الأكاديمية العربية الدولية

الأكاديمية العربية الدولية

المقررات الجامعية

www.aiacademy.info | care@aiacademy.info

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 Control.

إعـــداد الباحث

المـــهنـــدس خـــالـــد يـاســـين الـــشيـــخ

إشـــراف الـــدكـــتـــور

طـــاهـــر حـــســـن

دمـشـــق

للـــعـــام الـــدراســـي

2014-2015

فهرس المحتويات

1- مقدمة:

سوف أتناول في هذا البحث المتواضع التعريف بأمن نظم المعلومات وعناصرها ومكوناتها وما هي الغاية من نظم أمن المعلومات ومفاهيمها لما لهذا الموضوع وهو امن المعلومات من اهمية كبرى في تطبيقات المعلوماتية والحاسوب.

ومفهوم أمن المعلومات هو مفهوم قديم كان كثير الاستخدام في تشفير الرسائل وخاصة أيام الحروب بطرق كلاسيكية تقليدية أما الآن ومع انتشار عصر المعلوماتية وأدواته المختلفة والأداة الأساسية المرتبطة بالمعلوماتية وهو الحاسوب أصبح لأمن نظم المعلومات أهمية كبرى في حمابة البيانات والمعلومات التي تنتقل عبر شبكات الحاسب المختلفة بطرق ووسائل تضمن تحقيق أمن المعلومات Information Security ومفهوم امن المعلومات هو مفهوم واسع ويشمل الأمن على المستوى الفيزيائي والأمن على المستوى البرمجي (المنطقي).

2- ما هو الأمن؟ What is Security ?:

الأمن باختصار هو 3 أشياء :

i. الحماية Prevention: ويقصد بها الإجراءات الوقائية لحماية الممتلكات من التضرر.
ii. كشف وقوع الضرر Detection:اكتشاف شيء تم سرقته أو تعديله أو تخريبه.....
iii. رد الفعل Reaction:الإجراءات التي يجب القيام بها عند حدوث خرق لأمن المعلومات سواء عند حصول ثغرة أو تهديد معين.

- **الأمن** هو بالتعريف حماية الثروات أو الممتلكات (Assets)
- للأمن عدة فروع منها:
  - الأمن القومي
  - والأمن الاقتصادي
  - ...
  - وأمن الحواسب

3- لماذا نظم أمن المعلومات: What Information System Security ?

يمكن أن يتضح لنا الموضوع أكثر إذا نظرنا إليه في العالم الفيزيائي:

عند ما يريد شخص إرسال رسالة مهمة فإنه يتخذ كافة التدابير الأمنية اللازمة التي يعتقد أنها تضمن الحماية والوصول الامن لرسالته.

وفي المؤسسات غير المؤتمتة مثلاً يتم حفظ الأوراق الهامة في خزائن لها أقفال غير قابلة للنسخ ، ومحاولة تأمين عملية نقل آمنة لهذه الأوراق.

أما في المؤسسات المؤتمتة مثل الشركات الكبيرة فلا يستخدم الورق نهائياً لذلك هم بحاجة لتأمين الاحتياجات الأمنية ولكن بشكل رقمي.

كما أنه عند إرسال رسالة يجب التأكد من مصداقية مصدر الرسالة وضمان عدم إطلاع أي شخص على الرسائل.

ولكن يا ترى العالم المؤتمت أكثر أماناً من العالم الفيزيائي؟؟؟

الـ ISS(Information system security) ستجاوب على هذا السؤال.

4- تعريف أمن نظم المعلومات ISS:

لا يوجد ببساطة تعريف شامل لـ ISS لذلك في البداية سنحاول وضع تعريفين لها:

5-التعريف الأول:

ISS نعرفها من خلال الأشياء التي تتعامل معها فهي تؤمن الحماية للنظم الموجودة على الـ machine وهذا يتضمن db،ملفات، سجلات , وأمن OS وتؤمن حماية عمليات Accounting .

والجزء الثاني منها يؤمن الحماية للمعلومات التي يتم تبادلها بين الحواسب مثل نقل الملفات و الـ e-mail والتجارة الإلكترونية .....الخ

مثال:

عند محاولة ارسال رسالة نريد ضمان وصول آمن لها وحمايتها من الأشخاص العابثين الذين يحاولون بشتى الوسائل الوصول إليها Attackers لذلك نحن بحاجة لبناء

(Security Architecture)التي تتألف ببساطة مما يلي:

i. Security Policies: يحدد فيها من مسموح له بالوصول للمعلومات ومن غير مسموح له بذلك(تحدد ما هو المسموح وما هو غير المسموح).
ii. Security Mechanisms :وتعني كل الخوارزميات والبروتوكولات التي يمكن ان يستخدمها الشخص حتى تقوي Policies .
iii. Security services:التي تؤمن عمليات التشفير أو التعمية وعمليات الحماية والمنع....الخ.

6- مفاهيم هامة في ISS:

I. **Security vulnerability**:ويقصد بها نقاط الضعف الموجودة في نظام أمني ما (أي النقاط التي يمكن عبرها التسلل لداخل النظام).
نقطة الضعف أو الهشاشة (Vulnerability)هي حالة أو نقطة ضعف في تصميم النظام أو تنفيذه وقد يكون في البرمجيات (Software) أو في العتاد (Hardware) أو في طريقة إدارة النظام، أمثلة:

- غياب مضاد الفيروسات Anti-Virus
- وجود الأخطاء غير المعلنة في البرامج
- عدم حماية الدخول إلى Logging in بكلمة مرور
- عدم توفر أخصائيي المعلوماتية
- كلمات المرور المرسلة غير محمية
- كلمات المرور مخزنة في ملفات مفتوحة
- شخص نسي إغلاق البان خلفه (عن سوء نية أو دون قصد).

إذن عند معرفة وجود نقاط ضعف يجب أن يحدد الشخص المسؤول عن النظام الـ threats التهديدات المحيطة بنظامه والتي يمكن أن تترك النظام معرض للهجمات.

II. **التهديد(Threat)**: هي مجموعة الظروف أو الأفعال أو الأحداث التي توفر القدرة على إحداث اختراق أمني من خلال استغلال هشاشة النظام(نقاط الضعف)
عند تنفيذ التهديد يتم وقوع الـ attack.
أمثلة:

- شخص لديه القدرة على إحداث عمل غير مرغوب به
- حادثة طبيعية قد تحدث ضرراً ما.
- تعديل المعطيات.
- فيروسات الحاسب أو الكود الخبيث.

