جامعة الموصل /كلية التربية للعلوم الصرفة
قسم علوم الحاسوب

Fourth Class

Data Security

أستاذ المادة:
د. ثامر عبدالحافظ جرجيس

Lecture 1

Basic Data Security Concepts

CONTENTS

* Basic Data Security Concepts
* Why Data and Computer Security is important?
* Definitions
* What will happen if your computer gets hacked?
* What goes into protecting data?
* Types of software to Access Information
* Homework

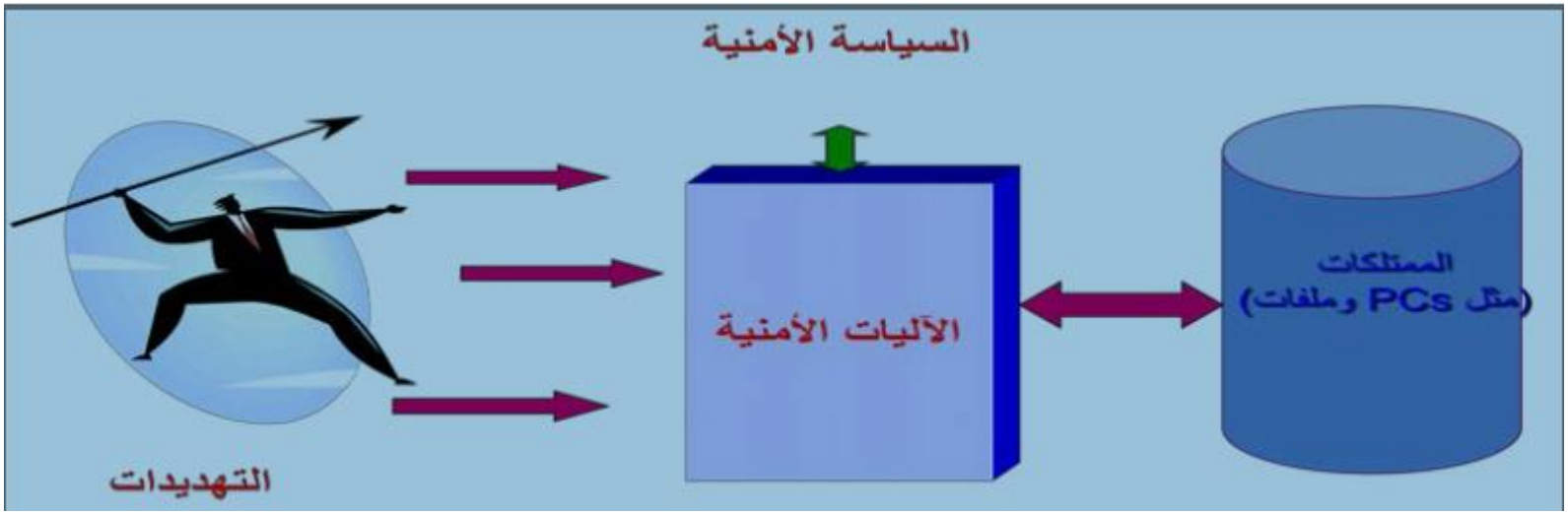
Basic Data Security Concepts

- **Data security** is one of the most daunting tasks for IT and infosec professionals. Each year, companies of all sizes spend a sizable portion of their IT security budgets protecting their organizations from hackers intent on gaining access to data through brute force, exploiting vulnerabilities .

- **Data security** refers to the process of protecting data from **unauthorized access** and data corruption throughout its lifecycle.

Why data security is important

- Safe guarding it from unauthorized access by internal or external people
- protects your company from financial loss, reputation damage, consumer confidence disintegration, and brand erosion
- Provide support for the critical business processes.
- Provide protection for the personal and sensitive information.



What will happen if your computer gets hacked?

- It could be used to hide some data and programs.
- Some one could access personal information.
- Some one could record all your keys that are used like passwords.
- It could generate a large amount of unwanted traffic.

what goes into protecting data?

- Data security has myriad aspects that protect information in motion and in use. Here are some technologies widely used by enterprises to protect data.
- Use a strong password when entering the system.
- Take backup.
- Use antivirus software.
- Use a firewall.

Definitions

- **Computer Security :-** is the protection of computing systems and the data that they store or access. It refers to the technological safeguards and managerial procedures that can be applied to computer hardware, programs, and data.

- **Network Security :-** measures to protect data during their transmission

- **Internet Security :-** measures to protect data during their transmission over a collection of interconnected networks

- **Information systems security :-** is the ability to provide the services required by the user community while simultaneously preventing unauthorized use of system resources

- **Security Mechanism :-** means the mechanism that is designed to detect, prevent, or recover from security attack. Remember that no single mechanism will support all functions required.

Definitions

- ***Privacy on Internet* :-** It means the measures to protect data during their transmission over a collection of interconnected networks. Social networking sites like Facebook, personal web pages have also become public sources of personal information.

- **Identification :-** the identification of a user, file, program, or other object is the unique name or number assigned to that object.

- **Threat :** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

- **Attack :** An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Types of software (Virus) to Access Information

- **There are several types of software that can be used to gain access to unauthorized data or information:-**
- **Trojan Horse**

* For the similarity of his work with the legend of Trojan Horse wooden which hid by a number of soldiers Greeks and they were the reason to open the city of Trojan.

* It is a kind of software which is loaded with major program and doing some hidden functions that are often concentrated to penetrate the system.

* Trojan horses may steal information or damage the host computer systems and may be used for the download by search engines or by installing online games or applications based on internet taking advantage of security gaps that allow unauthorized access to the system.

Types of software to Access Information

- **Salami Attack :**

* Is a process similar to the process slicer where small deducted
* This type of software is attacking the banks where the decimals deduct each amount daily and will be transferred to another account without being noticed and within days or months will get the beneficiary on the huge amounts of money.

- Homework

  What are the other types of virus programs that threaten information security?

Next lecture

Aspects of Information Security

شكرا لاصغاءكم

جامعة الموصل /كلية التربية للعلوم الصرفة
قسم علوم الحاسوب

Fourth Class

Data Security

أستاذ المادة:
د. ثامر عبدالحافظ جرجيس

Lecture 2

Aspects of Information Security

CONTENTS

* **Aspects of Information Security**
* **Security service**
* **Security attack**
* **Security mechanism**
* **Homework**

Aspects of Information Security

- ***The Security Architecture*** **focuses on three aspects of information security:**

  - **Security service**
  - **Security attack**
  - **Security mechanism**

Security Services

- A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

- The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security Services

6 security services :

1. **Confidentiality or Secrecy: The concept of *Confidentiality* relate to the protection of information and prevention of unauthorized access or disclosure. The ability to keep data confidential, or secret, is critical to staying competitive in today's business environments.**

Examples of Confidentiality:

- Student grade information is an asset whose confidentiality is considered to be very high
- Student enrollment information: may have moderate confidentiality rating; less damage if enclosed
- Directory information: low confidentiality rating; often available publicly

Security Services

2. Integrity : - deals with prevention of unauthorized modification of intentional or accidental modification.

- **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner
- **System integrity:** Assures that a system performs its operations in unimpaired manner

Examples of Integrity

* A hospital patient's allergy information (high integrity data): a doctor should be able to trust that the info is correct and current
* An online newsgroup registration data: moderate level of integrity
* An example of low integrity requirement: anonymous online poll

Security Services

3. Authentication : is the process by which the information system assures that you are who you say you are; how you prove your identity is authentic.

* **Methods of performing authentication are:**

User ID and passwords:

The system compares the given password with a stored password. If the two passwords match then the user is authentic.

Swipe card

which has a magnetic strip embedded, which would already contain your details, so that no physical data entry takes place or just a PIN is entered.

Digital certificate

an encrypted piece of data which contains information about its owner, creator, generation and expiration dates, and other data to uniquely identify a user.

key fob

small electronic devices which generate a new random password synchronized to the main computer

Biometrics

retinal scanners and fingerprint readers. Parts of the body are considered unique enough to allow authentication to computer systems based on their properties.

Security Services

4. Non-Repudiation : - prevents either sender or receiver from denying a transmitted message.

* when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

5. Access Control : The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

Security Services

6. Availability: - assures that the resources that need to be accessed are accessible to authorized parties in the ways they are needed. Availability is a natural result of the other two concepts (confidentiality and integrity).

* **Examples of Availability**
* **A system that provides authentication: high availability requirement**
* **If customers cannot access resources, the loss of services could result in financial loss**
* **A public website for a university: a moderate availably requirement; not critical but causes embarrassment**
* **An online telephone directory lookup: a low availability requirement**

Security attack

Any action that compromises the security of information owned by an organization.

Attacks types:-

* Passive Attack:- **does not affect the system, just take the wanted data and information.**

* Active Attack:- **affect the system in addition to have the wanted data and information.**

Passive Attack

Active Attack

- Homework

what are the types of passive and active attacks?

Next lecture

Computer Crimes

شكرا لاصغاءكم

جامعة الموصل /كلية التربية للعلوم الصرفة

قسم علوم الحاسوب

Fourth Class

Data Security

أستاذ المادة:

د. ثامر عبدالحافظ جرجيس

Lecture 3

Computer Crimes

CONTENTS

- **Security Mechanism/ Types of Security Mechanism**
- **Computer Crimes**
- **Types of computer crimes**
- **Examples of computer crimes**
- **Homework**

Network Security Mechanisms

- A process (or a device incorporating such a process)

- Feature designed to detect, prevent, or recover from a security attack

- no single mechanism that will support all services required

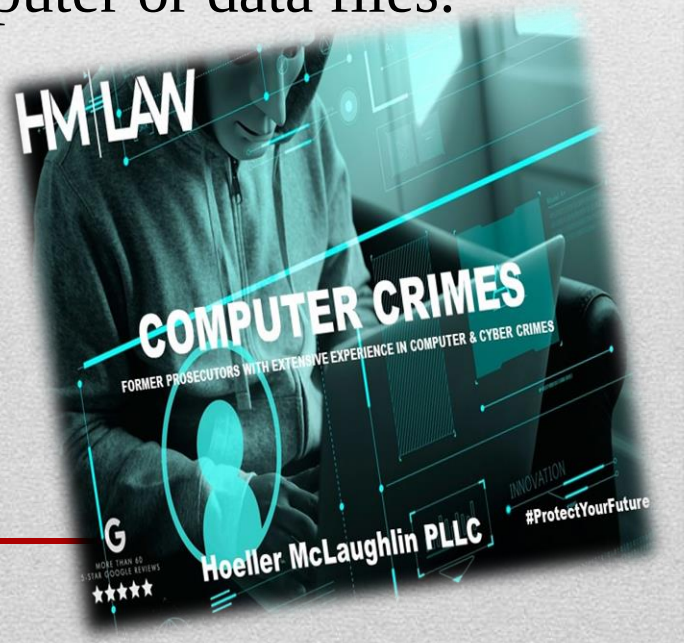
Types of Security Mechanism

- Cryptographic techniques
- Encryption algorithms
- Firewall
- Alternatives

- Alternatively referred to as cyber crime, e-crime, electronic crime, or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information.

- In some cases, this person or group of individuals may be harms and destroy or otherwise corrupt the computer or data files.

Computer Crimes



Types of computer crimes

- Viruses
- Tapping
- Impersonation
- Fraud

Examples of computer crimes

- **Copyright violation** - Stealing or using another person's Copyrighted material without permission.

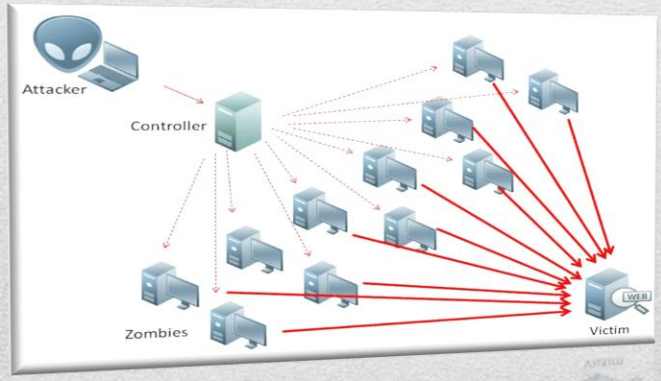
- **Cracking** - Breaking or deciphering codes designed to protect data.

- **Hacking:** threats, and blackmailing towards a business or person.

Examples of computer crimes

- **Cyberstalking** - Harassing or stalking others online.

- **Denial of Service attack** - Overloading a system with so many requests



- **Creating Malware** - Writing, creating, or distributing malware (e.g., viruses and spyware.)

Examples of computer crimes

- **Doxing** - Releasing another person's personal information without their permission.

- **Espionage** - Spying on a person or business.

- **Fraud** - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.

- **Scam** - Tricking people into believing something that is not true.

- **Software piracy** - Copying, distributing, or using software that was not purchased by the user of the software.

- **Spamming** - Distributed unsolicited e-mail to dozens or hundreds of different addresses.

Examples of computer crimes

- **Homework**

Ways of preventing computer crime ?

Next lecture

Information System Security Classification

شكرا لاصغاءكم

جامعة الموصل /كلية التربية للعلوم الصرفة

قسم علوم الحاسوب

Fourth Class

Data Security

أستاذ المادة:

د. ثامر عبدالحافظ جرجيس

Lecture 4

Information System Security Classification

CONTENTS

- **Classification**
- **Information System Security Classification**
- Physical security
- Personal security
- Operation Security
- **Firewall**
- **Homework**

- **Classification is the act or process by which information is determined to require protection against unauthorized disclosure and is marked to indicate its classified status. Safeguarding refers to using prescribed measures and controls to protect classified information.**

Classification

- Classified information does not only come in the form of paper documents; it comes in electronic and verbal forms too, and regardless of what form it is in, it must be appropriately protected.

- Effective execution of a robust information security program gives equal priority to protecting information

Information System Security Classification

Information System Security Classification

- Physical security
  - Personal security
    - Operation Security

Physical security

- is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, theft, vandalism and terrorism.

- is often overlooked -- and its importance underestimated -- in favor of more technical threats such as hacking, malware, and cyber spying.

- Protecting your personal information can help reduce your risk of identity theft.
- **There are four main ways to do it:**

- know who you share information with
- store and dispose of your personal information securely
- ask questions before deciding to share your personal information
- maintain appropriate security on your computers and other electronic devices.

Personal security

- **Keeping Your Personal Information Secure Offline**
- **Keeping Your Personal Information Secure Online**
- **Securing Your Social Security Number**
- **Keeping Your Devices Secure**

Personal security

- is a process that identifies critical information , determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary.

Operation Security

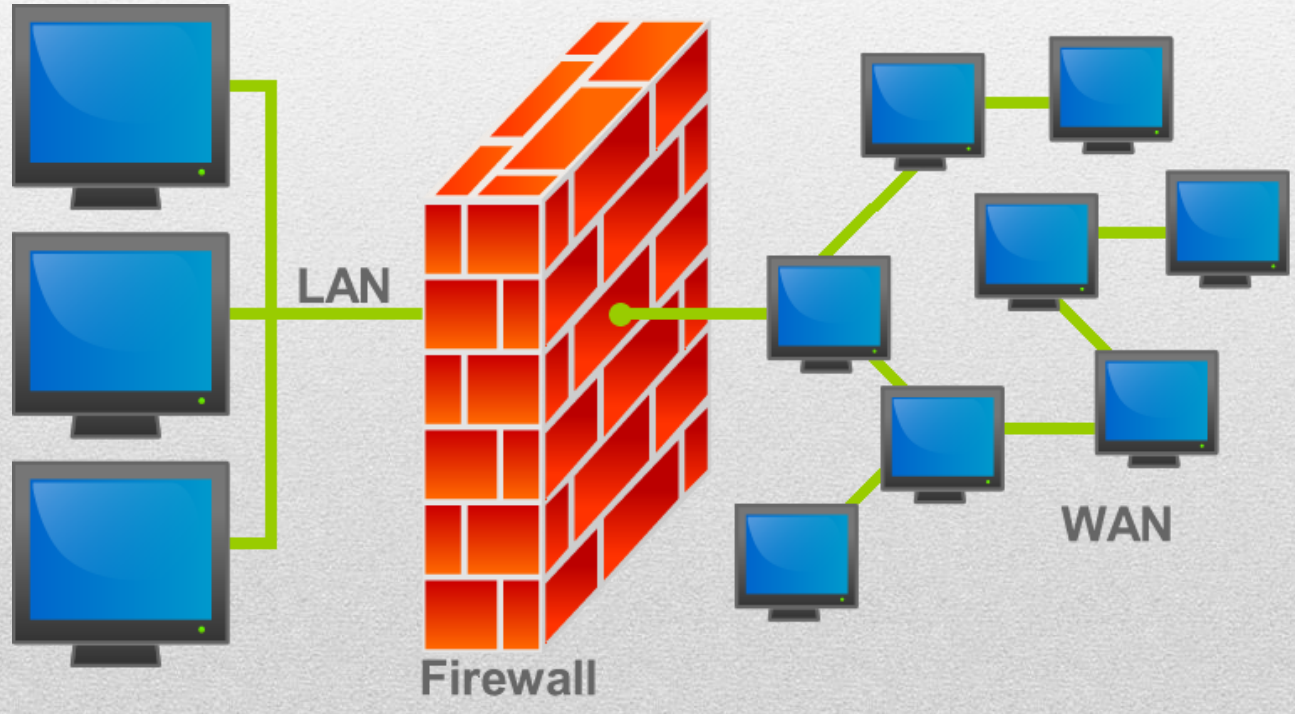
Operation Security

- is concerned with protecting individual pieces of data that can be aggregated to form a bigger picture.

