الجمهورية العربية السورية

جامعة دمشق

المعهد العالي للتنمية الإدارية

ماجستير التأهيل والتخصص في الريادة والإدارة بالإبداع

السنة الأولى

أمن نظم المعلومات والرقابة (التحكم)

Information System Security and Control

ISS and C.

نسخة معدلة

إعـــداد الباحث

المـــهنـــدس خـــالـــد يـاســين الـــشيــخ

إشـــراف الـدكـتـور

طـــاهـــر حـــســـن

دمـشــق

للـــعـــام الـــدراســـي

2014-2015

الـهـنـدســة الـمـعـلـومـاتـيـة بـجـامـعـة دمـشـق 2010

فهرس المحتويات

الموضوع	الصفحة
مقدمة	1
1- ما هو الأمن	1
2- أهمية أمن نظم المعلومات ISS في عالمنا	1
3- تعريف ISS	2
4- لماذا نحتاج لـــ ISS	3
5- مكونات النظام المعلوماتي في عالم ISS	4
6- جرائم المعلوماتية في عالم ISS	5
7- مكونات انظمة المعلومات	5
8- التطور التقني و أثره على أمن المعلومات	6
9- KEY TERMS مصطلحات رئيسية في عالم ISS	6
10- الهجمات التي تتعرض لها المعلومات في عالم ISS	11
11- أهداف أمنية تحققها ISS	11
12- التعمية (أو التشفير) cryptography	13
13- التوقيع الرقمي Digital Signature	19
14- مصطلحات يجب التعرف عليها في عالم ISS	20
الخاتمة	22
المراجع	23

المقدمة:

إن للمعلومات منذ القدم أهمية كبيرة في جميع مجالات الحياة وقد ظهرت حاجة الإنسان إلى المعلومات وتبادلها منذ القدم فقد ظهر هذا في الجيوش العسكرية ومفهوم أمن المعلومات هو مفهوم مرتبط بتطور العصور حيث لكل عصر طرقه وأدواته المبتكرة للحفاظ على المعلومات ونظرا لارتباط عصرنا الحالي بعصر المعلومات والتكنولوجيا فقد ظهرت الحاجة الملحة إلى نظام أمني يمكننا من خلاله إدارة مكوناته المختلفة سواء المادية منه أو البرمجية (المنطقية) وتأمين الأدوات والآليات المناسبة لحماية هذا النظام ومن هذا المنطلق سيتناول هذا البحث مفهوم ISS and C ودوره في حياتنا اليومية.

1- ما هو الأمن:

يعرف الأمن بأنه "العمل على التحرر من التهديد" وفي سياق النظام الدولي فهو "قدرة المجتمعات والدول على الحفاظ على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي تعتبرها معادية"

- وهو القدرة على حماية ممتلكات المنظمات بشتى أنواعها.
- هي الحالة أو المرحلة التي تصبح فيها آمناً و خالٍ من الأخطار

والأمن يدخل في جميع مستويات الحياة فهو مفهوم شامل وتتبع شموليته من كونه يدخل في جميع فروع الحياة.

من هنا فإن شمولية الأمن تعني أن له أبعادًا متعددة:

- ✓ **أولها:** البعد السياسي.. ويتمثل في الحفاظ على الكيان السياسي للدولة.
- ✓ **ثانيًا:** البعد الاقتصادي.. الذي يرمي إلى توفير المناخ المناسب للوفاء باحتياجات الشعب وتوفير سبل التقدم والرفاهية له.
- ✓ **ثالثًا:** البعد الاجتماعي.. الذي يرمي إلى توفير الأمن للمواطنين بالقدر الذي يزيد من تنمية الشعور بالانتماء والولاء.
- ✓ **رابعاً:** البعد المعنوي أو الأيديولوجي.. الذي يومن الفكر والمعتقدات ويحافظ على العادات والتقاليد والقيم.
- ✓ **خامساً:** البعد البيئي.. الذي يوفر التأمين ضد أخطار البيئة وخاصة التخلص من النفايات ومسببات التلوث حفاظاً على الأمن.
- ✓ **سادساً**: البعد المعلوماتي.. والذي يهدف إلى حماية سرية البيانات والمعلومات التي يتم تبادلها سواء في العالم الإلكتروني أو العالم الفيزيائي.

2- أهمية أمن نظم المعلومات ISS في عالمنا:

إن لـــ ISS أهمية كبيرة في حياتنا اليومية التي نعيشها سواء كان ذلك كان على المستوى المادي الملموس او المعنوي غير الملموس وللـــ ISS أهمية كبرى في حماية المعلومات التي يتم تداولها. حيث أن المعلومات لابد لها من وسيط يحتويها قد يكون الورق هو هذا الوسيط أو يكون مغنطيسيا كالأقراص الممغنطة أو الصلبة وقد يكون هذا الوسط عبارة عن كابلات تسري فيها نبضات، حتى الهواء الذي تسري فيه موجات كهرومغنطيسية يحتوي على المعلومات المنقولة وهو من وسائط المعلومات، فكل نوع له مخاطرة الخاصة به وله الإجراءات الأمنية التي تحفظ المعلومات فيه من التلف أو الضياع أو الاطلاع الغير المرخص به ومن الشائع أن تكون إحدى وسائل المحافظة على المعلومات من الضياع هي إعداد نسخة أخرى منها على وسيط مختلف كأن تحفظ بصورة ورقية للبرامج المخزنة للحاسب أو نحتفظ بشريط ممغنط كنسخة احتياطية في محتويات القرص الصلب حيث أنه عندما يتم تبادل معلومات بشتى أنواعها يجب أن نضمن أن يتم إطلاع هذه المعلومات من قبل أشخاص مخولين وكل شخص يقوم بالاطلاع على هذه المعلومات حسب صلاحيته فمثلاً: عند ما نقوم بوضع أوراق مكتوب عليها أشياء هامة ويتم وضعها في خزانة مقفلة يجب أن لا نسمح لأي شخص بفتح هذه الخزانة والاطلاع على ما تحويه إلا من قبل أشخاص مخولين بذلك وأيضاً عند ما يكون لدينا معلومات مخزنة على شبكة حاسوبية يجب أن نضمن أن لا يطلع على هذه المعلومات إلا أشخاص مخولين وكلاً حسب صلاحيته ومن هنا تأتي أهمية ISS في تحقيق أمن المعلومة.

- إن المخاطر التي تتعرض لها المعلومات ناتجة من عدد كبير من الأحداث التي يمكن أن ينتج عنها تخريب أو تدمير أو سرقة أو تعديل غير مشروع لجهة ما غير مخول لها بالتصرف في تلك المعلومات بصورة متعمدة أو غير متعمدة . و يدخل في نفس الإطار سوء الاستخدام من قبل المستخدم لتلك المعلومات سواء أكان بشراً أو أداة من الأدوات .
- من هنا ظهرت الحاجة لإيجاد نظام أمني يقوم بتوفير البيئة المناسبة للتعامل مع المعلومات .

3- تعريف ISS:

لا يوجد تعريف عام يمكن من خلاله أن نعرف ISS ولكن يمكن أن نعرف عنه من خلال الأشياء والأهداف التي من خلالها تسعى إلى تحقيق أمن المعلومة.