III. **أمن الحواسب:** حماية الممتلكات داخل الحاسب:

- أي حماية المعلومات والخدمات التي يقدمها الحاسب.
- أي حماية المعلومات المعالجة والمخزنة والمنقولة

IV. **الهجوم** (Attack): هو تحقيق أو تنفيذ لتهديد ما،

V. **الخطر** (Risk): هو إمكانية التعرض للضرر أو الخسارة.

VI. **المهاجم** (attacker): هو الشخص أو الكيان (Entity) الذي يقوم بالهجوم أي استغلال هشاشة نظام واستغلال نقاط الضعف بدافع معين.

- الشخص الذي يسرق ملفاتك أو يعدل عليها دون أذنك هو مهاجم

- الفيروس الذي يمحو الملفات هو مهاجم
- يوجد عدد من المرادفات للمهاجم: العدو (enemy) والخصم (adversary) والدخيل (intruder) و المتنصت (eavesdropper).
- أيضاً غالباً ما يتردد مصطلحان: الهاكر والكراكر أي المتسلل والمخرب.

VII. **المتسلل(Hacker):** هو شخص لديه خبرة معمقة في أنظمة التشغيل والبرمجيات ولغات البرمجة ويبذل جهد كبير لاكتشاف نقاط الضعف في أنظمة المعلوماتية ويشارك معلوماته مع الآخرين،ولكن لا يلحق الأذى بشكلٍ مباشر أو عن قصد.

VIII. **المخرب(Cracker):** هو الشخص الذي يقوم بانتهاك الأنظمة بسوء نية، أي ينفذ إلى الأنظمة بشكلٍ غير قانوني من أجل تحقيق أهداف مختلقة مثل محو معلومات أو تعديلها.
بمعنى آخر هو Hacker لكنه يمكن ان يخرب كل شيء.

7-أنواع الهجمات Attacks الأكثر شيوعاً في عالم ISS

I. **المقاطعة(Interruption):** تأخير أو رفض خدمة ليصبح النظام خارج الاستخدام.

مثال :شخص يهمه فقط التأثير على وصول المعطيات أو تبادلها سواء بتأخير وصولها أو منع وصولها أصلاً عن سوء أو حسن نية. مثل قطع أحد وصلات Switch.

II. **الاعتراض(Interception):** قراءة معلومات بطريقة غير شرعية أي الوصول إلى المعطيات بطريقة غير قانونية أي الأشخاص الذين يصلون لهذه المعطيات غير مخولين بذلك.

III. **التعديل(Modification):** تعديل المعلومات بطريقة غير شرعية مثل شخص يعدل على ملف مخزن على الحاسب دون علم صاحب الملف. وهي ممكنة حتى عن طريق hardware حين أننا نعلم أن نبضة كهرومغناطيسية كفيلة بتغير بت من 0 إلى 1.

IV. **انتحال الشخصية(Masquerade):** إدخال أو تخزين معلومات إلى النظام أو الشبكة لتظهر كأنها قادمة من مستخدم مخول. وهي غالباً في العالم الإلكتروني يمكن أن تحقق عن طريق معرفة الـ password + Login لشخص ما. ومن خلال عملية Spoofing من خلال أن يتبنى شخص الـ IP لحاسب معين(تغيير IP).

V. **النكران(Repudiation):** ادعاء عدم القيام بإرسال شيء.

- **نكران المصدر**(repudiation of origin): كأن ترسل رسالة إلى زميلك ثم تقول لاحقاً بأنك لم ترسل هذه الرسالة.

مثال: شخص يريد نقل نقوده من حساب لآخر عن طريق البنك (عبر بطاقة) وعندما تأتي الفاتورة ينكر الشخص بأنه قام بهذا التحويل.

VI. **تحليل المرور(Traffic Analysis):** مراقبة الاتصال الشبكي بهدف استخلاص معلومات حول الاتصال.بغض النظر عن المحتوى مثل مكان وعنوان أطراف الاتصال وحجم الاتصال وتكراره.

VII. **إعادة الإرسال(Replay):** إعادة إرسال رسالة تم اعتراضها سابقاً على الشبكة

أي اعتراض رسالة لرسالة منقولة عبر الشبكة ثم إرسالها لاحقاً لإنتاج تأثير غير مخول.

8- مراحل تطبيق حل أمني في عالم ISS

I. **السياسة الأمنية**(Security Policy):

- أي تحديد الأهداف الأمنية المطلوبة
  - مثال: في النظم المُشاركةلا نسمح إلا للأشخاص المرخص لهم النفاذ إلى النظام.
  - مثال: النفاذ إلى المخدم لا نسمح إلا للأشخاص المخولين.
- السياسة الأمنية: هي مجموعة القواعد التي تحدد ما هو مسموح وما هو مرفوض،
  - مثال: يسمح للأشخاص المخولين النفاذ إلى جداول الرواتب.

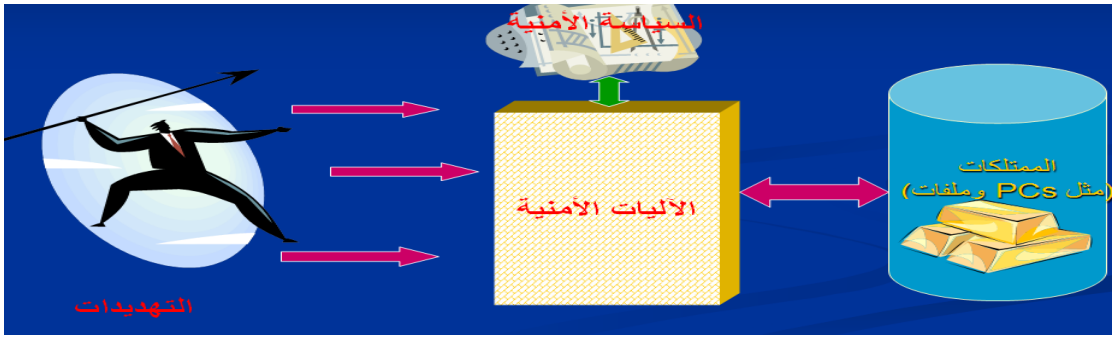
II. **الآليات الأمنية**(Security mechanisms):

- اختيار الأدوات التي تساعد على تحقيق الأهدافIIS التي حددت تحت إطار السياسة الأمنية.
  - مثال: الاعتماد على كلمات المرور في ضبط النفاذ إلى النظام المُشارك
  - مثال: استخدام بروتوكول الدفع (Payment protocol) للتأكد من أن الزبون دفع رسم الدخول إلى خدمة الويب.