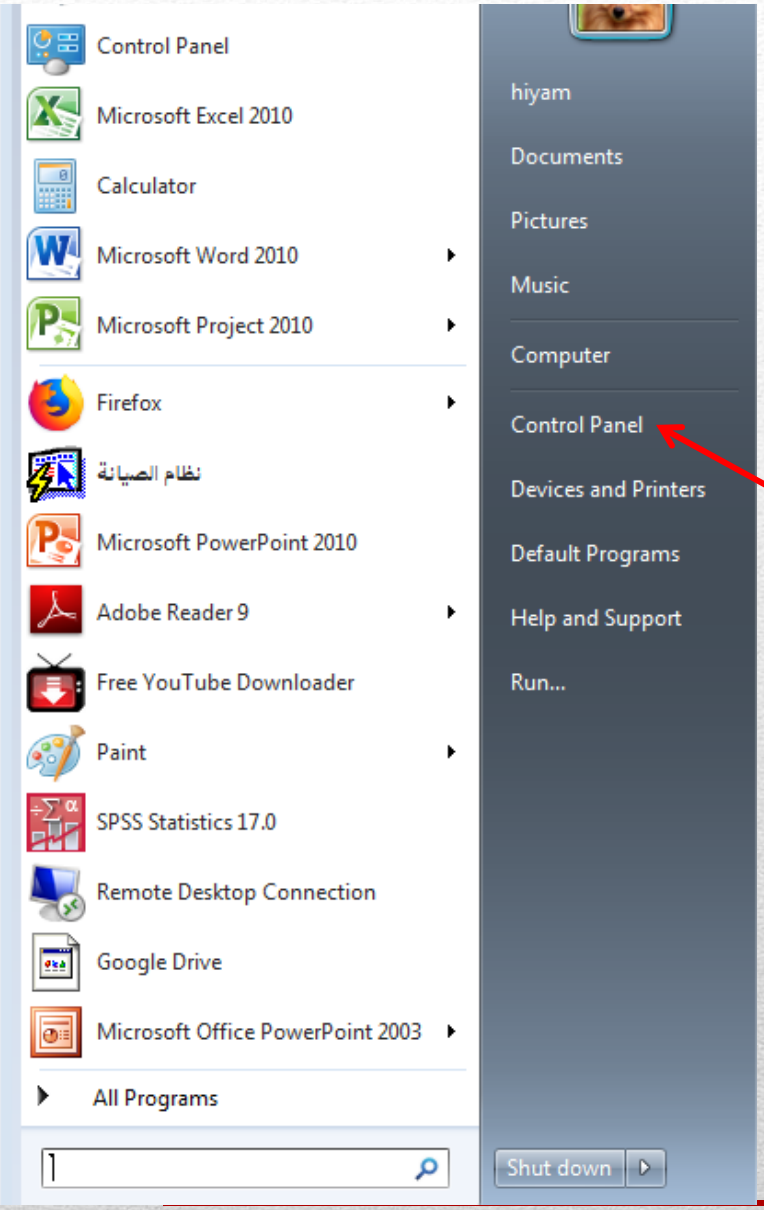
- is generally concerned with protecting against non-sensitive data being aggregated together, it often still uses technical countermeasures that are used to protect sensitive data.

ما هو الجدار الناري؟

الجدار الناري هو الحاجز الذي يفصل الحاسوب أو أي جهاز آخر عن الاتصال وإرسال واستقبال البيانات فيسمح لبرامج معينة بنقل واستقبال البيانات ويقوم بضرب حضر أمني عن أي أشياء أخرى مشكوك في أمرها



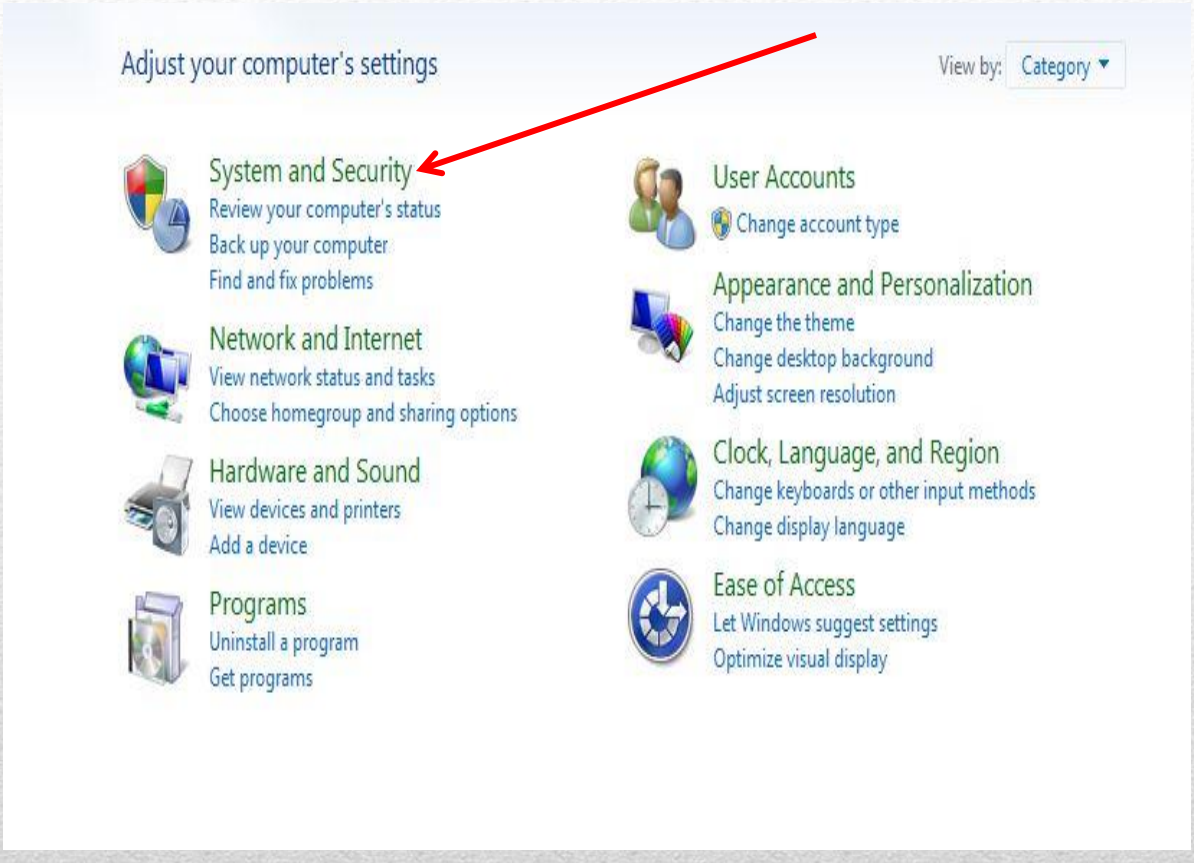
Firewall



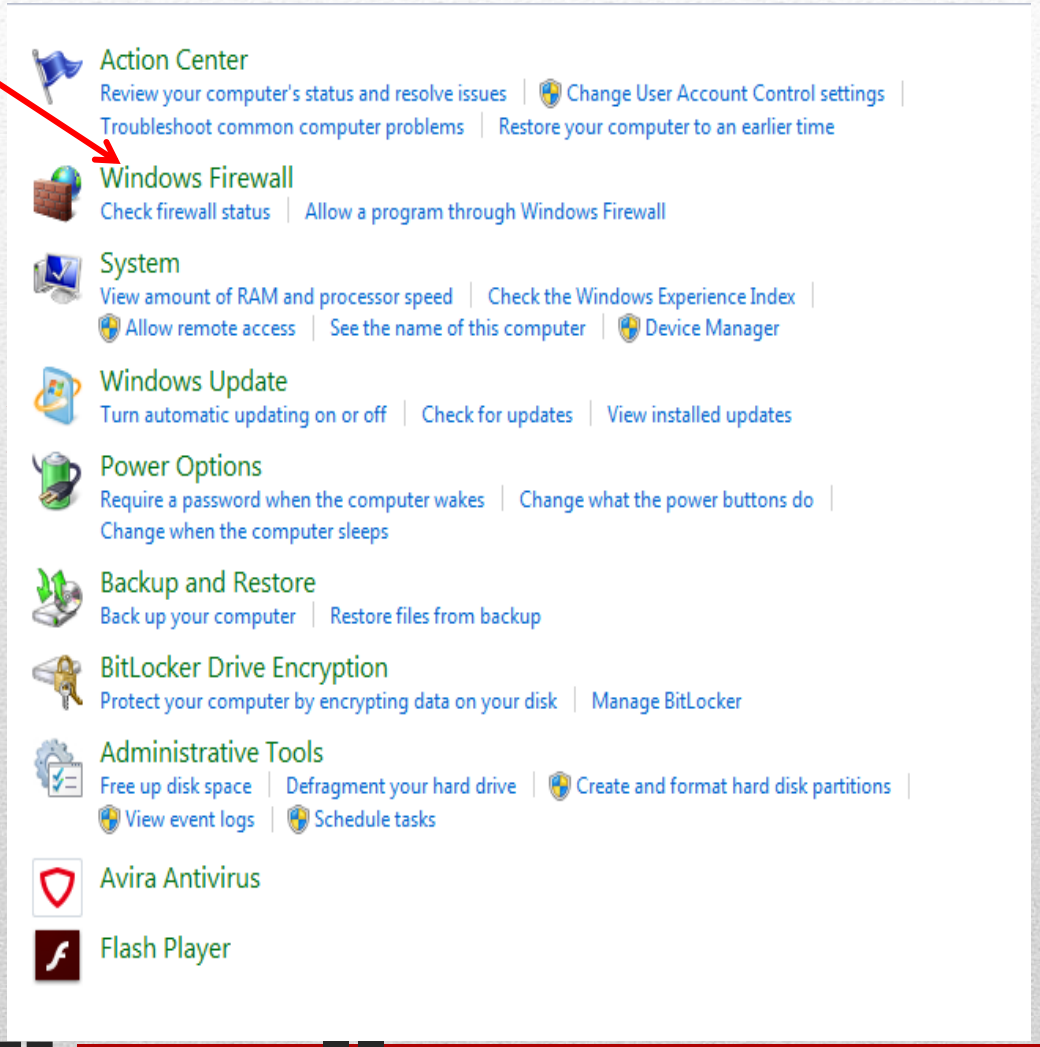
أولا من قائمة start أنقر على خيار control panel

كيفية تفعيل الجدار الناري على الاجهزة

كيفية تفعيل الجدار الناري على الاجهزة

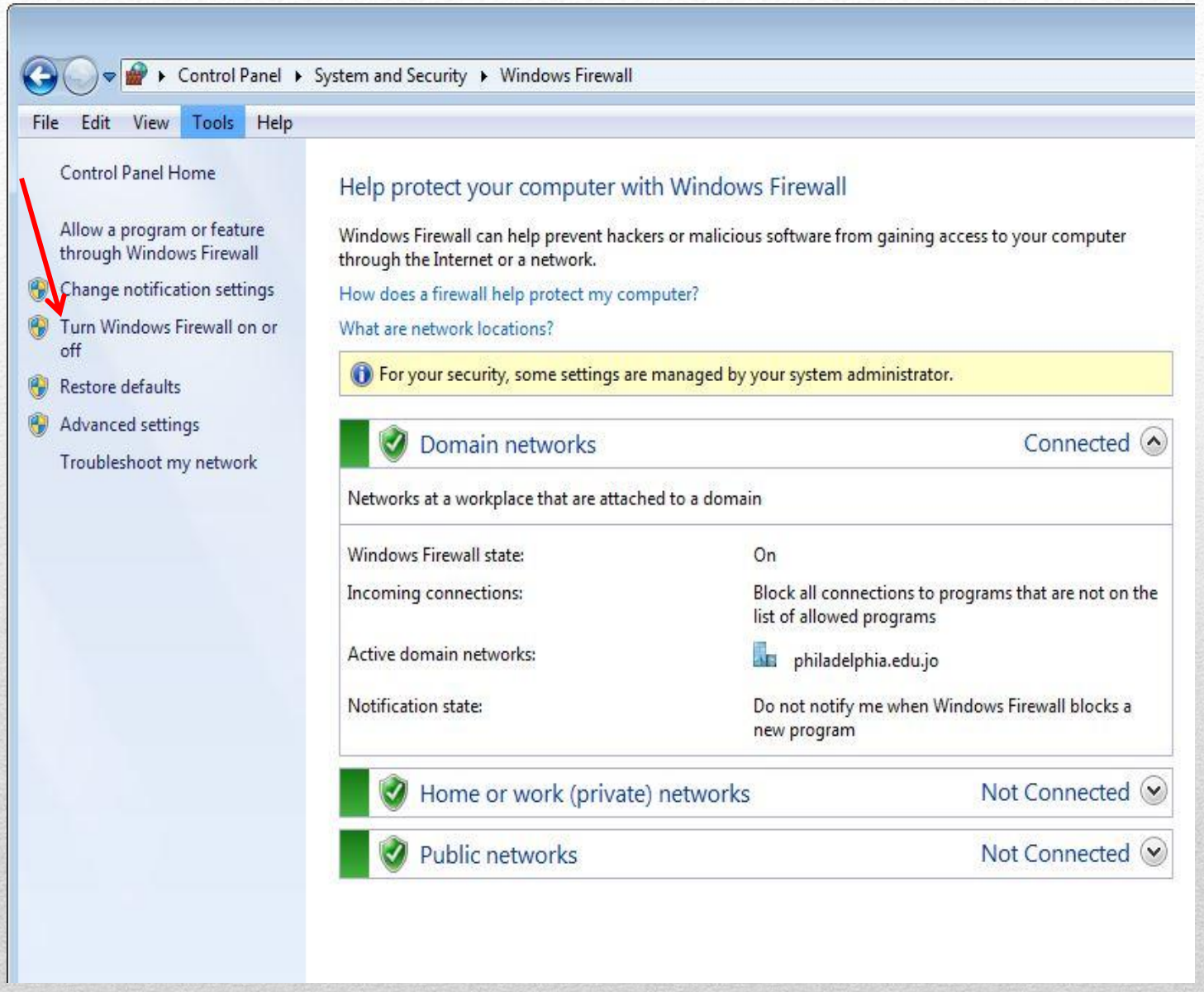


ثم النقر على خيار System and Security



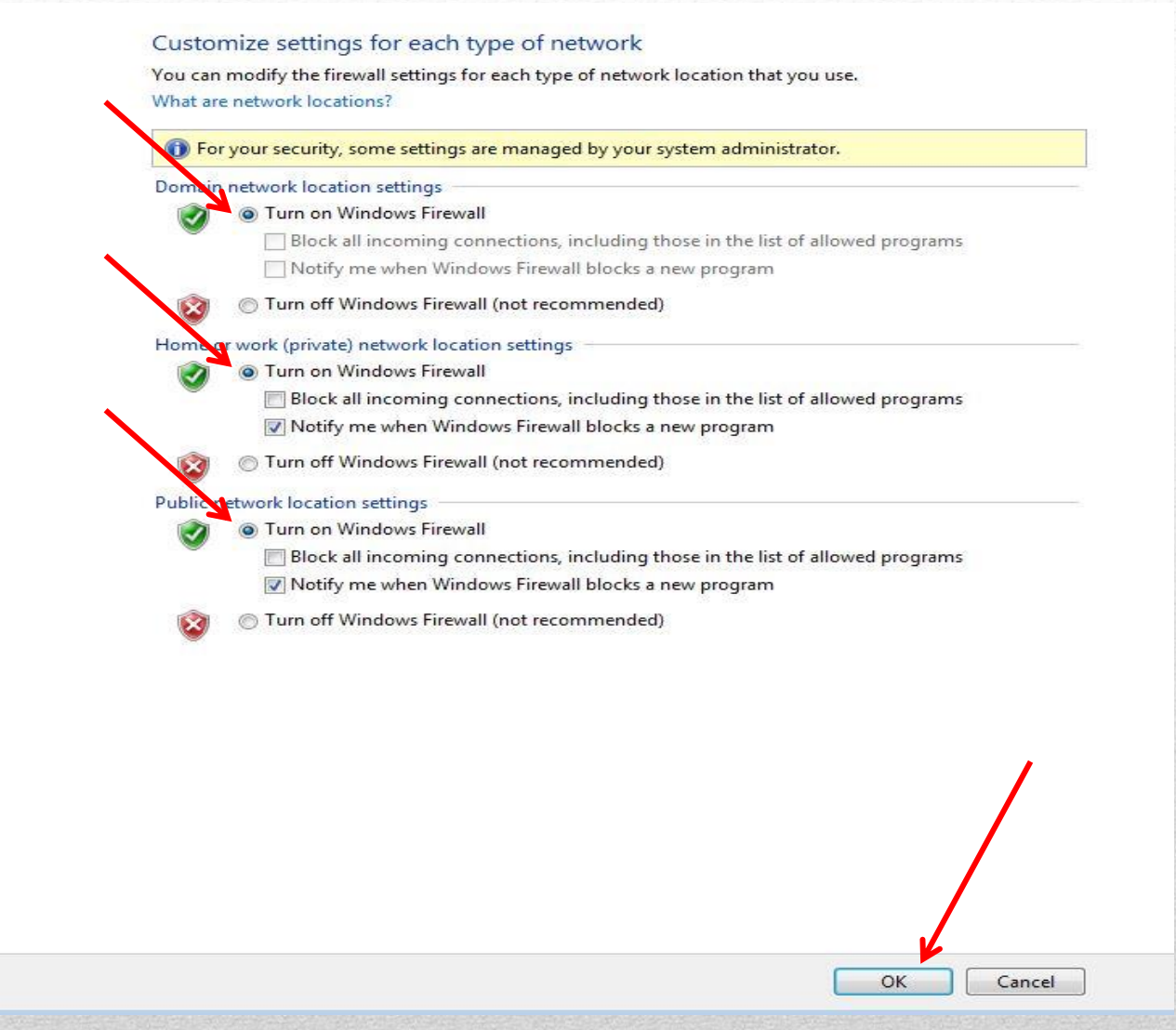
ثم النقر
على خيار
Windows
Firewall

Firewall



ثم النقر على خيار Turn Windows Firewall on or off

Firewall



ثم النقر على خيار Turn on Windows Firewall ثم النقر على Ok

Firewall

- # Homework

Why it's better to classify your data?