يمكننا تناول ISS من زوايا عدة:

فمن خلال الزاوية العلمية والأكاديمية هو العلم الذي يتم من خلالها إيجاد نظريات واستراتيجيات لتأمين الحماية للبيانات والمعلومات من مختلف المخاطر ونقاط الضعف والتهديدات التي يمكن أن تسبب الدمار والخراب للأنظمة القائمة عليها سواء كانت هذه الأنظمة برمجية(منطقية) أو فيزيائية (ملموسة).

من خلال زاوية تكنولوجية حيث تمكن ISS من تأمين الأدوات والوسائل التي نستخدمها في تحقيق أمن المعلومات من أي هجوم أو خطر أو ثغرة أمنية يمكن من خلالها تنفيذ أي تهديد يلحق الأذى بالممتلكات المادية أو المعنوية سواء كان مصدر هذا الخطر داخل المنظمة أو خارجها.

من زاوية حقوقية تمكن ISS من خلالها من منع الأشخاص أو المنظمات بمختلف أنواعها من الاعتداء المادي أو الإلكتروني من خلال وضع قانونين وقواعد وإجراءات صارمة تلزم الأشخاص والمنظمات بالتقيد بها ضمن أسس أمنية واضحة.

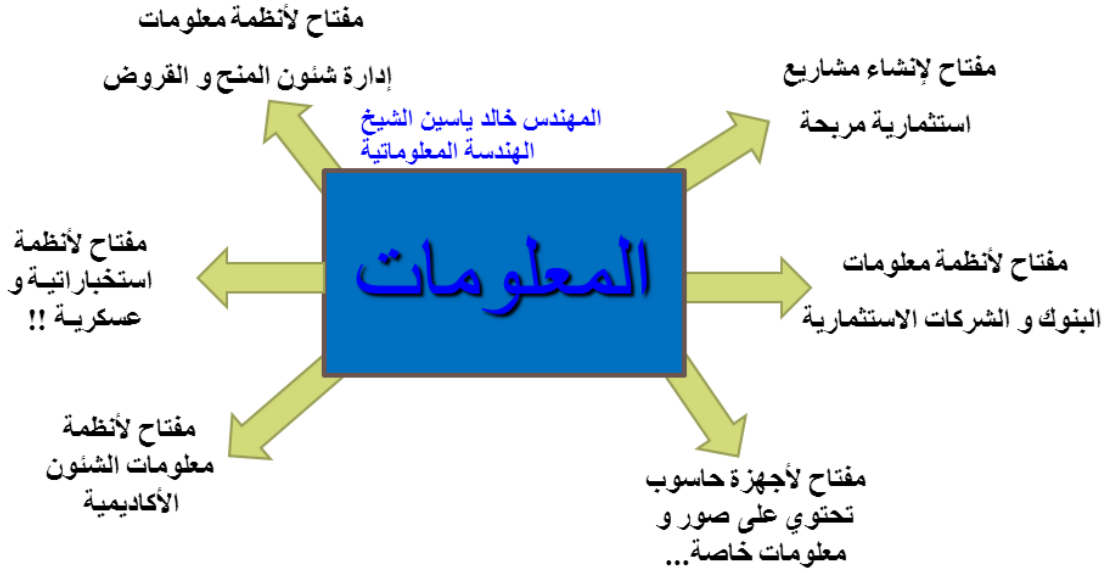
- يمكن تقسيم أمن المعلومات إلى : **أمن شخصي وأمن المنشأة (والشبكة).**
- **أمن الشخصي** : هي الخطوات والإجراءات الكفيلة التي يقوم بها الموظف بنفسه ، بمقر عمله وخارجه ، تحول دون كشف أسرار عمله من معلومات إلى أشخاص غير مخولين بأية صورة وشكل.
- **أمن المنشأة (و الشبكة)**: هي القوانين والإجراءات التي تتبناها المنشأة وتقوم بتطبيقها لتحول دون كشف أسرارها إلى جهة ليست مخولة.

وبشكل عام فإنه يقصد **بأمن نظم المعلومات:**

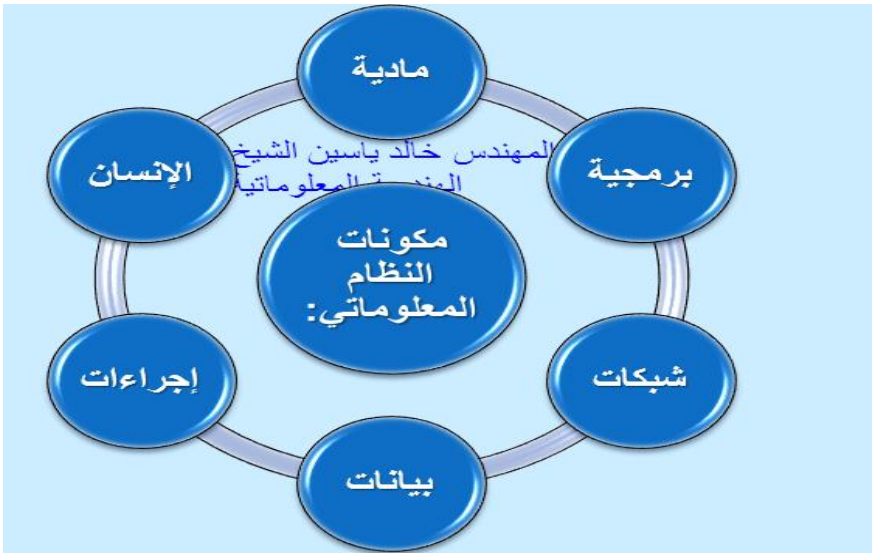
- حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة وذلك في جميع مراحل تواجد المعلومة (التخزين – النقل – المعالجة).
- هو حماية المعلومات و الأنظمة البرمجية Software والمعدات الفيزيائية HARDWARE التي تعالج و تخزن و تنقل المعلومات .

4- لماذا نحتاج لـــ ISS:

1. القطاعات الأمنية والعسكرية والاقتصادية تعتمد على صحة ودقة المعلومات.
2. حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق تغطي المخاطر التي يمكن أن تظهر عند التعامل مع الأطراف الأخرى.
3. الحاجة المتزايدة لإنشاء بيئة إلكترونية آمنة تخدم القطاعين الخاص والعام.
4. النمو السريع في استخدامات التطبيقات الإلكترونية والتي تتطلب بيئة آمنة.
5. الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية وذلك من أجل استمرارية الأعمال التجارية.
6. مع تطور التقنية المعلوماتية وازدهارها توفرت فرصاً للإجرام الإلكتروني.
7. حماية Privacy بما تتضمن من المعلومات الشخصية.
8. حماية ممتلكات الشركة وخاصة إذا كانت تقدم خدمة Hosting.
9. كسب الفوائد التنافسية أي قوة النظام الأمني تؤمن تفوق على المنافسين.
10. للامتثال للمتطلبات النظامية والمسؤولية القانونية.
11. حماية العمل أو المركز الوظيفي حيث لابد من قدرة الموظف على تحمل مسؤولية الحماية الأمنية المناسبة لكل ما هو مسؤول عنه في الشركة لئلا تستغني عن خدماته.



5- مكونات النظام المعلوماتي في عالم ISS:



6- جرائم المعلوماتية في عالم ISS:

- هي تعبير شامل يشير إلى جريمة تتعلق باستعمال إحدى وسائل تقنية المعلومات لغرض خداع الآخرين وتضليلهم، أو من أجل تحقيق هدف معين لجهة معينة.
- تُكبد جرائم المعلوماتية الحكومات والمنشآت خسائر تقدر بمليارات الدولارات سنوياً.
- في أحدى الدراسات التي أجريت على قطاع المصارف أن نسبة 70% من هذه الجرائم تتم بتواطؤ المجرمين والمبرمجين وموظفي المصارف.