III. **البحث عن نقاط الضعف** (Vulnerabilities الممكنة في النظام والتي يمكن أن تترك النظام معرض للهجمات.

IV. آليات صيانة:

- تحسين الحل عن طريق معالجة نقاط الضعف
- واقتراح آليات جديدة



معظم ما سبق يمكن تحقيقه عن طريق التعمية **Cryptography**.

9- التعريف الثاني لـــ IIS : يمكن تعريفها من خلال أهدافها التي يمكن أن تحققها.

10 - أهداف IIS:

I. **السرية (Confidentiality) أو الخصوصية (Privacy):** يقصد بها الحفاظ على سرية المعلومات المرسلة أو المخزنة.

- السماح للأشخاص المخولين فقط الإطلاع على المعطيات أو الأغراض.
- تضمن الثقة عدم تعرض البيانات للاختراق.

– **أنواع اختراقات السرية:**

- اختراقات مقصودة (تعتمد على هجوم مباشر متعمد)

– أمثلة:

- التقاط حركة المرور على الشبكة
- سرقة ملف كلمات المرور
- مسح البوابات (port scanning)
- social engineering

- اختراقات غير مقصودة (أخطاء بشرية، إهمال، سوء تصرف).

- أمثلة:
  - عدم تعمية البيانات المتبادلة بشكل تام و صحيح،
  - ترك نقاط دخول أمنية مفتوحة،
  - اختراقات بسبب أنشطة المستخدمين، أو مدير النظام،
  - عدم تطبيق السياسة الأمنية بشكل جيد.
- **حماية السرية:**
  - التعمية
  - استخدام الحشو في حركة المرور على الشبكة
  - التحكم بالنفاذ
  - توعية المستخدمين

II. **السلامة أو التكاملية (Integrity):** أي التأكد من أن المعلومات التي خزنت لم يطرأ عليها أي تغيير.

- السماح للأشخاص المخولين فقط تعديل المعطيات أو الأغراض
- تضمن الثقة بأن البيانات لم تعدل عن حالتها الأصلية المحمية.

- **التكاملية هي:**
  - منع الكيانات غير المخولة من إجراء تعديلات
  - منع الكيانات غير المخولة من إجراء تعديلات غير مرخص لهم إجراءها
  - بقاء العلاقة بين الأغراض صحيحة ومترابطة ومحققة
- **اختراقات التكاملية:**
  - اختراقات مقصودة (تعتمد على هجوم مباشر متعمد).
    - مثل: الفيروسات والنفاذ غير المرخص بهدف الكتابة أو المحو، إلخ
  - اختراقات غير مقصودة (أخطاء بشرية، إهمال، سوء تصرف)

- مثل: حذف ملفات خطأ و إدخال بيانات غير صحيحة وتعديل وأخطاء في الأوامر،..... الخ.

- **حماية التكاملية:**
  - التحكم بالنفاذ
  - نظم كشف الاقتحام
  - اختبار وظائف الإدخال
  - الخ

مثال: عند محاولة القيام بـ install لنظام linux نلاحظ كتابة اسم الملف MD5 check حيث يتم التأكد من تكاملية الملفات قبل تنزيلها (MD5 هي خوارزمية من خوارزميات توابع التهشير hash function)

III. **الوثوقية authentication**: للتحقق من هوية المرسل(التحقق من هوية الجهة المرسلة لرسالة).

- **ولها نوعين:**

- وثوقية الكيان (Entity authentication): التأكد من هوية الكيان وترتبط بوصلة منطقية (Logical connection)، يجب أن يكون طرفي الاتصال Online أي مشاركين بالاتصال في نفس الوقت. تدعى أيضاً وثوقية مستخدم User Authentication
- وثوقية رسالة (Message authentication): التأكد من مصدر الرسالة وتدعى أيضاً وثوقية مصدر المعطيات(data origin authentication)

ملاحظة هامة: بشكل ضمني إذا حققنا هدف Message authentication فهذا يعني أننا حققنا data origin authentication لأنه مجرد ما تغيرت المعطيات يتغير المصدر لذلك فهما هدفين مرتبطين ببعضهم البعض.

IV. **عدم النكران**(Non-Repudiation): هو هدف يقوم بمنع شخص معين من نكران أي التزام معين أو اتفاق معين.
مثال: شخص x أرسل رسالة معينة فإنه يجب أن يكون لدى المستقبل وسيلة لأن يثبت بأن هذه الرسالة وصلت من الشخص x. مثل عمليات التحويل بين البنوك.

V. **التوافرية أو الإتاحية(Availability):**

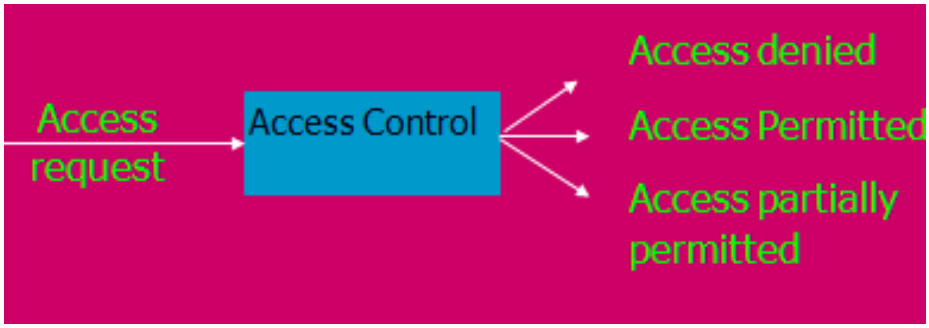
أن يتمكن المخولون من الوصول إلى الأغراض المرخص لهم الوصول لها بدون أي مقاطعة و في الأوقات المرخصة لهم .