Next lecture

Type of Attacks

شكرا لاصغاءكم

جامعة الموصل /كلية التربية للعلوم الصرفة
قسم علوم الحاسوب

Fourth Class

DATA SECURITY

أستاذ المادة:
د. ثامر عبدالحافظ جرجيس

Lecture 5

Type of Attacks in computer system

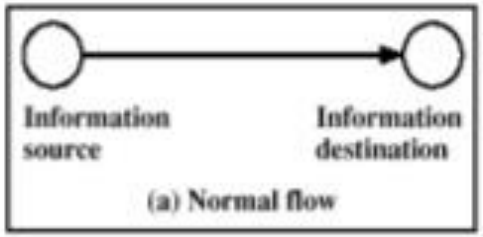
CONTENTS

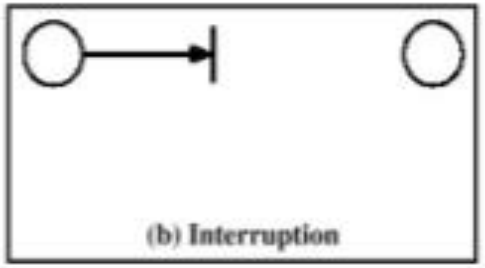
- Type of Attacks
  - Interception Attacks
    - Interruption Attacks
      - Modification Attacks
        - Fabrication Attacks
- Homework

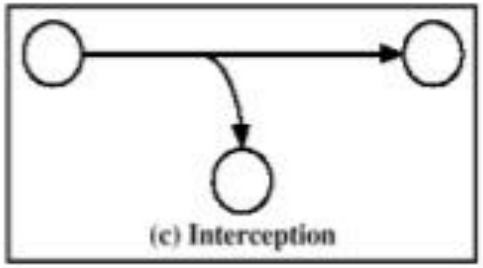
- *In computer networks and systems, **security attacks** are generally classified into two groups, namely active **attacks** and passive **attacks**. Passive **attacks** are used to obtain information from targeted computer networks and systems without affecting the systems.*

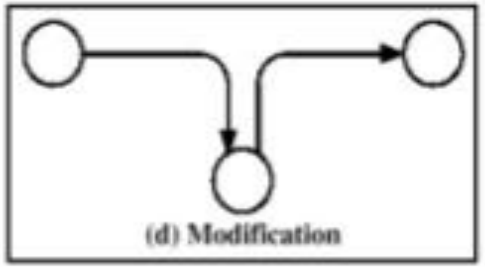
- ***Security Attacks***

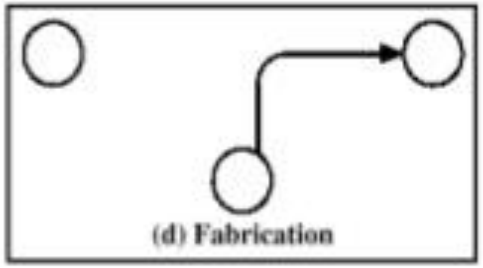
Type of Attacks in Computer Systems



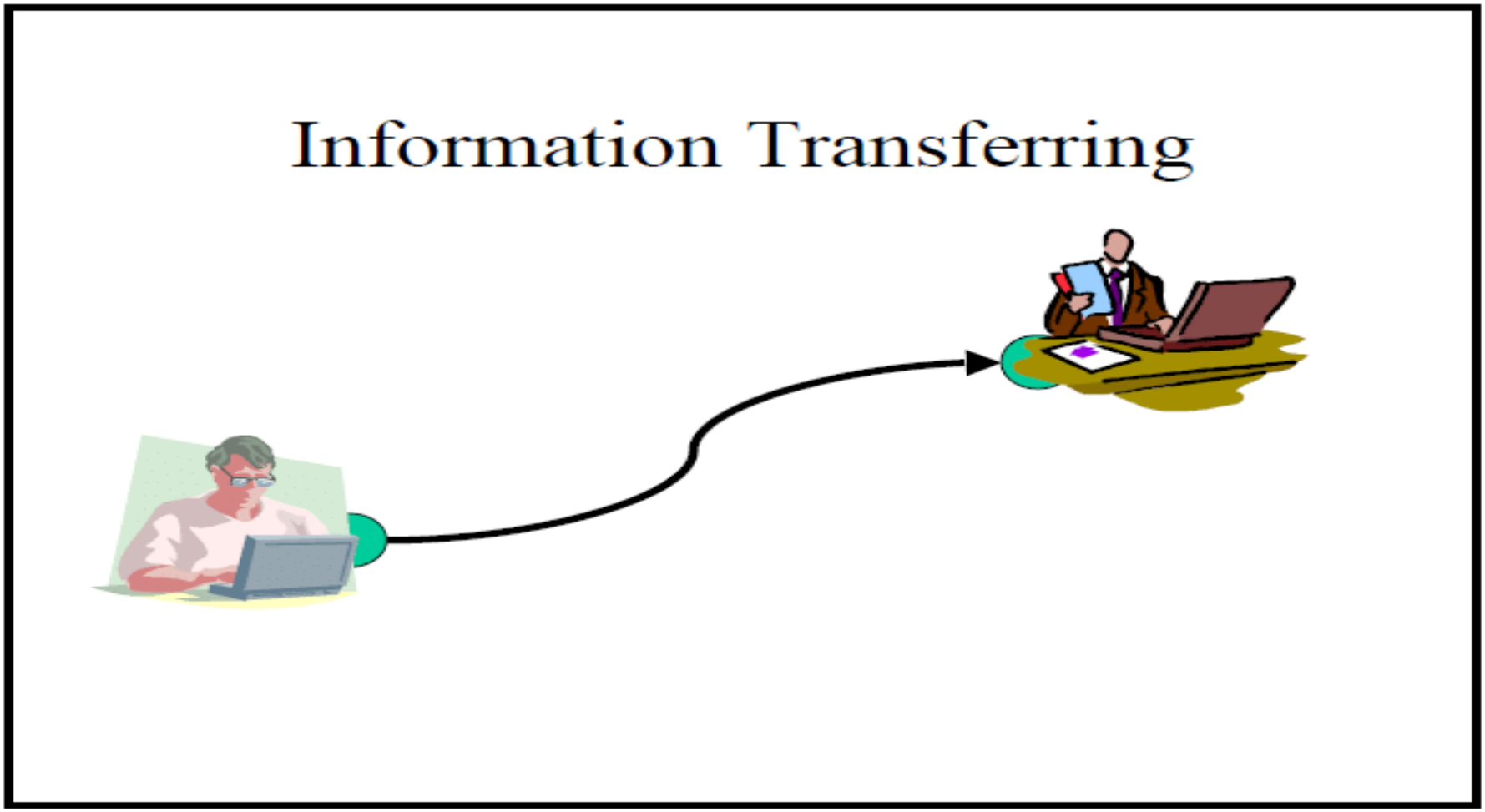








Normal Flow Information

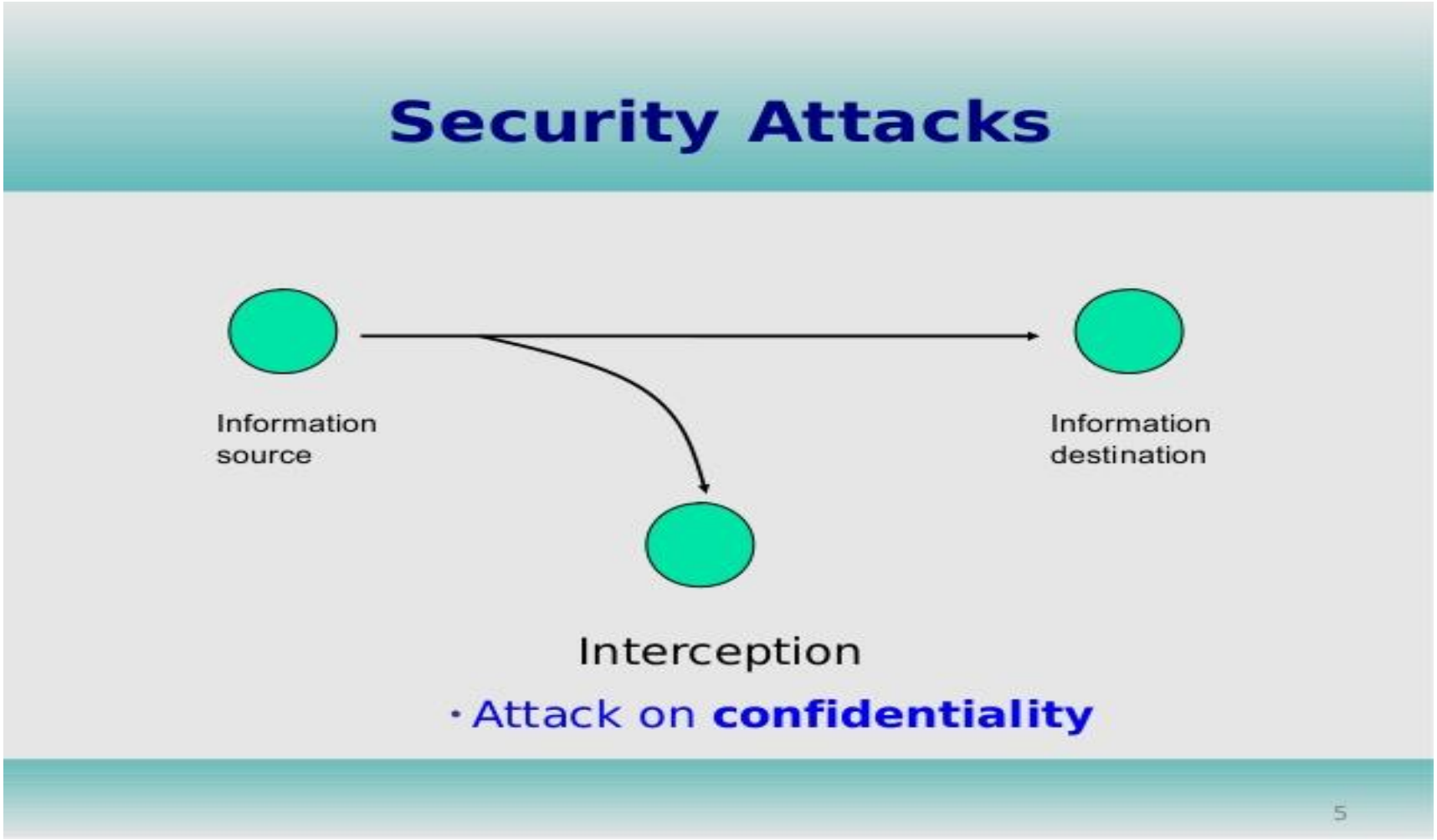


Interception Attacks

- *The attack affects the confidentiality*

- *The data or message which is sent by the sender is intercepted by an unauthorized individual where the message will be changed to the different form or it will be used by the individual for his malicious process.*

Interception Attacks

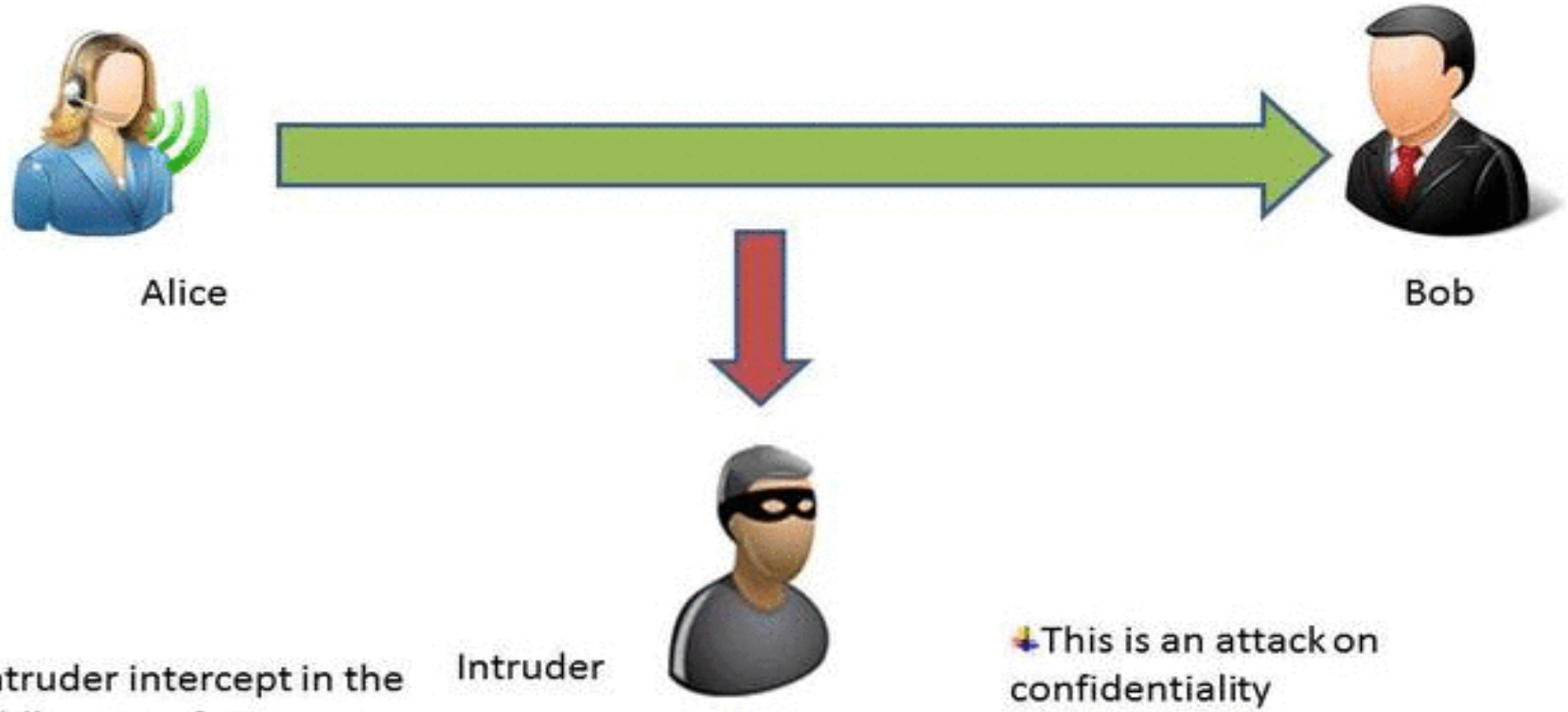


Examples

- ***Include wiretapping to capture data in a network, and the unlawful copying of files or program.***

Security Attacks...