تصنيف جرائم المعلوماتية:

1. جرائم هدفها نشر المعلومات:

مثل الحصول على أرقام البطاقات الائتمانية، والحسابات المصرفية ومعلومات استخباراتية.

2. جرائم هدفها نشر معلومات غير صحيحة:

مثل نشر المعتقدات الخاطئة أو التشكيك في معتقدات معينة.

3. استخدام تقنية المعلومات كوسيلة لأداء الجريمة:

مثل تزوير بطاقات الائتمان والتحويل بين الحسابات المصرفية.

4. جرائم لها علاقة بانتشار تقنية المعلومات:

مثل قرصنة البرامج الأصلية وبيعها بأسعار بخسة.

7- مكونات أنظمة المعلوماتComponents of Information Systems

1- البرامج SOFTWARE.
2- الأجزاء المادية HARDWARE.
3- العملياتOperations :
4- البيانات DATA .
5- المستخدمين PEOPLE .
6- الإجراءات و اللوائح PROCEDURES .

1- البرامج SOFTWARE

تتكون البرامج من التطبيقات Applications المختلفة و نظم التشغيل Operating Systems و أدوات الأوامر Command Utilities .

2- الأجزاء المادية HARDWARE

هي المكونات التي تحتوي و تشغل البرامج المختلفة و يتم تخزين البيانات و نقلها خلال تلك الوسائط . ونجد أن قوانين الحماية المادية لهذه المكونات تتعامل معها كجزء من الأصول التي يجب حمايتها من الإتلاف أو السرقة .

3- العمليات Operations

تعتبر العمليات لا غني عنها لأي نظام أمن، فهي جوهرية وذات طبيعة مستمرة. ويحكم أداة عمليات أمن المعلومات مجموعة من المعايير كتلك التي قررتها المنظمة الدولية للتوحيد القياسي ISO التي تعتبر ذات قيمة كبيرة لأي نظام أمن معلومات .وتطبق

العمليات بطريقة منظمة كما تراجع باستمرار في إطار الخبرة المتراكمة بغية استبعاد الأخطاء والمخاطر.

4- **البيانات DATA**
البيانات المخزنة و التي تتم معالجتها و التي تنقل خلال نظام الكمبيوتر يجب حمايتها والتي تمثل الهدف الأساسي لمعظم الهجمات على المعلومات وقد تكون البيانات أيضاً موجود في العالم الفيزيائي والعالم البرمجي على حد سواء أيضاً.

5- **المستخدمين PEOPLE**
إن المستخدم كجزء أساسي لا يتجزأ من بيئة أنظمة المعلومات يجب أن يكون مشتركاً في تطبيق قواعد الحماية للنظام ، ويجب تعليمهم و تدريبهم التدريب اللازم للحرص على الأمور الأمنية في نظام المعلومات و إلا فإن إهمال ذلك الجانب من الحماية قد يؤدي إلى بعض المخاطر و الهجمات على المعلومات.

6- **الإجراءات و اللوائح PROCEDURES**
هي القواعد و الخطوات المكتوبة لإنجاز مهمة معينة وتكون هذه الإجراءات واللوائح ملزمة لعناصر ومكونات نظام عناصر المنظمة وفق سياسة أمنية واضحة.

8- التطور التقني و أثره على أمن المعلومات:

- تطور في مجال الحاسوب
- تطور في أنظمة الاتصال
- تطور في أنواع البيانات
- تطور في أنواع الهجمات
- زيادة في الثغرات الأمنية
- نقص في الكوادر المؤهلة لحماية المعلومات أمنياً

9- KEY TERMS مصطلحات رئيسية في عالم ISS:

✓ **الأصول ASSETS** :
هي ممتلكات و موارد المنظمة التي يجب حمايتها و التي يمكن أن تكون منطقية كمواقع الانترنت و المعلومات و البيانات و يمكن أن تكون مادية كالمستخدمين و الأجزاء المادية .

✓ **الهجوم ATTACK :**

هو العملية التي من خلالها تتم المحاولة في تسبيب الضرر للمعلومات و الأنظمة الداعمة لها بصورة متعمدة أو غير متعمدة وهو تحقيق للتهديد .و تنقسم إلى نوعين:

- **Passive Attack**

و كمثال له إذا قرأ أحد الأشخاص غير المصرح لهم بعض المعلومات الهامة عن طريق الصدفة . أو يكتفي الدخيل بالمراقبة دون التعديل كالتنصت على الكابلات.

- **Active Attack**

و هو محاولة شخص أو نظام للدخول في أحد أنظمة المعلومات و الحصول على معلومات غير مصرح له بها (كأن يقوم الدخيل بالتعديل على البيانات التي يتنصت عليها كتزوير أو تعديل بيانات المحولات المصرفية).

✓ **التحكم CONTROL**

✓ **الحماية SAFEGUARD**

✓ **الإجراء المضاد COUNTERMEASURE**

- هذه المصطلحات ترمز لطرق و قواعد و إجراءات أمنية يمكن عن طريقها حماية المعلومات و تقليل المخاطر و سد الثغرات في أنظمة المعلومات .

✓ **الثغرة VULNERABILITY**:

هي الضعف أو الأخطاء في نظام معين أو طريقة حماية أمنية معينة يمكن من خلالها تعريض المعلومات للأخطار . ويمكن ان تكون الثغرة سوء في تصميم النظام على المستوى البرمجي أو الفيزيائي.

- هي نقاط الضعف في وسائل الحماية.

✓ **التهديدات THREATS** :

التهديد هو أي كيان يمثل خطر محتمل لمكونات النظام

- يجب على كل منظمة أن تصنف الأخطار الحالية و المستقبلية وفقاً لحالة تلك المنظمة الأمنية و استراتيجيتها و مستوى تعرضها للهجمات .
- التهديد هو أي شخص أو شيء أو فكرة تشكل خطر على أي مكون من مكونات النظام قد يكون الخطر على : integrity ,confidentiality , availability,…. .
- التهديد قد يسمح بـ legitimate use الاستخدام غير الشرعي لمكونات النظام .

➢ **التهديدات غير المتعمدة INADVERTENT ACTS**

- هي التهديدات أو الأفعال التي تحدث بدون وجود أي نية سيئة مثل الأخطاء البشرية أو التباين في جودة خدمة معينة من قبل مقدم الخدمة أو عدم استقرار الطاقة .
- الأخطاء البشرية أو الأعطال التي تحدث عن طريق مستخدمين مخول لهم بالتعامل مع نظام المعلومات بدون تعمد يمكن تجنب الكثير من هذه التهديدات عن طريق التحكم في شكل الإجراءات المتبعة في تنفيذ العمليات و عن طريق التدريب لأولئك المستخدمين .

- التباين في تقديم خدمة معينة من قبل مقدم الخدمة يعني أن المنتج أو الخدمة التي طلبت لم تصل إلى المنظمة كما هو متوقع (خدمة الإنترنت و الاتصالات و الطاقة هي أمثلة لخدمات تؤثر جودتها عند وصولها على أداء المنظمة ككل).
- عدم استقرار الطاقة هو تهديد يمكن أن يحدث دائماً بزيادة غير متوقعة للكهرباء أو نقص أو انعدام في توصيل التيار مما يؤدي إلى حدوث أعطال في مكونات نظام المعلومات الخاص بالمنظمة.
- إرسال بيانات إلى عنوان خاطئ.