تقدم التوافرية مستوى عالٍ من الثقة بأنه يمكن للمخولين الدخول إلى البيانات، الأغراض ، و الموارد المرخص دخولهم إليها وفي الأوقات المرخصة لهم.

- **أنواع اختراقات التوافرية:**
  - اختراقات مقصودة (تعتمد على هجوم مباشر متعمد)
    - مثل: هجمات رفض الخدمة (DoS) وتدمير الأغرض ومقاطعات الاتصالات.
  - اختراقات غير مقصودة (أخطاء بشرية، إهمال، سوء تصرف)
    - مثل: حذف ملفات خطأً واستخدام أجزاء العتاد أو البرامج بشكل مبالغ فيه.

- **حماية التوافرية**
  - تصميم أنظمة تسليم وسيطة ملائمة
  - تقنيات ضبط نفاذ فعالة،
  - مراقبة الأداء و حركة مرور الشبكة
  - استخدام الجدران النارية
  - اعتماد مبدأ الاحتياطي **(redundancy)** للأنظمة الحساسة
  - صيانة واختبار نظم التخزين الاحتياطي.

VI. **التحكم بالنفاذ Access Control**:تنظم العمليات التي تُنفذ على المعطيات المراد حمايتها أي لا يصل إلى المعطيات إلا الأشخاص المخولين بذلك.
- تهدف إلى ضبط العمليات التي تنفذ من قبل المواضيع (Subjects) على الأغراض (Objects) من أجل منع الأفعال يمكن أن تلحق الضرر بالمعطيات (أي الأغراض).



- **مراحل التحكم بنفاذ:**

1. **التعريف: تعريف الموضوع الذي يريد أن ينفذ إلى الغرض**
2. **الوثوقية: التأكد من هوية الموضوع الذي ينفذ إلى الغرض**
3. **التخويل: التأكد من صلاحيات نفاذ الموضوع الذي ينفذ إلى الغرض**
4. **المحاسبة والتدوين: تسجيل أنشطة الموضوع.**

VII. **التخويل authorization**:منح صلاحيات لشخص معين.

مثال: الشخص x يحق له الوصول إلى المعطيات لكن دون تعديل. أما الشخص y يحق له الوصول إلى المعطيات مع تعديل في الغرض رقم 5 فقط.

ويوجد ما يعرف **infrastructure** public key.وهذه التقنية تمنح سلطات وشهادات لأشخاص للقيام بتوقيع أوتشفير.....

VIII. **التوقيع الرقمي Digital Signature**:طريقة لربط المعطيات بشخص معين أو كيان معين.

IX. **Validation**: ربط شيء معين بزمن معين وبعد هذا الزمن لا يعود هذا الشيء متاح.

X. **Others**:

- **الطابع الزمني:Time stamping**أي ربط قيم زمنية برسالة أو بمعلومة معينة.
- **Receipt:**بعد بعث الرسالة يجب أن يصل إقرار.
- **Revocation:**سحب شيء معين من الاستخدام بعد انتهاء صلاحيته.

من الأهداف السابقة تستطيع التعمية أو التشفير Cryptography بتحقيق أربعة منهم وهم:

- ✓ السرية (Confidentiality) أو الخصوصية (Privacy).
- ✓ السلامة أو التكاملية (Integrity).
- ✓ الوثوقية authentication .
- ✓ عدم النكران(Non-Repudiation).

وهذه الأهداف الأمنية الأربعة كفيلة بتشكيل إطار عمل لتحقيق بقية أهداف ISS.

إذن نحن نريد القيام بـ **Cryptography حتى نحقق بعض أهداف ISS.**

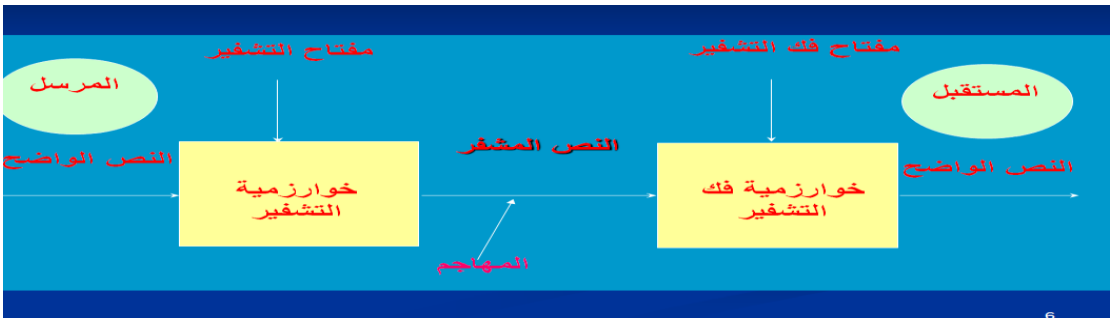
11- التعمية (Cryptography):

- ظهرت التعمية قبل حوالي ألفي عام واقتصرت على الكتابة السرية أي تقديم السرية للرسائل المتبادلة وانحصر استخدامها على التطبيقات العسكرية والحكومية
- تطورت التعمية خلال العقود الماضية لتشمل استخدام الرياضيات في تعريف مجموعة من التقنيات التي تساعد على تحقيق مجموعة أوسع من الأهداف الأمنية مثل السرية والتكاملية والوثوقية وعدم النكران، ولم يعد يقتصر استخدام التعمية على الاستخدامات الحكومية بل انتشرت وبشكل واسع في التطبيقات التجارية (لا سيما التجارة الالكترونية والمؤسسات المصرفية) ، حيث تساعد التعمية على تخزين المعطيات ونقلها عبر شبكة غير آمنة مثل الانترنت بطريقة تكون فيها (المعطيات المنقولة عبر الشبكة) غير قابلة للقراءة(إذا تمت حمايتها بالتعمية) إلا من قبل الشخص المعني باستلامها.
- علم استخدام الرياضيات لتحقيق أهداف أمنية مثل السرية والوثوقية والتكاملية وعدم النكران.