Interception



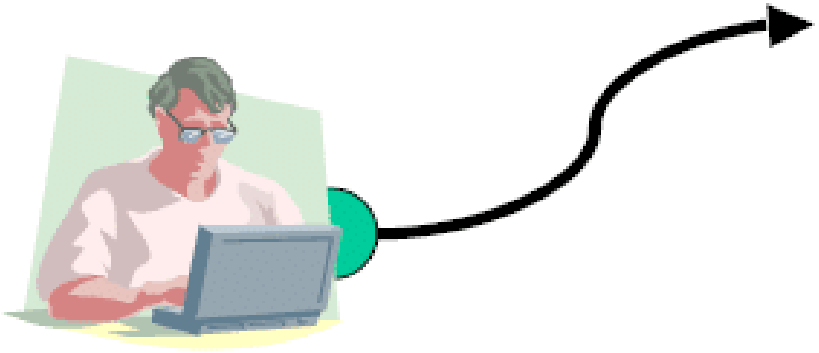
- Intruder intercept in the middle view of message
- This is an attack on confidentiality
- A passive intruder

Interruption Attacks

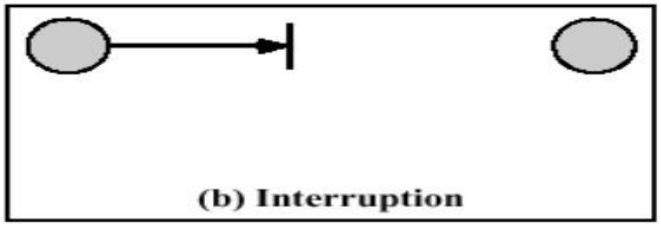
- ***The attack affects the Availability.***

- ***In an interruption attack, a network service is made degraded or unavailable for legitimate use.***

Attack: Interruption



Interruption



Examples

- ***destruction of a piece of hardware, such as a hard disk***
- ***the cutting of a communication***
- ***the disabling of the file management system.***

Security Attacks

Interruption

Alice

Bob

Intruder

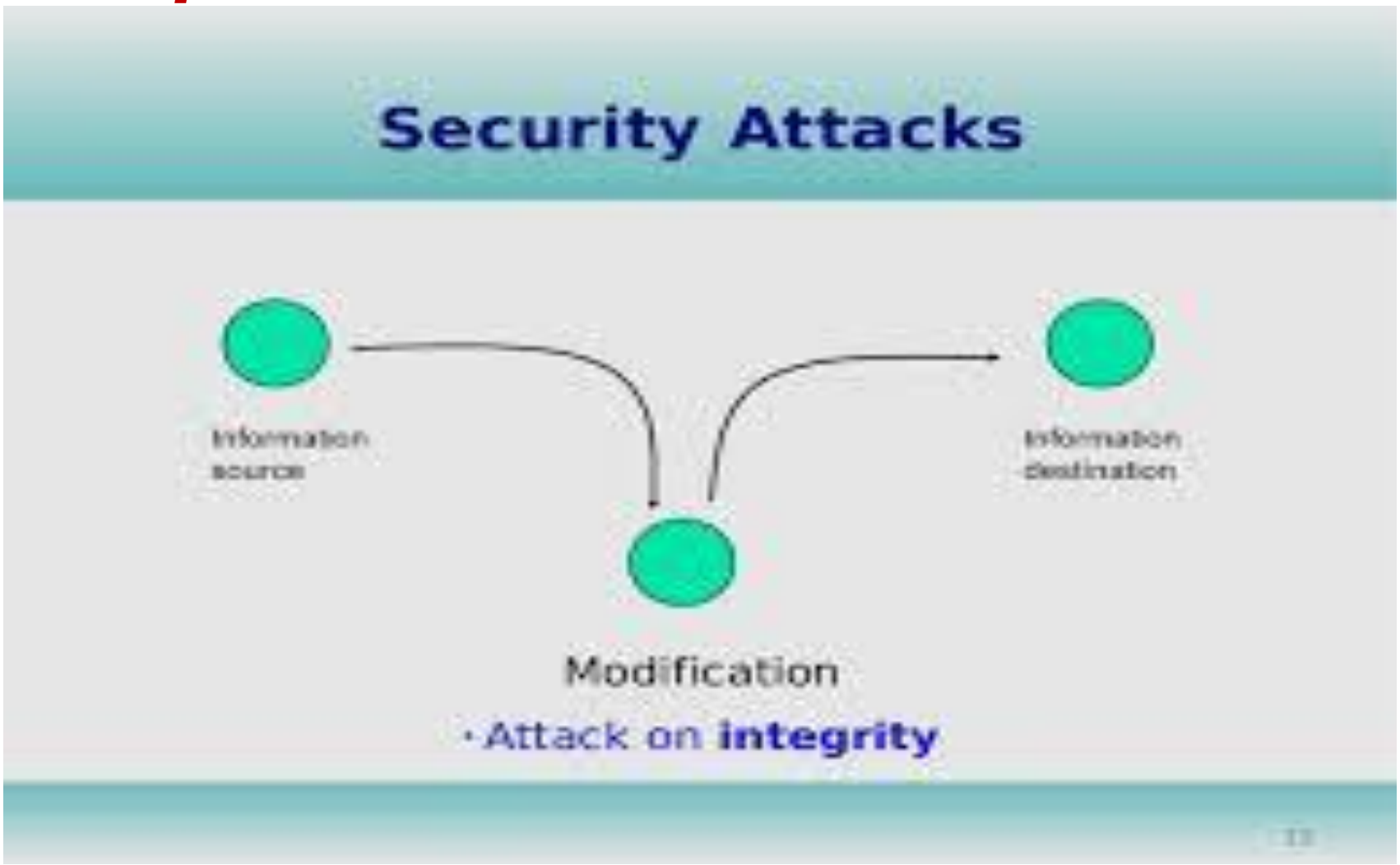
- Intruder intercept in the middle and stop communication
- This is an attack on availability
- An active intruder

Modification Attacks

- ***The attack affects the Integrity.***

- ***Modification attacks involve tampering with our information. Such attacks might primarily be considered an integrity attack but could also represent an availability attack. If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file.***

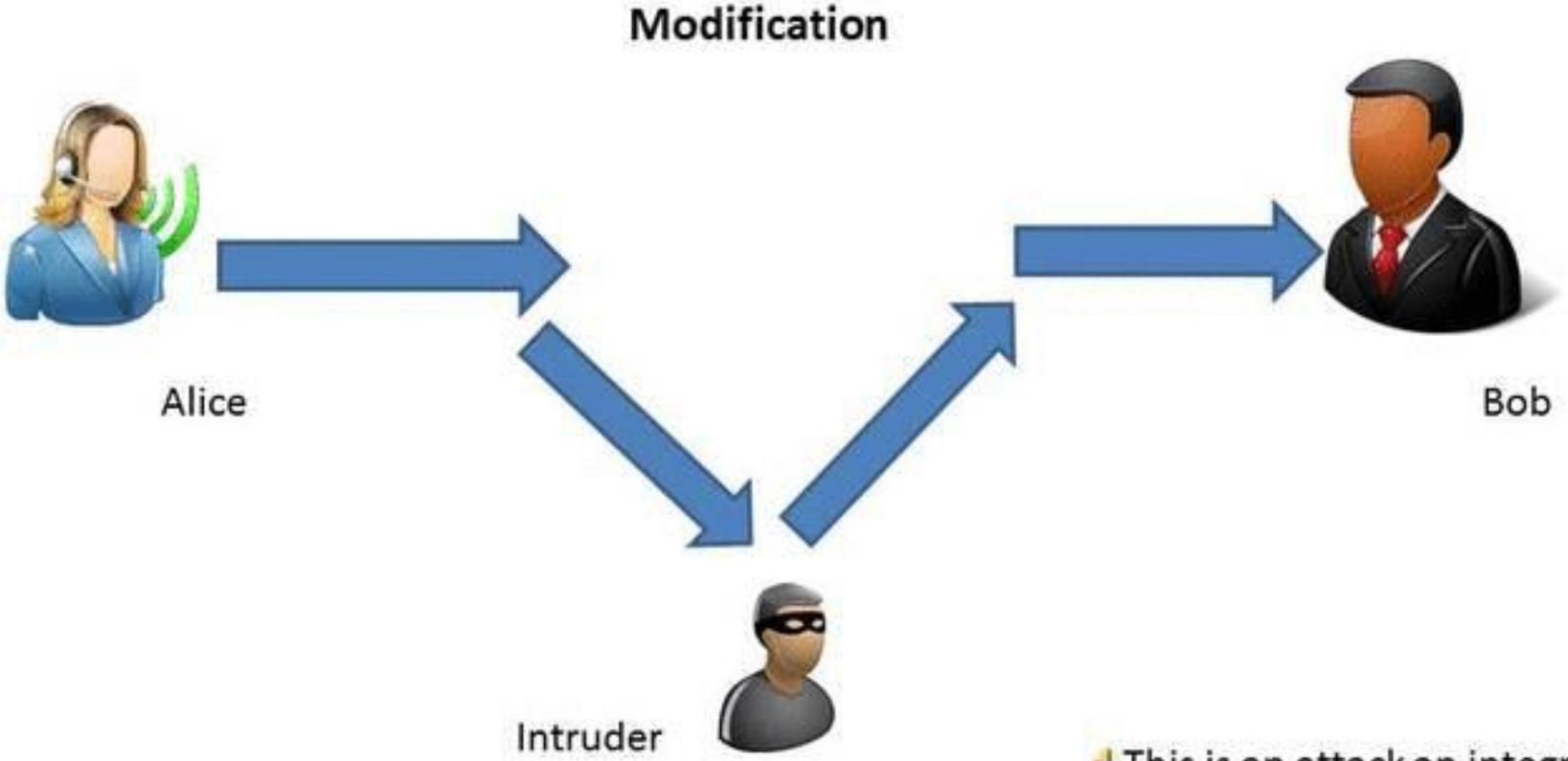
Modification Attacks



Examples

- ***Include changing values in a data file, altering a program so that it performs differently , and modifying the content of messages being transmitted in a network.***

Security Attacks....



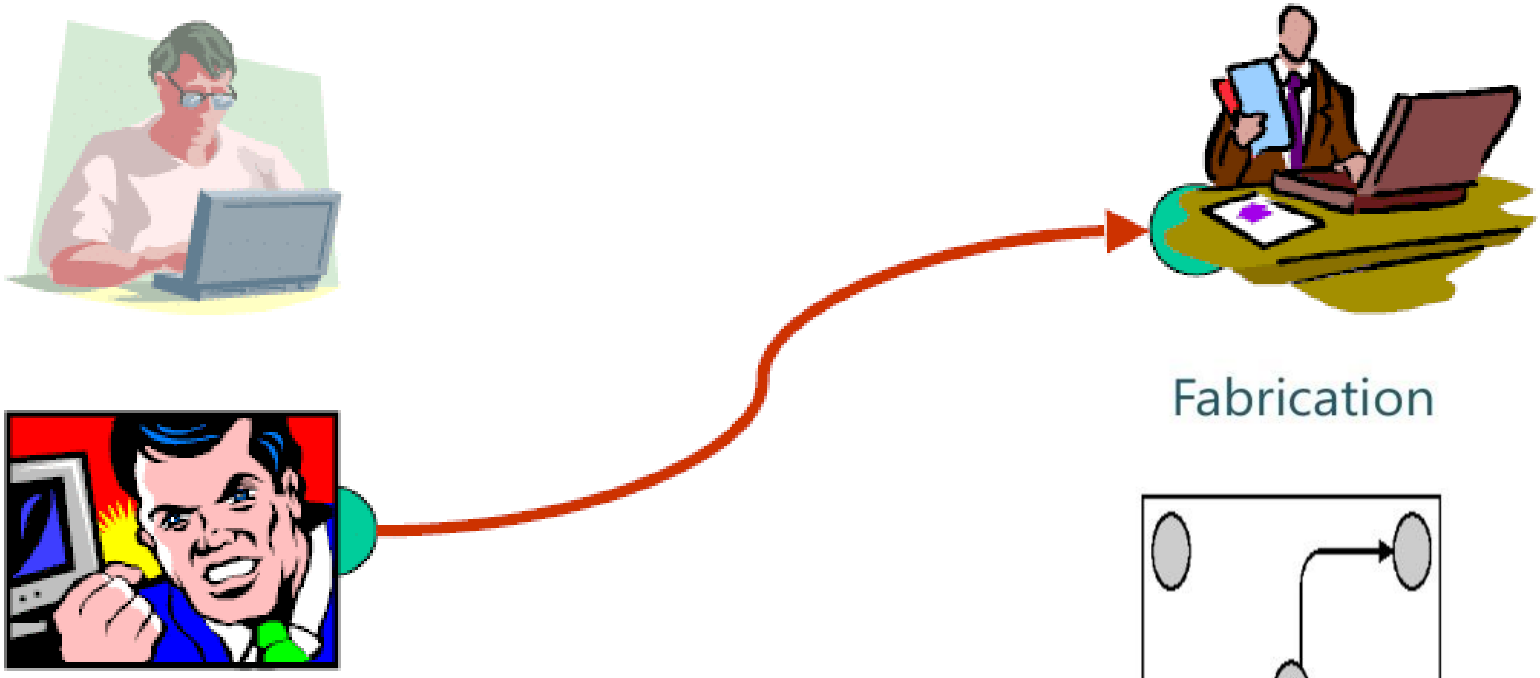
- Intruder intercept in the middle & modify the message
- This is an attack on integrity
- An active intruder

Fabrication Attacks

- ***The attack affects the Authentication.***

- ***Fabrication: In this type of attack a fake message is inserted into the network by an unauthorized user as if it is a valid user. This results in the loss of confidentiality, authenticity and integrity of the message.***

Attack: Fabrication



Fabrication

Examples

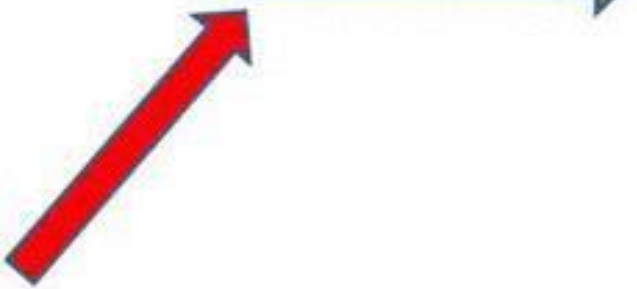
- ***Include the insertion of spurious messages in a network or the addition of records to a file.***

Security Attacks...

Fabrication

Alice

Bob



Fabricated message

Intruder

- Intruder fabricate a message and send impersonating the sender
- This is an attack on authenticity
- An active intruder

- Homework

What is the risk and what are its types?

Next lecture

Networking Simple Principle

شكرا

لكم

جامعة الموصل /كلية التربية للعلوم الصرفة

قسم علوم الحاسوب

Fourth Class

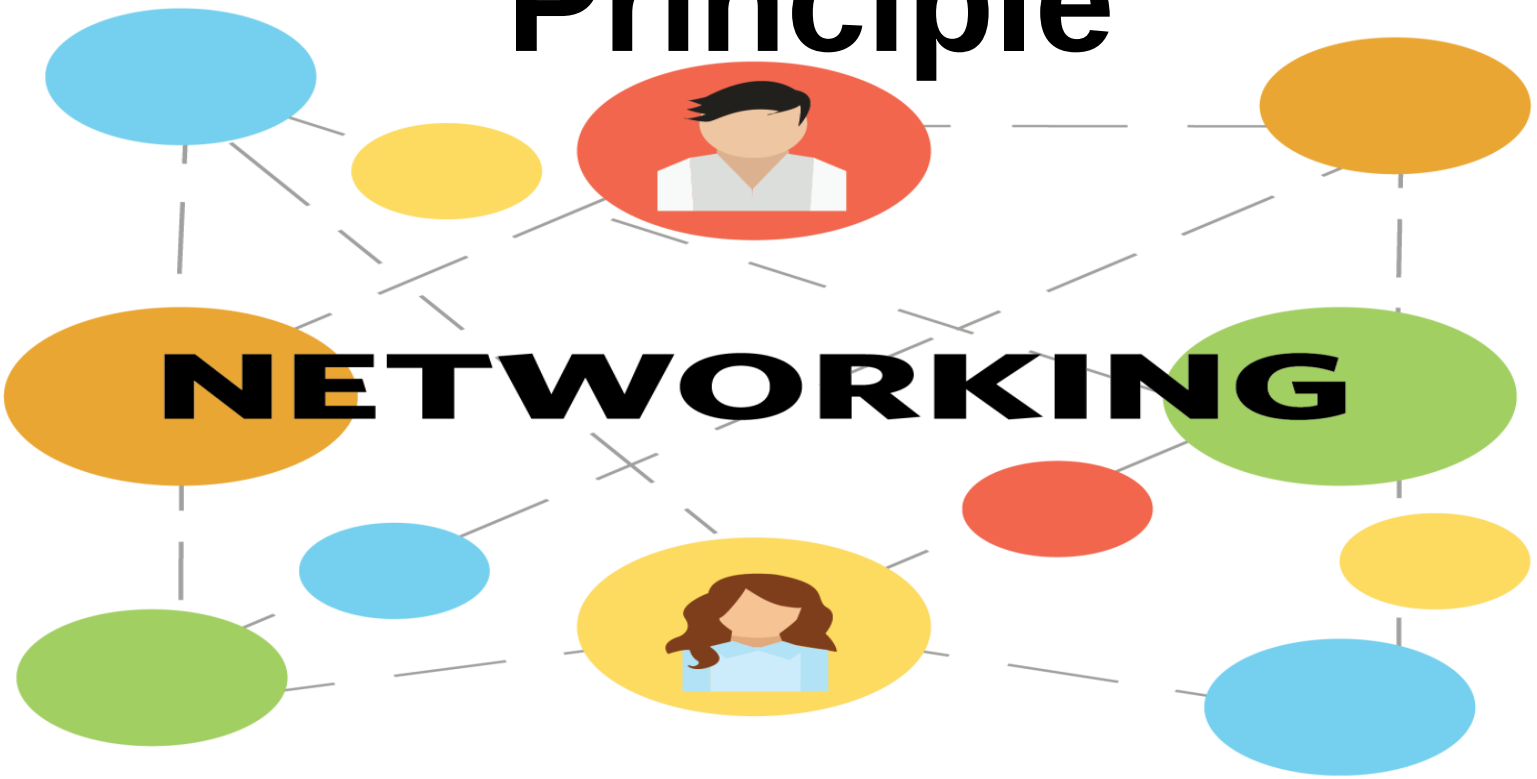
Data Security

أستاذ المادة:

د. ثامر عبدالحافظ جرجيس

Lecture 6

Networking Simple Principle



CONTENTS

What Is Networking?