➢ **التهديدات المتعمدة DELIBRATE ACTS**:

- مجموعة من التهديدات التي صممت لإتلاف أنظمة المعلومات المختلفة ، و مقدار التلف الناتج يمكن أن يكون طفيفاً مثل إرسال بريد الكتروني يحمل إعلاناً تجارياً و يمكن أن يؤدي إلى كارثة مثل انهيار المباني و تشمل تلك :

✓ **التجسس ESPINAGE (TRESPASS)**

✓ **التخريب VANDALISM**

✓ **سرقة المعلومات INFORMATION THEFT**

✓ **البرامج المدمرة MALICIOUS CODE**

التجسس ESPINAGE -TRESPASS

■ و هي أنشطة تتم الكترونياً أو يدوياً مما يؤدي إلى كسر السرية المطلوبة في المعلومات مثل معرفة حجم تداول البيانات في الشبكة باستخدام برامج التنصت ، التجسس البشري مثل الوقوف خلف احد المستخدمين لمعرفة كلمة المرور التي تخصه من خلال طباعتها على لوحة المفاتيح .

التخريب VANDALISM

- يهدف إلى تخريب العمليات التي يقوم بأدائها الكمبيوتر أو النظام و الذي بدوره سيؤدي إلى خرق التوفر المطلوب في المعلومات أو إلى تشويه صورة المنظمة الخارجية لدى المتعاملين معها .

سرقة المعلومات INFORMATION THEFT

- السرقة هي عملية غير شرعية يتم بموجبها الحصول على ممتلكات الآخرين . و داخل المنظمة يمكن أن تكون تلك الملكية متعلقة بمكونات مادية ، الكترونية ، منطقية.
- وتسريب أو سرقة المعلومات تهديد ينتهك الـــ Confidentiality.

البرامج الشريرة MALICIOUS CODE(malware)

- تشمل كل البرمجيات التي صممت بهدف مهاجمة أنظمة المعلومات المختلفة . و التي صممت لتخريب و تدمير أو تأخير أو حرمان خدمة معينة من الوصول للجهة المعينة.
- وهي من الأمثلة الشهيرة في مجال أنظمة المعلومات مثل VIRUSES,WORMS,TROJAN HOURSES
- البرامج الخبيثة تهديد ينتهك الأهداف الأمنية مثل السرية والتكاملية و التوافرية .....

✓ **التهديدات الطبيعية NATURE ACTS**:

- هي تلك التهديدات التي تحدث بسبب قوة الطبيعة التي لا يمكن التحكم بها أو منعها و تؤدي إلى تعطيل أو تدمير وسائط التخزين أو نقل أو معالجة المعلومات مثل الزلازل و البراكين و الأعاصير .

✓ **الأخطاء التقنية TECHNICAL FAILURES**

- في بعض الأحيان يحدث تلف للمواد المادية و البرمجيات بدون أي سبب مرئي أو معروف أو بطريقة غير متوقعة . مما يؤدي إلى الكثير من الآثار السلبية لمعظم المنظمات التي لم تحتاط لتلك المشاكل الغير متوقعة

✓ **الأخطاء الإداريةMANAGEMENT FAILURES**:

- تحدث هذه التهديدات نتيجة لنقص في التخطيط و التعامل مع العقبات التي تواجه المنظمة من قبل إدارة المنظمة في تطبيق التقنيات الأمنية المناسبة.

✓ **الخطر RISK** :

هو احتمالية تهديد النظام - احتمالية اكتشاف الثغرات - احتمالية أخطاء التصنيع أو الأخطاء البرمجية .

- قياس نقاط الضعف (أي ما هو احتمال استغلال نقطة ضعف).

✓ **وسائل الحماية Safeguards:**

مثل تقنية التحكم بالمراقبة (مراقبة الشبكة) أو إجرائيات procedure معينة (في حال حدوث أمر ما يتم إجراء معين) وأيضاً كل من Auditing ,Guideline تصنف تحت وسائل الحماية أي:

— **Safeguards= control ,monitoring, procedure ,guideline, auditing,……etc.**

- ✓ **المخترقون**:

هم أشخاص يتمتعون بموهبة وقدرة عاليتين على كتابة وتصميم البرامج، وفهم عميق لكيفية عمل الحاسب الآلي مما يسهل عليهم اختراق أنظمتها وتغييرها.

هناك نوعين من المخترقين:

الأول : الهاكر (White Hat).

هم في العادة أشخاص فائقو الذكاء يسيطرون بشكل كامل على الحاسب، ويجعلون البرامج تقوم بأشياء أبعد بكثير مما صممت له أصلا. لذلك نجد أن بعض الشركات العملاقة توظف أمثال هؤلاء الهاكر لتستفيد من مواهبهم سواء في الدعم الفني، أو حتى لإيجاد الثغرات الأمنية في أنظمة هذه الشركات.

الثاني: الكراكر(Black Hat).

هم من يسخرون ذكائهم بطريقة شريرة، وهم يهتمون بدراسة الحاسب والبرمجة ليتمكنوا من سرقة معلومات الآخرين الشخصية، ويغير أولئك المخربون، أحيانا، المعلومات المالية للشركات، أو يكسرون أنظمة الأمان، ويقومون بأعمال تخريبية أخرى.

الفرق ما بين الهاكر و الكراكر:

- ➢ **الكراكر**:

1. يمتلك القدرة على اختراق أنظمة التشغيل والبرامج الغير مجانية والتلاعب في برمجتها وإعطاؤها رقم خاص لكي تعمل.
2. ويقوم بكسر الأنظمة الأمنية لأهداف تخريبية، فقد يكون هدفه سرقة معلوماتك أو في أسوأ الأحيان القضاء على النظام المعلوماتي الإلكتروني، بشكل كلي.
3. كثير منهم يقوم بسرقة البرامج و توزيعها مجانا لهدف، فمنهم من يضع ملف الباتش بين ملفات هذا البرنامج.
4. الكراكر دائما عمله تخريبي ولا ينفع سوى نفسه أو من يدفع له.

- ➢ **الهاكر:**

1. يحاول فقط أن يتعرف على كيفية عمل النظام والبرامج لكي يساعد في تطويرها وتحسينها.
2. لديه القدرة الكاملة على اختراق أنظمة التشغيل عبر الانترنت.
3. يقوم الهاكر بحل المشاكل و بناء الأشياء، و يؤمن بالعمل التطوعي.
4. الهاكر دائما عمله بناء ومفيد و ينفع الآخرين.

10- الهجمات التي تتعرض لها المعلومات في عالم ISS:

الهجمات التي تتعرض لها المعلومات كثيرة منها ما هو مادي ومنه ما هو برمجي(منطقي) منها على سبيل المثال:

- ✓ هجوم حجب الخدمة DOS Attack (Denial of service Attack) ويمكن أن يتم فيزيائيا بسبب عدم وجود مثلاً حارس يقوم بحراسة الجهاز المادي الذي من خلاله تتم عملية نقل.أو معالجة للمعلومات مثل سرقة السويتش أو قطع كبل شبكة.

