البيت الأبيض .

وستكون مهمة المكتب الجديد تنسيق عملية واسعة لحماية الشبكات الحكومية بقيمة مليارات الدولارات ، ومن الشبكات التي يراد تعزيز أمنها تلك المستخدمة في تنظيم النقل الجوي ومعاملات البورصة ، وكان المتحدث باسم البيت الأبيض روبرت جيبس قد قال الأسبوع الماضي أن التقييم الشامل المكورة هو الخطورة الأولي نحو تأمين بنية أمريكا المعلوماتية في وقت تعرضت فيه البنتاجون لحوالي [44]إلف هجوم في العام [2007] وحدها نفذتها جيوش ووكالات استخبارات أجنبية وكذلك أشخاص بعينهم.

في السودان تعرضت عدد من المؤسسات للاختراق مؤخرا سواء كانت شركات الإتصالات أو مواقع حكومية [حساسة] الشئ الذي يجب أن تراعي فيه الحكومة توجهها نحو مشروع الحكومة الالكترونية في توفير وتدعم امن الشبكات المعلوماتية لمجابهة إمكانية اختراق تلك المواقع مستقبلا.

وأشار.د.عادل عبد العزيز . الأمين العام للجمعية السودانية لتقانة المعلومات أنه عندما تفكر الدولة في إستخدام تقانات المعلومات والاتصال في أعمالها المختلفة من أجل

تقديم الخدمات للمواطنين فيما يعرف بالحكومة الالكترونية لابد من التخطيط لأمن المعلومات ذلك لأن كل معلومات الدولة والمعلومات الأساسية عن الشركات والقطاع الخاص تكون محفوظة داخل مخدمات تتعامل مع شبكات الاتصال فلابد من حمايتها من كل دخول غير المشروع سواء كان دخولا فيزيائي أو دخول عن طريق البرمجيات فيما يعرف بعمليات الهاكرز لحماية الشبكات في إطار امن المعلومات التي تتضمن جوانب تشريعية لأحكام السياسات المتعلقة بأمن المعلومات علي مستوي الأجهزة والبرامج [الهارد وير و السوفت وير] ، إضافة إلي وجود جانب أخر يتمثل في التدريب و الإستشارات .

ويقول د.عادل أن الجهات الكبيرة في السودان تمكنت من عمل شبكات وقواعد بيانات ضخمة كشركات الإتصالات وبعض الوزارات والمؤسسات والهيئات حصنت معلوماتها بنظم لأمن المعلومات بعضها قوي جداً كما في شركات الاتصالات الأربع الموجودة لدينا في السودان .

وأضاف أن علي المستوي التشريعي تم إصدار قانون جرائم المعلوماتية لسنة 2007 وهو يشكل أطارا قانوني قوي جداً لحماية منظومات الشبكات والاتصالات من الدخول غير المشروع أو التعدي أو سرقة البيانات ، وعلي المستوي المعرفي توجد [30] كلية حاسوب وهندسة إتصالات علي مستوي الجامعات السودانية جميعها تدرس أمن المعلومات كمادة أساسية وهنالك مراكز عملية متخصصة في هذا المجال كمركز النيل ، تم إنشاؤه بالتعاون بين الهيئة القومية للإتصالات وجامعة الخرطوم .

ونوه عادل أن الاتجاه في السودان نحو تطبيق الحكومة الالكترونية سيستلزم الاهتمام بهذا الجانب وتوظيف كل الإمكانيات البشرية والمادية من أجل حماية الشبكات و المعلومات.

مقدمة في علم التشفير :

عُرف علم التشفير أو التعمية منذ القدم، حيث استخدم في المجال الحربي والعسكري ، فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة ، وكذلك ذكر أن العرب لهم محاولات قديمة في مجال التشفير. و استخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب ، فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه تصعب عليه فهمها. وأفضل طريقة استخدمت في القدم هي طريقة القصير جوليوس وهو أحد قياصرة الروم. أما في عصرنا

الحالي فقد باتت الحاجة ملحة لاستخدام هذا العلم "التشفير" وذلك لإرتباط العالم ببعضه عبر شبكات مفتوحة ، وحيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة ، عسكرية كانت أم مدنية. فلابد من طرق تحفظ سرية المعلومات. فقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات.

ومازال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للكمبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.

ما هو التشفير أو التعمية (Cryptography):-

التشفير هو 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 لـه. وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (**Cryptoanalysis**) هو علم لكسر و خرق الاتصالات الآمنة.

