COMPUTER AND DATA SECURITY

University of Baghdad
College of Education for Pure Science / Ibn Al-Haithem
Department of Computer Science
Fourth Class

Dr. Haifaa Jassim
2021-2022

Chapter 1
Introduction to
Computer Security

What is Computer Security?

Computer Security is the protection of computing systems and the data that they store or access.

Why is Computer Security Important?

Computer Security allows the University to carry out its mission by:

- Enabling people to carry out their jobs, education, and research
- Supporting critical business processes
- Protecting personal and sensitive information

Why do I need to learn about Computer Security?
Isn't this just an IT Problem?

Good Security Standards follow the "90 / 10" Rule:

- ***10% of security safeguards are technical***
- ***90% of security safeguards rely on the computer user ("YOU") to adhere to good computing practices.***

Example:
The lock on the door is the 10%. You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. You need both parts for effective security.

What Does This Mean for Me?

- This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, devices and data secure.
  This means *Information Security is **everyone's** responsibility*

- Members of the UCSC community are also responsible for familiarizing themselves and complying with all University policies, procedures and standards relating to information security.

  Security Objectives

- Learn "**good computing security practices.**"
- Incorporate these practices into your everyday routine. Encourage others to do so as well.
- Report anything unusual – Notify your supervisor and the ITS Support Center if you become aware of a suspected security incident.

The Internet can be a hazardous place:

How many attacks to computers on campus do you think take place everyday?

- Thousands of attacks **per minute** bombard our campus network.
- An unprotected computer can become infected or compromised **within a few seconds** after it is connected to the network.

A compromised computer is a hazard to everyone else, too – not just to you.

Quiz: A hacked computer can be used to... *(select all that apply)*

a) Record keystrokes and steal passwords.
b) Send spam and phishing emails.
c) Harvest and sell email addresses and passwords.
d) Access restricted or personal information on your computer or other systems that you have access to.
e) Infect other systems.
f) Hide programs that launch attacks on other computers.
g) Illegally distribute music, movies and software.
h) Distribute child pornography.
i) Generate large volumes of traffic, slowing down the entire system.

Of course, the answer is "All of the above."

A compromised computer can be used for all kinds of surprising things.

يمكن استخدام الكمبيوتر المخترق لجميع أنواع الأشياء المفاجئة.

Many cyber security threats are largely avoidable. Some key steps that everyone can take include:

- Use good, cryptic passwords that can't be easily guessed - and keep your passwords secret.
- Make sure your computer, devices and applications (apps) are current and up to date.
- Make sure your computer is protected with up-to-date anti-virus and anti-spyware software.
- Don't click on unknown or unsolicited links or attachments, and don't download unknown files or programs onto your computer or other devices.
- Remember that information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept

- To help reduce the risk, look for "https" in the URL before you enter any sensitive information or a password (the "**s**" stands for "secure")
- Also avoid standard, unencrypted email and unencrypted Instant Messaging (IM) if you're concerned about privacy.

Protecting Campus Networks:

Computers posing a serious threat will be blocked or disconnected from the campus network. Passwords known to be compromised will be scrambled.

"Campus network and security personnel must take immediate action to address any threats that may pose a serious risk to campus information system resources.... If the threat is deemed serious enough, the account(s) or device(s) presenting the threat will be blocked or disconnected from network access."

What are the consequences for security violations?

- Risk to security and integrity of personal or confidential information. e.g. identity theft, data corruption or destruction; lack of availability of critical information in an emergency, etc.
- Loss of valuable business information
- Loss of employee and public trust, embarrassment, bad publicity, media coverage, news reports
- Costly reporting requirements in the case of a compromise of certain types of personal, financial and health information
- Internal disciplinary action(s) up to and including termination of employment, as well as possible penalties, prosecution and the potential for sanctions / lawsuits

Computer Crimes:جرائم الكمبيوتر

How can systems be easily compromised?

كيف يمكن اختراق الأنظمة بسهولة؟

- **Social engineering:هندسة اجتماعية**
  Persuade others to give away their passwords over the phone.
  إقناع الآخرين بالتخلي عن كلمات المرور الخاصة بهم عبر الهاتف
- **Electronic pickpockets:السراق الإلكترونيين**
  Use computers to transfer or change assets to their advantage
  استخدام أجهزة الكمبيوتر لنقل أو تغيير الأصول لصالحهم

- **Unauthorized access to computer files**
  - **Accessing confidential employee records**
  - **Theft of trade secrets and product pricing**

- **الوصول غير المصرح به إلى ملفات الكمبيوتر**
  - **الوصول إلى سجلات الموظفين السرية**
  - **سرقة الأسرار التجارية وتسعير المنتجات**

- **Unlawful copying of copyrighted software**
  - **Casual sharing of copyrighted software**
  - **Assembly-line copying**

- **النسخ غير القانوني للبرامج المحمية بحقوق النشر**
  - **المشاركة العرضية للبرامج المحمية بحقوق الطبع والنشر**
  - **نسخ خط التجميع**

- **Bomb**
  - **Program to trigger damage**
  - **Scheduled to run at a later date**
  - **May be found in software for general public, especially shareware**

- **قنبلة**
  - **برنامج لإحداث الضرر**
  - **من المقرر تشغيله في وقت لاحق**
  - **يمكن العثور عليها في البرامج لعامة الناس ، وخاصة البرامج التجريبية**

- **Data diddling**
  - **Changing data before or as it enters the system**

- **التلاعب بالبيانات**
  - **تغيير البيانات قبل أو عند دخولها إلى النظام**

- **Denial of service attack (DOS)**
  - **Hackers bombard a site with more request for service than it can possible handle**
  - **Prevents legitimate users from accessing the site**
  - **Appearance of requests coming from many different sites simultaneously**

- **هجوم رفض الخدمة(DOS)**
  - **يقصف المتسللون موقعًا بطلب خدمة أكبر مما يمكن التعامل معه**
  - **يمنع المستخدمين الشرعيين من الوصول إلى الموقع**
  - **ظهور الطلبات الواردة من العديد من المواقع المختلفة في وقت واحد**

- **Piggybacking**
  - **Original user does not sign off properly**
  - **Intruder gains accesses to files via the original user id**
- **Salami technique**
  - **Embezzlement**

- **Scavenging**
  - **Search garbage and recycling bins for personal information**

- **Piggybacking**
  - **لا يقوم المستخدم الأصلي بتسجيل الخروج بشكل صحيح**
  - **يتمكن الدخيل من الوصول إلى الملفات عبر معرف المستخدم الأصلي**
- **تقنية السلامي**
  - **الاختلاس : حصل على هذا الاسم من طريقة اضافة القطع الصغيرة من اللحم والتي تجمع معا في الشرائح حيث عمله مشابه لطريقة عمل الشرائح حيث يقتطع مبلغ صغير من المال من كل حساب جاري والجزء المقتطع صغير جدا بحيث في الحالات الطبيعية لا يلاحظ.**
- **الكسح**
  - **البحث في صناديق القمامة وإعادة التدوير للحصول على معلومات شخصية**

- **Trapdoor**
  - **illicit program left within a completed legitimate program**
  - **Permits unauthorized and unknown entry to the program**
- **Trojan horse**
  - **illegal instructions placed inside a legitimate program**
  - **Program does something useful and destructive at the same time**
- **Zapping**
  - **Software to bypass security systems**

- **Trapdoor**
  - **ترك برنامج غير مشروع ضمن برنامج شرعي مكتمل**
  - **تصاريح الدخول غير المصرح به وغير المعروف إلى البرنامج**
- **حصان طروادة**
  - **التعليمات غير القانونية الموضوعة داخل برنامج شرعي**
  - **يقوم البرنامج بعمل مفيد ومدمّر في نفس الوقت**
- **الانطلاق**
  - **برنامج لتجاوز أنظمة الأمان**

Security involving programs
الحماية المتعلقة بالبرامج

1- Information access problems مشاكل الوصول إلى المعلومات

Trapdoors: is secret undocumented entry point into a module.

Trapdoors هي نقطة غير موثقة الى النظام في برنامج ما.
توضع (تحشر) بعض الاحيان خلال رمز التطوير وذلك لعدة احتمالات:-

1. **To test the module.**
2. **To provide hooks by which to connect future modification or enhancements.**
3. **To allow access the event of future errors.**
4. **To can allow a programmer access into a program once it is placed into production.**

Causes of Trapdoors:

ان المبرمج عادة يزيل Trapdoors اثناء عملية التطويرلكنها ممكن ان توجد في البرامج المنتجة بسبب كون المبرمج :-

1. **Programmer forgets to remove them.**
2. **Programmer intentionally leaves them in the program to assist in the rest of testing.**
3. **Programmer intentionally leaves them in the program to assist in maintenance of the finished program.**
4. **Programmer intentionally leaves them in the program to assist in areola to have a covert means of access to the Ronnie after it becomes an accepted production program.**

- **ان الفقرة الاولى غير مقصودة اي خطأ أمني غير متعمد.**
- **ان الفقرة الثانية و الثالثة هما فقرتان لامنية النظام.**
- **ان الفقرة الرابعة هي الخطوة الاولى لمهاجمة النظام من قبل المبرمج.**

Trojan Horse: It performs a hidden function in addition to its stated function.
حصان طروادة: يؤدي وظيفة خفية بالإضافة إلى وظيفته المحددة.

- **Discovery**
  - **Difficult**
  - **Accidental**
  - **85% of computer crimes are never reported**
- **Prosecution**
  - **Legal representatives lack technical knowledge to understand the crime**

- **اكتشاف الجرائم**
  - **صعب**
  - **عرضي**
  - **85٪ من جرائم الكمبيوتر لم يتم الإبلاغ عنها مطلقًا**
- **الملاحقة القضائية**
  - **يفتقر الممثلون القانونيون إلى المعرفة الفنية لفهم الجريمة**

Pests:

- **Invade the computer system and cause something unexpected to occur.**
- **May interfere with function of PC**

الآفات:

- **غزو نظام الكمبيوتر وتسبب في حدوث شيء غير متوقع.**
- **قد تتداخل مع وظيفة جهاز الكمبيوتر**

Worms:

- **Rare**
- **Transfers over a network**
- **Plants as a separate file on the target's computer**

الديدان:

- **نادر**
- **تتنتقل عبر شبكة**
- **تغرس كملف منفصل على كمبيوتر الهدف**

Viruses

- **illicit instructions that pass themselves on to other programs**
  - **Benign**
  - **Damaging to computer**
- **Digital vandalism**

الفيروسات

- **التعليمات غير المشروعة التي تنقل نفسها إلى برامج أخرى**
  - **حميدة**
  - **إتلاف الكمبيوتر**
- **التخريب الرقمي**

Virus Transmission:

- **Networks**
- **Diskettes / CD**

Virus *Getting Infected*

- **Executing the virus program**
- **Booting from a diskette containing an infected boot sector including accidentally leaving a "non-system disk" in the floppy drive**
- **Downloading an infected file and executing it**
- **Opening an infected e-mail attachment**
- **By viewing e-mail in some versions of Microsoft Outlook**

الاصابة بالفيروس

- **تنفيذ برنامج الفيروسات**
- **التشغيل من قرص مرن يحتوي على قطاع تمهيد مصاب بما في ذلك ترك "قرص غير تابع للنظام" في محرك الأقراص المرنة بطريق الخطأ**
- **تنزيل ملف مصاب وتنفيذه**
- **فتح مرفق بريد إلكتروني مصاب**
- **من خلال عرض البريد الإلكتروني في بعض إصدارات Microsoft Outlook**

Virus *Precautions*

- **Be wary of free software from the Internet or friends**
- **Only install programs from diskettes in sealed packages**
- **Use virus-scanning software to check any file or document before loading it onto your hard disk**

الاحتياطات من الفيروسات

- **كن حذرًا من البرامج المجانية من الإنترنت أو الأصدقاء**
- **قم بتثبيت البرامج فقط من الأقراص المرنة في حزم مختومة**
- **استخدم برنامج فحص الفيروسات لفحص أي ملف أو مستند قبل تحميله على القرص الثابت**

Programs that leak Information برامج تسريب المعلومات

ان هذا النوع من البرامج يقوم بتسريب المعلومات وايصالها الى اشخاص لايحق لهم الحصول عليها . ان التسمية العامة لهذا النوع من المسارات الغير طبيعية للاتصالات هو covert channels

Covert channels: it is a hidden means for the program to communicate information.

القنوات السرية: هي وسيلة خفية للبرنامج لتوصيل المعلومات.

2- Service Problems مشاكل الخدمات

في هذا النوع من المشاكل فأن البرامج تصمم للتأثير على عمل النظام والخدمات التي يقدمها للمستخدمين الشرعيين مسببة توقف هذه الخدمات و فشلها و هذا الفشل الامني يسمى (Denial of service) .
يمكن تصنيف هذه المشاكل الى الانواع التالية:

1) Greedy Program:

It is a program that changes the sequence of importance for programs, for example, research that requires a very large time to be implemented, so it is placed with a minimum of importance to be implemented at night in order not to affect the work of the system and its services that it provides to users, the greedy

program will transfer its importance and make it the maximum importance and thus implement it during the morning Which leads to the system occupying it and preventing it from providing its services to more important businesses.

وهو برنامج يقوم بتغيير تسلسل الاهمية للبرامج مثلا ابحاث يتطلب تنفيذها وقت كبير جدا لذلك توضع بالحد الادنى من الاهمية ليتم تنفيذها ليلا وذلك لكي لاتؤثر على عمل النظام وخدماته التي يقدمها الى مستخدمين، يقوم ال greedy program بتحويل اهميتها وجعلها بالحد الاقصى من الاهمية وبالتالي تنفيذها اثناء الصباح والذي يؤدي الى اشغال النظام بها ومنعه من تقديم خدماته الى اعمال اكثر اهمية منها.

2) Viruses :

It is a program that can infect other programs by modifying them.

هي امتداد منطقي الى greedy program وهو برنامج يستطيع ان يصيب بالعدوى برامج اخرى عن طريق تحويرها او تغييرها ويتم هذا التحوير عن طريق اضافة نسخة منه (viruses) الى ذلك البرنامج.

3) Worms :

It is a group of viruses that use the network of machine management in computer systems and behaves freely on the network and to release its worms program. As with viruses, worms can establish themselves in most computer programs.

هي مجموعة من امدادات ال viruses تستخدم شبكة ادارة الالات في انظمة الحاسبات لتتصرف بحرية على الشبكة ولتحرر worms program لها وكما في ال viruses فان ال worms ممكن ان ترسخ نفسها في اغلب برامج الحاسوب.

3- Program development controls against program attacks

في هذا الموضوع سوف تتم مناقشة السيطرات التي تقودنا اثناء تطوير البرنامج لمساعدتنا في التأكد من نوعية وامانة المنتج

1) Modularity:

Modularization is the process of dividing a task into subtasks each module performs a separate independent part of the task.

ان modularity تعرض خدمات وفوائد تطوير البرامج بالاضافة الى الفوائد الامنية
ان وحدات البرنامج يجب ان تكون واسعة وكبيرة لاداء الواجبات المطلوبة فيها.
هناك عدة فوائد من كتابة البرنامج على شكل مكونات صغيرة متعددة:

There are several benefits of writing the program as multiple small components:

1. **Maintainability** **قابلية الصيانة**
2. **Understandability** **قابلية الفهم**
3. **Correct ability** **قابلية التصحيح**
4. **Testability** **قابلية الاختبار**
5. **Reusability** **اعادة الاستخدام**

2) Encapsulation : الاحاطة

Is the process of isolating a model from the negative effects of other models that interact, and this apparent and emerging isolation is within the design.

هي عملية عزل الموديل عن التأثيرات السلبية للموديلات الاخرى التي تتفاعل وهذا العزل الظاهر والناشئ يكون في اساس التصميم.

- **ان النموذج المصمم جيدا غير مرتبط مع نماذج اخرى اي تكون مستقلة ان هذه الخاصية تسمى Encapsulation في هذا الموديل عند التشغيل الابتدائي سوف يحاط بواسطة درع الذي يمنع الوصول الغير مرغوب فيه من الخارج.**
- **ان المشاركة تكون قليلة لذلك سوف يقل الاستخدام المتبادل ما بين النماذج قدر الامكان.**

- **ان تحييد التعامل المتبادل سوف يقلل من قنوات التغطية covert channels التي تنشأ لغرض خرق النظام.**

3) Information Hiding اخفاء المعلومات

It is a concealing the way that a module does its task.
هو إخفاء الطريقة التي تؤدي بها الوحدة مهمتها.
ان Information Hiding مرغوب فيه لان المبرمج لايستطيع القيام بأي تغيير خبيث على النموذج ما لم يعرف كيف يقوم النموذج بعمله.

ان الخصائص الثلاثة اعلاه تمثل ممارسات جيدة للامنية لانها تجعل النماذج مفهومة، محللة وموثوقة.