وكمثال على هذه الهجمات التي تتم في الطبقة الفيزيائية إحدى الطبقات السبع في التقسيمات الشبكية حيث أنه في هذه الطبقة الهجمات تعد خطرة على الشبكة ولعلها أهمها قطع الكوابل التي تربط الشبكات ببعضها البعض ويمكن أيضا في حالة الوصول الى الكابلات التنصت على Traffic networkالمعطيات الشبكية المار فيها بكل سهولة.

الحماية : للحماية من هذه الهجمات يمكن أن نقوم بتأمين الكابلات الممددة وإغلاق كل الغرف التي تمر فيها الكابلات بشكل مباشر .

- ✓ ويمكن أن يكون هجوم dos بشكل برمجي من خلال استغلال ثغرة أمنية معينة . وهجوم DOS من خلاله النظام خارج الخدمة وغير متاح Unavailable وهو هجوم يمكن أن يتم على الطبقات السبع للتقسيمات الشبكية من خلال انتحال شخصية أو زرع برامج خبيثة وشريرة كالتروجان والفيروس والديدان والقنابل البرمجية والأبواب الخلفية.....الخ

- ✓ رفض الخدمة DOS(Denial of Service):تهديد ينتهك الـ Availability. مع الإشارة إلى أن انتهاك الـ Availabilityيمكن أن يتم عن طريق سوء بتصميم النظام الأمني.

- ✓ هجوم IP Spoofing في الطبقة الثالثة network يحقق التهديدات التالية:

1- Masquerade
2- Integrity Violation
3- Illegitimate use threats
4- Information leakage threat
5- Denial of Service threat

11- أهداف أمنية تحققها ISS:

- ✓ **التوافرية أو الاتاحية AVAILABILITY:**

توفر المعلومات بجاهزية كاملة كلما أراد أحد المستخدمين الشرعيين هذه المعلومات وهنا يعمل هجوم حجب الخدمة الذي يسبب توقف الضحية (المخدم مثلاً) عن العمل أو مثلا عملية قطع كابل مادي لأحد وصلات الشبكة الحاسوبية.

- ✓ **السرية CONFIDENTIALITY**:
حماية المعلومات بشكل سري من كل الأشخاص غير المخولين لرؤيتها وتسمى أيضاً Privacy أو Secrecy .
- ✓ **التكاملية وسلامة المحتوى INTEGRITY:**
التأكد من سلامة المعلومات أي أنه لم يتم تعديل هذه المعلومات بوسائل غير مشروعة أو عن طريق أشخاص غير مخولين بذلك (أي دخلاء).
- ✓ **الفائدة UTILITY** :
هي الحالة أو المرحلة التي تكون فيها المعلومات ذات قيمة أو جدوى لتحقيق غرض ما أو هدف معين .

و هذا يعني أن المعلومات إذا كانت متوفرة للمستخدم ولكنها ليست في الصورة التي يتوقعها فهي في هذه الحالة غير مفيدة.

- ✓ **الملكية POSSESSION**:
هي الحالة أو المرحلة التي تمتلك فيها أو تتحكم في المعلومات ، و يقال أنها محققة لشروط الملكية إذا كانت تلك المعلومات تحت تحكم و تصرف مالك المعلومات .

- ✓ **التوثيق Authentication**:
هي التحقق من هوية الشخص أو الكيان أي أن الشخص أو الكيان الذي يدعي هوية معينة هو فهلا صاحب هذه الهوية (التحقق من مصدر المعلومات).
لها نوعان:
  - Entity Authentication
  - Origin Authentication

- ✓ **المحاسبة Accountability:**
حيث يمكننا معرفة من قام بماذا .... ومتى... أي تحديد هوية صاحب الإجراء والإجراء والوقت الذي قام به بهذا الإجراء ونعني بالإجراء حدث ما كعملية logon مثلاً أو طلب خدمة ما وهذا تحديداً مفهوم المحاسبة التي لا يمكن أن تتم بدون عملية Authentication.

- ✓ **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation:** عدم نكران المرسل (أنه أرسل) أو المستقبل (أنه استقبل).
- ✓ **التوقيع الرقمي Digital signature:**
في هذه الحالة يتم ربط هوية المرسل بالرسالة التي يقوم بإرسالها.

- ✓ **التحكم في النفاذ Access Control:**
وفي هذه الحالة يتم الولوج او الوصل للمعلومات من قبل أشخاص أو كيانات برمجية او مادية مخولين وكلاً حسب درجة الصلاحية الممنوحة.
(منع وصول الأشخاص غير المخولين لخدمات معينة: كالوصول لموارد الاتصال أو منعهم من عمليات القراءة أو الكتابة).

- ✓ **التخويل Authorization:**

نضمن في هذه الحالة أن المعلومات يتم الوصول والاطلاع عليها من قبل أشخاص أو كيانات مصرحة وهذا الهدف مرتبط ارتباط وثيق بهدف التحكم بالنفاذ.

12- التعمية (أو التشفير) cryptography:

يعرف (cryptography)بأنه علم ودراسة الكتابة السرية وتعتبر هذه التسمية يونانية الأصل وتتكون من كلمتين الأولى كريبتو (crypto) وتعني سرّي و الكلمة الثانية هي غراف (graph) و التي تعني كتابة.
الكريبتوغراف و بشكل عام هو تحويل النص الواضح إلى نص مشفّر وغير مفهوم(مبهم).

- هو الحقل المهتم بالتقنيات اللغوية و الرياضية لتحقيق أمن المعلومات و خاصة في عملية الاتصال.

يمكننا القول بان الكريبتوغراف يستخدم عمليتين رئيستين وهما:
1- التشفير : (encryption) وهو تحويل النص الواضح (plaintext) إلى نص مشفّر (ciphertext)غير مقروء(مبهم) ،غير مفهوم.
2- فك التشفير : (decryption) وهي تحويل النص المشفّر (cipher text) إلى نص واضح plaintext ويمكن قراءته.

ملاحظة : نلاحظ مما سبق أن كل من العمليتين معاكسة للأخرى.

يستخدم الكريبتوغرافي في حماية المعلومات القيّمة و المهمة من الأشخاص الغير مخولين في الاطلاع أو التعديل عليها .
تعتبر هذه المشكلة خاصة بعملية الاتصال بين مرسل ومستقبل و تتضمن عملية الاتصال ثلاثة عناصر رئيسية وهي:

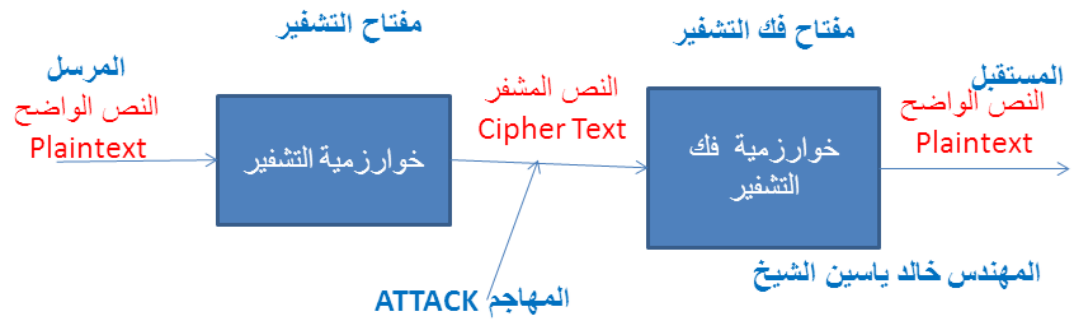
1-المرسل. (sender)
2-المستقبل . (receiver)
3-قناة الاتصال. (channel)

بشكل عام يعتبر العنصر الثالث (قناة الاتصال) هو سبب المشكلة لأنه العنصر الأقل أمنا بين العناصر الأخرى فقد يكون هناك بعض المتطفلين على قناة الاتصال بين المرسل والمستقبل أو قد يكون هناك عملية تسريب للمعلومات عن طريق قناة الاتصال.