- ***Networking is the exchange of information and ideas among people with a common profession or special interest***

- *The term **computer networking** refers to linking multiple devices so that they can readily share information and software resources.*

Networking principle

- Good network design should create a user experience that the network is transparent, resilient and ubiquitous, with the right balance of quality, speed, security, control and cost. These principles help designers deliver this experience for their users when designing networks.

APPLICATIONS:

- Sharing of resources such as printers
- Sharing of expensive software's and database
- Communication from one computer to another computer
- Exchange of data and information among users via network
- Sharing of information over geographically wide areas.

COMPONENTS OF COMPUTER NETWORK

- Two or more computers
- Cables as links between the computers
- A network interfacing card(NIC) on each computer
- Switches
- Software called operating system(OS)

NETWORK BENEFITS

- The network provided to the users can be divided into two categories:
- i. Sharing
- ii. Connectivity

BENEFITS OF COMPUTER NETWORK

- o Increased speed
- o Improved security
- o Electronic mail
- o Reduced cost
- o Centralized software managements
- o Flexible access

DISDAVATAGES OF NETWORKS

- o High cost of installation
- o Requires time for administration
- o Failure of server
- o Cable faults

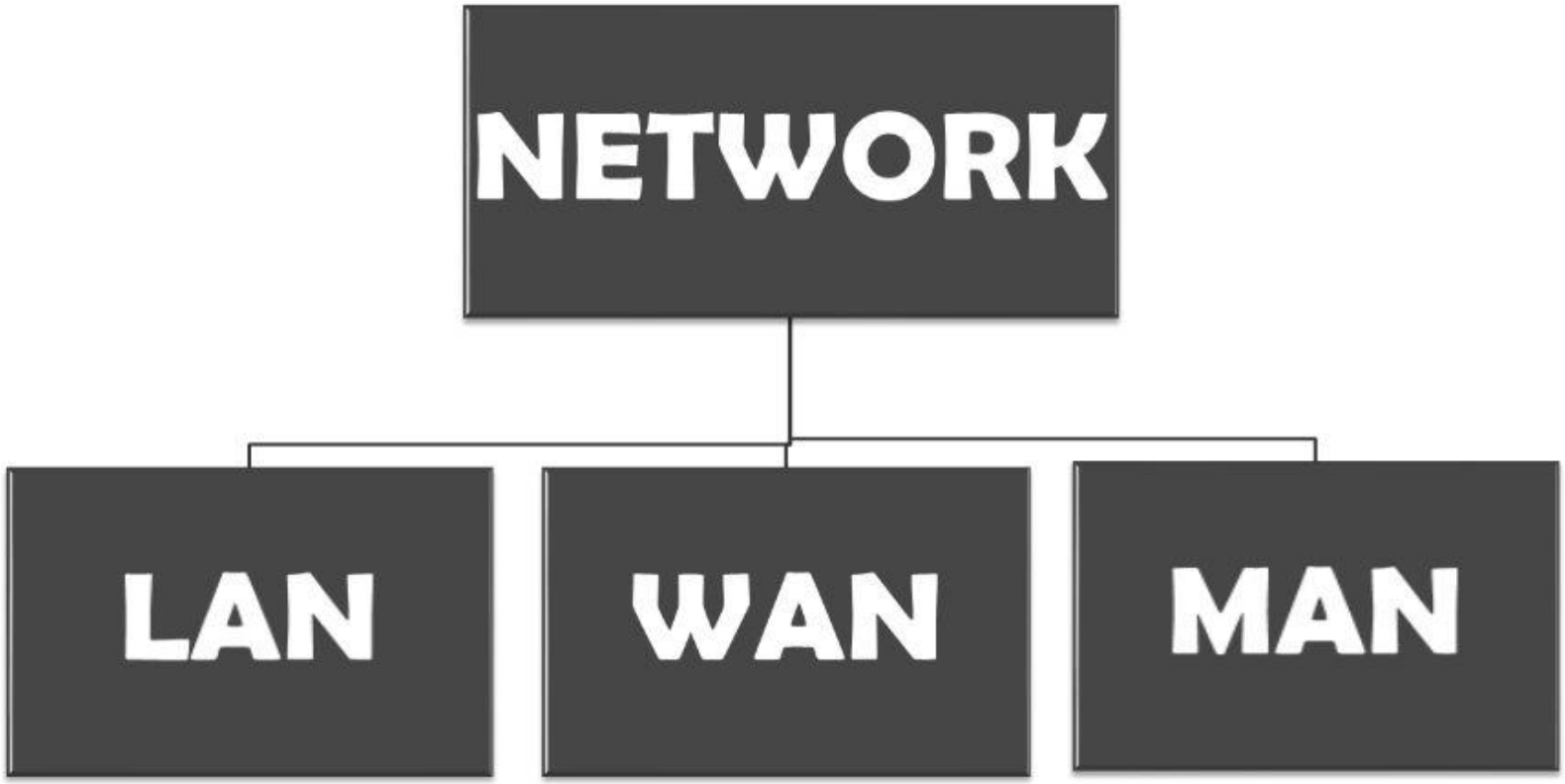
SHARING RESOURCES

Types of resources are:

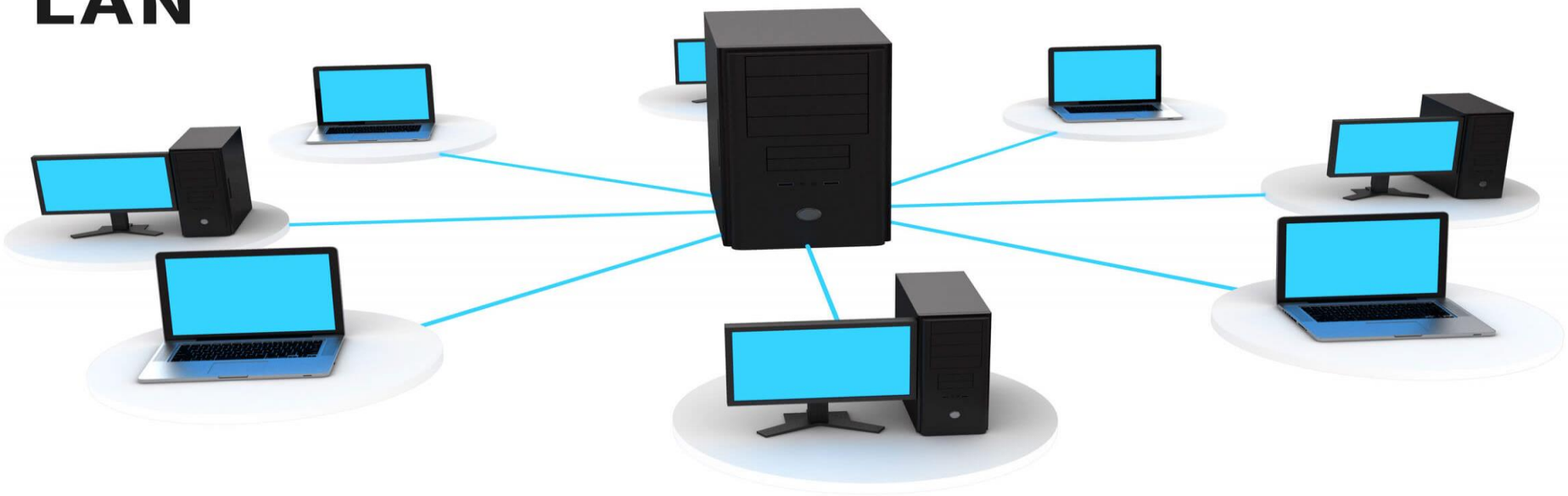
- 1. **Hardware:** A network allows users to share many hardware devices such as printers , modems, fax machines, CD ROM, players, etc.

- 2. **Software:** sharing software resources reduces the cost of software installation, saves space on hard disk.

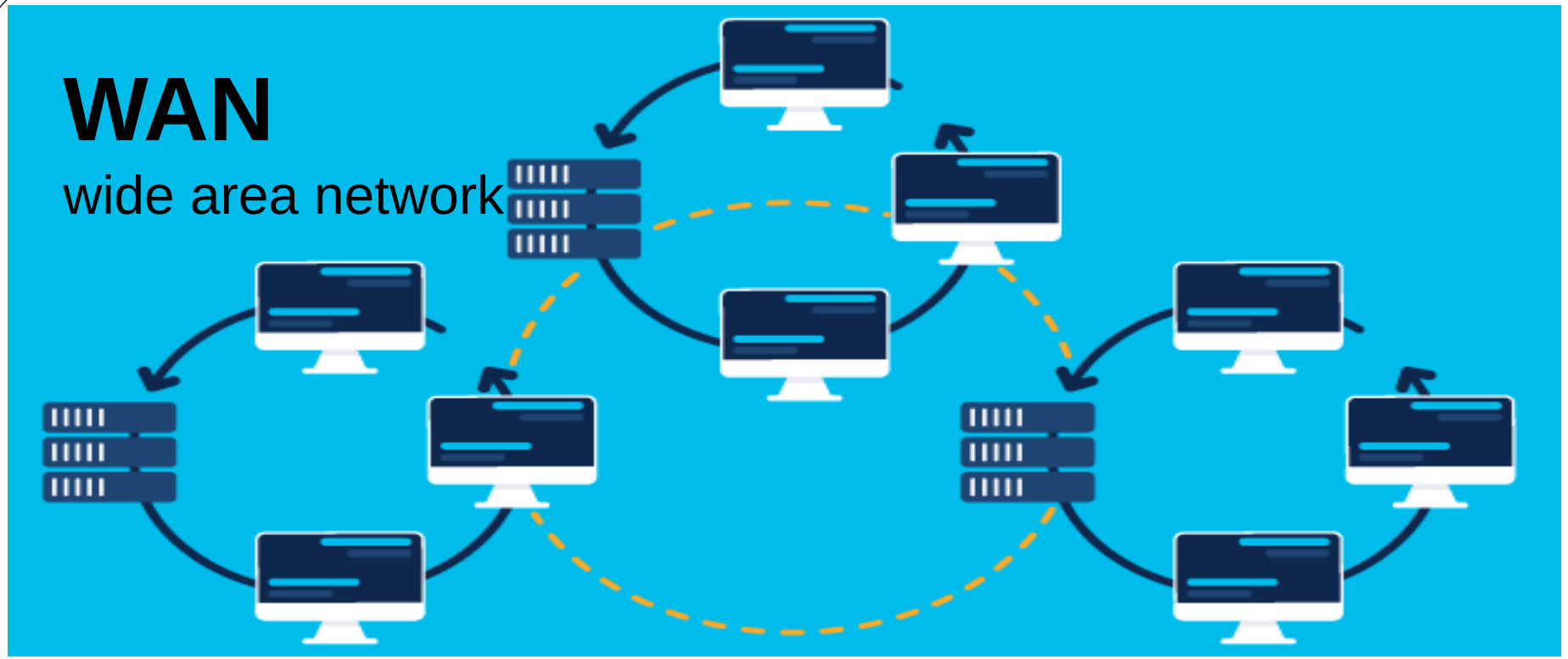
CLASSIFICATION OF AREA BY THEIR GEOGRAPHY



LAN



- **LAN is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings.**
- **In LAN all machines are connected to a single cable.**
- **Exchange of information and sharing of resources becomes easy because of LAN.**
- **It is usually a privately owned network.**



- When network spans over a large distance or when the computers to be connected to each other are at widely separated locations . A wide area network(WAN) is installed.

- Most WAN networks are used to transfer large blocks of data between its users.

MAN
METROPOLITAN AREA NETWORK

- It is in between LAN & WAN technology that covers the entire city.
- It uses similar technology as LAN.
- It can be a measure of connecting a number of LAN’s or a large network so that resources can be shared LAN to LAN as well as device to device.

Next lecture

Steps to Better Security

THANKS FOR YOUR LISTENING!

جامعة الموصل /كلية التربية للعلوم الصرفة

قسم علوم الحاسوب

Fourth Class

Data Security

أستاذ المادة:

د. ثامر عبدالحافظ جرجيس

Lecture 7

- **Steps to Better Security**

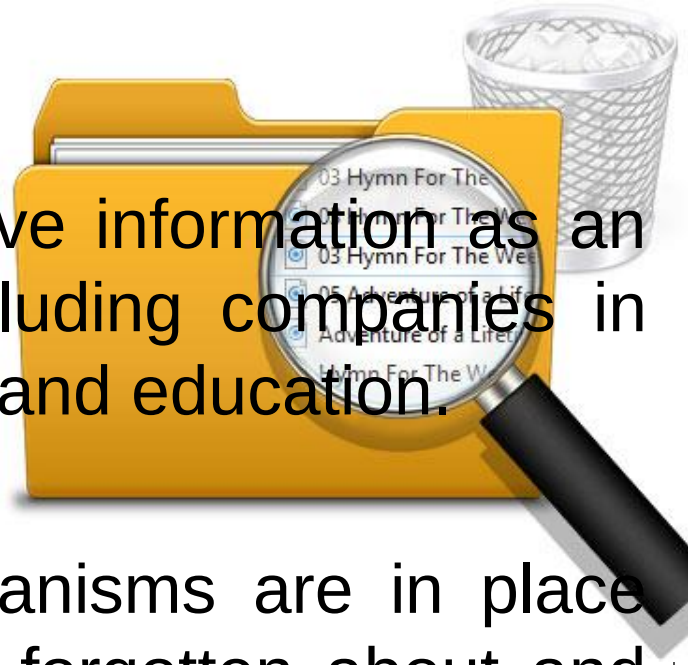
CONTENTS

- **Steps to Better Security**
  - **Encrypt all devices**
  - **Delete redundant data**
  - **Update your programs regularly**
  - **Back-up your data regularly**
  - **Establish strong passwords**
- **Security best practices**
- **Homework**

Encrypt all devices

- In today's world, more and more people are choosing to work on mobile or personal devices. How can you ensure that these devices are trustworthy?
- Make sure that all data is stored in an encrypted format and remains encrypted during migrations.

Delete redundant data



- Many organizations deal with sensitive information as an essential part of their business; including companies in healthcare, finance, the public sector and education.

- Ensuring information disposal mechanisms are in place helps prevent stale data from being forgotten about and stolen at a later date.

- Having a system for shredding, erasing or otherwise modifying redundant data to be indecipherable will go a long way to ensuring your employees don’t stash it away.

Establish strong passwords

- Many organizations are still employing relaxed password policies, leading to simple, generic and easy-to-hack passwords for critical accounts, which have access to the sensitive and valuable data.

- Implementing strong passwords is the first step you can take to strengthen your security in this area. Use reasonably complex passwords and change them at least every 90 days. Never use passwords like “12345” or “Admin1”.

- Don’t ever write down your passwords and leave them on your workstation for other people to find.

- **Back-up your data regularly**

- This should already be a critical part of your IT security strategy.

- With secure backups in place, you can survive everything .

- As a security best practice, backup data should be stored in a secure, remote location away from your primary place of business.

- **Update your programs regularly**

- **Make sure your computer is properly patched and updated. This is often the best way to ensure its adequately protected.**
- **Your security applications are only as good as their most recent update.**
- **Since hackers are constantly adapting to exploit weaknesses in earlier software versions, it is advisable to update these applications regularly.**

Security best practices

- Protect your data. ...
- Avoid pop-ups, unknown emails, and links. ...
- Use strong password protection and authentication. ...
- Connect to secure Wi-Fi. ...
- Enable firewall protection at work and at home. ...
- Invest in security systems. ...
- Install security software updates and back up your files. ...