Independent Testing: الاختبار المستقل

- **ان الغرض من الاختبار هو لمعرفة مدى صحة البرنامج فالاختبار الذي يجد الاخطاء هو اكثر فائدة من الاختبار الذي لايجد شئ فمع بيان الاخطاء سوف نعرف ان الاختبار دقيق.**
- **ان من الضروري استخدام فريق مستقل ليقوم. بالاختبار.**
- **ان عملية الاختبار سوف تؤكد لنا بان النظام يعمل وفقا لما صمم من اجله.**
- **من الناحية الامنية فان الاختبار مهم ليكشف فيما اذا كان مبرمج المشروع قد اخفى برنامج في النظام كنقطة ضعف لخدمة اغراض خاصة به.**

Proofs of program correctness:

- **ان الغرض من الامنية هو التاكد من ان البرنامج يعطي نتائج محددة ومحسوبة بشكل صحيح.**
- **ان نتائج ال halting problem معوقة والتي توضح بانه لايوجد تقنية عامة لتحديد فيما اذا كان البرنامج اعتباطي وسيتوقف عند معالجة اي مدخلات عشوائية او اعتباطية arbitrary input .**

Program verification: it is a process can demonstrate formally the correctness of a certain specific program.
التحقق من البرنامج: إنها عملية يمكن أن تثبت رسميًا صحة برنامج معين.

Program correctness proofs are hindered by several factors:
هناك عدة عوامل تعرقل إثبات صحة البرنامج:

- **يعتمد على المبرمج او على قانونية نقل جمل البرنامج الى التطبيق المنطقي، ان عملية البرمجة عرضة للخطأ اثناء النقل.**
- **من الصعب معرفة صحة البرنامج من التأكيدات الاولية ومن المعنى الضمني للجمل.**
- **ان الحالة الحالية لبرنامج التحقق هي مطورة بشكل اقل جودة عن code production .**

4- Operating System Controls on Use of Programs

ضوابط نظام التشغيل على استخدام البرامج

تعتمد هذه السيطرات في عملها على انظمة التشغيل حيث يمكن السيطرة على جميع المبرمجين من خلالها وبذلك يمكن تحقيق امنية عالية على software .
في هذا الجزء سوف نوجز انواع الحماية التي يوفرها operating system ضد خدع و عيوب البرامج programs flaws .

Trusted Software:

Which mean code believed to be save both by doing functional correctness. What was designed to do and nothing more and by enforcing its correctness on program that run under it.

وهو ما يعني أن الكود يعتقد أنه يحفظ كليهما من خلال القيام بالصحة الوظيفية. ما تم تصميمه للقيام به ولا شيء أكثر وفرض صحته على البرنامج الذي يعمل تحته.

قد يكون operating system هو جزء من trusted software .

- **ان المطور الموثوق به سوف يصمم النموذج الصحيح.**
- **ان المبرمج الموثوق به سوف يكتب الجمل الضرورية فقط للبرنامج.**
- **ومن المهم الوثوق بعدم استخدام نظام التشغيل للوصول الغير مخول والذي يسيطر على الوصول لتنفيذ النماذج. مثال على ذلك ان نظام التشغيل ربما يستخدم لتحديد وصول بعض المستخدمين الى ملفات محددة ولا يسمح لهم بالوصول الى غيرها.**

Relying on good analysis and testing, the software has gained reliability and good reputation through several characteristics:

بالاعتماد على التحليل الجيد والاختبار ان ال software اكتسب الموثوقية والسمعة الجيدة من خلال عدة خصائص:

Characteristics of trusted software:

1- Functional correctness

ماذا يجب ان يعمل البرنامج وهل يعمل بشكل صحيح

2- Enforcement of integrity

يتم صيانة وحفظ صحة البيانات والتي تتعرض للايعازات الخاطئة او الغير مخولة (اي الصادرة من مستخدمين غير مخولين)

3- Limited privilege

ان البرنامج يسمح بالوصول الى بيانات سرية، ولكن هذا الوصول قليل ولايمكن لاي شخص امرار اي تخويل الى شخص او برنامج غير موثوق به

4- Appropriate security level

ان البرنامج قد فحص وصنف على درجة الموثوقية التي حصل عليها حسب نوع البيانات والمحيط الذي سوف يستخدم فيه.

Trusted Programs:

Programs that are used to carry out sensitive operations for users without allowing them direct access to sensitive and important data.

هي البرامج التي تستخدم لانجاز عمليات حساسة للمستخدمين بدون السماح لهم بالوصول المباشر للبيانات الحساسة والمهمة.

Mutual Suspicion:

It is the process of accessing a specific program by two users, one of whom may have manipulated or modified the program.

هي عملية الوصول الى برنامج معين من قبل مستخدمين قد يكون احدهما قد تلاعب او حورالبرنامج.

Was developed to describe the relationship between two programs.

Confinement:

It is a technique used by an operating system on a suspected program.

إنها تقنية يستخدمها نظام التشغيل على برنامج مشتبه به.
يعتمد ال confinement على مبدا مشابه للتصنيفات العسكرية للبيانات ، حيث تصنف الى سري او سري للغاية ، البرنامج الغير الموثوق يستطيع الوصول فقط الى فسح فارغة من المستويات مخصصة لهذا النوع من الوصول لتضليل المخترق.

Compartmented information: معلومات مجزأة

هي عملية مشابهة لل confinement حيث يتم تقسيم كل البيانات او البرامج الى مجاميع منفصلة بحيث يستطيع البرنامج الوصول الى البرامج او البيانات ضمن مجموعته فقط ، فاذا كان البرنامج غير موثوق به فان الوصول الى البيانات يكون محدد وبذلك يكون تأثيره محدد على مجموعته فقط . يستفاد من هذه الطريقة في فصل ال viruses وتحديد اخطارها ومنعها من الانتشار.

Access Log:

It is a listing of who accessed which computer objects when and for what amount of time.

ان access log هو ملف او جهاز مخصص لتسجيل الفعاليات التي تجري على النظام
مثال على ذلك عملية الدخول والخروج الى النظام وعملية الوصول او الوصول الغير مخول لملف معين ، تنفيذ البرامج او استخدام الاجهزة الملحقة الاخرى كالطابعة.

Chapter Two
Security

2.1 Introduction

In this chapter, we will introduce the notion of computer security, provide some basic definitions and discuss the features that a good security system should provide.

2.2 What is security?

In the broadest sense security can be defined as the protection of assets. There are three main aspects to security:
بالمعنى الواسع ، يمكن تعريف الأمن على أنه حماية الأصول. هناك ثلاثة جوانب رئيسية للأمن:

- **Prevention منع**
- **Detection كشف**
- **reaction رد فعل**

Consider security in the traditional sense – for example, securing your house against burglary. You may take steps to prevent a burglary such as locking the doors and windows and installing a burglar alarm. If a burglary did occur, you would be able to detect this because items would be missing and the burglar may have caused damage to your house while breaking in. You might react to the burglary by reporting it to the police, working out what had been stolen and making an insurance claim.
ضع في اعتبارك الأمان بالمعنى التقليدي - على سبيل المثال ، تأمين منزلك ضد السطو. يمكنك اتخاذ خطوات لمنع السطو مثل قفل الأبواب والنوافذ وتركيب جهاز إنذار ضد السرقة. في حالة حدوث عملية سطو ، ستكون قادرًا على اكتشاف ذلك لأن العناصر ستكون مفقودة وربما تسبب السارق في إلحاق

الضرر بمنزلك أثناء اقتحام المنزل. قد تتفاعل مع عملية السطو بإبلاغ الشرطة عنها ، واكتشاف ما تم سرقته وتقديم مطالبة التأمين.

2.2.1 How is information security different?

Although the definition of security given above still applies when we are talking about information, there are some major differences between traditional security and information security.

- **Information can be stolen – but you still have it.**
  If a physical item such as a car is stolen then the thief has possession of the car and you no longer have it. If a thief steals a file from your computer, he will probably make a copy of the file for himself and leave the original on your computer. Hence you still have the file but it has also been stolen.

- **Confidential information may be copied and sold – but the theft might not be detected.**
  If your car has been stolen it is not hard to detect the fact – the car is missing! However as mentioned above, a thief who steals computer files may leave the files on your computer and only copy them for himself. Nothing appears to have changed on your computer so you may not be aware that anything untoward has happened.

- **The criminal may be on the other side of the world.**
  If a thief steals your car you at least know where he was when he stole the car. However, it is possible to hack into computer systems remotely from anywhere in the world. This makes it very hard to know who is responsible for catching a computer

criminal. Is it the police in the country where the computer is, or the police in the country where the criminal is?

Although there is no single definition of computer security, we can say that:

Computer security deals with the prevention and detection of unauthorized actions by users of a computer system.

This subject deals with the theory of computer security. You should be aware that unfortunately things that are great in theory do not always work in practice. As Schneier says in *Secrets and Lies*:

Theory works best in ideal conditions and laboratory settings. We can design idealized operating systems that are provably secure, but we can't actually build them to work securely in the real world. The real world involves design trade-offs, unseen variables and imperfect implementations.

Schneier kept a log of 'security events' for the first week of March 2000. He recorded approximately 100 events during this time including hackers launching denial-of-service attacks, leakage of personal data from supposedly secure websites, email worms and viruses, and websites being defaced. Most of these attacks and vulnerabilities were the result of the perpetrator bypassing the security mechanism, or exploiting a weakness in the system such as an overflowing buffer.

احتفظ Schneier بسجل لـ "الأحداث الأمنية" للأسبوع الأول من شهر مارس 2000. وسجل ما يقرب من 100 حدث خلال هذا الوقت بما في ذلك قراصنة شنوا هجمات رفض الخدمة ، وتسريب البيانات الشخصية من مواقع الويب التي يُفترض أنها آمنة ، والفيروسات المتنقلة والفيروسات عبر

البريد الإلكتروني ، و يتم تشويه المواقع الإلكترونية. كانت معظم هذه الهجمات ونقاط الضعف ناتجة عن تجاوز الجاني للآلية الأمنية ، أو استغلال نقطة ضعف في النظام مثل فائض المخزن المؤقت.

2.3 Features of a security system

In order to prevent and detect unauthorized actions by its users a good security system should provide (some of) the following features:

- **confidentiality**
- **integrity**
- **availability**
- **non-repudiation**
- **authentication**
- **access controls**
- **accountability**

We will look at each of these features in turn. Note that different authors on computer security disagree as to which of these features are the most important. It will depend on the main purpose of the system – is confidentiality paramount or is the prevention of denial of service attacks more important? This will depend on the system in question. For example a computer system which holds personal medical records must certainly provide access controls in order to ensure that personal information does not fall into the wrong hands, and integrity to ensure that the information stored is accurate. Other features such as non-repudiation and availability may not be so important in this case. On the other hand, it is essential for a computer system which transfers money electronically to guarantee

non-repudiation and accountability in order to prevent and/or detect dishonest transactions occurring.

In this context, the term *unauthorized* implies not only malicious or criminal, but could also be accidental. For example, a breach of confidentiality arises maliciously if a spy deliberately hacks into a computer and looks at confidential material stored there. It happens accidentally if the material is left out on a desk and is seen by the office cleaner.

2.3.1 Confidentiality

***Confidentiality* is the prevention of unauthorized disclosure of information. In other words, confidentiality means keeping information private or safe. Confidentiality may be important for military, business or personal reasons. Confidentiality may also be known as *privacy* or *secrecy*.**

السرية هي منع الكشف غير المصرح به عن المعلومات.
بمعنى آخر ، السرية تعني الحفاظ على خصوصية المعلومات أو الحفاظ عليها. قد تكون السرية مهمة لأسباب عسكرية أو تجارية أو شخصية. قد تُعرف السرية أيضًا باسم الخصوصية أو السرية.

2.3.2 Integrity

***Integrity* is the prevention of unauthorized writing or modification of information.**
Integrity in a computer system means that there is an external consistency in the system – everything is as it is expected to be. *Data integrity* means that the data stored on the computer is the same as what is intended.

النزاهة هي منع الكتابة غير المصرح بها أو تعديل المعلومات.

تعني النزاهة في نظام الكمبيوتر أن هناك اتساقًا خارجيًا في النظام - كل شيء كما هو متوقع. سلامة البيانات تعني أن البيانات المخزنة على الكمبيوتر هي نفسها المقصودة.

2.3.3 Availability

Availability **is the prevention of unauthorized with-holding of information.**
Information should be accessible and usable upon appropriate demand by an authorized user. *Denial of service* attacks are a common form of attack against computer systems whereby authorized users are denied access to the computer system. Such an attack may be orchestrated by the attacker flooding the system with requests until it cannot keep up and crashes. Authorized users are unable to access the system. Consider the damage that such an attack may cause to an electronic commerce site such as an internet shop.

التوفر هو منع الاحتفاظ غير المصرح به للمعلومات.
يجب أن تكون المعلومات قابلة للوصول ويمكن استخدامها عند الطلب المناسب من قبل مستخدم مصرح له. هجمات رفض الخدمة هي شكل شائع للهجوم على أنظمة الكمبيوتر حيث يُحرم المستخدمون المصرح لهم من الوصول إلى نظام الكمبيوتر. قد يتم تدبير مثل هذا الهجوم بواسطة المهاجم الذي يغمر النظام بالطلبات حتى يتعذر عليه مواكبة الأمر وتعطله. المستخدمين المصرح لهم غير قادرين على الوصول إلى النظام. ضع في اعتبارك الضرر الذي قد يسببه مثل هذا الهجوم لموقع التجارة الإلكترونية مثل متجر الإنترنت.

2.3.4 Non-repudiation

Non-repudiation **is the prevention of either the sender or the receiver denying a transmitted message.**

عدم التنصل هو منع إما المرسل أو المتلقي إنكار رسالة المرسلة.

A computer security system must be able to prove that certain messages were sent and received, who sent the message, who received the message and perhaps what the message said. For

example, suppose a dishonest trader sends an electronic message to a stock broker telling him to buy £2,000 worth of shares in CryptoCom. The next day the price of CryptoCom shares soars. The trader now pretends that his original message said to buy £20,000 worth of shares. Conversely if the share price fell he might pretend that the original message said to buy shares in KryptoCom instead. Non-repudiation means that the trader is not able to deny his original message.
Non-repudiation is often implemented by using *digital signatures.*

يجب أن يكون نظام أمان الكمبيوتر قادرًا على إثبات إرسال رسائل معينة واستلامها ، ومن أرسل الرسالة ، ومن تلقى الرسالة وربما ما ورد في الرسالة. على سبيل المثال ، افترض أن متداولًا مخادعًا أرسل رسالة إلكترونية إلى سمسار الأوراق المالية يطلب منه شراء ما قيمته 2000 جنيه إسترليني من الأسهم في .CryptoCom في اليوم التالي ، ارتفعت أسعار أسهم .CryptoCom يتظاهر التاجر الآن أن رسالته الأصلية قالت إنه اشترى ما قيمته 20 ألف جنيه إسترليني من الأسهم. على العكس من ذلك ، إذا انخفض سعر السهم ، فقد يتظاهر بأن الرسالة الأصلية تقول شراء أسهم في KryptoCom بدلاً من ذلك. عدم التنصل يعني أن التاجر غير قادر على إنكار رسالته الأصلية. غالبًا ما يتم تنفيذ عدم التنصل باستخدام التوقيعات الرقمية.

2.3.5 Authentication

***Authentication* is proving a claim – usually that you are who you say you are, where you say you are, at the time that you say it is.**
Authentication may be obtained by the provision of a password or by a scan of your retina for example.
المصادقة تثبت ادعاءً - عادةً ما تكون أنت من تقول أنت ، أينما تقول أنت ، في الوقت الذي تقوله فيه. يمكن الحصول على المصادقة من خلال توفير كلمة مرور أو عن طريق فحص شبكية العين على سبيل المثال.

2.3.6 Access controls

***Access controls* provide the limitation and control of access to authorized users through identification and authentication.**
A system needs to be able to identify and authenticate users for access to data, applications and hardware. In a large system there

may be a complex structure determining which users and applications have access to which objects.

توفر ضوابط الوصول الحد من الوصول إلى المستخدمين المصرح لهم والتحكم فيه من خلال تحديد الهوية والمصادقة.

يحتاج النظام إلى أن يكون قادرًا على تحديد المستخدمين والمصادقة عليهم للوصول إلى البيانات والتطبيقات والأجهزة. في نظام كبير ، قد يكون هناك هيكل معقد يحدد المستخدمين والتطبيقات التي يمكنها الوصول إلى أي كائنات.

2.3.7 Accountability

Accountability **means that the system is able to provide audit trails of all transactions.**

The system managers are accountable to scrutiny from outside the system and must be able to provide details of all transactions that have occurred. Audit trails must be selectively kept (and protected to maintain their integrity) so that actions affecting security can be traced back to the responsible party.

تعني المساءلة أن النظام قادر على توفير مسارات تدقيق لجميع المعاملات.

يتحمل مديرو النظام مسؤولية التدقيق من خارج النظام ويجب أن يكونوا قادرين على تقديم تفاصيل جميع المعاملات التي تمت. يجب الاحتفاظ بمسارات التدقيق بشكل انتقائي (وحمايتها للحفاظ على سلامتها) بحيث يمكن تتبع الإجراءات التي تؤثر على الأمن إلى الطرف المسؤول.

Learning activity نشاط التعلم

Consider the following scenario and think about the questions at the end.

A student suspects there is a vulnerability on a system in a university public access laboratory. She tests this by trying to exploit the vulnerability. She succeeds, and obtains privileges that she would not normally have. She reports both the hole and her exploiting it to

the system staff, who in turn report it to the manager of the laboratory. The manager files charges of breaking into the computing system against the student.