- تاريخيا اهتم علم التعمية فقط بالتشفير أي وسائل تحويل المعلومات من شكلها الطبيعي المفهوم إلى شكل غير مفهوم ولقد اهتم الإنسان منذ آلاف السنين على هذا العلم لحجب المعلومات السرية عن أعداءه.
- وقد اقتصر استخدام علم التعمية في القرون الماضية في الحفاظ على أمن المعلومات العسكرية والمراسلات الدبلوماسية وحماية الأمن الوطني. لكن نطاق تطبيقات التعمية توسع كثيراً في العصر الحديث بعد تطور الاتصالات وحدوث ثورة الاتصالات والمعلومات لما تتطلبه من وثوقية أحيانا وضمان عدم الاختراق ومنع التجسس والقرصنة الإلكترونية وتأمين سبل التجارة الإلكترونية.

ومن خلال التعمية نحصل على أهداف ISS:
- الخصوصية أو السرية.
- تكامل وسلامة البيانات والمعلومات.
- التحقق والوثوقية.
- عدم الإنكار.

ونظام المعمى بشكل عام يعمل وفق الشكل التالي:



التشفير بالمفتاح المتناظر Symmetric Key cryptography:

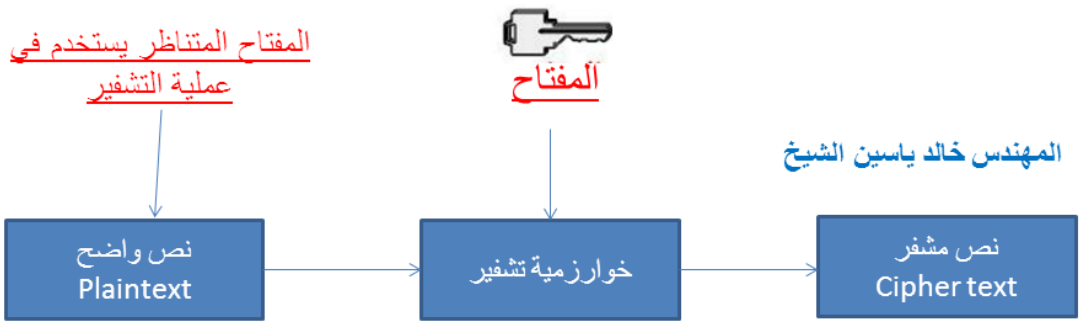
نستخدم نفس المفتاح للتشفير ولفك التشفير (ويجب أن تكون نفس المفتاح ونفس الخوارزمية المستخدمة بين المرسل والمستقبل) لذلك سميت بخوارزميات تشفير متناظرة.

مثال:

خالد مهندس معلوماتية بقسم تقانة المعلومات وقد وصلت له رسالة من رئيس القسم الأستاذ منذر وهذه الرسالة تحتوي علة معلومات سرية جدا خاصة بمعلومات عن حالة الشبكة بالمديرية .
وقرر خالد ومنذر الحفاظ على هذه الرسالة السرية لديهما فقط فما هو السبيل لذلك؟ قد يستطيع خالد حفظ الرسالة عنده في درج المكتب (لكنه يخاف من أن تسرق من الدرج) أو ربما يستطيع حفظ الرسالة برأسه ولكن للأسف الرسالة طويلة !!!!
وقد يقو خالد بحفظ الرسالة في جهازه المحمول ووضع باسورد لجهازه المحمول ولكن هذا ليس كافي ولا حتى آمن فقد يسرق اللاب توب وبعد يستطيع أي شخص لديه إلمام بسيط بالحاسوب أن يدخل إلى الجهاز ويكتشف الرسالة.

وأخيراً قرر المهندس خالد بتشفير وتعمية هذه الرسالة ويجب في هذه الحالة ان يكون معه مفتاح تشفير secret Key وخوارزمية تشفير وفك تشفير (نفس المفتاح يستخدم لتشفير ولفك التشفير)

طريقة التشفير هذه تسمى التشفير بالمفتاح المتناظر(المتماثل) Symmetric Key cryptography والبعض يسميها secret Key cryptography وايضاً تسمى بالتشفير التقليدي **Conventional Encryption**.



في التشفير المتناظر نستخدم نفس المفتاح للتشفير ولفك التشفير ونفس الخوارزمية.
مثلاً استخدمنا الخوارزمية AES في عملية التشفير مع المفتاح 10 عند فك التشفير يجب أن نستخدم الخوارزمية AES مع المفتاح 10 للحصول على النص الواضح والمطلوب.

- إذا في التشفير المتناظر أو المتماثل يكون مفتاح التشفير ومفتاح فك التشفير نفسه ويجب أن يبقى سري بين المرسل والمستقبل.

الهجوم على البيانات المشفرة Attacks on Encryption Data:

المخترق هو الشخص الذي يريد سرقة المعلومات ولكي يحصل على هذه المعلومات يجب أن يستطع فك شفرة البيانات ويوجد طريقتان :

1- **الهجوم على المفتاح Attacks on Key:**
هنا يقوم المخترق بتطبيق هجوم يسمى القوة العنيفة Brute-Force attack وطريقة هذا الهجوم هو أن يقوم بتجريب كل المفاتيح (مفتاح مفتاح) إلى أن يصل إلى المفتاح المطلوب (تجريب كل الاحتمالات الممكنة).
لذلك يجب تكبير حجم المفتاح لضمان عملية حماية أكبر.

2- **كسر الخوارزمية Braking The Algorithm**

أنواع التشفير المتناظر Symmetric Cipher(Key Cryptography):

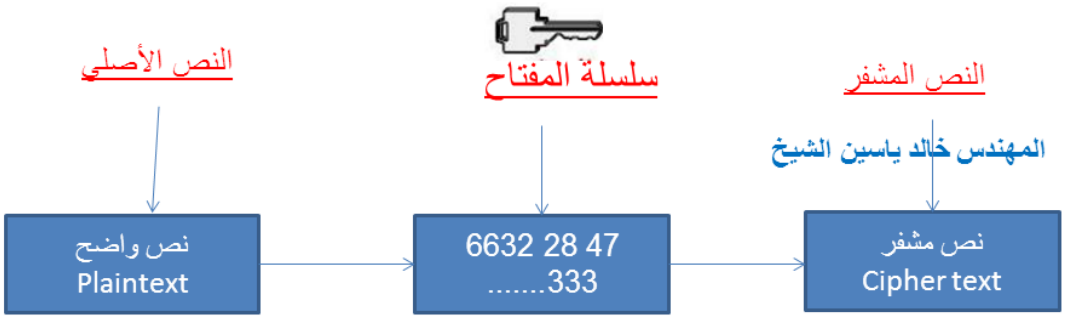
هناك نوعين أساسيين من التشفير المتناظر:

1- شفرات التدفق Stream Cipher.
2- شفرات الكتل Block Cipher.