Homework

Steps to Better Security


thank
you

جامعة الموصل /كلية التربية للعلوم الصرفة

قسم علوم الحاسوب

Fourth Class

Data Security

أستاذ المادة:

د. ثامر عبدالحافظ جرجيس

Lecture 8

- **Steps to Better Security**

CONTENTS

- Steps to Better Security
  - Encrypt all devices
  - Delete redundant data
  - Update your programs regularly
  - Back-up your data regularly
  - Establish strong passwords
- Steps to Better Security
  - Use Network Drives for Sensitive or Important Files
  - Do Not Let Another Person Use Your User Account
  - Malware prevention
  - User education and awareness
  - Review your privacy settings

- **Use Network Drives for Sensitive or Important Files**

- *All files that contain sensitive information, or that are critical to the work should be stored on a network drive – but only as long as they are needed.*

- **Do Not Let Another Person Use Your User Account**

- *Your user account represents all the computing resources that you personally have been authorized to access.*

- *By letting someone else use your user account, you are letting them access resources for which they may not have approval. Anything that they may do will, ultimately, be your responsibility.*

- **Malware prevention**

- *There are many ways malware can infect an organization's systems. It could be sent in an email attachment, worm through a vulnerability or be plugged into an office computer via a removable device.*

- *To mitigate these risks, organizations should implement anti-malware software and policies designed to help prevent employees from falling victim.*

- **User education and awareness**

- *Employees play an essential role in their organization's security practices, so they need to be taught their responsibilities and shown what they can do to prevent data breaches.*

- *Training can come in many forms, from introductory e-learning to classroom-based certification courses. It’s up to you to decide which level of training is appropriate for your employees.*

- **Review your privacy settings**

- *Review the settings on social networks and sharing sites to make sure your are sharing your data with whom you intend to.*

Thank you

جامعة الموصل /كلية التربية للعلوم الصرفة

قسم علوم الحاسوب

Fourth Class

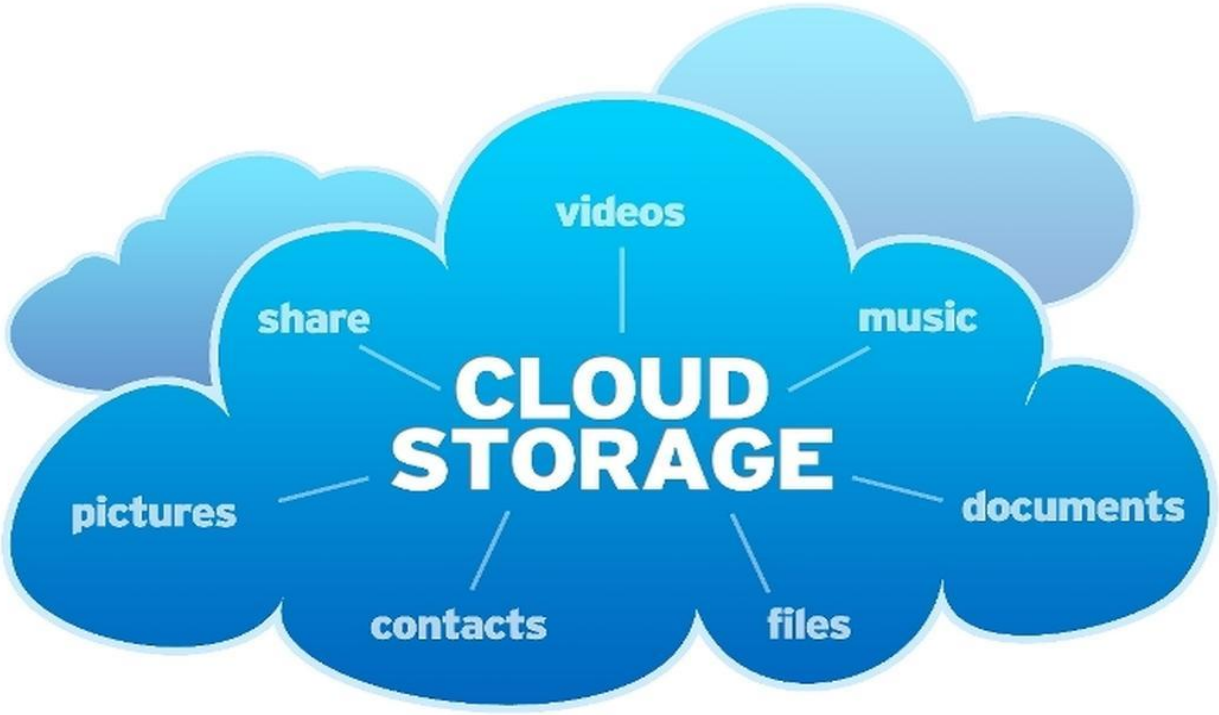
Data Security

أستاذ المادة:

د. ثامر عبدالحافظ جرجيس

Lecture 9

- **Cloud Storage**



CONTENTS

- **What is cloud storage?**
- **local data storage Vs. *Cloud storage***
- **Commonly used platforms**
- **Basic Features**
- **What are the limitations?**
- **Advantages of cloud storage**
- **cloud storage – business benefits**

What is cloud storage?

Cloud storage is a model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers , and the physical environment is typically owned and managed by a hosting company

Data (or files) are said to be stored in the cloud when they are saved on a remote server, which is easily accessible from anywhere with internet access. This allows access to the data from any device connected to the internet, including computers, tablets and smartphones

- **local data storage Vs *Cloud storage***

- *In local data storage, where data is stored on the hard drive of a local desktop or a laptop*

- *Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network (typically the Internet).*

- **Commonly used platforms**

Google Drive

Dropbox

iCloud

amazon cloud drive

Google Drive

- This is a ‘pure’ cloud computing service, with all the apps and storage found online. You can use it via desktop computers, tablets like the iPad or on smartphones.

- All of Google's services could be considered cloud computing really: Gmail, Google Calendar, Google Reader, Google Voice, and so on.

- Microsoft’s One Drive is very similar to Google Drive and offers much the same services.

- **Dropbox**

- *Commonly used by staff to store their documents and images. You might set your phone to automatically send all pictures you take with it into your Dropbox account, so that even if you lose your phone, the pictures will still be available to you up in space; you might use it to access your documents at home, and then save changes to it.*

Apple iCloud

- Apple's cloud service is primarily used by Apple users for online storage and synchronization of their mail, contacts, calendar, and more.

- if you make a change to a document, say, on one of your devices, it will automatically update it so that when you next access it.

- If you have loads of data up there (perhaps pictures or films you have made) then you will need to pay for extra storage – as indeed you do for all of these services

Common Features

- *A three platforms are third party services.*
- *All offer a basic amount of free storage:*

– *Dropbox: 5 GB*

– *OneDrive (linked to Microsoft live account): 7 GB*

– *Google Drive (linked to Gmail account): 15 GB*

- *After that, the user has to pay a yearly or monthly subscription fee.*

Basic Features

- All platforms can easily be accessed via a web browser.
- All also offer apps for ease of access from a smartphone or tablet.
- All three feature a directory structure similar to that of a computer drive; this facilitates navigation and organization

- **Additional Features**

- Online editing: OneDrive and Google Drive
- offer the possibility of editing documents inside a web browser.
- No additional software is needed.
- Folders or specific files can be shared with others; this facilitates collaboration.

- **What are the limitations?**

- Limited storage.

- Many colleagues are unwilling to pay for a service they need for

- work, and the amount of free storage with all of these providers is limited.

Advantages of cloud storage

- Usability
- Bandwidth
- Accessibility
- Disaster Recovery
- Cost Savings

cloud storage – business benefits

- There's no need for CDs, external hard drives, or localized servers.
- Data is quickly and automatically updated in the cloud and available for your retrieval whenever you need it.
- Should your office become the victim of a burglary, fire, or natural disaster, your data is safe and secure in the cloud, even if your physical assets are destroyed.

cloud storage – business benefits

- One of the greatest benefits of cloud storage is its ability to grow with its users.

- With no need for physical, on-site storage space, you can have a smaller workspace, less equipment to buy

- **Next lecture**

  Encryption

Thank you

جامعة الموصل /كلية التربية للعلوم الصرفة
قسم علوم الحاسوب

Fourth Class

DATA SECURITY

أستاذ المادة:
د. ثامر عبدالحافظ جرجيس

Lecture 10

- **Encryption**

CONTENTS

- **Basic classification of encryption**
- **Symmetric-key or (or secret-key)**
- **Asymmetric (or public-key)**
- **The key**
- **The General Requirements of Cryptosystem**
- **Components of a Cryptosystem**
- **Basic Cryptographic Algorithms**

Basic classification of encryption key-based algorithms

- Symmetric-key or (or secret-key)
- Asymmetric (or public-key)

Symmetric-key or (or secret-key)

- ***Symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key)***

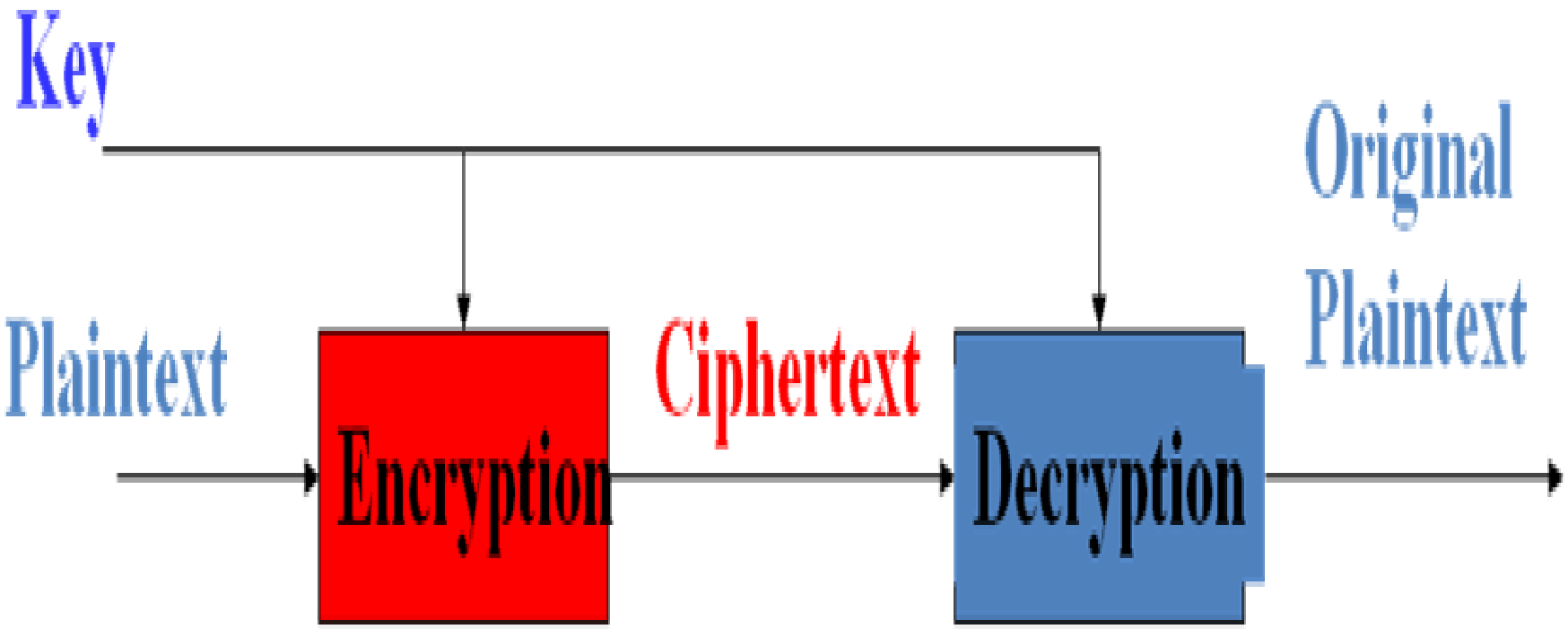
Symmetric-key or (or secret-key)

- **two main types:**

- **stream ciphers** – operate on individual characters of the plaintext

- **block ciphers** – process the plaintext in larger blocks of characters

Symmetric Encryption



Asymmetric (or public-key)

- algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key.

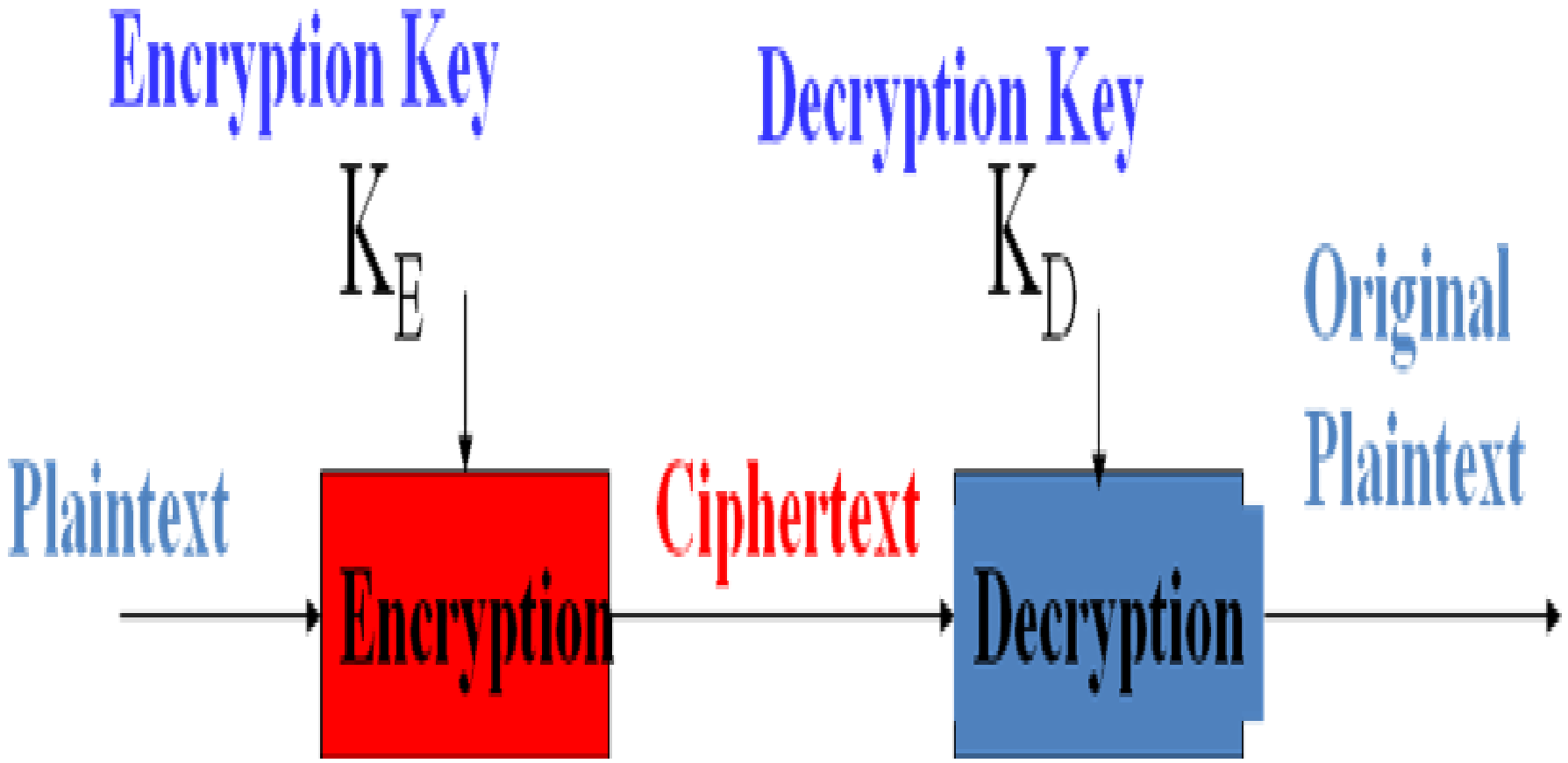
- permit the encryption key to be public (it can even be published in a newspaper), allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message.

The key

- ***The encryption key is also called the public key***

- ***The decryption key the private key or secret key.***

Asymmetric Encryption



The General Requirements of Cryptosystem

- ***Cryptosystem must satisfy three general requirements:***

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

- 2) The system must be easy to use.

- 3) The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithms Encryption or Decryption.

Components of a Cryptosystem

- The various components of a basic cryptosystem are as follows : -

- **Plaintext.** It is the data to be protected during transmission.

Encryption Algorithm

- It *is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.*

Ciphertext

- *It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.*

Decryption Algorithm

- *It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.*

Encryption Key & Decryption Key

- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.

Encryption Key & Decryption Key

- **Decryption Key** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

- For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

Basic Cryptographic Algorithms

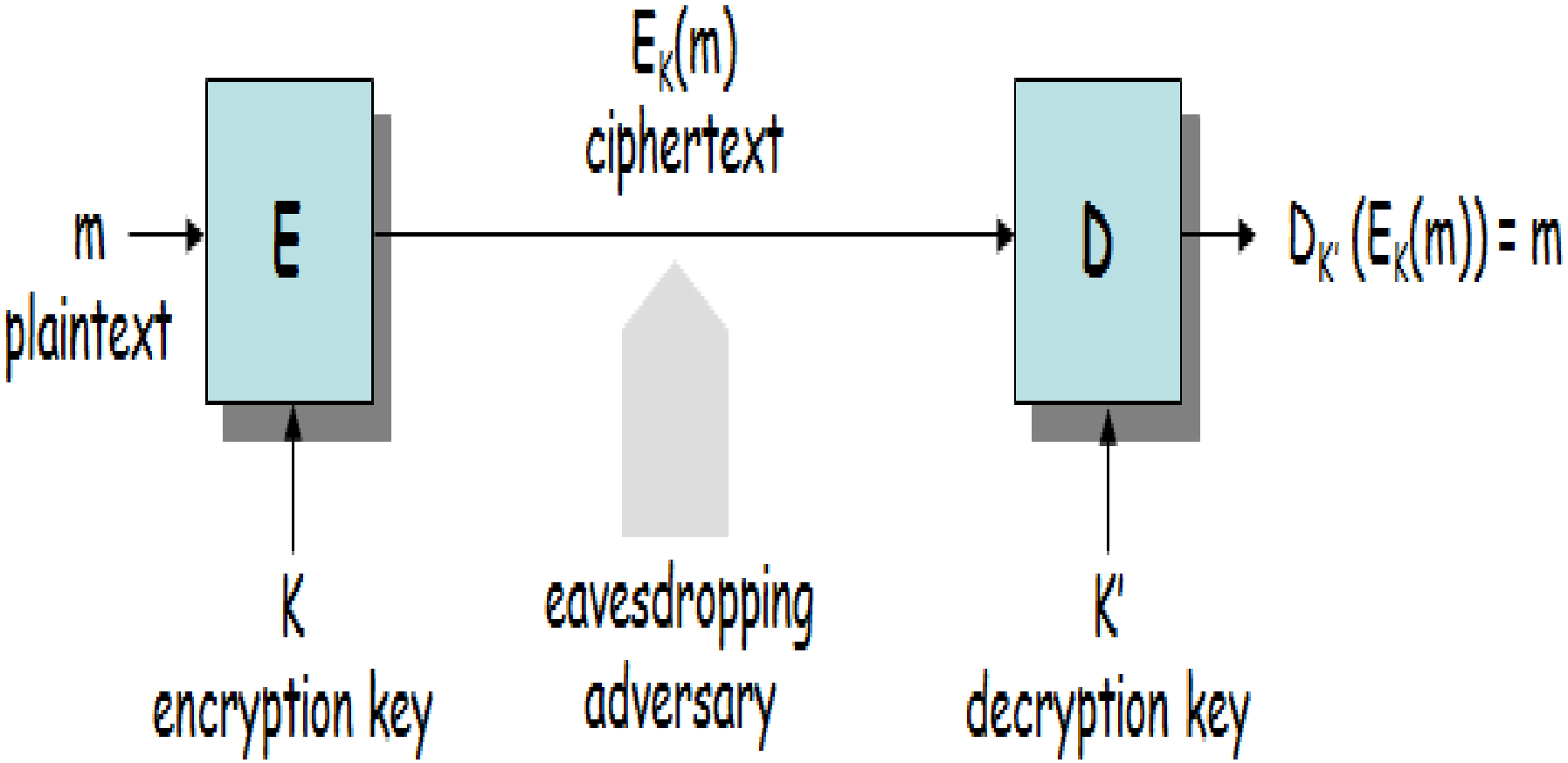
- A **cipher** is the method of encryption and decryption.
- Some cryptographic methods rely on the secrecy of the algorithms.
- **Keyless Cipher** is a cipher that does not require the use of a key.