تأمل السيناريو التالي وفكر في الأسئلة في النهاية.
يشتبه طالب في وجود ثغرة أمنية في نظام في مختبر وصول عام بالجامعة. إنها تختبر ذلك بمحاولة استغلال الثغرة الأمنية. لقد نجحت ، وحصلت على امتيازات لم تكن تتمتع بها عادة. تقوم بالإبلاغ عن الحفرة واستغلالها لموظفي النظام ، الذين يقومون بدورهم بإبلاغ مدير المختبر بها. يوجه المدير اتهامات لاقتحام نظام الحوسبة ضد الطالب.

The student has to appear before the Student Judicial Authority – she is in trouble!

يجب على الطالبة المثول أمام السلطة القضائية الطلابية - إنها في ورطة!

1. **Did the student act ethically by testing the system for the security hole before reporting it?**
   1. هل تصرف الطالب بشكل أخلاقي من خلال اختبار النظام للثغرة الأمنية قبل الإبلاغ عنها؟
2. **Did the manager act ethically by filing charges against the student?**
   2. هل تصرف المدير بشكل أخلاقي بتوجيه التهم ضد الطالب؟
3. **The manager told the system staff not to bother fixing the hole, because the action taken by the SJA would deter any further break-ins through the hole. Was the manager's action appropriate?**

3. قال المدير لموظفي النظام ألا يكلفوا عناء إصلاح الثقب ، لأن الإجراء الذي اتخذته SJA من شأنه أن يردع أي عمليات اقتحام أخرى عبر الفتحة. هل كان تصرف المدير مناسبًا؟

2.4 Security attacks

Information transmitted over electronic lines is vulnerable to passive wiretapping, which threatens secrecy, and to active wiretapping, which threatens authenticity (see Figure 1). Passive wiretapping (eavesdropping) refers to the interception of messages, usually

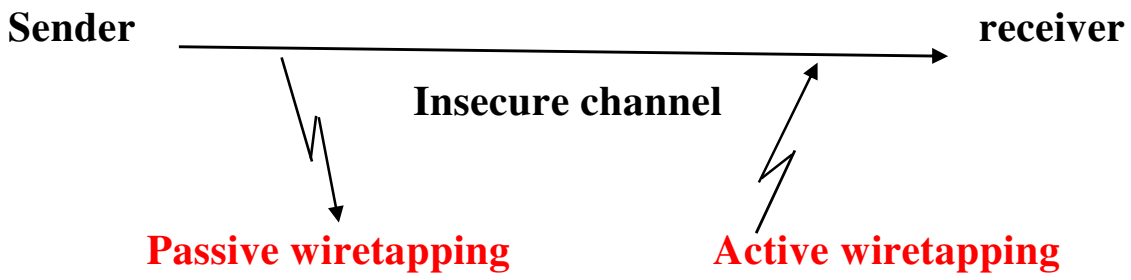
without detection. Although it is normally used to disclose message contents, in computer networks it can also be used to monitor traffic flow through the network to determine who is communicating with whom. Protection against disclosure of message contents is provided by enciphering transformations and by the cryptographic techniques. Protection against traffic flow analysis is provided by controlling the endpoints of encryption.

التنصت السلبي (التنصت) يشير إلى اعتراض الرسائل ، عادة بدون اكتشاف.

Active wiretapping (tampering) refers to deliberate modifications made to the message stream. This can be for the purpose of making arbitrary changes to a message, or of replacing data in a message with replays of data from earlier messages (e.g., replacing the amount field of a transaction "CREDIT SMITH'S ACCOUNT WITH $10" with the amount field of an earlier transaction "CREDIT JONES'S ACCOUNT WITH $5000"). It can be for the purpose of injecting false messages, injecting replays of previous messages (e.g., to repeat a credit transaction), or deleting messages (e.g., to prevent a transaction "DEDUCT $1000 FROM SMITH'S ACCOUNT"). Encryption protects against message modification and injection of false messages by making it infeasible for an opponent to create ciphertext that deciphers into meaningful plaintext. Note, however, that whereas it can be used to detect message modification, it cannot prevent it.

يشير التنصت النشط (التلاعب) إلى التعديلات المتعمدة التي تم إجراؤها على تدفق الرسائل.

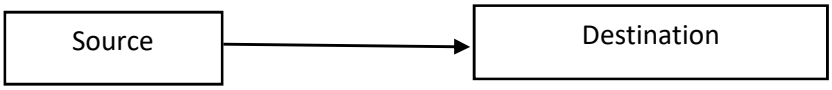
FIGURE 1. Threats to secure communication.



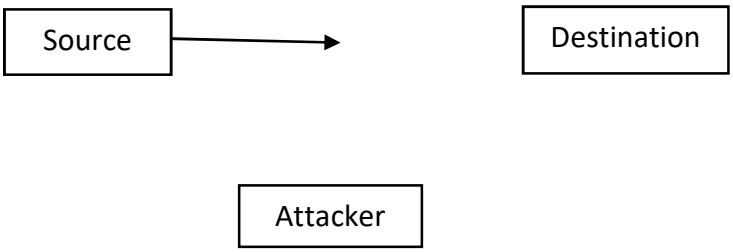
There are a number of ways in which an attacker can disrupt communications.

هناك عدد من الطرق التي يمكن للمهاجم من خلالها تعطيل الاتصالات.

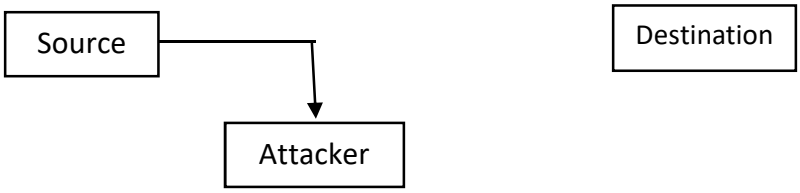
Normally, information goes from the source to the destination.



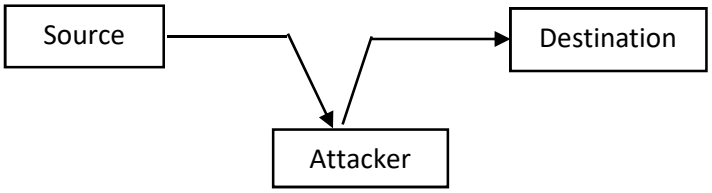
1. Communication is *interrupted* if the attacker does not allow the information to reach the destination.



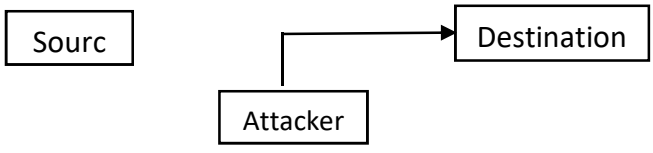
2. **Communication is *intercepted* if the attacker interrupts the communication and receives the source information.**



3. ***Modification* occurs when the attacker intercepts the communication, alters it in some way, and then sends it on to the destination. The attacker intends to deceive the destination into thinking that the modified communication has come directly from the source. This is also known as a *Man-in-the-middle attack*.**



4. **An attacker may also make up a communication and send it to the destination pretending that it has come from the source. This is called *fabrication*.**



2.5 Important Definitions for Security تعريفات مهمة

Computer security: refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs, and data to assure that organizational assets and individual privacy are protected.

أمن الكمبيوتر: يشير إلى الضمانات التكنولوجية والإجراءات الإدارية التي يمكن تطبيقها على أجهزة الكمبيوتر والبرامج والبيانات لضمان حماية الأصول التنظيمية والخصوصية الفردية.

Data Security: is the protection of data against accidental or intentional destruction, disclosure, or modification.

أمن البيانات: هو حماية البيانات من التدمير أو الإفشاء أو التعديل العرضي أو المتعمد.

Or Data Security: refers to protection of data against accidental or intentional disclosure to unauthorized persons, or unauthorized modifications or destructions.

أمن البيانات: يشير إلى حماية البيانات من الإفشاء العرضي أو المتعمد للأشخاص غير المصرح لهم ، أو التعديلات أو الإتلاف غير المصرح به.

Privacy: refers to the rights of individuals and organizations to determine for themselves when, how and to what extent information about them is to be transmitted to others.

الخصوصية: تشير إلى حقوق الأفراد والمنظمات في أن يقرروا بأنفسهم متى وكيف وإلى أي مدى يتم نقل المعلومات المتعلقة بهم إلى الآخرين.

Or Privacy: is a concept which applies to an individual. It is the right of an individual to decide what information(s) he wishes to share with other and also what information(s) he is willing to accept from others.

او الخصوصية: مفهوم ينطبق على الفرد. من حق الفرد أن يقرر ما هي المعلومات التي يرغب في مشاركتها مع الآخرين وأيضًا المعلومات التي يرغب في قبولها من الآخرين.

Integrity: it refer not only to the correctness of data (message or file) but its origin, its validity or it degree of authority.

النزاهة: لا تشير فقط إلى صحة البيانات (رسالة أو ملف) ولكن أصلها أو صحتها أو درجة سلطتها.

Data integrity: exists when data does not differ from its source documents and has not been accidentally or maliciously altered, disclosed, or destroyed.

تكامل البيانات: توجد عندما لا تختلف البيانات عن المستندات المصدر الخاصة بها ولم يتم تغييرها أو الكشف عنها أو إتلافها عن طريق الخطأ أو بشكل متعمد.

Or Data Integrity: it is the property that data has not been altered or destroyed in an unauthorized manner.

سلامة وتكامل البيانات: هي خاصية عدم تغيير البيانات أو إتلافها بطريقة غير مصرح بها.

System Integrity: is the ability of a system to operate according to specifications even in the face of deliberate attempts to make it behave differently.

تكامل النظام: هو قدرة النظام على العمل وفق المواصفات حتى في مواجهة المحاولات المتعمدة لجعله يتصرف بشكل مختلف.

Confidentiality: is a concept which applies to data. It is the status accorded to data which has been agreed upon between the person or organization furnishing the data and the organization receiving it and which describes the degree of protection to be provided.

السرية: مفهوم ينطبق على البيانات. إنها الحالة الممنوحة للبيانات التي تم الاتفاق عليها بين الشخص أو المنظمة التي تقدم البيانات والمؤسسة التي تتلقاها والتي تصف درجة الحماية التي يتعين توفيرها.

Or Confidentiality: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

او السرية: الخاصية التي لا يتم توفير المعلومات أو الكشف عنها لأفراد أو كيانات أو عمليات غير مصرح بها.

Identification: the identification of user, terminal, file, program, or other object is the unique name or number assigned to that object. It is only claim of identity.

التعريف: تعريف المستخدم أو الجهاز أو الملف أو البرنامج أو أي كائن آخر هو الاسم الفريد أو الرقم المخصص لذلك الكائن. إنه فقط ادعاء الهوية.

Or Identification: the process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to EDP system.

أو تحديد الهوية: العملية التي تتيح ، بشكل عام ، عن طريق استخدام أسماء فريدة يمكن قراءتها آليًا ، التعرف على المستخدمين أو الموارد على أنها مطابقة لتلك الموصوفة سابقًا لنظام EDP.

Authentication: authentication verifies that a person (object) is who he or she (it) claims to be.

المصادقة: تتحقق المصادقة من أن الشخص (الشيء) هو من يدعي أنه (هو).

Authentication:

1) **The act of identifying or verifying the eligibility of station, originator, or individual to access specific categories of information.**
2) **A measure designed to provide protection against fraudulent transmissions by establishing the validity of transmission, message, station, or originator.**

المصادقة:

1) عملية تحديد أو التحقق من أهلية المحطة أو المنشئ أو الفرد للوصول إلى فئات معينة من المعلومات.
2) إجراء مصمم لتوفير الحماية ضد عمليات الإرسال الاحتيالية من خلال إثبات صحة الإرسال أو الرسالة أو المحطة أو المنشئ.

Authentication: the granting to a user, a program, or a process the right of access.

المصادقة: منح مستخدم أو برنامج أو عملية حق الوصول.

Or Authentication: is whether a person or object is legitimately entitled to a protected resource.

أو المصادقة: هي ما إذا كان الشخص أو الشيء مؤهلًا شرعيًا لمصدر محمي.

Chapter Three

Cryptography and data Security

3.1 *CRYPTOGRAPHY*

Cryptography is the science and study of secret writing. A cipher is a secret method of writing, whereby plaintext (or cleartext) is transformed into cipher text (sometimes called a cryptogram). The process of transforming plaintext into cipher text is called encipherment or encryption; the reverse process of transforming ciphertext into plaintext is called decipherment or decryption. Both encipherment and decipherment are controlled by a cryptographic key or keys. (See Figure 1).

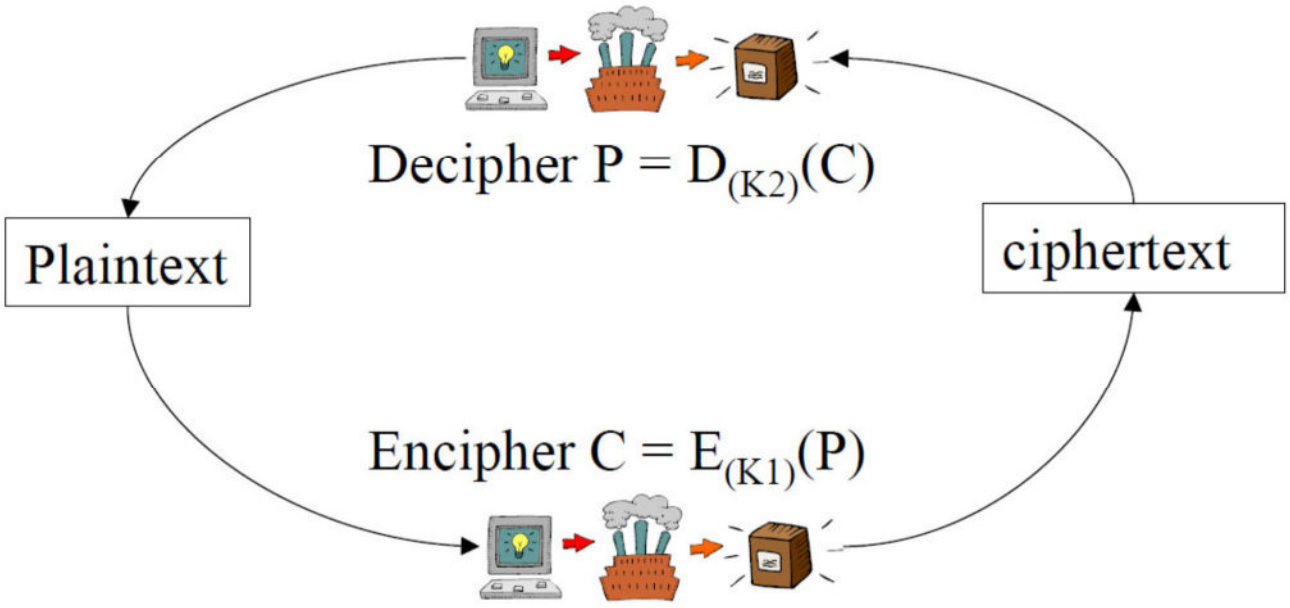


Figure (3.1)

3.2 ***CRYPTOGRAPHIC SYSTEMS***

This section describes the general requirements of all cryptographic systems, the specific properties of public-key encryption, and digital signatures.

A cryptographic system (or cryptosystem for short) has five components:

1. **A plaintext message space, M or P.**
2. **A ciphertext message space, C.**
3. **A key space, .K.**
4. **A family of enciphering transformations, E_K: M ⟹ C**
5. **A family of deciphering transformations, D_K: C ⟹ M**

Cryptosystems must satisfy three general requirements:

1. **The enciphering and deciphering transformations must be efficient for all keys.**

1. يجب أن تكون خوارزميات التشفير وفك التشفير فعالة لجميع المفاتيح.

2. **The system must be easy to use.**

2. يجب أن يكون النظام سهل الاستخدام.

3. **The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithms E or D.**

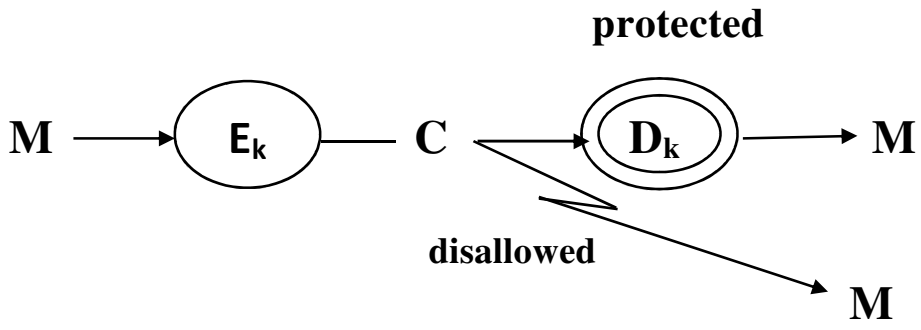
3. يجب أن يعتمد أمن النظام على سرية المفاتيح فقط وليس على سرية الخوارزميات E أو D.

Secrecy requirements

1. **It should be computationally infeasible for a cryptanalyst to systematically determine the deciphering transformation D_k from intercepted ciphertext *C,* even if the corresponding plaintext M is known.**

2. **It should be computationally infeasible for a cryptanalyst to systematically determine plaintext M from intercepted ciphertext C.**

FIGURE 3.2 Secrecy.