- **شفرات التدفق Stream Cipher:**

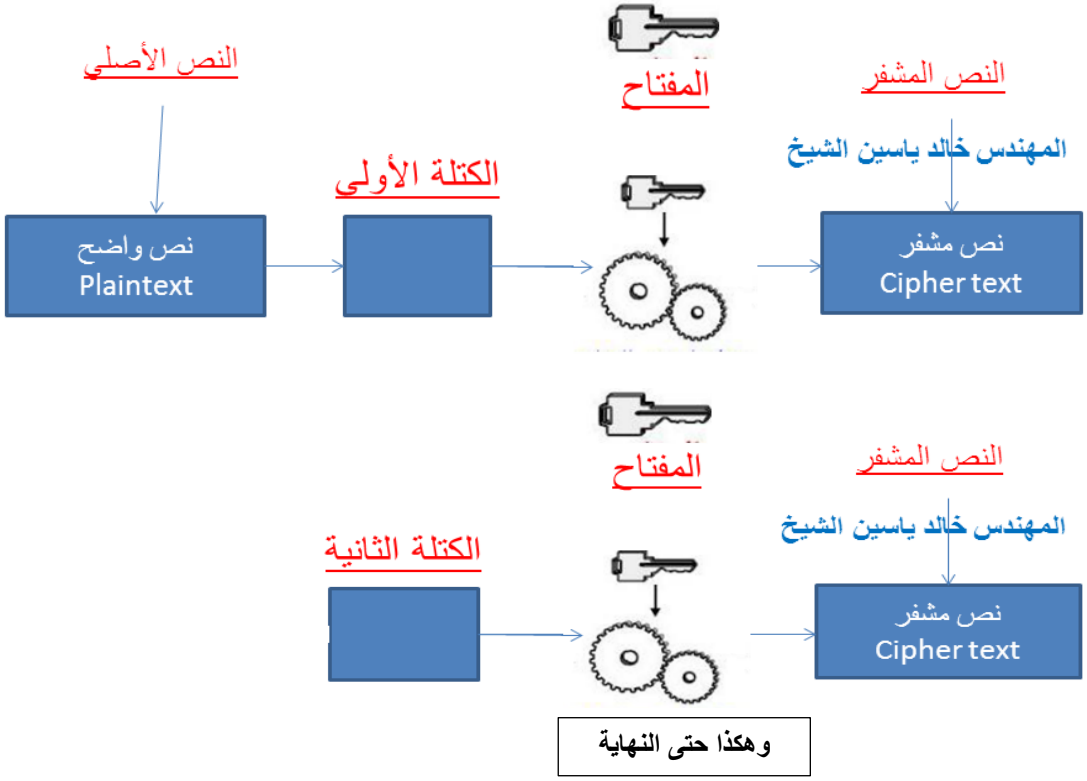
هنا نتعامل مع بت بت أو بايت بايت وليس كتلة كتلة وعملية توليد المفتاح Key Stream من الممكن أن تعتمد على النص المشفر السابق ومن الممكن لا (هناك نوعين من خوارزميات التدفقي متزامن ونوع غير متزامن).

- عملية الأمن في stream Cipher تعتمد على قوة Key Stream.

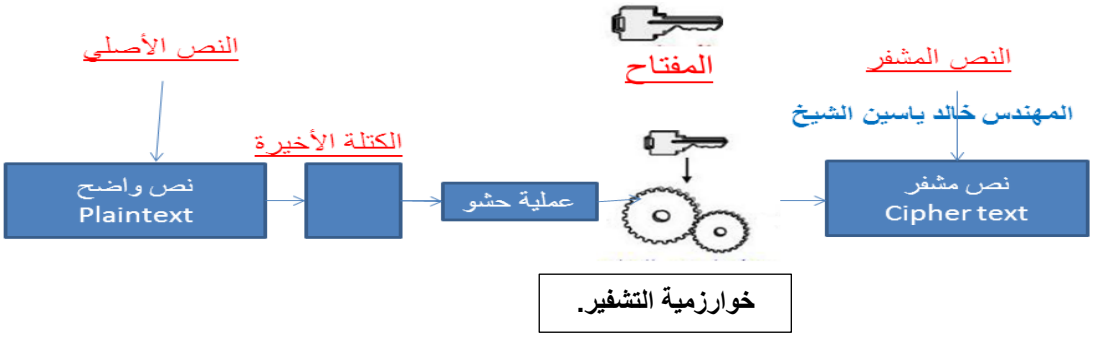


- **شفرات الكتل Block Cipher:**

تقوم بتقسيم النص الأصلي إلى عدد من الكتل كل كتلة بحجم عين مثلا 64 بت أو 56 بت او 128 بت حسب نوع الخوارزمية.



قد يكون هناك حشو padding:



- قوة هذه الخوارزميات الكتلية تعتمد بشكل اساسي على تابع التشفير لأنه نفسه سوف يطبق على الكتل لذلك يجب أن يكون معقد كفاية بحيث يصعب كسره.

- **أمثلة لخوارزميات Block Cipher:**

1- DES(Data Encryption Standard).

2- IDEA

3- AES

4- RC5

5- RC6

6- SAFE

7- Triple DES

8-.....الخ

طبعا لكل خوارزمية طول كتلة معينة ونقاط ضعف وقوة وكل خوارزمية تطبق حسب معيار السياسة الأمنية الموضوعة في المنظمة.

- **التشفير بالمفتاح العام Public Key Cryptography:**

هي استخدام مفتاحين مفتاح عام public Key للتشفير ومفتاح خاص private Key لفك التشفير.

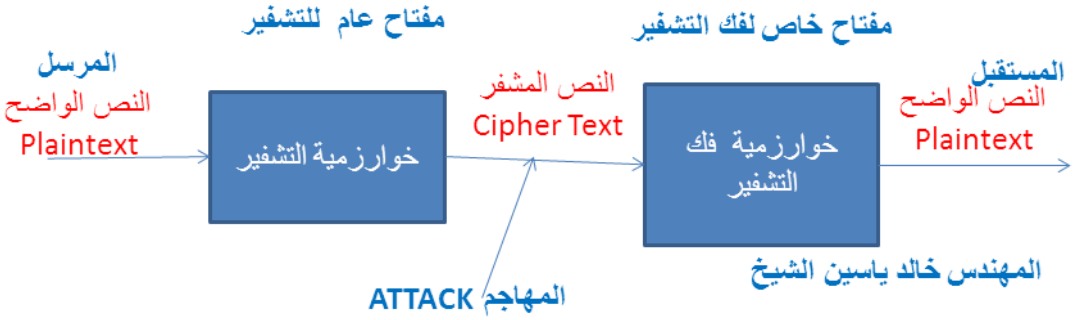
حيث لدينا مفتاح عام يكون معروف للجميع وأي شخص يمكنه الحصول عليه ويستخدم فقط للتشفير.

ومفتاح خاص يكون غير معروف (معروف من قبل شخص واحد) وهو يستخدم لفك التشفير فقط.