Basic Cryptographic Algorithms

- All modern algorithms use a **key** to control encryption and decryption; a message can be decrypted only if the key matches the encryption key.

- The key used for decryption can be different from the encryption key, but for most algorithms they are the same.

Classical model of encryption



Thank you

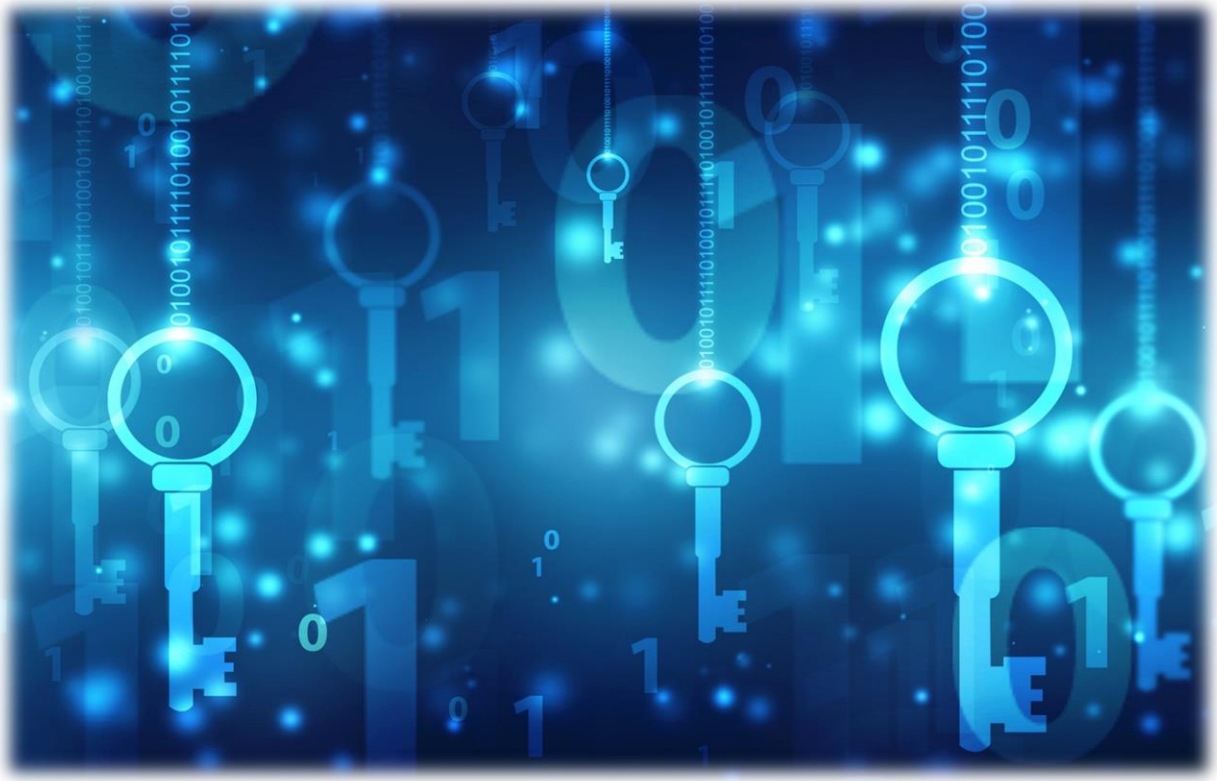
جامعة الموصل
كلية التربية للعلوم الصرفة
قسم علوم الحاسوب
Fourth Class

Data Security

أستاذ المادة:
د. ثامر عبدالحافظ جرجيس

Lecture 11

- **Symmetric and Public Key Systems**



CONTENTS

- **Symmetric-key**
- **Public-Key Cryptography**
- **Public-Key Characteristics**
- **Public-Key Applications**
- **Cryptography, Cryptanalysis**
- **Attacks on Cryptosystems**

Symmetric-key or (or secret-key)

- ***Symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key)***

Symmetric-key or (or secret-key)

- **two main types:**

- **stream ciphers** – operate on individual characters of the plaintext

- **block ciphers** – process the plaintext in larger blocks of characters

Private Key Encryption (Symmetric)

Public-Key Cryptography

- public-key/two-key/asymmetric cryptography involves the use of two keys:

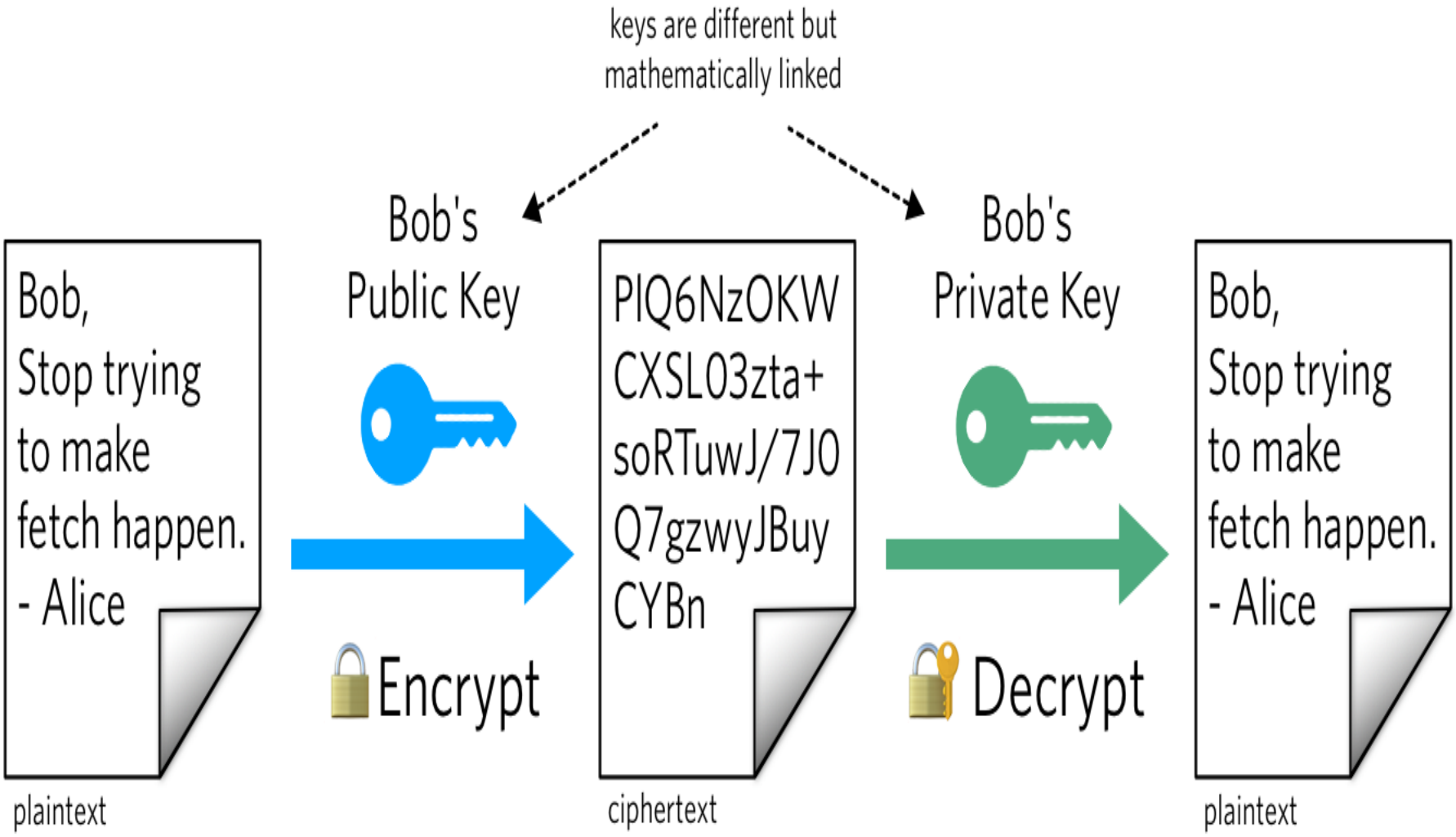
  - **a public-key**, which may be known by anybody, and can be used to encrypt messages, and verify signatures

  - **a private-key**, known only to the recipient, used to decrypt messages, and sign (create) signatures

Public-Key

is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures

Public Key Cryptography



Public-Key Characteristics

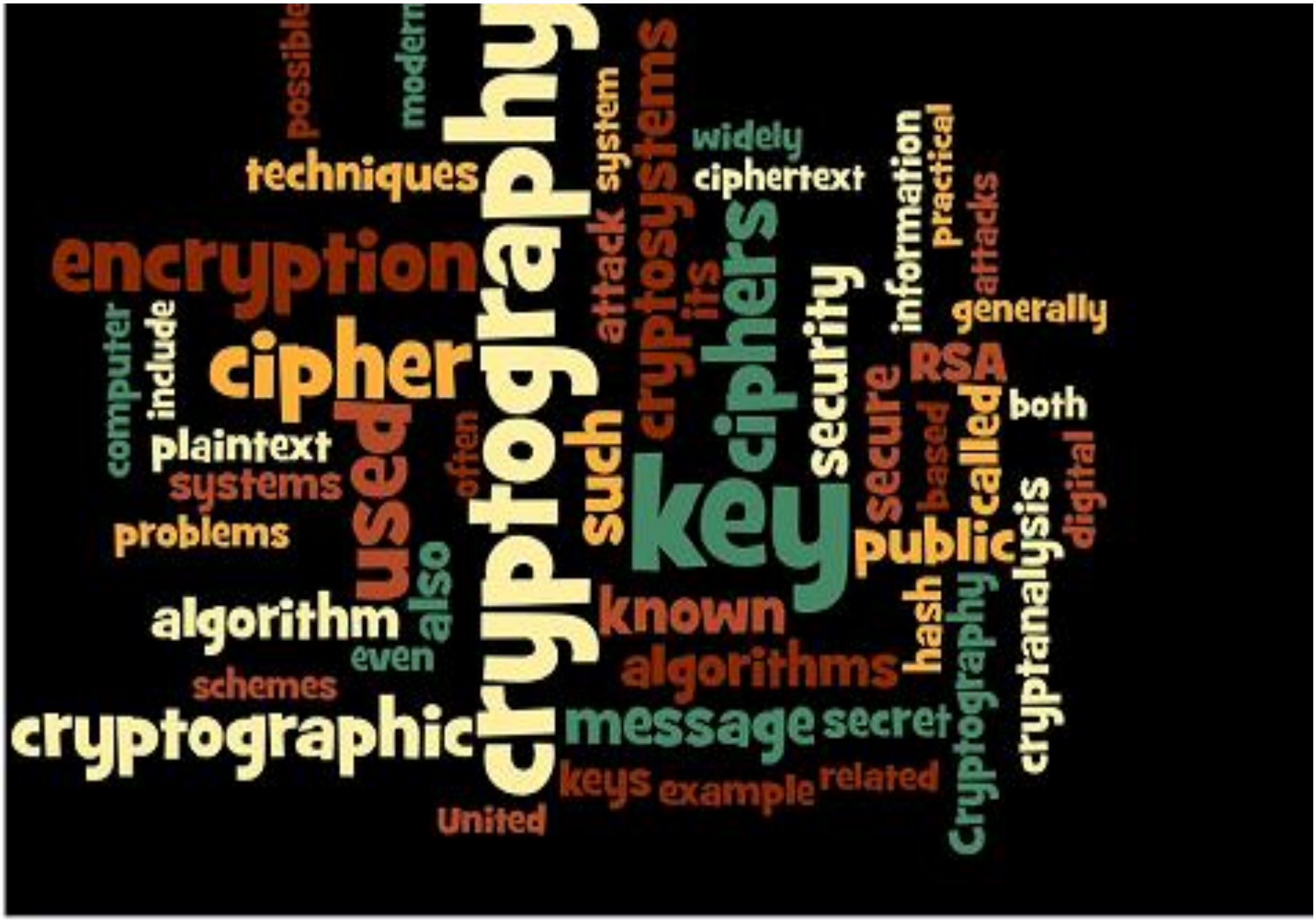
- it is computationally infeasible to find decryption key knowing only algorithm & encryption key

- it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known

- either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)

Public-Key Applications

- can classify uses into 3 categories:
- ***encryption/decryption (provide secrecy)***
- ***digital signatures (provide authentication)***
- ***key exchange (of session keys)***


cryptography
encryption
cipher
key
ciphers
cryptosystems
used
techniques
ciphertext
widely
information
practical
attacks
generally
security
RSA
public
secure
called
both
digital
cryptanalysis
Cryptography
hash
algorithms
known
message
secret
cryptographic
algorithm
plaintext
systems
problems
computer
include
possible
modern
attack
system
its
such
often
also
even
schemes
keys
example
related
United

Cryptography, Cryptanalysis, Cryptology

- **Cryptography** is the art or science of keeping messages secret.

- **Cryptanalysis** is the art of **breaking** ciphers, i.e. retrieving the plaintext without knowing the proper key.

- **Cryptology** is the branch of mathematics that studies the mathematical foundations of cryptographic methods.

- People who do cryptography are **cryptographers**, and practitioners of cryptanalysis are **cryptanalysts**.

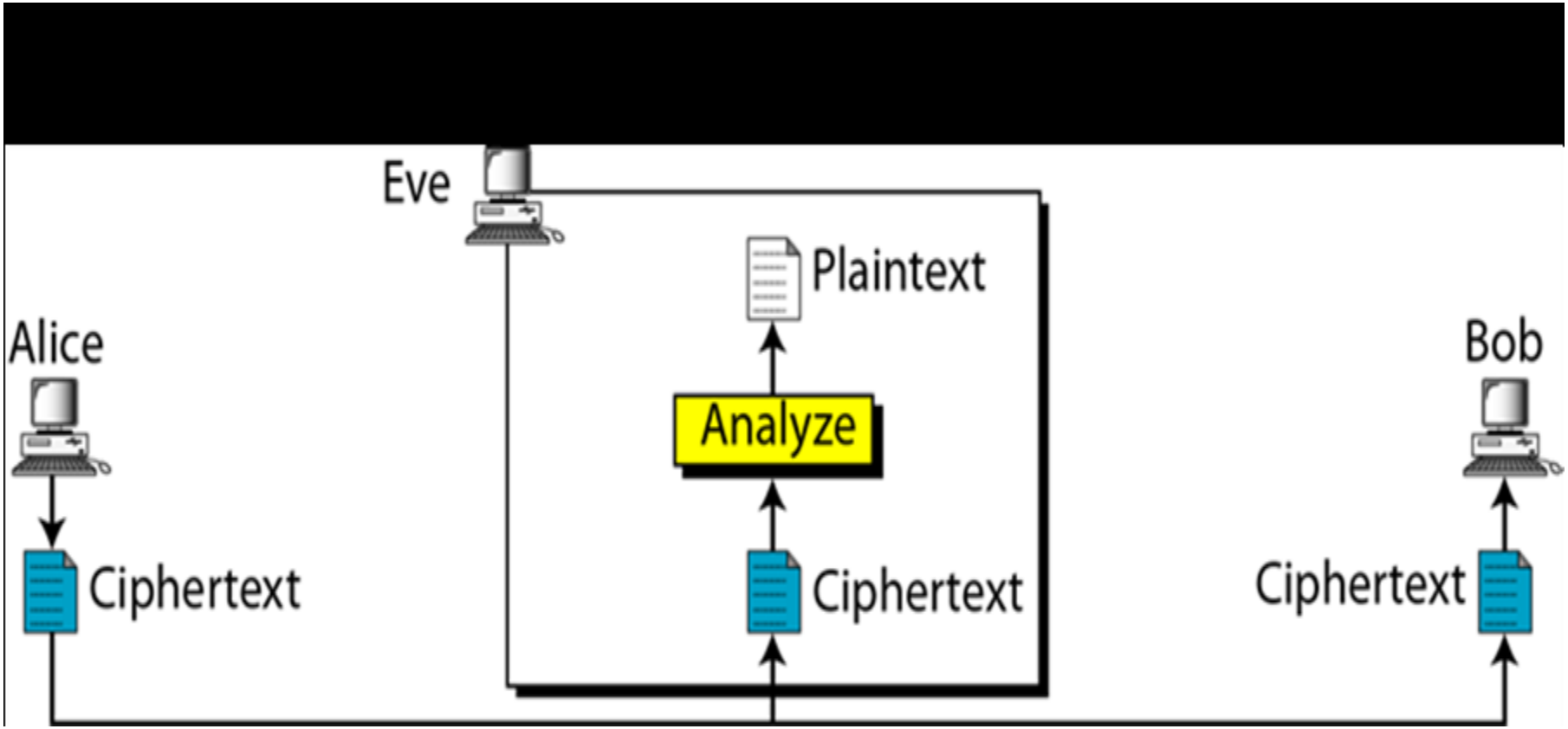
- **Cryptography** deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications.