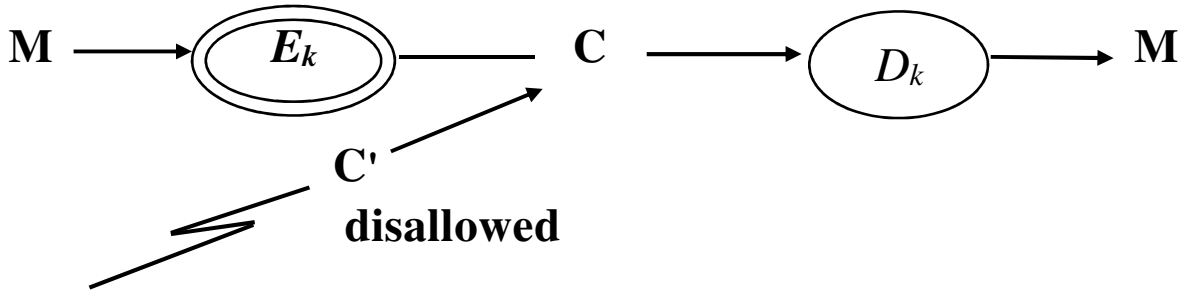


Authenticity requirements

1. **It should be computationally infeasible for a cryptanalyst to systematically determine the enciphering transformation E_k given *C,* even if the corresponding plaintext M is known.**

2. **It should be computationally infeasible for a cryptanalyst to systematically find ciphertext C' such that $D_K(C')$ is valid plaintext in the set M.**

FIGURE 3.3 Authenticity



3.3 *CRYPTANALYSIS:*

Cryptanalysis is the science of recovering the plaintext of a message without access to the key. Successful cryptanalysis may recover the plaintext or the key. It also may find weaknesses in a cryptosystem that eventually lead to the previous results. (The loss of a key through non cryptanalytic means is called a compromise.)

تحليل الشفرات هو علم استعادة النص الصريح للرسالة دون الوصول إلى المفتاح. قد يؤدي تحليل الشفرات الناجح إلى استعادة النص العادي أو المفتاح. قد تجد أيضًا نقاط ضعف في نظام تشفير تؤدي في النهاية إلى النتائج السابقة. (يُطلق على فقدان مفتاح من خلال وسائل غير تحليلية حلاً وسطًا).

There are four general types of cryptanalytic attacks. Of course, each of them assumes that the cryptanalyst has complete knowledge of the encryption algorithm used:

هناك أربعة أنواع عامة من هجمات تحليل الشفرات. بالطبع ، يفترض كل منهم أن محلل التشفير لديه معرفة كاملة بخوارزمية التشفير المستخدمة:

1. Ciphertext-only attack. The cryptanalyst has the ciphertext of several messages, all of which have been encrypted using the same encryption algorithm. The cryptanalyst's job is to recover the plaintext of as many messages as possible, or better yet to deduce

the key (or keys) used to encrypt the messages, in order to decrypt other messages encrypted with the same keys.
Given: $C_1 = E_k(P_1)$, $C_2 = E_k(P_2)$,...$Ci = E_k(P_i)$
Deduce: Either P_1, P_2,...P_i; k; or an algorithm to infer P_{i+1} from $C_{i+1} = E_k(P_{i+1})$

1. هجوم نص مشفر فقط. يمتلك محلل التشفير على نص مشفر لعدة رسائل ، تم تشفيرها جميعًا باستخدام نفس خوارزمية التشفير. تتمثل مهمة محلل التشفير في استعادة النص العادي لأكبر عدد ممكن من الرسائل ، أو من الأفضل استنتاج المفتاح (أو المفاتيح) المستخدمة لتشفير الرسائل ، من أجل فك تشفير الرسائل الأخرى المشفرة بنفس المفاتيح.
المعطى: $C_1 = E_k(P_1)$ ، $C_2 = E_k(P_2)$ ...، $C_i = E_k(P_i)$
استنتج: إما P_1، P_2 ...، P_i ؛ k؛ أو خوارزمية لاستنتاج P_{i+1} من $C_{i+1} = E_k(P_{i+1})$

2. Known-plaintext attack. The cryptanalyst has access not only to the ciphertext of several messages, but also to the plaintext of those messages. His job is to deduce the key (or keys) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key (or keys).
Given: P_1, $C_1 = E_k(P_1)$, P_2, $C_2 = E_k(P_2)$,...P_i, $C_i = E_k(P_i)$
Deduce: Either k, or an algorithm to infer P_{i+1} from $C_{i+1} = E_k(P_{i+1})$

2. هجوم نص عادي معروف. يمكن لمحلل التشفير الوصول ليس فقط إلى النص المشفر للعديد من الرسائل ، ولكن أيضًا إلى النص العادي لتلك الرسائل. وظيفته هي استنتاج المفتاح (أو المفاتيح) المستخدمة لتشفير الرسائل أو خوارزمية لفك تشفير أي رسائل جديدة مشفرة بنفس المفتاح (أو المفاتيح).
المعطى: P_1 ، $C_1 = E_k(P_1)$، P_2، $C_2 = E_k(P_2)$ ... P_i، $C_i = E_k(P_i)$
استنتج: إما k ، أو خوارزمية لاستنتاج P_{i+1} من $C_{i+1} = E_k(P_{i+1})$

3. Chosen-plaintext attack. The cryptanalyst not only has access to the ciphertext and associated plaintext for several messages, but

he also chooses the plaintext that gets encrypted. This is more powerful than a known-plaintext attack, because the cryptanalyst can choose specific plaintext blocks to encrypt, ones that might yield more information about the key. His job is to deduce the key (or keys) used to encrypt the messages or an algorithm to decrypt any new messages encrypted with the same key (or keys).
Given: P_1, $C_1 = E_k(P_1)$, P_2, $C_2 = E_k(P_2)$,...P_i, $C_i = E_k(P_i)$, where the cryptanalyst gets to choose P_1, P_2,...P_i
Deduce: Either k, or an algorithm to infer P_{i+1} from $C_{i+1} = E_k(P_{i+1})$

3. هجوم بنص عادي مختار. لا يمتلك محلل التشفير حق الوصول إلى النص المشفر والنص العادي المرتبط به للعديد من الرسائل فحسب ، بل إنه يختار أيضًا النص العادي الذي يتم تشفيره. هذا أقوى من هجوم نص عادي معروف ، لأن محلل التشفير يمكنه اختيار كتل نص عادي معينة لتشفيرها ، تلك التي قد توفر مزيدًا من المعلومات حول المفتاح. وظيفته هي استنتاج المفتاح (أو المفاتيح) المستخدمة لتشفير الرسائل أو خوارزمية لفك تشفير أي رسائل جديدة مشفرة بنفس المفتاح (أو المفاتيح).
معطى: P_1 ، $C_1 = E_k(P_1)$ ، P_2 ،$C_2 = E_k(P_2)$ ،... P_i ، $C_i = E_k(P_i)$، حيث يختار محلل التشفيرP_1 ، P_2 ،... P_i
استنتج: إما k ، أو خوارزمية لاستنتاج P_{i+1} من $C_{i+1} = E_k(P_{i+1})$

4. Adaptive-chosen-plaintext attack. This is a special case of a chosen-plaintext attack. Not only can the cryptanalyst choose the plaintext that is encrypted, but he can also modify his choice based on the results of previous encryption. In a chosen-plaintext attack, a cryptanalyst might just be able to choose one large block of plaintext to be encrypted; in an adaptive-chosen plaintext attack he can choose a smaller block of plaintext and then choose another based on the results of the first, and so forth.

4.الهجوم التكيفي بنص عادي مختار. هذه حالة خاصة لهجوم نص عادي مختار. لا يمكن لمحلل التشفير اختيار النص العادي المشفر فحسب ، بل يمكنه أيضًا تعديل اختياره بناءً على نتائج التشفير

السابق. في هجوم مختار بنص عادي ، قد يكون محلل الشفرات قادرًا فقط على اختيار كتلة واحدة كبيرة من نص عادي ليتم تشفيرها ؛ في هجوم نص عادي تم اختياره بشكل تكيفي ، يمكنه اختيار كتلة أصغر من النص العادي ثم اختيار آخر بناءً على نتائج الأول ، وهكذا دواليك.

There are at least three other types of cryptanalytic attack.

هناك ثلاثة أنواع أخرى على الأقل من هجمات تحليل الشفرات. ، لا يفترض كل منهم أن محلل التشفير لديه معرفة بخوارزمية التشفير المستخدمة:

5. Chosen-ciphertext attack. The cryptanalyst can choose different ciphertexts to be decrypted and has access to the decrypted plaintext. For example, the cryptanalyst has access to a tamperproof box that does automatic decryption. His job is to deduce the key.

Given: C_1, $P_1 = D_k(C_1)$, C_2, $P_2 = D_k(C_2)$,...C_i, $P_i = D_k(C_i)$

Deduce: *k*

This attack is primarily applicable to public-key algorithm. A chosen-ciphertext attack is sometimes effective against a symmetric algorithm as well. (Sometimes a chosen-plaintext attack and a chosen-ciphertext attack are together known as a chosen-text attack.)

5. هجوم النص المشفر المختار. يمكن لمحلل التشفير اختيار نصوص مشفرة مختلفة لفك تشفيرها والوصول إلى النص العادي الذي تم فك تشفيره. على سبيل المثال ، يمكن لمحلل التشفير الوصول إلى صندوق مقاوم للعبث يقوم بفك التشفير تلقائيًا. وظيفته هي استنتاج المفتاح.

المعطى: C_1 ، $P_1 = D_k(C_1)$ ،C_2 ،$P_2 = D_k(C_2)$ ...، C_i ، $P_i = D_k(C_i)$

استنتج: k

هذا الهجوم قابل للتطبيق بشكل أساسي على خوارزمية المفتاح العام. أحيانًا يكون هجوم النص المشفر المختار فعالًا ضد الخوارزمية المتماثلة أيضًا. (في بعض الأحيان يُعرف هجوم النص العادي المختار وهجوم النص المشفر المختار معًا باسم هجوم النص المختار).

6. **Chosen-key attack. This attack doesn't mean that the cryptanalyst can choose the key; it means that he has some knowledge about the relationship between different keys. It's strange and obscure, not very practical.**

6. هجوم المفتاح المختار. هذا الهجوم لا يعني أن محلل الشفرات يمكنه اختيار المفتاح ؛ هذا يعني أن لديه بعض المعرفة حول العلاقة بين المفاتيح المختلفة. إنه أمر غريب وغامض ، وليس عمليًا جدًا.

7. **Rubber-hose cryptanalysis. The cryptanalyst threatens, blackmails, or tortures someone until they give him the key. Bribery is sometimes referred to as a purchase-key attack. These are all very powerful attacks and often the best way to break an algorithm.**

7. تحليل الشفرات بالخرطوم المطاطي. يقوم محلل الشفرات بتهديد أو ابتزاز أو تعذيب شخص ما حتى يعطيه المفتاح. يشار أحيانًا إلى الرشوة على أنها هجوم شراء مفتاح. هذه كلها هجمات قوية جدًا وغالبًا ما تكون أفضل طريقة لكسر الخوارزمية.

3.4 STEGANOGRAPHY:

Steganography serves to hide secret messages in other messages, such that the secret's very existence is concealed. Generally the sender writes an innocuous message and then conceals a secret message on the same piece of paper. Historical tricks include invisible inks, tiny pin punctures on selected characters, minute differences between handwritten characters, pencil marks on typewritten characters, grilles which cover most of the message except for a few characters, and so on.

More recently, people are hiding secret messages in graphic images. Replace the least significant bit of each byte of the image

with the bits of the message. The graphical image won't change appreciably—most graphics standards specify more gradations of color than the human eye can notice—and the message can be stripped out at the receiving end. You can store a 64-kilobyte message in a 1024 ×1024 grey-scale picture this way. Several public-domain programs do this sort of thing.

Peter Wayner's mimic functions obfuscate messages. These functions modify a message so that its statistical profile resembles that of something else: the classifieds section of The New York Times, a play by Shakespeare, or a newsgroup on the Internet [1584,1585]. This type of steganography won't fool a person, but it might fool some big computers scanning the Internet for interesting messages.

3.4 إخفاء المعلومات

يعمل Steganography على إخفاء الرسائل السرية في الرسائل الأخرى ، بحيث يتم إخفاء وجود السر ذاته. بشكل عام ، يكتب المرسل رسالة غير ضارة ثم يخفي رسالة سرية على نفس قطعة الورق. تشمل الحيل التاريخية أحبارًا غير مرئية ، وثقوبًا صغيرة على الأحرف المحددة ، واختلافات دقيقة بين الأحرف المكتوبة بخط اليد ، وعلامات قلم الرصاص على الأحرف المكتوبة على الآلة الكاتبة ، والشبكات التي تغطي معظم الرسالة باستثناء عدد قليل من الأحرف ، وما إلى ذلك.
في الآونة الأخيرة ، يخفي الناس رسائل سرية في الصور الرسومية. استبدل الجزء الأقل دلالة من كل بايت من الصورة بقطع الرسالة. لن تتغير الصورة الرسومية بشكل ملحوظ - تحدد معظم معايير الرسومات تدرجات لونية أكثر مما يمكن للعين البشرية أن تلاحظه - ويمكن تجريد الرسالة من الطرف المستقبل. يمكنك تخزين رسالة 64 كيلوبايت في صورة 1024 × 1024 بمقياس رمادي بهذه الطريقة. العديد من برامج المجال العام تفعل هذا النوع من الأشياء.

تعمل وظائف محاكاة بيتر واينر على تعتيم الرسائل. تقوم هذه الوظائف بتعديل رسالة بحيث يكون ملفها الإحصائي مشابهًا لشيء آخر: قسم الإعلانات المبوبة في صحيفة نيويورك تايمز ، أو مسرحية

لشكسبير ، أو مجموعة أخبار على الإنترنت [1585،1584]. هذا النوع من إخفاء المعلومات لن يخدع أي شخص ، ولكنه قد يخدع بعض أجهزة الكمبيوتر الكبيرة التي تقوم بمسح الإنترنت بحثًا عن رسائل شيقة.

Cryptography and Network Security

by

Haifaa Jassim

from

Xiang-Yang Li

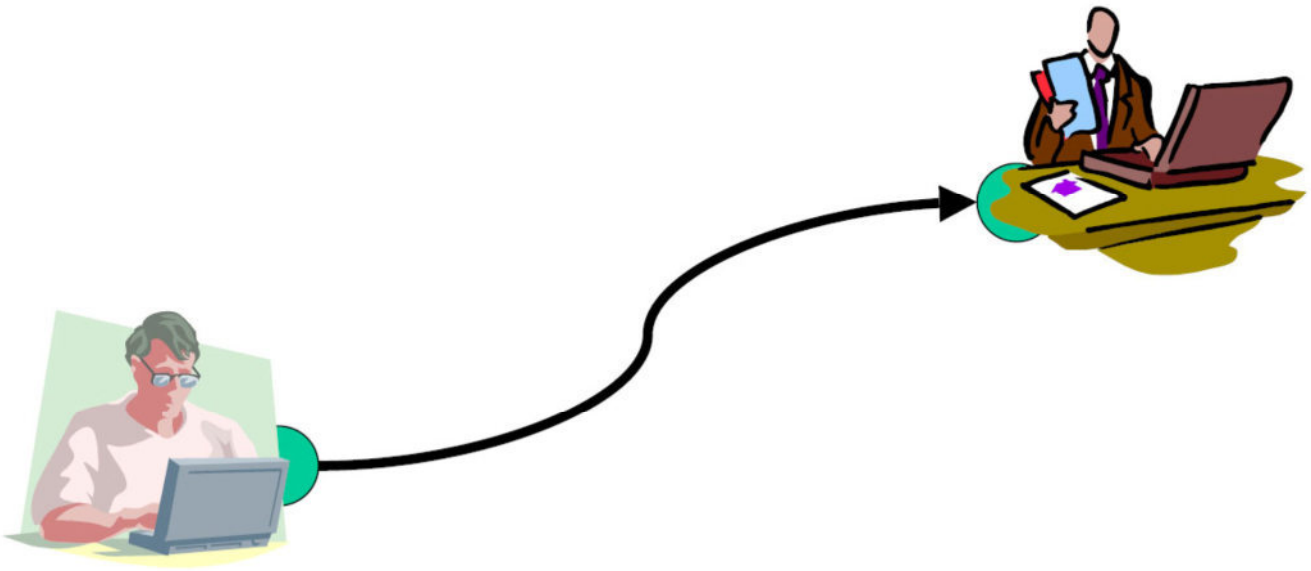
Introduction

The art of war teaches us not on the likelihood of the enemy's
not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