- **آليات التعمية:**

- **التشفير**: يؤمن السرية والتكاملية ووثوقية كيان ووثوقية رسالة.
- **كود وثوقية رسالة(MAC (Message Authentication Cod**: يستخدم في التكاملية ووثوقية رسالة ووثوقية كيان.
- **التوقيع الرقمي**: يؤمن الوثوقية (رسالة وكيان) والتكاملية وعدم النكران.
- **تحليل التعمية (Cryptanalysis):** دراسة التقنيات الرياضية التي تحاول أن تحبط تقنيات التعمية.
- **علم التعمية (Cryptology)**: هو دراسة التعمية وتحليل التعمية

- **نظام التعمية (Cryptosystem):** مجموعة من أساسيات التعمية (Cryptographic primitives) التي تستخدم في تحقيق مجموعة أهداف أمنية. ويدعى أيضاً بـ **المُعمِّي** (Cipher) أو **النظام المُعمِّي** (Cipher system)



- ✓ يدعى النص قبل تشفيره بـ**النص الواضح** (Plaintext or Clearest)
- ✓ تدعى عملية تحويل النص الواضح إلى نص مشفر بـ **التشفير** (Encryption).
- ✓ يدعى النص بعد تعميته بـ**النص المشفر** (Cipher text).
- ✓ تدعى عملية تحويل النص المشفر إلى نص واضح بـ**فك التشفير** (Decryption).
- ✓ **خوارزمية التشفير**: تنجز مجموعة من العمليات على النص الواضح، وتأخذ كدخل مفتاح تشفير.
- ✓ **خوارزمية فك التشفير**: تنجز مجموعة من العمليات على النص المشفر، وتأخذ كدخل مفتاح فك تشفير.

12- أنواع خوارزميات التعمية

تقسم خوارزميات التعمية إلى ثلاثة أقسام رئيسية:

- خوارزميات التعمية التناظرية (symmetric cryptography): يمكن حساب مفتاح فك التشفير مباشرةً انطلاقاً من مفتاح التشفير،اي معرفة مفتاح التشغير تكفي لمعرفة مفتاح فك التشفير، وفي أغلب الأحيان يستخدم مفتاح التشفير كمفتاح فك التشفير. أي ان المفتاحين متطابقين، ويجب أن يكون مفتاح التشفير سرياً بين المستقبل والمرسل.
  - قبل البدء بأي عملية تبادل للرسائل يجب على المرسل والمستقبل إيجاد الطريقة المناسبة لتبادل المفتح السري أو للاتفاق عليه.

- **خوارزميات التعمية اللاتناظرية (asymmetric cryptography)**: يملك الشخص المشارك في الاتصال مفتاحين: مفتاح تشفير ومفتاح فك تشفير ولا يمكن حساب مفتاح فك التشفير من مفتاح التشفير إلا من قبل صاحب المفتاحين. اي كل شخص يريد أن يشارك في الاتصال يجب أن يكون لديه زوج مفاتيح واحد للتشفير وأخر لفك التشفير.

- **خوارزميات التهشير أو الاختصار (Hashing) :** تُنتج هذه الخوارزميات قيم خرج بطول ثابت (بحسب نوعية الخوارزمية) وذلك مهما بلغ طول رسالة الدخل. بالرغم من أنه لاتحتاج هذه الخوارزميات إلى مفتاح تعمية إلا أنها تستخدم في التوقيع الرقمي وإنتاج كود وثوقية رسالة (Message Authentication Code – MAC).

❖ **التعمية التناظرية أو التعمية المعتمدة على مفتاح مشترك (Shared key)** :هي بالتعريف مجموعة التقنيات التي تعتمد على مفتاح سري مشترك بين طرفي الاتصال، أي لا يعلم بالمفتاح أي شخص آخر.

- هذه التعمية تدعى أيضاً بتعمية المفتاح الوحيد (Single-key cryptography). أو تعمية المفتاح السري secret key cryptograhpy ، او التعمية التقليدية

- تتكون خوارزمية التعمية التناظرية من تابعين مرتبطين رياضياً: تابع تشفير وتابع فك تشفير.

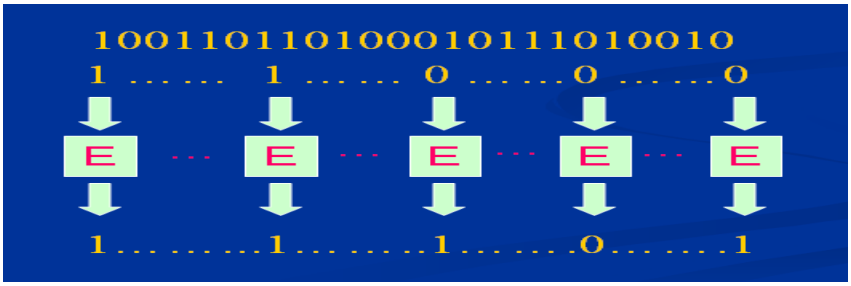
  - يعتمد حساب قيمة تابع التشفير على معاملي دخل (2 input parameters): النص الواضح والمفتاح السري.

  - ويعتمد حساب قيمة تابع فك التشفير على معاملي دخل (2 input parameters): النص المشفر والمفتاح السري.

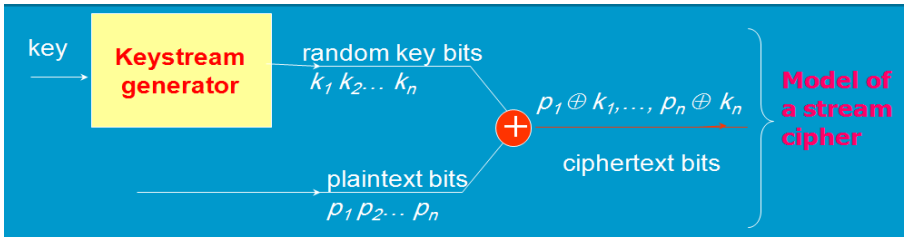
- تعتمد قوة هذه الخوارزميات على سرية المفتاح وليس على الخوارزمية نفسها لأنه غالباً ما تكون هذه الخوارزميات منشورة. أي أن معرفة الخوارزمية المستخدمة في التشفير لا تكفي وحدها لفك تشفير النص المشفر.

- يمكن تقسيم خوارزميات التعمية التناظرية، بحسب طريقة معالجة الخوارزمية للنص المراد تشفيره، إلى نوعين: تشفير كتلي (Block Cipher) وتشفير دفقي (stream cipher).