أمثلة لخوارزميات التشفير اللامتناظر:

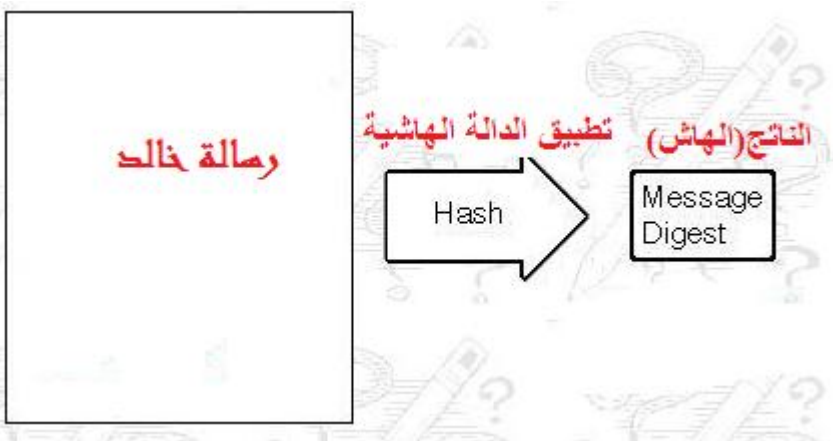
1- RAS

2- خوارزمية Algamal (نسبة لمخترعها للعالم العربي المصري إبراهيم الجمل).



13-التوقيع الرقمي Digital Signature:

تقنية للتأكد من هوية مرسل الرسالة. حيث تدخل الرسالة إلى إحدى خوارزميات التهشير Hash Algorithm ويخرج الناتج ويسمى بالهاش أو ملخص الرسالة message digest .



يقوم المرسل بتشفير الهاش باستخدام مفتاحه الخاص.

يقوم المستقبل بفك تشفير التوقيع (الناتج هو الهاش) باستخدام المفتاح العام للمرسل

ويقوم بتطبيق الدالة الهاشية التي طبقها المرسل.

- ✓ يؤمن التوقيع الرقمي الوثوقية والتكاملية وعدم النكران.
- ✓ أمثلة لخوارزميات التوقيع RSA و ElGamal (DSS or DSA).
- ✓ تابع الهاش عبارة عن خوارزمية تقوم بتحويل الرسالة ذات أطوال متغيرة إلى خرج ذو طول ثابت. والقيمة الناتجة بعد عملية الضغط hash code تسمى بـــ hash value أو message Digest.
- ✓ أمثلة لخوازميات التهشير MD5 خرجها دائما 128 بت، SHA-1 خرجها دائما 160 بت.
- ✓ توابع الضغط سريعة جداً.
- ✓ توابع التهشير تحقق الوثوقية والتكاملية.

مقارنة بين انظمة المفتاح المتناظر والغير متناظر	
symmetric	Asymmetric
تستعمل نفس المفتاح	تستعمل مفتاحين
يجب على المفتاح أن يبقى سري	لا يحتاج المفتاح المعلن أي سرية
في بيئة متعددة المستخدمين هناك صعوبة في عملية إدارة المفاتيح	إدارة المفاتيح أسهل نوعاً ما
سريعة نسبياً	بطيئة نسبياً
يفضل استخدامها في عمليات التشفير للمعلومات الضخمة	يفضل استخدامها في عمليات تشفير المعلومات الصغير الحجم(كمفاتيح الخوارزميات المتناظرة)أي في تحقيق عملية نقل المفاتيح Key Transport

14- مصطلحات يجب التعرف عليها في عالم ISS:

- **السياسة الأمنية Security Policy**: هي مجموعة من القواعد التي تحدد السلوك الأمني بشكل صريح وهي تطبق ضمن Domain أو مجال.

فهي:

- تحدد مسؤولية المنظمة أي لم هي موجودة وماذا ستفعل.
- توصف طرق استثمار وتشغيل المنظمة.

- توصف ما هي الخدمات الأمنية التي يجب أن تكون متوافرة لهذه المنظمة.

والسياسية الأمنية هي عملية مستمرة ودائمة التطور أي لا نضعها مرة واحدة.
وقد تكون السياسية الأمنية عامة جداً ومعناه أنه لا يحق لأحد أن يطلع على المعلومات إلا إذا كان مخولاً authorized وهذا كلام عام جداً ومن الممكن أن نفصل الكلام السابق أكثر مثلاً: عن أي معلومات نتحدث؟؟؟(بيانات شخصية ،حسابات، رواتب .....) ما هي الموارد؟ من هم المخولين؟ ....الخ.

- **الآليات الأمنية Security mechanisms:**

وهي وسائل تزود الخدمة المنية أو هي الآلية التيي تنشئ وتقدم الخدمات الأمنية. ولها نوعان:

1- **Specific Security mechanisms**: صممت لتقديم خدمات أمنية معينة. من هذه الآليات مثلاً:
   - ✓ Encryption:آلية لتقديم أهداف أمنية مثل السرية والوثوقية.....
   - ✓ التوقيع الرقمي يؤمن non-repudiation لمصدر الرسالة
   - ✓ Access control Mechanisms:آلية لتقديم خدمة التحكم بالنفاذ عن طريق:
     - Access control lists.
     - Security Labels: أي ربط كل غرض أو موضوع بـ Label معين. فمثلا ممنوع على كل user معه label قيمته 12 أن يتعامل مع الأغراض ذات الـ Label رقم 3.
   - ✓ Data Integrity mechanisms:تضمن خدمة سلامة البيانات وخدمة الوثوقية.
   - ✓ Authentication Exchanges:تقدم خدمة entity authentication الضرورية عند تبادل مفاتيح التشفير.
   - ✓ Traffic padding :تقدم خدمة السرية confidentiality وهي آلية حشو لتضليل وإخفاء المعلومات.
   - ✓ Notarization: وهي آلية الوساطة العدلية أي يجب الوثوق بطرف ثالث لتحقيق خدمة امنية معينة.

2- **Pervasive Security mechanisms**:

وهي غير مرتبطة بخدمة معينة مثل Auditing, logging ,monitoring.
ولها خمسة انماط:

1- Trusted functionality
2- Security labels
3- Event detection
4- Security audit trail
5- Security recovery

وكلها تدعم السياسات الأمنية وتمنع التهديدات بطرق غير مباشرة.

1- Trusted functionality: أي يجب الوثوق بأي آلية أمنية تقدم خدمة امنية مثلا: يجب الوثوق بخوارزمية التشفير التي نستخدمها لتحقيق آلية التشفير التي تمنحنا خدمة السرية أي يجب تأمين طرق أو وسائل تجعلنا نتأكد من صحة عمل الخوارزمية أو قوتها.

2- Security labels:تصنيف الأغراض كما ذكرت سابقاً ضمن labels وكذلك subject ثم تحديد علاقات بينها بشكل يضمن سياستي الأمنية وهي طرق غير ملزمة بخط محدد وإنما تعود لطبيعة كل سياسة.

الخاتمة:

مفهوم ISS وأدواته التي تساهم في تحقيق الرقابة والتحكم في الأنظمة المعلوماتية على جميع المستويات البرمجية و المادية على حد سواء هو مفهوم هام جدا ومجالات استخداماته واسعة في جميع المؤسسات الحكومية والشركات العالمية والبنوك ولم تقف ISS and C عند هذا الحد بل حتى أن ISS جزء من حياتنا اليومية.

وحاولت في هذا البحث تناول ISS and control بشكل مقتضب وسريع.

والله ولي التوفيق

دمشق

المهندس خالد ياسين الشيخ

الهندسة المعلوماتية بجامعة دمشق 2010

الـــــمراجـــــع

1- مراجع مواقع الإنترنت

1- www.informatics.ed.ac.uk/teaching/courses/cs
2- http://www.tech-wd.com/wd/2010/01/07/book-in-information-security/
3- http://download-pdf-ebooks.in/2602-free-book