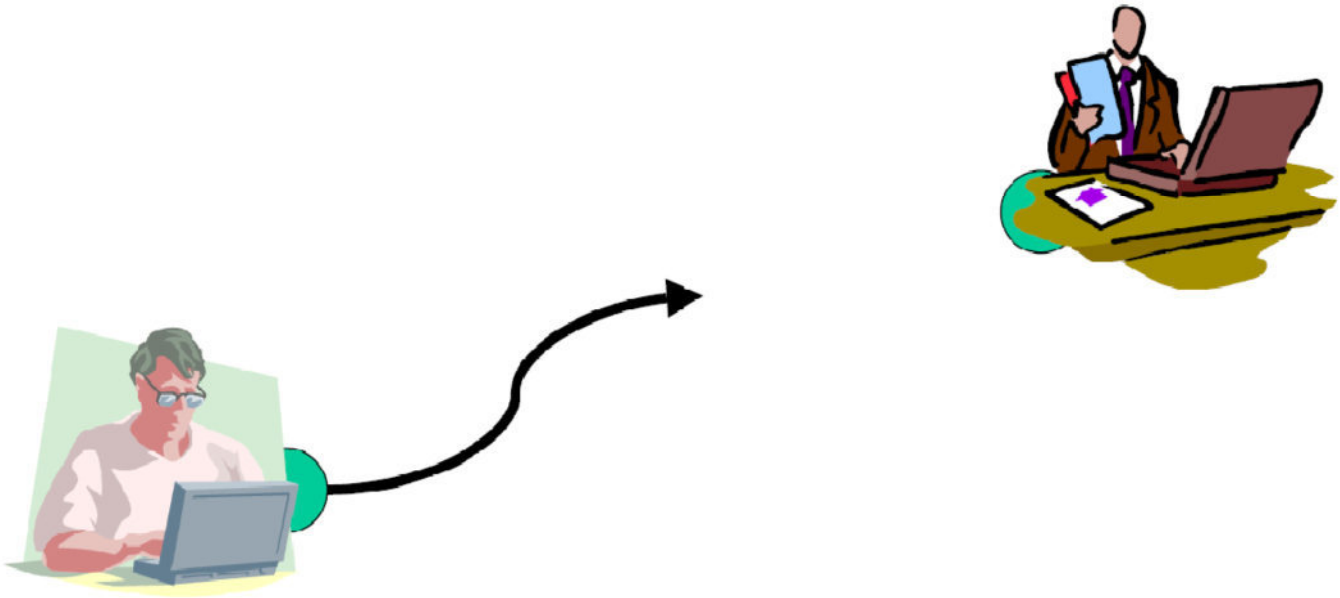
--The art of War, Sun Tzu

2

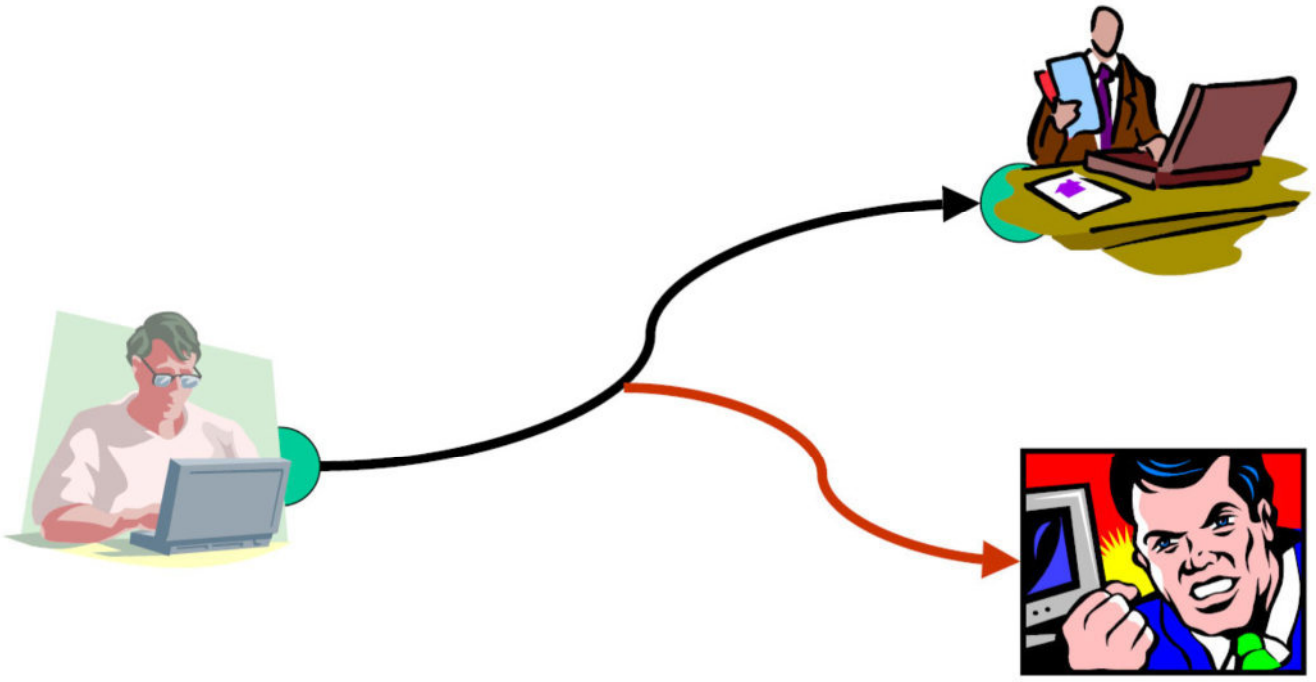
Information Transferring Attack:



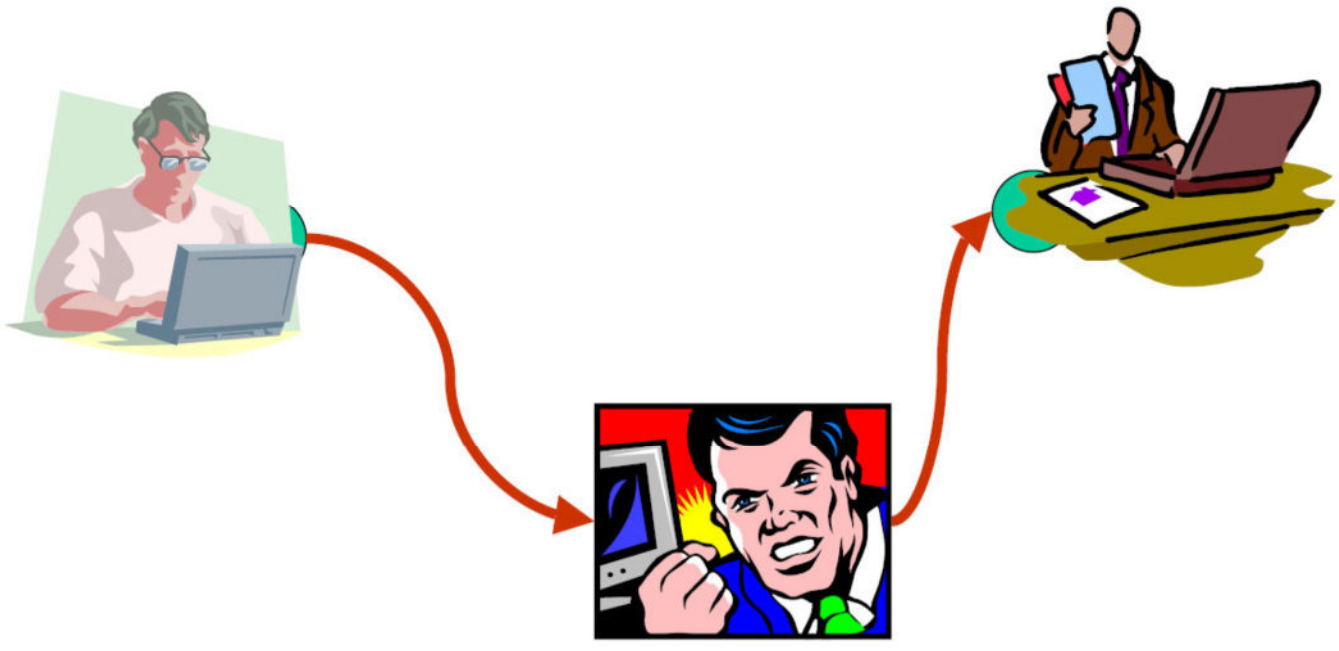
Attack: Interruption



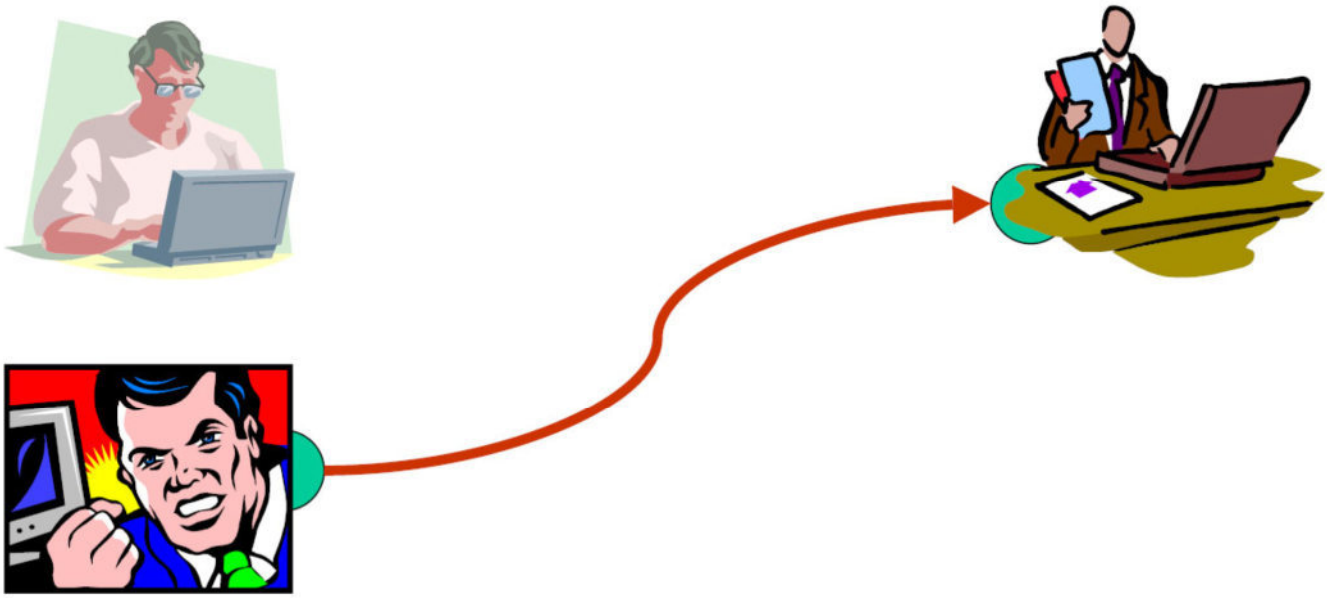
Attack: Interception



Attack: Modification



Attack: Fabrication



Attacks, Services and Mechanisms

- Security Attacks
  - Action compromises the information security
- Security Services
  - Enhances the security of data processing and transferring
- Security mechanism
  - Detect, prevent and recover from a security attack

Important Features of Security

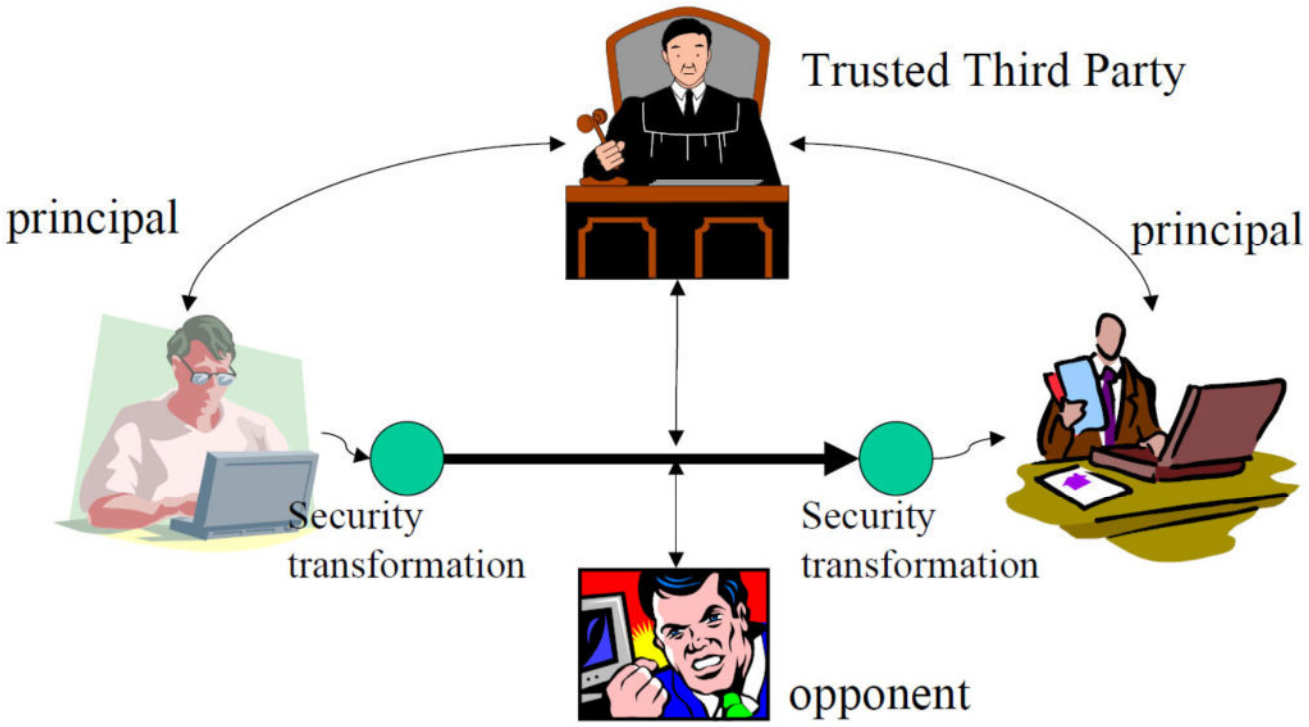
- Confidentiality, authentication, integrity, nonrepudiation, non-deny, availability, identification,

……

Attacks

- Passive attacks
  - ➢ Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - ➢ Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

Network Security Model



Cryptography

- Cryptography is the study of **Secret** (crypto-) **writing** (-graphy)
- Concerned with developing algorithms:
  - Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or

- Verify the correctness of a message to the recipient (**authentication**)
- Form the basis of many technological solutions to computer and communications security problems

Basic Concepts

- Cryptography

The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

- Plaintext

The original intelligible message

- Ciphertext

The transformed message

- Cipher

An algorithm for transforming an intelligible message into unintelligible by transposition and/or substitution

- Key

Some critical information used by the cipher, known only to the sender & receiver

- Encipher (encode)

The process of converting plaintext to ciphertext

- Decipher (decode)

The process of converting ciphertext back into plaintext

- Cryptanalysis

The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **codebreaking**

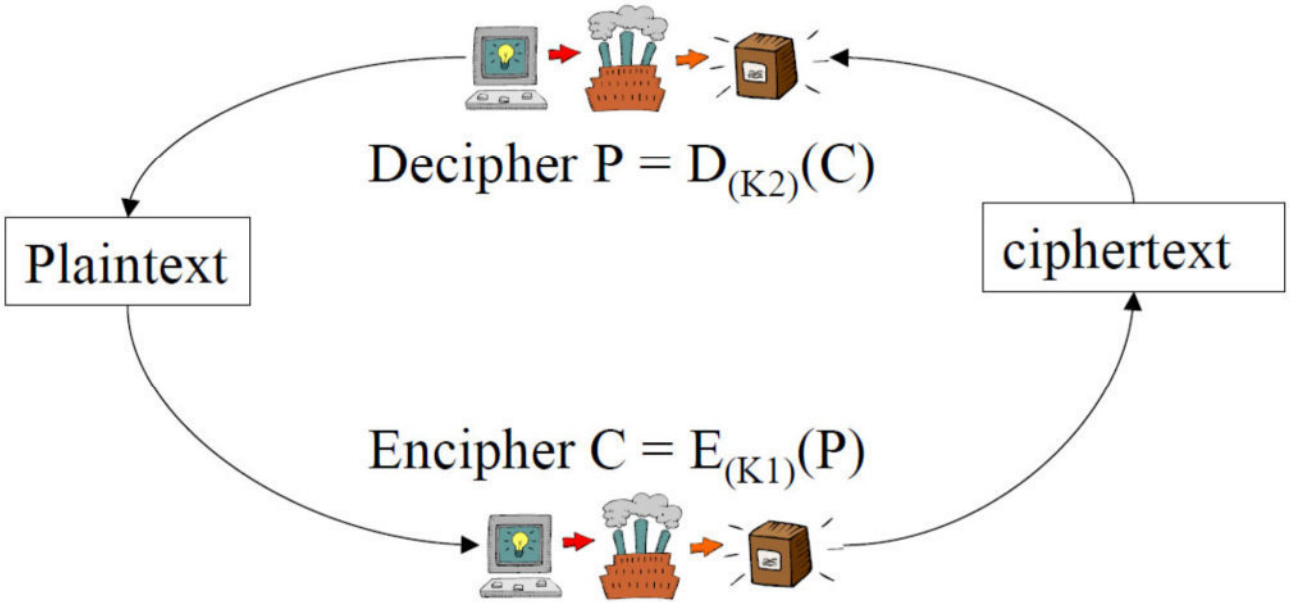
- Cryptology

Both cryptography and cryptanalysis

- Code

An algorithm for transforming an intelligible message into an unintelligible one using a codebook

Encryption and Decryption



K1, K2: from keyspace

Security

Two fundamentally different security

- Unconditional security

No matter how much computer power is available, the cipher cannot be broken

- Computational security

Given limited computing resources (e.G time needed for calculations is greater than age of universe), the cipher cannot be broken.