التشفير الدفقي (stream cipher)هي عملية تشفير كل محرف أو بت من النص الوضح بمفردها.



- في الشكل السابق: يتكون النص المراد تشفيره من مجموعة من البتات وعملية التشفير تجري كما يلي:
- أولاً: يُدخل إلى خوارزمية التعمية البت الأولى مع مفتاح التشفير وينتج عن هذه العملية أول بت من النص المشفر.
- بعد ذلك يدخل إلى خوارزمية التعمية البت الثانية مع مفتاح التشفير وينتج عن هذه العملية ثاني بت من النص المشفر.
- وتستمر العملية بهذه الطريقة إلى أن ينتهي النص المراد تشفير.
- غالباً ما تكون خوارزميات التشفير الدفقي بسيطة مثلاً أن تكون مكونة من عملية XOR
- يستخدم التشفير الدفقي مفتاح تشفير لإنتاج مفتاح دفقي (stream key) بطول النص المراد تشفيره.

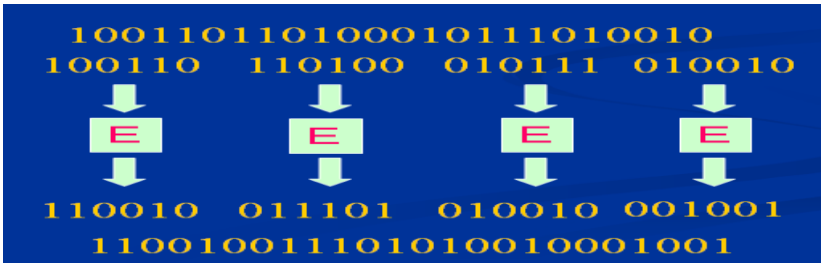


- في الشكل : خوارزمية التشفير هي فقط عملية XOR
- إنتاج المفتاح الدفقي لا تعتبر من خوارزمية التشفير.

من أهم خوارزميات هذا النوع من التشفير:

- **One-Time Pad (OTP):** خوارزمية تستخدم المفتاح التدفقي مرة واحدة فقط. اي لا تكرر استخدام المفتاح الدفقي لأكثر من عملية تشفير واحدة هذه الخوارزمية هي خوارزمية فيرنن ولكن المفتاح الدفقي لا يستخدم إلا مرة واحدة.
- **RC4**: خوارزمية تشفير تدفقي تعمل على طول مفتاح متغير. له تطبيقات في شبكات المحمول ، ويستخدم في الطبقة الآمنة SSL

التشفير الكتلي هي عملية تشفير تعتمد على تجزئة النص الواضح إلى كتل متساوية في الطول قبل أن يتم تشفير كل كتلة بمفردها لينتج عنها كتل مشفرة بنفس طول الكتل غير المشفرة.



- 1- نقسمه إلى اطوال متساوية.
- 2- ندخل الكتلة الاولى إلى خوارزمية التشفير مع المفتاح السري لينتج عنها كتلة مشفرة مكونة من بتات طولها نفس كتلة الدخل.
- 3- وهكذا مع باقي الكتل.
- 4- الكتل المشفرة تشكل النص المشفر.
- طول الكتل يعتمد على خوارزمية التشفير
- بعكس خوارزميات التشفير الدفقي خوارزميات التشفير الكتلي معقدة (تعتمد على توابع رياضية معقدة).

<u>من أهم خوارزميات التشفير التناظري الكتلي:</u>

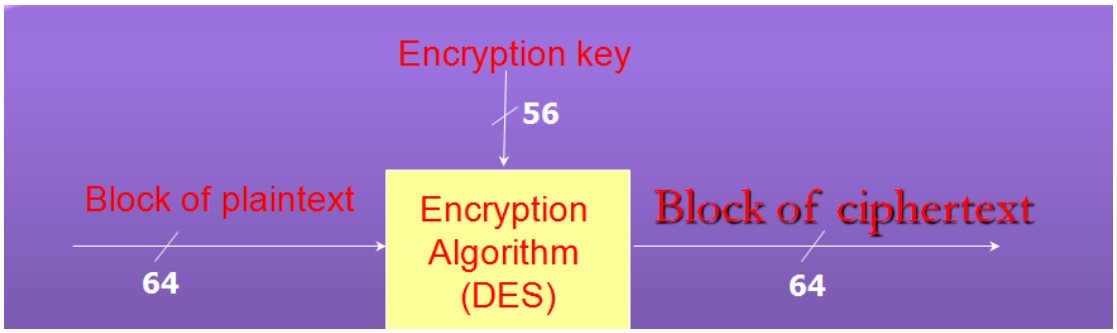
I. DES (Data Encryption Standard): يعمل على كتل بطول 64 بت ومفتاح بطول 56 بت. كانت هذه الخوارزمية وحتى فترة قريبة الأكثر انتشاراً واستخداماً إلا أنه ومع زيادة قدرة الأجهزة الحاسوبية على المعالجة السريعة فإنه لم تعد هذه الخوارزمية آمنة بسبب القدرة على إيجاد مفتاح التشفير عن طريق استخدام هجوم Brute force الذي يجرب كل المفاتيح الممكنة الممثلة على 56 بت. لذلك استبدلت هذه الخوارزمية بـ 3DES و AES.

II. 3DES: يعتمد على تنفيذ خوارزمية DES ثلاث مرات. طول مفتاحه إما 128 بت أو 192 بت. يعد 3DES بديل مؤقت لـ DES.

III. AES (Advanced Encryption Standard): أقترح في العام 2001 ليحل مكان DES. يعمل AESعلى كتل بطول 128 بت ومفاتيح بطول 128 أو 192 أو 256 بت.

خوارزميات أخرى أقل انتشارا: IDEA و Blowfish و RC2 و RC5.