أهداف التشفير:-

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:-

1. السرية أو الخصوصية (**Confidentiality**):-

هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.

2. تكامل البيانات (**Integrity**):-

وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.

3. إثبات الهوية (**Authentication**):-

وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).

4. عدم الجحود (**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 هو دالة رياضية تستخدم في عملية التشفير وفك التشفير. وهو يعمل 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. فيما يلي رسم توضيحي صورة(1).

صورة1: طريقة عمل التشفير.

أنواع التشفير:-

حالياً يوجد نوعان من التشفير وهما كالتالي:-

1. **التشفير التقليدي**. (**Conventional Cryptography**).
2. **تشفير المفتاح العام**. (**Public Key Cryptography**).

1. التشفير التقليدي:-

يسمى أيضاً التشفير المتماثل (**Symmetric Cryptography**). وهو يستخدم مفتاح واحدٌ لعملية التشفير وفك التشفير للبيانات. 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 زيد إرسال رسالة مشفرة إلى عبيد، عليه إيجاد طريقة آمنة لإرسال المفتاح إلى عبيد. فإذا حصل أي شخص ثالث على هذا المفتاح فإن بإمكانه قراءة جميع الرسائل المشفرة بين زيد وعبيد. فيما يلي رسم توضيحي صورة (2).

صورة2: توضح عمل التشفير باستخدام المفتاح الواحد.

بعض الأمثلة على أنظمة التشفير التقليدي:-

i . **شفرة قيصر:** وهي طريقة قديمة ابتكرها القيصر جوليوس لعمل الرسائل المشفرة بين قطاعات الجيش وقد أثبتت فاعليتها في عصره. ولكن في عصرنا الحديث ومع تطور الكمبيوتر لا يمكن استخدام هذه الطريقة وذلك لسرعة كشف محتوى الرسائل المشفرة بها.

المثال التالي يوضح طريقة عمل شفرة قيصر: إذا شفرنا كلمة "SECRET" واستخدمنا قيمت المفتاح 3، فإننا نقوم بتغيير مواضع الحروف ابتداءً من الحرف الثالث وهو الحرف "D"، وعليه فان ترتيب الحروف سوف يكون على الشكل التالي:

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

الحروف بعد استخدام القيمة الجديدة لها من المفتاح "3" تكون على الشكل الحالي:

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

الآن قيمة الـ A ← D، B ← E، C ← F، وهكذا.

بهذا الشكل فان كلمة "SECRET" سوف تكون "VHFUHW". لتعطي أي شخص آخر إمكانية قراءة رسالتك المشفرة؛ يجب أن ترسل له قيمة المفتاح "3".

ii. **تشفير البيانات القياسي (DES):** طُور هذا النظام في نهاية السبعينيات من قبل وكالة الأمن القومي الأمريكية، وهذا النظام بات من الجدوى عدم استخدامه مع تطور أنظمة الكمبيوتر وزيادة سرعة معالجته للبيانات، حيث أنه قد يتم كشف محتوى رسائل مشفرة به في وقت قصير.

iii. **blowfish, AES, IDEA, 3DES,**: وهي أنظمة حديثة ومتطورة وأثبتت جدواها في عصرنا الحالي في مجال التشفير.

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

2. تشفير المفتاح العام :

أو ما يعرف بالتشفير اللامتماثل (**Asymmetric Cryptography**). تم تطوير هذا النظام في السبعينات 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. المفتاح العام يرسل لجميع الناس أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد. فمن

يحتاج أن يرسل لك رسالة مشفرة فإنه يستخدم المفتاح العام لتشفيرها ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص. فيما يلي رسم توضيحي صورة (3).

صورة 3 : توضح عمل التشفير باستخدام المفتاح العام والمفتاح الخاص.

بعض الأمثلة على أنظمة تشفير المفتاح العام.

PGP, DSA, Deffie-Hellman, Elgamal, RSA

جميع هذه الأنظمة تعتمد على مبدأ التشفير اللاتماثلي أو التشفير باستخدام المفتاح العام والمفتاح الخاص.

مزايا وعيوب التشفير التقليدي والتشفير باستخدام المفتاح العام:-

التشفير التقليدي أسرع بكثير باستخدام أنظمة الكمبيوتر الحديثة، ولكنه يستخدم مفتاح واحد فقط. فهو عرضة أكثر 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 والمصادر المتطلبة لعملية كشف النصوص غير مشفرة من النصوص المشفرة. نتيجة التشفير القوي هو نص مشفر يصعب كشفه مع الوقت أو توفر الأدوات اللازمة لذلك.