History

Ancient ciphers

- Have a history of at least 4000 years
- Ancient Egyptians enciphered some of their hieroglyphic writing on monuments
- Ancient Hebrews enciphered certain words in the scriptures
- 2000 years ago Julius Caesar used a simple substitution cipher, now known as the Caesar cipher
- Roger bacon described several methods in1200s

- Geoffrey Chaucer included several ciphers in his works
- Leon Alberti devised a cipher wheel, and described the principles of frequency analysis in the 1460s
- Blaise de Vigenere published a book on cryptology in 1585, & described the polyalphabetic substitution cipher
- Increasing use, esp in diplomacy & war over centuries.

Classical Cryptographic Techniques

Two basic components of classical ciphers:

- **Substitution:** letters are replaced by other letters
- **Transposition:** letters are arranged in a different order

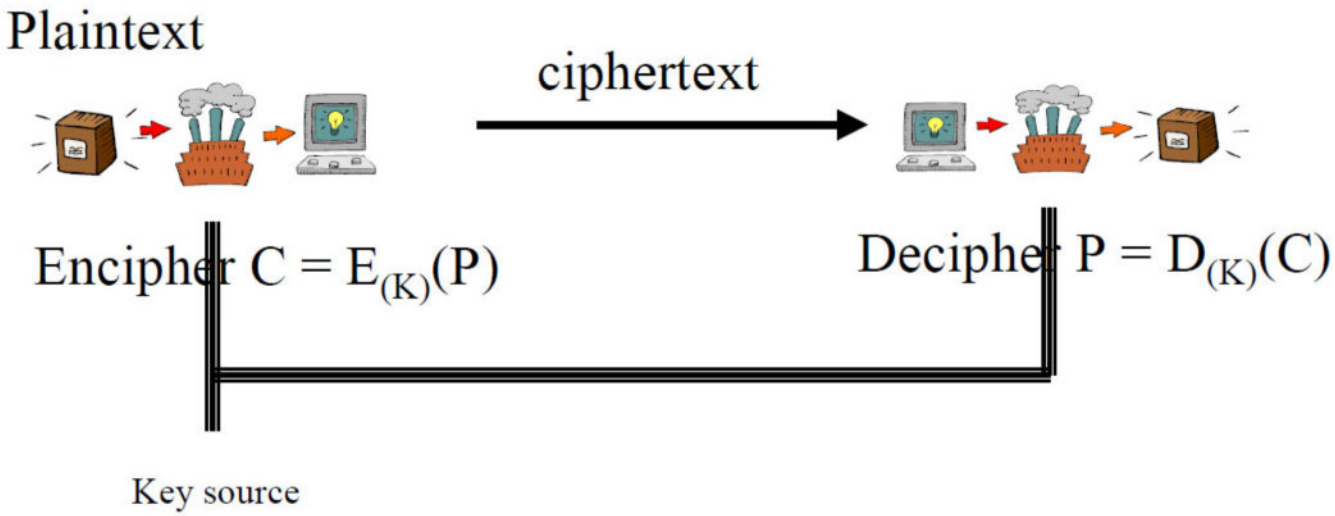
These ciphers may be:

- **Monoalphabetic**: only one substitution/ transposition is used, or
- **Polyalphabetic:** where several substitutions/ transpositions are used

Product cipher:

- several ciphers concatenated together

Encryption and Decryption



Key Management

- Using secret channel
- Encrypt the key
- Third trusted party
- The sender and the receiver generate key
  - The key must be same

Attacks

- Recover the message
- Recover the secret key
  - Thus also the message
- Thus the number of keys possible must be large!

د. هيفاء عباس محسن
الموضوع: امن البيانات والحو
المرحلة الرابعة
قسم علوم الحاسوب

كلية التربية للعلوم
الصرفة/ابن الهيثم

Computer and Data Security

Ref / المصادر

1) Applied Cryptography, Bruce Schneier, 1996.

2) Cipher Systems: The protection of Communication
H. Beker, F. Piper, 198.

3) Cryptography & Data Security, D.E.R. Denning, purdue university, 1983.

4) A new Dimension in Computer Data Security,
C.H. Meyer, S.M. Matyas, 1982

Content:

1) Introduction:

- Definitions & terminology مصطلحات وتعاريف
- Mathmatical Background الاسس الرياضية والتعاريف

2) Traditional Systems انظمة التشفير التقليدية

- Substitution انظمة الاستبدال (التعويض)
- Transposition الانظمة الانتقالية
- More complex systems انظمة اكثر تعقيد
- O.T.P (one Time pack system)
قطاع المفتاح مرة واحدة

3) Type of systems {
- Symmetric / Asymmetric }
- Block / stream } systems.
- public key / one key }

4) Stream Algorithms
{ SEAL, RC4, WAKE } + DES
- stream cipher
- stream cipher with chaining,
- synchronons / self- synchronons stream cipher.

5) Public Key Algorithms خوارزميات المفتاح العام
{ Diffie Hellman, RSA, RABIN, ELGAMAL, E.C. }

6) Keys & Key Management
Key Length, production of keys, Key transfer, storing keys
Backup keys, using keys, Master Key, -- etc.

7) cipher Systems
protocols / security / Authentication /
Digital Signature / secret sharing / secret splitting

8) Designing a Cipher System

Requirements / Tests / implementation / prove or disprove of secure Algorithms.

- Cryptology : is the Science of Cryptography & Cryptanalysis.
- Cryptography : is the Science of secret writing.
- plaintext (P) : is the original text (understood by anyone)
- Cipher text (C) : is an encrypted plaintext {sometimes called Cryptogram}.
- Cipher (Cryptographic Algorithm) : is "a secret" Method of writing, or is a method of Encipherment & Decipherment.
- Encipherment (Encryption) : is the process of transforming P to C.
- Decipherment (Decryption) : is the process of transforming C to P.
- A key : is a controller for E & D.

- cryptanalysis : is the Science of Methods of breaking ciphers.

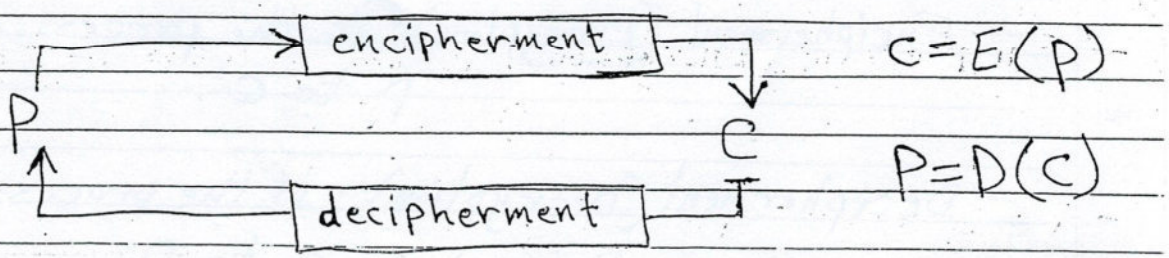
- Type of attacks:

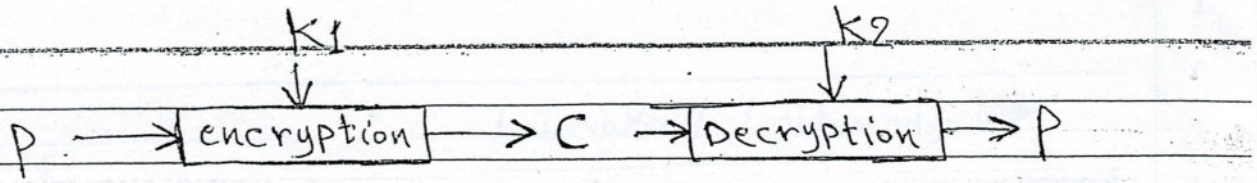
1) Ciphertext only attack. في هذه الطريقة محلل الشفرة يجب ان يحدد Key وحده من خلال اعتراض سيل النص المشفر
2) Known-plaintext attack.
3) Chosen-plaintext attack.
4) Chosen-Ciphertext attack.
5) Adaptive-plaintext attack.

- A cipher System is strong (Computationally secure), if it cannot be broken by systematic analysis with available resources.

- Threats: التهديدات

-passive : does not interfer with a system.
-Active : interfer with a system.





$C = E_{K_1}(P)$ $P = D_{K_2}(C) = D_{K_2}(E_{K_1}(P))$.

- A cryptosystem: Algorithm + keys + all possible plaintexts and ciphertext

- Types of Cryptosystem depending on keys:

1) Symmetric Algorithms (conventional system)

secret-key / single-key / one-key Algorithm.

i.e. $K_1 = K_2$ or

K_2 can be calculated from K_1 or vise versa.

2) Asymmetric Algorithms / public-key Algorithms /

Two-keys Algorithms: $K_1 \neq K_2$ and

K_2 can not be calculated from K_1

encryption-key: is a public-key,

decryption-key: is a privat-key.

Mathematical Background

Number theory

a, b integer , $n > 0$

$a \bmod n = r \qquad 0 \leq r \leq n-1$

$a \equiv b \bmod n$ a is congruent to b modulo n

iff

$a \bmod n = b \bmod n$ or

$a * K + b = n$, K is integer or

$n \mid (a-b)$: n divides $(a-b)$

Ex:

$17 \equiv 2 \bmod 5$

$17 \equiv 7 \bmod 5$

b is called the residue of a modulo n

Comment:

I : integers.

I mod n with addition & multiplication from a commutative ring.

Now

$$a^t \bmod n = \left[\prod_{i=1}^{t} (a \bmod n) \right] \bmod n$$

EX:

$3^5 \bmod 7$, $3^5 = 243$

$243 \bmod 7 = 5$

now:

$3 \times 3 \bmod 7 = 2$ $\quad$ $2 * 2 \bmod 7 = 4$

$4 * 3 \bmod 7 = 5$.

Computing inverse:

Given $a \in [0, n-1]$, find x (the inverse of a) s.t.

$a x \bmod n = 1$

EX:

$3 * 7 \bmod 10 = 1$

- if $a \in [0, n-1]$ then a has a unique inverse mod n when a & n are relatively prime i.e. $\gcd(a, n) = 1$
- This does not give an algorithm to find the inverse.
- The reduced set of residues mod n is the subset of residues $\{0, 1, 2, \ldots, n-1\}$ relatively prime to n

EX: reduced set of residues mod 10 is: $\{1, 3, 7, 9\}$.

- if n is prime then it is reduced set of residues $\{1, 2, 3, \dots, n-1\}$. i.e. complete set of residues except 0.

So: if p & q are two primes then

$\phi(p) = p-1$; no. of integers $< p$ that are relatively prime to p

$\phi(q) = q-1$

Then: if $n = pq$, p and q are two primes.

$$\phi(n) = \phi(pq) = \phi(p)\,\phi(q) = (p-1)(q-1)$$

EX: $p=3 \rightarrow q=5$

$$\phi(n) = \phi(15) = (3-1)(5-1) = 8$$

i.e. There are 8 elements $< n$ in the reduced set of residues modulo 15: $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

Generally

if $n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$ then

$$\phi(n) = \prod_{i=1}^{t} p^{e_i - 1} (p_i - 1)$$

Ex: $n = 24 = 2^3 \cdot 3^1$

$\phi(24) = 2^{3-1} \cdot (2-1) \cdot 3^{1-1} \cdot (3-1) = 2^2 * 2 = 8$

$\phi(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$

notice $\gcd(n, x) = 1$ القاسم المشترك الاكبر لكل عدد من اعداد المجموعة $\phi(24)$ مع n يساوي 1

Fermat's Theorem:

Let p be prime, $\forall a$ s.t. $\gcd(a, p) = 1$

$a^{p-1} \bmod p = 1$

Ex $p = 7$, $a = 2, 3, 5$

$2^{7-1} \bmod 7 = 2^6 \bmod 7 = 64 \bmod 7 = 1$

$3^{7-1} \bmod 7 = 729 \bmod 7 = 1$

$5^{7-1} \bmod 7 = 15625 \bmod 7 = 1$

- Euler generalization

if $\gcd(a, n) = 1$ then $a^{\phi(n)} \bmod n = 1$

- if $a\,x \bmod n = 1$, $\gcd(a,n) = 1$ then

the solution for the inverse x is :

$$x = a^{\phi(n)-1} \bmod n$$

notice if n is prime then

$$x = a^{\phi(n)-1} \bmod n = a^{(n-1)-1} \bmod n = a^{n-2} \bmod n$$

Ex: $a=3$, $n=7$ then

$$x = 3^{7-2} \bmod 7 = 3^5 \bmod 7 = 243 \bmod 7 = 5$$

So 5 is the inverse of 3 modulo 7.

i.e. $3 * 5 \bmod 7 = 1$

- There is an iterative version of Euclidean algorithm to compute the inverse by computing :

$g_{i+1} = g_{i-1} \bmod g_i$; $i = 1, 2$ — until $g_i = 0$

where $g_0 = n$, $g_1 = a$

$g_i = u_i n + v_i a$ when $g_i = 0$ then $g_{i-1} = \gcd(a,n)$

solution $x = v_i$ if $v_i < 0$ the $x = v_i + n$.

Ex: $n = 7, a = 3$

i	g_i	u_i	v_i
0	7	1	0
1	3	0	1
2	1	1	-2
3			

$g_{i+1} = 7 \bmod 3 = 1$

next $g_{i+1} = 3 \bmod 1 = 0$

or

$7 = 2 * 3 + 1$

$3 = 3 * 1 + 0$

$-2 + n = -2 + 7 = 5 = x$

$x = v_i + n$ إذا $v_i < 0$

a هو inverse لـ x و

$u_i \quad n \quad v_i \quad a$

$7 = 1 * 7 + 0 * 3$

$3 = 0 * 7 + 1 * 3$

$1 = 1 * 7 + (-2) * 3$

Information theory

- Amount of information in a message measured by the average number of bits needed to encode all possible messages in an optimal encoding.
- This measure is called the entropy of the message:

$H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$ when $p(x_i)$ is the probability of x_i.

$$H(X) = \sum_{i=1}^{n} p(x_i) \log_2 \left(\frac{1}{p(x_i)}\right) = \sum_{x} p(x) \log_2 \left(\frac{1}{p(x_i)}\right)$$

Ex/ suppose $p(male) = p(female) = \frac{1}{2}$

$$H(X) = \frac{1}{2}\log_2^2 + \frac{1}{2}\log_2^2 = \frac{1}{2} + \frac{1}{2} = 1$$

$\log_2\left(\frac{1}{P(X)}\right)$ represents the no. of bits needed to encode X in an optimal encoding,

$H(X)$ gives the expected number of bits in optimally encoded messages.

Ex/ Let $p(A) = \frac{1}{2}$, $p(B) = p(C) = \frac{1}{4}$

$\log_2\left(\frac{1}{P(A)}\right) = \log_2 2 = 1 \Rightarrow$ one bit needed to encode A

$\log_2\left(\frac{1}{P(B)}\right) = \log\left(\frac{1}{P(C)}\right) = \log_2 4 = 2 \Rightarrow$ two bits needed to encode B & C

Ex/ $A = 0$, $B = 10$, $C = 11$

$H(X) = \frac{1}{2} * 1 + 2 * \frac{1}{4} * 2 = 1.5$

So encoding of

A A B A C B → 6 char.

0 0 10 0 11 10 = 9 bit.

Thus $\log_2^n$ bits needed to encode each message

Ex/ if $p(x) = \frac{1}{n}$ for all x_i, $i = 1, 2, \ldots, n$ i.e equally likely $H(X) = n\left(\frac{1}{n}\log_2^n\right) = \log_2^n$

For a message M of length N, number of letters say n then

$$H(M) = \log_2 n$$

rate of a language is r

$$r = \frac{H(M)}{N}$$

EX/: for english language with equally likely of occurenc of letters

$$H(M) = \log_2 26 \simeq 4.7 \text{ bits/letter},$$

The redundancy of a language D

$D = R - r$, for english $R = 4.7$ (Max: equally likely)

given $r = 1.3$ for english

$D = 4.7 - 1.3 = 3.4$ bits/litter

means that each english letter carries 3.4 bit of redundant information.

Traditional Systems ciphers :

- traditional related to all ciphers used before seventies.
- They are divided into :

1) Substitution ciphers (استبدالية (تعويضية
2) Transposition ciphers (ابدالية) انتقالية

1- Transposition Ciphers :

- Transposition means arrangement of letters according to some scheme.

(a) Simple Transposition

1) - Columner transposition الابدال العمودي

ex/ plaintext : Cryptography

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

$\Longrightarrow$ C = RoP PRY CTA YGH
1 2 3 4

- It is a matrix, Both sides agree on a key (Keys).

2) A fixed period d, with a permutation function

$f : Z_d \rightarrow Z_d$

Ex: plaintext : cryptography , d=4 , f = 2413

d=4	4	4
CRYP	TOGR	APHY
1 2 3 4	1 2 3 4	1 2 3 4

C= RPCY ORTG PYAH
2 4 1 3 2 4 1 3 2 4 1 3
d= represents block length.

b) Double Transposition

repeat simple transposition twice, each time with a different key.

2- Substitution Ciphers :

Four Types :

1) simple
2) homophonic
3) polyalphabetic
4) poly-gram (polygraphic)

1) simple substitution

- replace each plaintext letter with a corresponding ciphertext letter.