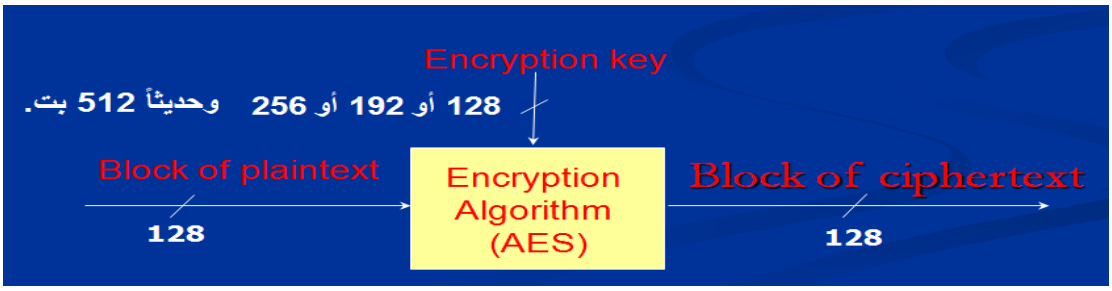
- **<u>Data Encryption Standard (DES)</u>**
  - ✓ طول الكتلة: 64بت
  - ✓ مفتاح التشفير56 بت.



- **Advanced Encryption Standard(AES)**

✓ طول الكتلة: 128بت

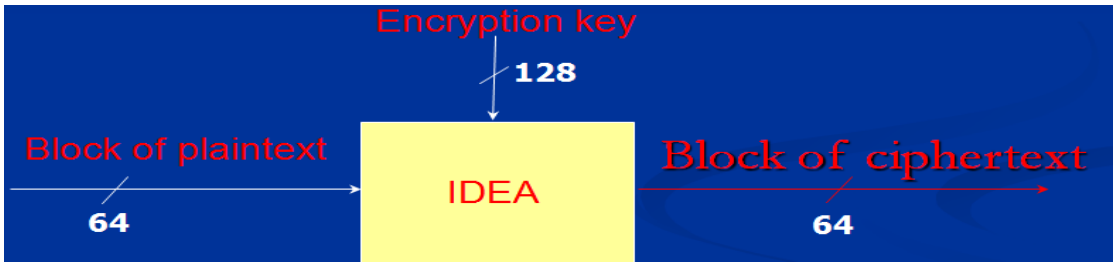
✓ مفتاح التشفير: 128 أو 192أو 256 بت وحديثاً 512 بت.



- **International Data Encryption Algorithm(IDEA)**

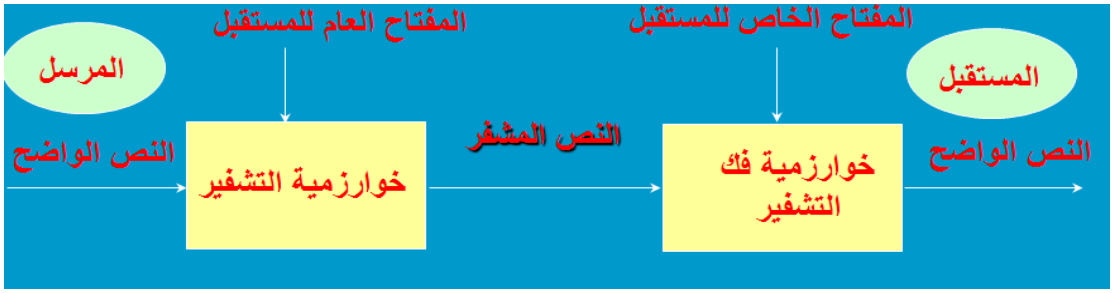
✓ طول الكتلة: 64 بت.

✓ مفتاح التشفير 128 بت.



❖ التعمية اللاتناظرية:

- تدعى أيضاً **تعمية المفاتيح العامة:**
  - Public-Key Cryptography
- تستخدم زوج مفاتيح:
  - مفتاح عام (public key)يستخدم لتشفير المعطيات
  - ومفتاح خاص (Private key) مرتبط بالمفتاح العام ويستخدم لفك التشفير.



- ينشر الطرف المستقبل مفتاحه العام ويحتفظ بمفتاحه الخاص بشكل سري
- يمكن لأي شخص أن يستخدم المفتاح العام لتشفير المعطيات التي يريد أن يرسلها إلي صاحب المفتاح.
  - ✓ لا يمكن لأي شخص آخر أن يفك تشفير هذه المعطيات.
  - ✓ لا يمكن لأي شخص آخر أن يستنتج المفتاح الخاص انطلاقاً من المفتاح العام
  - ✓ تعتمد قوة هذه الخوارزميات على طول الكتلة وعلى طول المفتاح
- أمثلة: RSA و ElGamal.

❖ خوارزميات التهشير

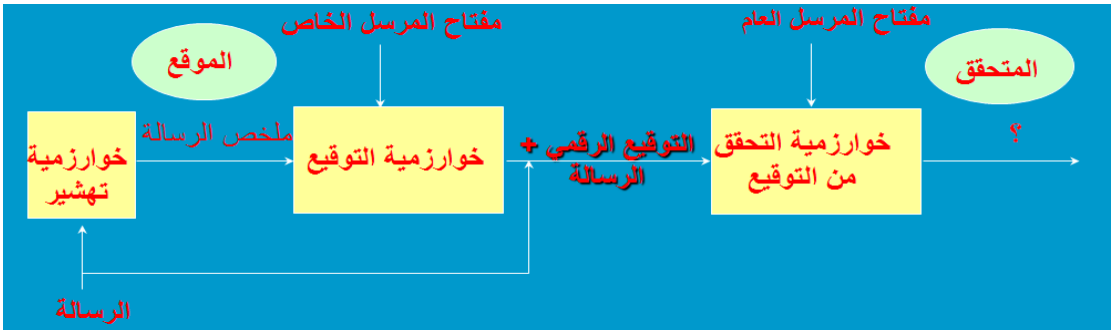
- خوارزميات التهشير (Hashing Algorithms) هي توابع تهشير باتجاهٍ وحيد (One-way hash functions) أي يمكن حساب التابع بسهولة ولكن من الصعب جداً حساب الرسالة انطلاقاً من معرف خرج التابع.

- يدعى خرج توابع التهشير بـ:
  - **ملخص الرسالة** (Message Digest) أو**قيمة التهشير** (Hash value).