EX Keyword : Cryptographic system

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

To encipher Cryptography ⇒ C= YKXFNDGKCFAX

- In simple Substitution there are;

① standard – standard.

$C = (P + K) \bmod 26$ where A=0, B=1, ..., Z=25

This is called shifted alphabet by K positions.

EX/ Caesar cipher uses with K=3

P = A B C D ... Z

C = D E F G ... C

$P = (C - K) \bmod 26$ معادلة فك الشفرة

② Standard – Reverse.

$C = (K - P) \bmod 26$

P = A B ... Z K=9

C = J I ... M L K

shift opposite direction

$P = (K - C)$ معادلة فك الشفرة

(3). Mixed alphabet.

Like; (1) Keywords as above

(2) Multiplicative

$C = (pK) \bmod 26$, where $\gcd(K,26) = 1$

Ex)

K=9

A	B C	D E F	G H I	J	...	Z
A	J S	B K T	C L U	D	...	R

(3) shift + Multiplicative

$C = (pK_1 + K_2) \bmod 26$

$9 \times 25 = 225$

$225 \bmod 26$

(4) Randomly.

(2) Homophonic Substitution

- a homophonic substitution cipher maps each plaintext letter into a set of ciphertext elements (called homophones)

Ex:

A	B	C	D	...	M	N	...	Z
3	17	60	4		71	11		31
25	55	80			26	50		83
31	90				08	98		
36								
74								

- notice no. of homophones assigned to each plaintext letter is proportional to its frequency.

EX/ encipher BABAANDMAMA

17 3 55 25 31 11 4 71 31 26 36

D. Beale Ciphers :

use fig 2.6 /Page 71

i- use the first letter of each word from aplaintext (ex. a book)

ii- number the words : 1, 2, 3, --, text length as words

iii- to encipher aplaintext letter use its no. from ii.

EX :

- Plaintext from a book :

01 02 03 04 05 06 07

when, in the course of human events,

- to encipher : the ⟹ C = 03 06 07

t h e

في هذه الطريقة يخصص لكل حرف مجموعة من الاعداد التي يتم اختيارها باستذكار نص معين يحتوي على عدد من الكلمات وهذه الكلمات التي يتم ترقيمها بالتسلسل ويتم التشفير بتعويض كل حرف في النص الصريح بعدد معين الذي هو رقم الكلمة في النص التي تبتدئ بهذا الحرف

2) Multiequivalent Substitution :-

use a table or a matrix, where each letter maps into several ciphertext elements.

لبناء نظام الدرجة الثانية (second-order homophonic) (كل نص مشفر يعطي نصين صريحين مفهومين)
الاعداد من 1 الى n^2 يتم ترتيبها في مصفوفة K ذات بعد n*n بشكل عشوائي
حيث n تمثل عدد الحروف الهجائية كل صف او عمود في المصفوفة K يعود الى احد الحروف
الهجائية (لكل رمز a في الصف a في المصفوفة K يعرف مجموعة واحدة من
(homophonic) والعمود a يعرف مجموعة اخرى من الـ (homophonic)
النص الصريح M يبدل برسالة زائفة X ومن ثم يتم الحصول على النص المشفر C
بتطبيق المعادلة $C_i = K[m_i, x_i]$ حيث $i = 1, 2$ ——

* بما انه لكل نص مشفر هناك نصين صريحين مفهومين لذلك عند تحليل الشفرة سوف يحصل
الحلل على نصين ذات معنى وبالتالي عليه ان يقرر اي الرسالتين تم ارسالها ما يزيد
من درجة الريبة.

3) Polyalphabetic Substitution Cipher

poly. sub. cipher use Multiple substitutions, while simple sub. cipher are considered as monoalphabetic sub. cipher.

استخدمت هذه الطريقة من قبل الجيش الامريكي في الحرب العالمية الثانية.
الجدول الخاص بهذه الطريقة موجود في صفحة 75 من الكتاب.
يتم في هذه الطريقة اجراء تعويضات متعددة لذلك يكون التوزيع التكراري للحروف الهجائية
غير مفيد لتحليل هذه الشفرات وذلك لكون ترددات حروف النص المشفر متقاربة.

في هذا النوع عدة احرف ممكن ان تخصص لحرف واحد من اجل تعويضها للحصول على النص المشفر
وكذلك نفس الحرف ممكن ان يكون مخصص لعدة احرف

1) Vigenere cipher (16th century)
القرن السادس عشر

في طريقة Vigenere يتم اختيار كلمة مفتاحية Keyword معينة بطول d ومن ثم يتم وضعها تحت النص الصريح واذا كان طول النص اكبر من طول الكلمة المفتاحية فانه يتم تكرار الكلمة المفتاحية كما في المثال كررنا كلمة Ali لذلك يقال على هذا النوع من الانظمة انها انظمة تعويضية دورية periodic وذات دورة d

Key \ Plaintext	A	B	C	D	...	Z
A	A	B	C	D	...	Z
B	B	C	D	E	...	A
⋮	⋮	⋮	⋮	⋮		⋮
Z	Z	A	B	C	...	Y

هو عملية shift للامام

$C = E(p) = (k+p) \bmod 26$ it is a shift.

EX/ p = CRYPTOGRAPHY
(1 2 3 4 5 6 7 8 9 10 11 12)

K = ALI ALI ALI ALI ← Key word

C = CCG PEW GCI PSG ← using the table

- encrypt 2nd letter using the equation

A=0, B=1 ..., Z=25

$E(R) = (R+L) \bmod 26 = (17+11) \bmod 26 = 2 = C$

موقع R في الترتيب الهجائي ↑ موقع L في الترتيب الهجائي

2) Beaufort cipher

وهو نظام مشابه للنظام السابق مع اختلاف واحد هو استخدام التسلسل المعكوس لحروف الهجائية

$$E(p) = (K - p) \bmod 26$$

Key \ Plaintext	A	B	C	D	—	—	Z
A	A	Z	Y	X	—	—	B
B	B	A	Z	—	—	—	C
C	C	B	A	—	—	—	D
D	D	C	B	—	—	—	—
⋮							
Z	Z	Y	X	—	—	—	A

3) Running-Key Ciphers

Security of polyalphabetic substitution ciphers reside in keylength. In running-key cipher, keylength = plaintext length.

ex/ using a text from a book as a key.

P = T H E T R E A S U R E — — —

K = T H E S E C O N D C I — — — — — using vigenere cipher

C = M O I L V G C F X T M

* what is the difference with Beale ciphers

4) Polygram substitution ciphers.

Previous methods encipher a single plaintext letter at a time
Polygram substitution encipher larger blocks of letters at a time.

1) playfair cipher. (1854)

i- Key is a 5x5 matrix, gives 25 letters (j is excluded)

ii- pairs of plaintext letters enciphered at a time.

EX: a Keyword = GOOD MORNING IRAQ

1	2	3	4	5
G	O	D	M	R
N	I	A	Q	B
C	E	F	H	K
L	P	S	T	U
V	W	X	Y	Z

To encipher: CR YP TO GR AP HY
GK TW MP QG SI TM

2) Hill cipher

Perform linear transformation. Suppose we are enciphering two plaintext letters at a time:

$$C_1 = (K_{11}P_1 + K_{12}P_2) \bmod n$$

$$C_2 = (K_{21}P_1 + K_{22}P_2) \bmod n$$

OR $$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \bmod n$$

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \bmod n$$

تعتبر المصفوفة K هي مفتاح الطريقة ويتم فك الشفرة بأخذ معكوس المصفوفة K

Ex/ Let $K = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix}$, $K^{-1} = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$ Mod 26

$$K K^{-1} = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

To encipher EG $\Rightarrow \begin{pmatrix} 4 \\ 6 \end{pmatrix}$

تمثل ارقام الابجدية

a=0, b=1, c=2, d=3, E=4

F=5, G=6

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 4 \\ 6 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 24 \\ 16 \end{pmatrix} \Rightarrow Y\,Q$$

$$= \begin{pmatrix} 24 \\ 42 \end{pmatrix} \bmod 26 = \begin{pmatrix} 24 \\ 16 \end{pmatrix}$$

24 Mod 26 = 24 = Y
42 Mod 26 = 16 = Q

3) Product Ciphers

Product Ciphers means combening transposition with substitution to get a uniform distribution of plaintext over the set of all possible ciphertexts.

EX): use one substitution followed by a transposition

New Ciphers

1) LUCIFER (1973): use transformation that applies substitution & transpositions alternatively.
figure 2.12, page 90

2) DES (1977): figure 2.13, page 91

Vernam Cipher & one-time pad (OTP)

- In OTP: Keys are randomly generated sequence of letters (bits) used once with a substitution cipher.

- Vernam (1917) used Baudat code (Based on coding 32 chars with a non repeated keys punched on paper tape, process it bit by bit mod 2 (page/ 86 Denning)

$C = (P+K) \bmod 2$

or $C = P \oplus K$

$C \oplus K = (P \oplus K) \oplus K = P$

EX/

$P = 1\ 1\ 0\ 0\ 0$ ($2^4\ 2^3\ 2^2\ 2^1\ 2^0$)

$K = 1\ 0\ 0\ 1\ 0$

$C = 0\ 1\ 0\ 1\ 0$

Exclosive OR

input	output
0 0	0
0 1	1
1 0	1
1 1	0

- If Key sequence are used twice then OPT is a running-Key cipher:

$C1 = P_1 \oplus K$

$C2 = P_2 \oplus K$

$C = C_1 \oplus C_2 = P_1 \oplus P_2$

Type of Systems: — chapter 9 (APPLIED)

Depending on enc./Dec. Keys:

1. Symmetric Algorithm.

$C = E_K(P)$, $P = D_K(C)$.

K is secret / single Key / one-Key Algorithm.

i.e. the same Key for enc. & Dec.

or the Key of Dec. can be calculated from enc. Key.

2. Asymmetric Algorithm. / public key Algo.

Two Keys: one for enc. & the second for Dec.

i.e. $C = E_{K_1}(P)$, $P = D_{K_2}(C)$.

Normally, K_1 is public, K_2 is secret.

Depending on Cryptographic Techniques يمكن ان يقسم حسب تقنية التشفير

- Block ciphers
- stream ciphers

1. Block Ciphers :-

breaks p into blocks $p_1, p_2, \dots p_n$ and enciphers each block p_i with the same key K

تقسيم النص الى قطع متساوية وعملية التشفير تتم لكل قطعة على حدة بنفس المفتاح

i.e. $C = E_K(p) = E_K(p_1)\, E_K(p_2) \dots E_K(p_n)$

$C_1 \quad C_2 \quad C_n$

Examples :

1) playfair : it is a block cipher of size 2 letters.

2) Hill : it is a block cipher of size d letters.

3) DES : it is a block cipher of size 64 bits

4) Electronic Code Book / Code Book (ECB)

correspond plaintext block to a ciphertext block.

manually : choose 1000 – 10000 plaintext blocks in a two part book : one for encipherment sorted on plaintext. The second part sorted on ciphertext

هذه الطريقة استخدمت من قبل الدبلوماسيين الالمانية في الحرب العالمية الثانية

تستخدم قاموس يحتوي على عدد كبير من الكلمات ولكل كلمة code معين

وهذا القاموس موجود لدى الطرفين المرسل والمستلم

Electronic :

each Key has different code book .
Book size is bigger than of manual.

Some Advantages

* it is some what faster than stream cipher, each time n characters executed
وجود امكانية المعالجة المتوازية لاكثر من Block في نفس الوقت
* Transmission errors in one ciphertext block have no effect on other blocks.
هذه الطريقة اسرع من stream cipher في كل وقت n من الاحرف تنفذ ،
الخطأ الذي يحدث في واحد من ciphertext block لا يؤثر على بقية Blocks

من محاسن هذه الطريقة ايضاً ان كل Block من النص الصريح يتم تشفيره بصورة مستقلة وهذه الخاصية مهمة في اللغات ،
فاذا تم تشفير بـ ECB mode فان اي قيد يمكن اضافته او حذفه وتعديله وتشفير وفك تشفرته بصورة مستقلة عن بقية القيود

Some Disadvantages :-

* Identical blocks of plaintext produce identical blocks of ciphertext (headings / Ends)
ciphertext المتشابهة في plaint text تعني متشابهة في blocks
* Easy to insent / delete blocks.
في حالة الاضافة و حذف الـ Blocks
* Modifying blocks.
تعديل blocks

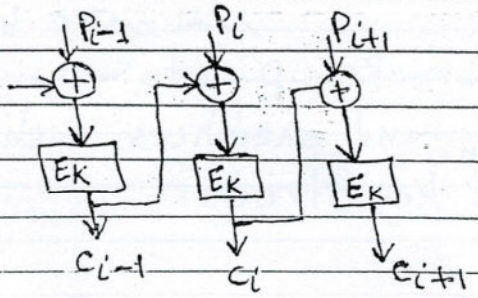
Cipher Block Chaining mode CBC

لمعالجة بعض المشاكل اقترح نظام جديد ضمن block
عملية التشفير لايمكن ان تبدأ الا بعد ان يملأ block كاملاً

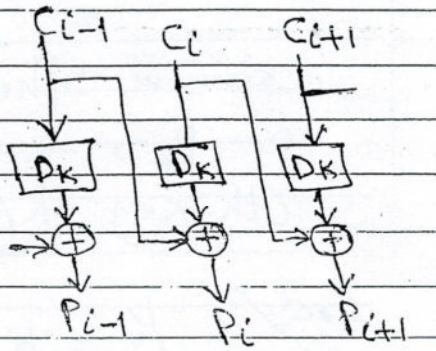
The plaintext is XORed with the previous ciphertext block before it is encrypted.

يحول النص الى Binary ونعمل XOR

$$C_i = E_K(P_i \oplus C_{i-1})$$
$$P_i = C_{i-1} \oplus D_K(C_i)$$



CBC Encryption



CBC Decryption

Advantages :-

1) * not possible to add / Modify / delete a block.
لا توجد امكانية الاضافة والحذف والتعديل
* Identical plaintext blocks encrypted mostly to different ciphertext blocks (headers problem).
we can add an initialization vector (IV) to encipher the first block. (Ex. Time stamp is a good IV)

Problems:

Error in a cipher block C_i effect all blocks of plaintext starting from block i, If one bit error in C_i then will be one bit error in all plaintext blocks starting from P_i.

2) Stream Ciphers

a stream ciphers breaks P into characters (bytes/bits) $P_1, P_2, \ldots, P_n$ and enciphers each P_i with the ith key K_i of key stream.

$K = K_1, K_2 \ldots K_n$, $P = P_1 P_2 \ldots P_n$

$C = E_K(P) = E_{K_1}(P_1) E_{K_2}(P_2) \ldots E_{K_n}(P_n) = C_1 C_2 \ldots C_n$

$P = D_K(C) = D_{K_1}(C_1) D_{K_2}(C_2) \ldots D_{K_n}(C_n)$.

$P = P_1 P_2 \ldots P_n$

* A stream cipher is periodic if the key stream repeats after d characters (bytes/bits), for some fixed d.
otherwise it is non periodic.

Ex: - OTP and running Key ciphers are non periodic.
- Vigenere cipher is periodic.

* for short period, a cipher like a block cipher than a stream cipher.

اذا كانت الفترة قصيرة فان التشفير اقرب الى block منه الى stream

K K

$k_1, k_2 \text{---} k_d$, $k_1, k_2 \text{---} k_d$

نظام التشفير الانسيابي يكون دوري اذا كانت سلسلة Key تتكرر بعد فترة d من char, للفترة الثابتة d اما الحالات الاخرى يكون غير دوري

Most stream ciphers use simple XOR operation for encryption / Decryption.

$$C_i = E_{K_i}(P_i) = P_i \oplus K_i$$
$$D_{K_i}(C_i) = C_i \oplus K_i = (P_i \oplus K_i) \oplus K_i = P_i$$

Stream Cipher

Synchronous | self-Synchronous

1- Synchronous stream cipher : Key stream is generated independently of the plaintext stream.

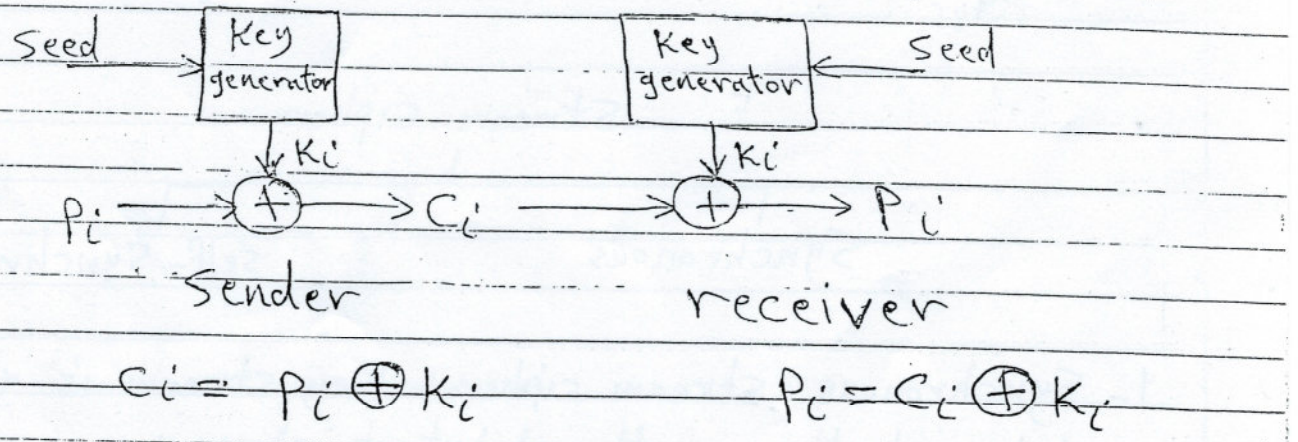
* if a ciphertext character (bit) lost during transmission then sender & receiver must resynchronize their key generators before proceeding further.

اذا فقد character او bit من ciphertext اثناء الارسال فان المرسل والمستلم سوف يعيدون العملية من جديد قبل الاستمرار بالعمل.

i.e./ Keystream $K = k_1, k_2, \ldots, k_n$ is generated independently of plaintext stream. Key stream is generated by a deterministic algorithm. Keys generated must have some random properties.

سلسلة Key تولد بصورة مستقلة عن النص الواضح، سلسلة Key تولد بواسطة خوارزمية واضحة الخوارزمية يجب ان يكون لها بعض الخواص العشوائية.

* The Key generator initial stat initialized by a seed no.
* No finite Key-generator can generate truely random sequence. So we have a pseudo-random no. generator.



$C_i = P_i \oplus K_i$ $\quad P_i = C_i \oplus K_i$

notice: identical parts of P are enciphered with different parts of the Key stream.

الاجزاء المتشابهة من P تشفر باجزاء مختلفة من سلسلة K

2- A self-Synchronous stream Cipher, each Key character (or bit) is derived from a fixed number(n) of preceding ciphertext characters (or bits)

Key يتم استخراجها اعتمادا على عدد bits أو الحرف السابقة

* if a bit lost or altered during transmission, the error affect the n characters & cipher resynchronous itself after n correct ciphertext characters.

EX AutoKey Ciphers:

starts with K_1, next Keys $K_i = P_{i-1}$ or C_{i-1}

Let P = RENAISSANCE

K = ⓓRENAISSANC → $K_i = P_{i-1}$

C = UVRNIAKSNPG → using vigenere

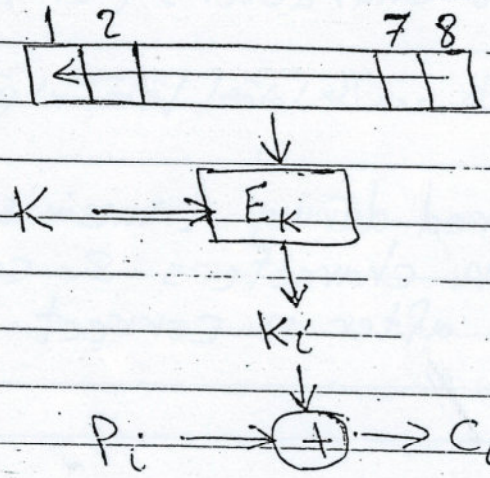
P = RENAISSANCE

K = ⓓuyLLTLDDQS → $K_i = C_{i-1}$

C = uyLLTLDDQSW → using vigenere

Another ex. is Cipher Feedback (CFB) plaintext is enciphered in small units (smaller than block size).

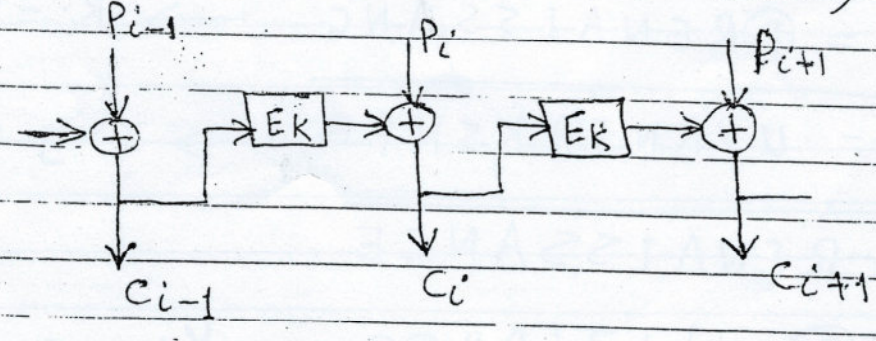
EX. 8 bits where we can use one bit cipher as a feedb
64 ≤ ≤ ≤ ≤ ≤ 8 bits ≤ ≤ ≤



- To start with IV is needed to fill the initial state.
- It must be unique for each message.

$$C_i = P_i \oplus E_K(C_{i-1})$$

$$P_i = C_i \oplus E_K(C_{i-1})$$



Public-Key systems

Denning [11]

Two-key systems introduced by Diffie & Hellman in 1976.

In a public-key system, normally each user has two keys:

1) public key for encryption E_A
2) private (secret) key for decryption D_A

- To encrypt a message M to user A, $C = E_A(M)$

  user A decrypt it $D_A(C) = D_A(E_A(M)) = M$

- Dictionary of publicKeys as a data base of keys
  لدينا قاموس يتضمن قاعدة بيانات للمفاتيح العامة

- Any one can have ciphertext of any plaintext (messages) But what is the no. of possible M & C ?! in public keys.

- Public-Key Algorithms are designed to resist (تقاوم) chosen-plaintext attack.

- So, Security resides in :-

1) difficulty of deducing the secret (private) Key from the public key.
   من الصعوبة استنتاج المفتاح السري من المفتاح العمومي
2) difficulty of deducing M from C
   من الصعوبة استنتاج الرسالة العربية من النص المشفر

- Public-Key Systems are used for encryption & some of them are used for:

I. Authentication. التوثيق
II. Digital Signature. التوقيع الرقمي
III. Key Distribution توزيع المفاتيح العامة

I. Authentication: verify the identity of sender التحقق من هوية المرسل

from A to B, encrypt M: $C = E_B(D_A(M))$

to decrypt it By user B;

$$E_A(D_B(C)) = E_A(D_B(E_B(D_A(M)))) = E_A(D_A(M)) = M$$

notice
1) A using his secret key first then the public key of B why?!

2) This achieve both security & Authentication. {like RSA}

3) $M = E_A(D_A(M)) = D_A(E_A(M))$ commutative op. عملية ابدالية

Digital Signature:

Process of signing messages s.t.:

1) Able to validate a signature of a Message.
القدرة على اثبات التوقيع للرسالة
2) No one can forge a signature.
لا احد يستطيع تزوير التوقيع
3) No one can disavow a signed message by him.
لا أحد يستطيع انكار الرسالة الموقعة من قبله

So:

1) A signs M by computing $C = D_A(M)$
2) B validates it by $E_A(C) = M$
3) A judge does $E_A(C) \rightarrow = M$ found by B

{DES, RSA} can be used for Digital Signature

---

1) Knapsack Algorithms: — 117

- Merkle & Hellman (1978) propose a public key system using Knapsack:

- A Knapsack problem:

Given $A = (a_1, a_2, \ldots, a_n)$ positive integers & positive integer C.

Find M s.t $M = (m_1, m_2, \ldots, m_2)$ where $C = AM$ or $C = \sum_{i=1}^{n} a_i m_i$

- It is NP-complete problem. Well known algorithm to solve NP-complete problems is $O(2^{n/2})$

n is the size of input.

- Simple Knapsack problem / super increasing Knapsack problem.

$A = (a_1, \ldots, a_n)$ s.t. $a_i > \sum_{j=1}^{i-1} a_j$

if is solvable, in linear time.

```
for i = n down to 1 do
  begin
    if c ≥ a_i then m_i = 1 else m_i = 0
      c := c - a_i * m_i
  end
if c = 0 then print M else no solution is found
```

{improve this procedure}

procedure التحسين لهذا

```
if c ≥ a_i then
  begin
    m_i = 1;
    c = c - a_i
  end
  else
    m_i = 0;
```

Ex: $A = (1, 3, 5, 10, 22)$, $C = 14$

$\Rightarrow M = (1, 1, 0, 1, 0)$

Now Merkle & Hellman convert it to a trapdoor Knapsack which is hard to solve.

1) choose $A = (a_1, \dots, a_n)$, $a_i > \sum_{j=1}^{i-1} a_j$

2) choose $u > 2a_n > \sum_{i=1}^{n} a_i$

3) choose w s.t. $\gcd(u, w) = 1$

4) compute w^{-1} : $w w^{-1} \bmod u = 1$

here $w^{-1} = w^{\phi(u)-1} \bmod u$ if u is prime, $\phi(u) = u-1$

else $\phi(u) = \prod_{i=1}^{t} p_i^{e_i - 1}(p_i - 1)$, $u = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$

5) Compute $E_A = w * A \bmod u$

E_A is public Key ; A, w^{-1} are secrets.

To encrypt : $C = E_A M$

To decrypt : $C' = w^{-1} C \bmod u$

you have A & C' solve linearly for M

$C' = AM$

notice :

$$\begin{aligned} C' &= W^{-1} C \bmod u \\ &= W^{-1} E_A M \bmod u \\ &= W^{-1}(W*A) M \bmod u \\ &= AM \bmod u \\ &= AM \end{aligned}$$

EX/

1) $A = (1,3,5,10)$
2) $u = 20$
3) $W = 7$; $\gcd(7,20) = 1$
4) $W^{-1} = 3$
5) $E_A = (7*1 \bmod 20, 7*3 \bmod 20, 7*5 \bmod 20, 7*10 \bmod 20)$
   $E_A = (7, 1, 15, 10)$

i.e $M = (0,0,0,0) \Rightarrow M = (1,1,1,1)$

Let $M = 13 \Rightarrow M = (1,1,0,1)$
$C = E_A * M$ تضاعف الرقم 13 في الباينري
$C = 7 + 1 + 10 = 18$

$D_A(C)$ as follows :

$C' = C W^{-1} \bmod u = 18 * 3 \bmod 20 = 14$
$C' = 14 = AM = (1,3,5,10) * M$
$M = (1,1,0,1) = 13$

notice $n \geq 200 - 400$ bits, $u \geq 100 - 200$ bits.

encipherment: requires at most n addition

decipherment: requires at most n subtraction & one multiplication in modular.

2- Pohlig.-Hellman Algorithm (1978)

2.7) Exponentiation ciphers 101

1) choose p a large prime s.t. $M < p$
2) To encrypt : $C = M^e \bmod p$
3) To decrypt : $M = C^d \bmod p$

How to choose e and d

1) choose d s.t. $\gcd(d, \phi(p)) = 1$
2) compute $e = d^{\phi(\phi(p))-1} \bmod \phi(p)$

or choose e and compute d (i.e. symmetric)

notice 1) e and d are secret if e and p are known ?! (if p is known ?!)

2) The security of it rests on the complexity of computing discrete logarithms in GF(p)
Galois field = Gf

i.e. $e = \text{Log}_M^C$ in GF(p)

- Best Know time $T = e^{\sqrt{\ln(p)\ln\ln(p)}}$ افضل وقت حسوب

if $p \geq 200$ bits $\Rightarrow T \geq 2.7 * 10^{11}$

Ex) Let $p=11$, $\phi(p) = p-1 = 10$ choose $d=7$

use Extended Euclid's Algo. to compute $e=3$

or:

$$e = d^{\phi(\phi(p))-1} \bmod \phi(p)$$

$$= 7^{4-1} \bmod 10 = 3$$

$e = inv(7, 10) = 3$

لان $7 * 3 \bmod 10 = 1$

لذا فان 3 هو الانفرس لـ 7

Let $M = 5$ then $C = M^e \bmod p = 5^3 \bmod 11 = 4$

to decrypt $M = C^d \bmod p = 4^7 \bmod 11 = 5$

notice e and d are secret.

3) Rivest-Shamir-Adleman (RSA) Algorithm

1) choose two large primes p & q then $n = pq$

$\Rightarrow \phi(n) = (p-1)(q-1)$

2) choose e s.t. $\gcd(e, \phi(n)) = 1$

3) use extended Euclid's Algorithm to compute

$$d = e^{\phi(\phi(n))-1} \bmod \phi(n)$$

To encipher $C = M^e \bmod n$

To decipher $M = C^d \bmod n$

} e and n is public. d is secret.

notice :

$$C^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n$$

$$= m^{k(p-1)(q-1)+1} \bmod n = m\, m^{k(p-1)(q-1)} \bmod n$$

$$= m\, m^{k\phi(n)} \bmod n = m \bmod n = m$$

$\{ed \equiv 1 \bmod \phi(n) \equiv 1 \bmod (p-1)(q-1)\}$

Ex/ Let $p = 5$, $q = 7$, $n = pq = 35$, $\phi(n) = (5-1)(7-1) = 24$

Let $d = 11$, $e = 11^{\phi(24)-1} \bmod 24 = 11^7 \bmod 24 = 11$

if $m = 2$ then

$$C = M^e \bmod n = 2^{11} \bmod 35 = 18$$

$M = c^d \bmod n = 18^{11} \bmod 35 = 2$

notice

1) Difficulty of the Algorithm depends on factoring n into p & q.

108 2) Each user have different n and e (both) why?!

4) ELGAMAL (1985)

- used for encryption & digital signature.
- It's security is based on the difficulty of calculating discrete Logarithms in a finite field.

Discrete Logarithms in a finite field

- $a^x \bmod n$ is easy to be computed
- But, Find x where $a^x \equiv b \pmod n$ is a hard problem

Ex if, $3^x \equiv 15 \bmod 17$ then $x = 6$

but $3^x \equiv 7 \bmod 13$ has no solution for x

page 396 Applied Cryptography

ELGAMAL Signature

1) Choose a prime p & two random no.s $g, x < p$ then calculate $y = g^x \bmod p$

2) public key: y, g, p. Both g, p can be shared by many users.

private key $= x$

3) To sign a message M

I. Choose a random no. K s.t. $\gcd(K, \Phi(p)) = 1$

II. compute $a = g^K \bmod p$

III. use Extended Euclid's Algo. to solve for b

$$M = (xa + Kb) \bmod (p-1)$$

IIII. The signature is the pair a and b.

K is Kept secret.

4) To verify a signature comfirm that

$$y^a a^b \bmod p = g^M \bmod p$$

notice : not possible to use K twice. It can break the Algo. & recover the value of x. How ?!

Ex) Let $p=11$, $g=2$, private key $x=8$

then $y = g^x \bmod p = 2^8 \bmod 11 = 3$

publickey : $y=3$, $g=2$, $p=11$

To authenticate $M=5$

choose K randomly = 9, $\gcd(9,10)=1$

$a = g^K \bmod p = 2^9 \bmod 11 = 6$

$M = (aX + Kb) \bmod (p-1)$

$5 = (8*6 + 9*b) \bmod 10 \Rightarrow b=3$

The signature is $a=6$, $b=3$

To verify sign.

$y^a a^b \bmod p = 3^6 6^3 \bmod 11 = 10$

$g^M \bmod p = 2^5 \bmod 11 = 10$

EL GAMAL Encryption

478

To encrypt a message M

I. choose random no. K s.t. $\gcd(K, \phi(p)) = 1$

II. compute

$$a = g^K \bmod p \;,\; b = y^K M \bmod p$$

Then C is the pair a and b.

To decrypt a and b

compute $M = b / a^x \bmod p$ since

$$b / a^x \equiv y^K M / a^x \equiv g^{xK} M / g^{xK} \equiv M \pmod p$$

Important:

Most public-Key Algorithms are based on:

1) Discrete Logarithm:

if p is a prime & g and M are integers then

Find x s.t. $g^x \equiv M \pmod p$

2) Factoring: if N is the product of primes then
   a) Factor N.
   b) Given M & C integers, find d s.t. $M^d \equiv C \pmod N$
   c) Given e & C, find M. s.t. $M^e \equiv C \pmod N$.
   d) Given an integer X, is $\exists y$ s.t. $X = y^2 \pmod N$

Public-Key Digital signature Algorithms:-

Like
1) Digital signature Algo. (DSA) - 1991.
2) Gost - 1994. (Russian)
3) ELGAMAL - 1985.
4) ONG-Schnorr-Shamir - 1984
5) ESIGN - 1990 (Japan)

DSA

* DSA is a digital signature Algorithm not used for encryption or key distribution.
* DSA was developed by the NSA ?!

Description of DSA

1) p is a prime no. with length L bits, where
   512 bits $\leq L \leq$ 1024 bits
   and multeple of 64.
2) q is 160 bit prime factor of p-1 (i.e $\emptyset(p)$).
3) $g = h^{(p-1)/q} \bmod p$, h is any no. $< p$.
4) x is a no. $< q$.
5) $y = g^x \bmod p$.

- p, q, and g are public & common for all users.
- for each user
  x is a private key, y is a public key. H(m) is a one way hash function.

To sign a message m

1) generate a random no. $k < q$ (k for each signature),
2) Compute $r = (g^k \bmod p) \bmod q$
   $s = (k^{-1}(H(m) + xr)) \bmod q$.
   r & s are the signature

$$H(M) = M^e \bmod p$$

To verify a signature, compute

1) $w = s^{-1} \bmod q$,
2) $u1 = (H(m) * w) \bmod q$,
3) $u2 = (rw) \bmod q$
4) $v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$.

if $v = r$ then the signature is verified

$$v = (((y^{u2} \bmod p) * (g^{u1} \bmod p)) \bmod p) \bmod q$$