توابع التهشير المستخدمة:

- MD5(Message Digest): ينتج خرج بطول 128 بت.
- SHA-1 (Secure Hash Algorithm): ينتج خرج بطول 160 بت.
- **تستخدم خوارزميات التهشير في:**
  - ✓ **التوقيع الرقمي** (Digital signature):
    - تشفر قيمة التهشير باستخدام المفتاح الخاص بالمرسل.
  - ✓ كود وثوقية رسالة MAC (Message Authentication Code):
    - يستخدم تابع التهشير كجزء من تابع آخر، يدعى تابع MAC، الذي يأخذ كدخل مفتاح سري مشترك بين المرسل والمستقبل.
- أمثلة على توابع MAC:
  - ✓ التابع HMAC (keyed-Hash MAC)، حيث يستخدم MAC في تأمين
    - **التكاملية والوثوقية**

13- التوقيع الرقمي: هو تقنية لربط هوية الموقع (أو المرسل) بالرسالة.



- **يعمل التوقيع الرقمي كما يلي:**
  - يقوم الموقع (signer) باستخدام خوارزمية توقيع رقمي ومفتاحه الخاص بتشفير اختصار الرسالة قبل أن يرسل خرج خوارزمية التوقيع مع الرسالة.

- يستخدم المستقبل (يدعى متحقق) المفتاح العام للمرسل لفك التشفير.
- يقارن المستقبل فك تشفير اختصار الرسالة مع اختصار الرسالة
- إذا تساوت القيمتان، عندئذٍ يكون التوقيع صحيح.

من أهم خوارزميات التوقيع الرقمي:

- RSA
- DSA (Digital Signature Algorithm) أو DSS (Digital Signature Standard).

14- تقنيات التعريف والوثوقية

- ✓ كلمات المرور passwords.
- ✓ Biometrics.
- ✓ علامات (Tokens).
- ✓ التذاكر (tickets).
- ✓ التوقيع لمرة واحدة (Single Sign On –SSO).

❖ كلمات المرور:

تعد كلمات المرور التقنية الأكثر انتشاراً في التعريف والوثوقية.

تتكون كلمات المرور من سلسة من المحارف (أرقام وأحرف ومحارف تحكم)،

تعد تقنية التعريف الأضعف وذلك للأسباب التالية:

- عادة يختار المستخدمين كلمات يسهل عليهم حفظها وبالتالي يسهل أن يخمنها المهاجمين.
- كلمات المرور المولدة عشوائياً يصعب حفظها لذلك لابد من تخزينها وهذا يعرضها للسرقة.
- غالباً ما يتشارك المستخدمون كلمات المرور مما يسهل كشفها.

❖ Biometrics

تستخدم هذه التقنية لتعريف المستخدم فقط (أي عندما يكون الموضوع هو انسان).

تعتمد هذه التقنية على اختيار صفة سلوكية أو فيزيولوجية تكون معرفة للموضوع بشكل وحيد وتتخذ كطابع مميز له. مثل: بصمة الإصبع، بصمة العين،.....

تعمل نظم التعريف من النوع Biometrics على الشكل التالي:

تحول المواصفات الفيزيائية (بصمة الاصبع مثلا) إلى نماذج رقمية (digital templates) لتخزن في قواعد معطيات.

عندما يقدم المستخدم نفسه من أجل الوثوقية، تقاس الصفات الفيزيائية من قبل قارئ (reader) وترمز رقمياً ثم تقارن مع النموذج المخزن.

❖ **علامات:**

هي أداة تولد كلمات المرور يحملها الموضوع معه. يمكن أن:

- تولد كلمة مرور واحدة ثابتة مثلاً بالاعتماد على قيم سرية مثل PIN
- أو تولد بشكل مستمر و عندها تكون كالآلة الحاسبة في كل مرة تستخدمها تولد كلمة مرور جديدة.

❖ **التذاكر:**

تعتمد هذه التقنية على وجود طرف ثالث يقوم بتعريف والتأكد من وثوقية الموضوع.

مثال

التذاكر التي يولدها مخدم Kerberos

تستخدم في وثوقية الموضوع عندما يطلب النفاذ إلى المخدمات ضمن الشبكة.

❖ **التوقيع لمرة واحدة:**

هي آلية تسمح بأن يتم التأكد من هوية الموضوع مرة واحد ة.

لدى دخوله إلى المخدم الذي يقدم عدد من الخدمات (مثل تخزين الملفات والطباعة)

و يسمح باستخدام هذه التقنية فقط في حال استخدام كلمات مرور قوية جدًا.

15- البرمجيات الخبيثة في عالم ISS

الكود الخبيث(البرمجيات الشريرة) (Malicious software, or malware) هو الكود الذي:

- يغير المعطيات أو يدمرها.
- يسرق المعطيات

- يسمح بنفاذ غير شرعي إلى المعطيات
- يستثمر النظم ويلحق الأذى بها
- يقوم بأفعال لا يريد المستخدم القيام بها.

بعض الأنواع الأكثر انتشاراً من الكود الخبيث: الفيروس (Virus) و الدودة (Worm) و حصان طروادة Trojan Horse .

16- الأمن المادي physical security

يهدف **الأمن الفيزيائي**(Physical Security)إلى الوقاية من التهديدات المادية مثل :

- النار والفيضانات والزلازل والتخريب أو التدمير المتعمد وتعطل المعدات ونقص المختصين.
- يوجد العديد من العناصر في بناء الأمن المادي. أحد أهم هذه العناصر هواختيار وتصميم الموقع الذي سيحوي البنية التحتية لتكنولوجيا المعلومات وللتطبيقات في مؤسستك.

17- متحكمات الأمن المادي

يمكن أن نقسم متحكمات الأمن المستخدمة لإدارة الأمن المادي إلى ثلاث مجموعات أساسية:

1. **متحكمات الأمن المادي الإدارية**

✓ مثل: بناء واختيار موقع وإدارة الموقع و ضبط المستخدمين والتدريب والإطلاع والاستجابة لحالات الطوارئ.

2. **متحكمات الأمن المادي التقنية**

✓ مثل: متحكمات الدخول وكاشفات المقتحمين والإنذارات والمراقبة التلفزيونية والتدفئة والتكييف ومزودات الطاقة، إلخ.

3. **متحكمات الأمن المادي المادية**

✓ مثل الأسيجة والأقفال والإضاءة ومواد البناء والحراس الأمنيين....الخ

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- المراجع العربية:

1- محاضرات أمن نظم المعلومات(الهندسة المعلوماتية)

د.غسان شدود.

جامعة دمشق(السنة الخامسة) 2009-2010م

2- مراجع مواقع الإنترنت

1- www.informatics.ed.ac.uk/teaching/courses/cs