Cryptanalysis and Attacks on Cryptosystems

- There are many cryptanalytic techniques. Some of the more important ones for a system implementer are

- **Ciphertext-only attack** (Only know algorithm / ciphertext, statistical, can identify plaintext): This is the situation where the attacker does not know anything about the contents of the message, and must work from ciphertext only. It is very hard.

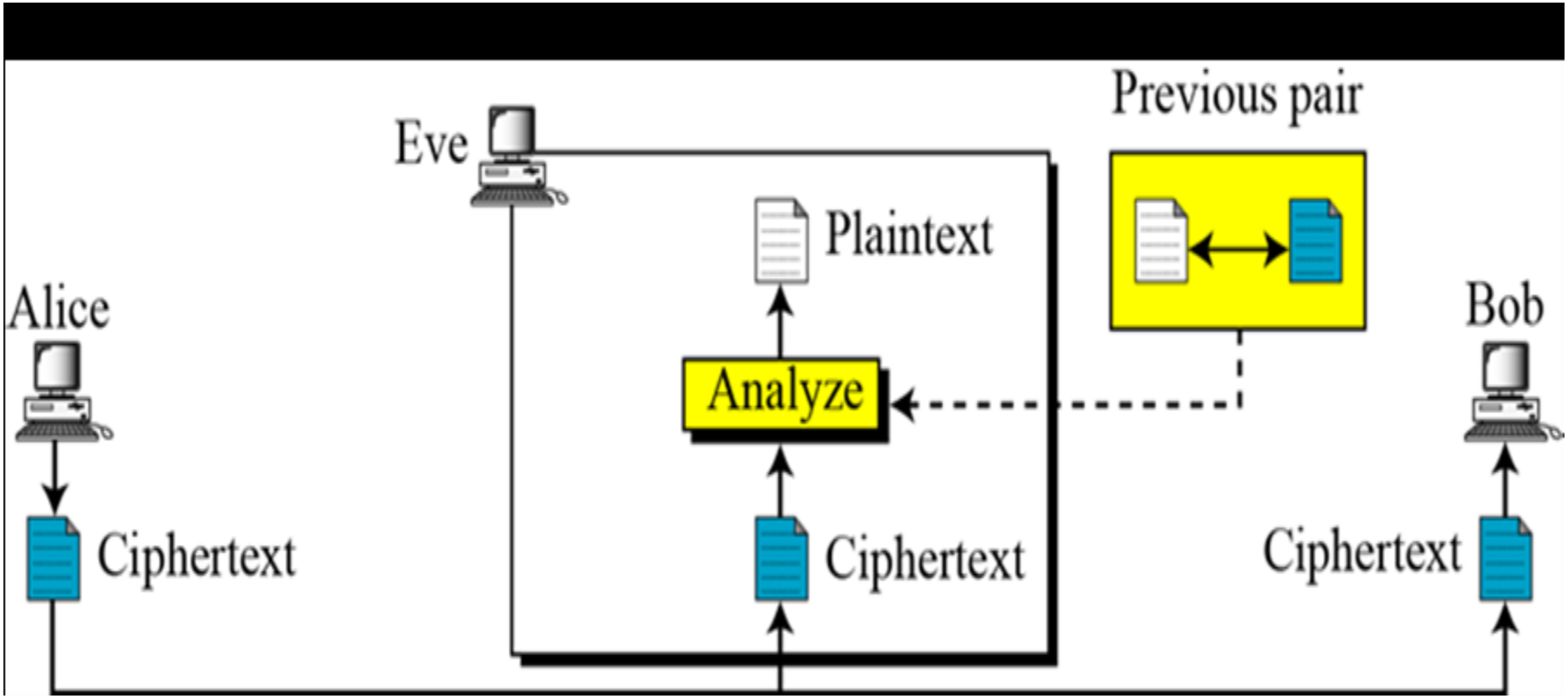
- **Ciphertext-only attack**



Known-plaintext attack

- ***Known-plaintext attack*** *(know/suspect plaintext & ciphertext to attack cipher): The attacker knows or can guess the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext blocks using this information. This may be done by determining the key used to encrypt the data.*

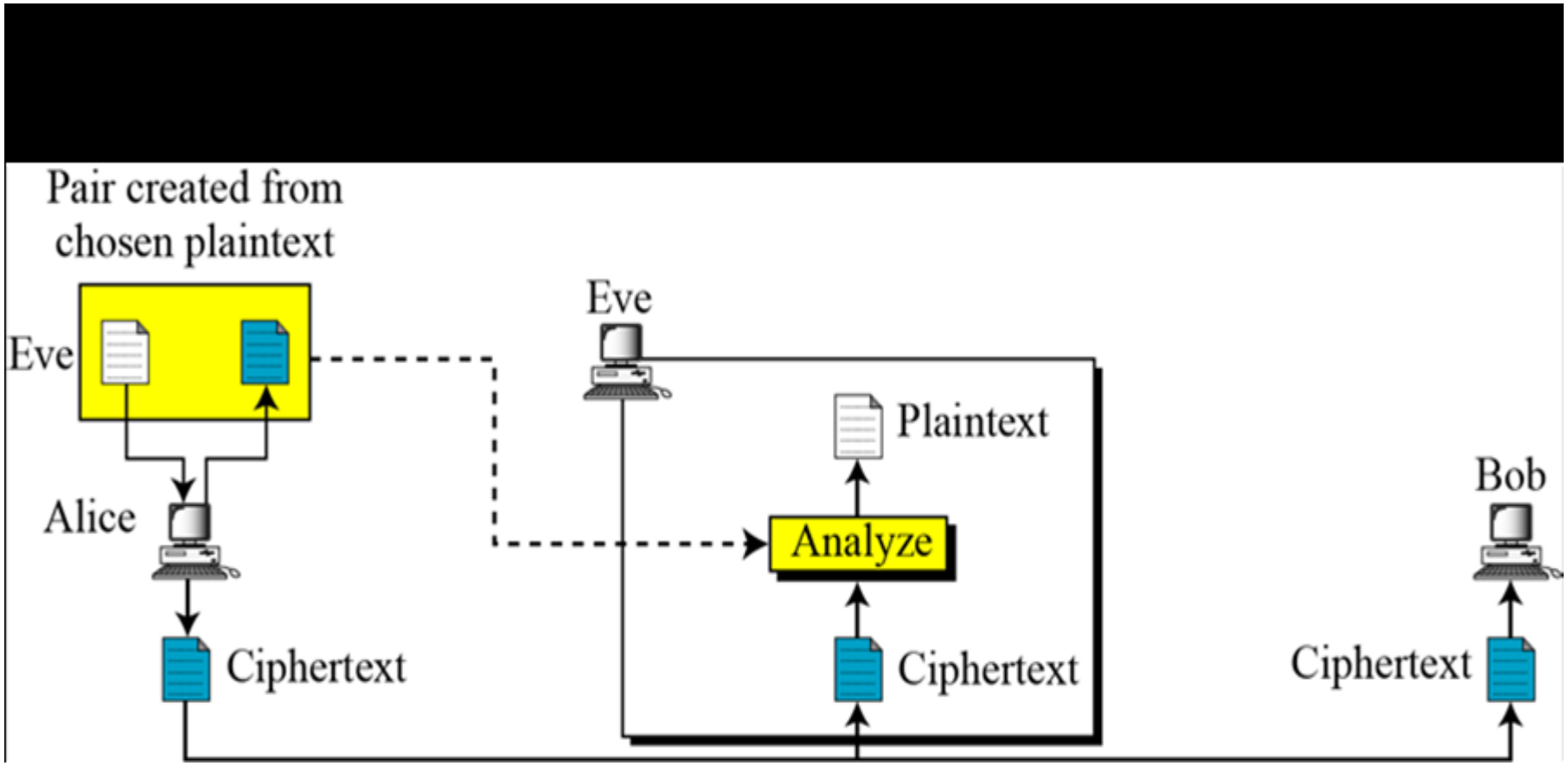
- **Known-plaintext attack**



Chosen-plaintext attack

- ***Chosen-plaintext attack*** *(selects plaintext and obtain ciphertext to attack cipher): The attacker is able to have any text he likes encrypted with the unknown key. The task is to determine the key used for encryption.*

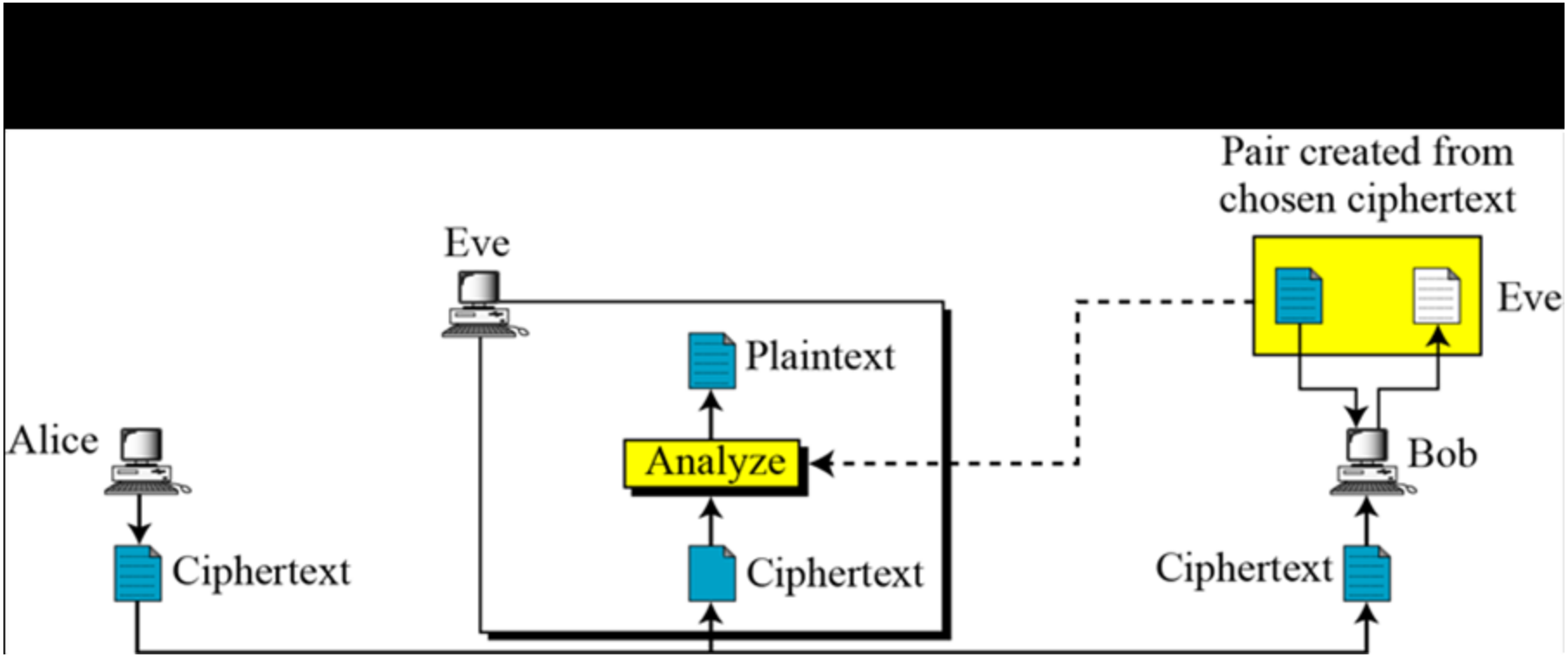
- **Chosen-plaintext attack**



Chosen Ciphertext Attacks

- ***Chosen Ciphertext Attacks*** *(select ciphertext and obtain plaintext to attack cipher)**:** Attacker obtains the decryption of any ciphertext of its choice (under the key being attacked)*

- **Chosen Ciphertext Attacks**



- **Next lecture**
- **Steganography**

Thank you

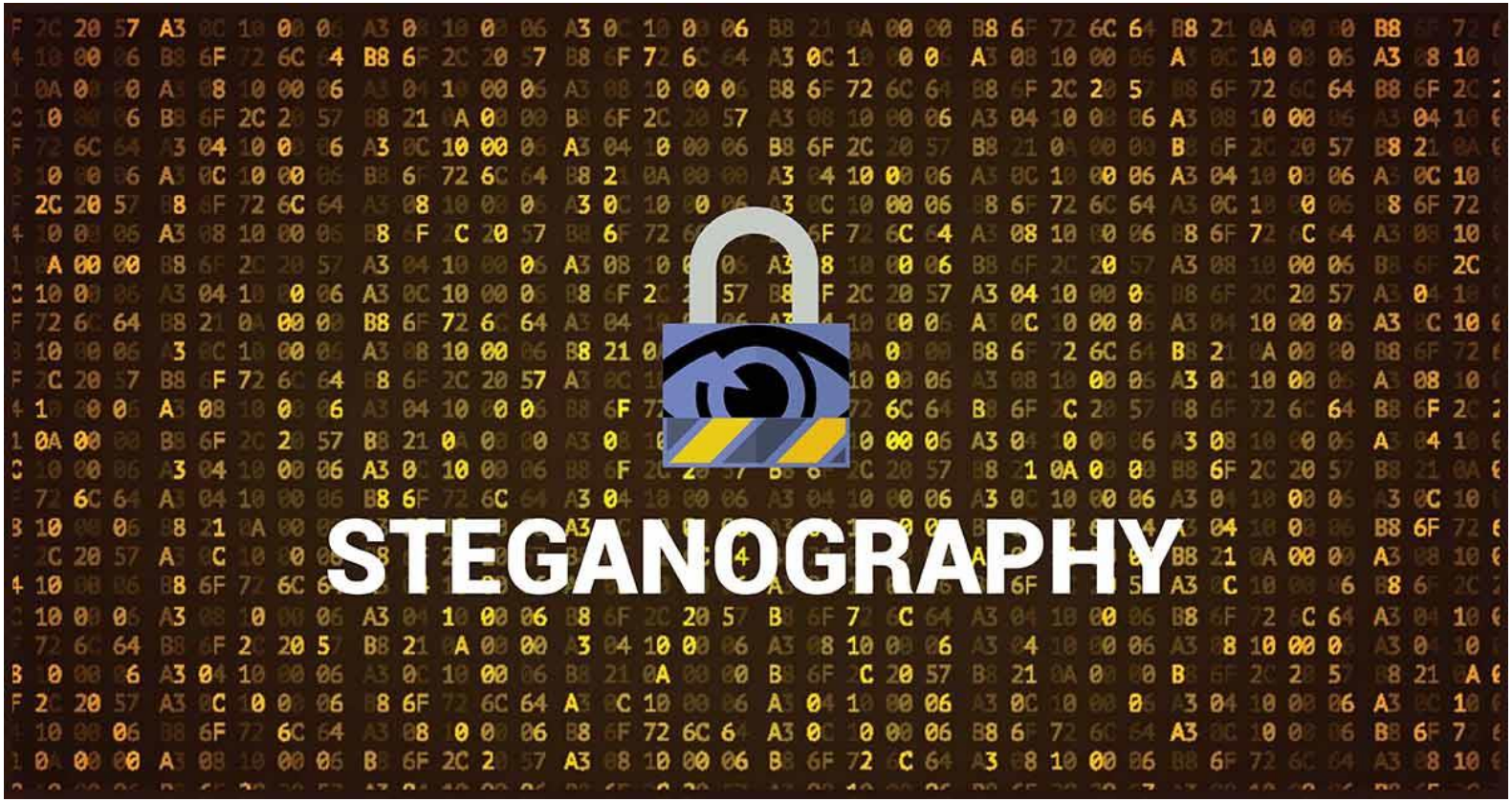
جامعة الموصل
كلية التربية للعلوم الصرفة
قسم علوم الحاسوب
Fourth Class

Data Security

أستاذ المادة:
د. ثامر عبدالحافظ جرجيس

Lecture 12

- **Steganography**



CONTENTS

- **Steganography**
- **Cryptography & Steganography**
- **Types of materials in steganography**
- **Categories of file formats**
- **Types of Steganography**
- **Differences between Steganography and Cryptography**

Steganography

- ***The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. Steganography is one such pro-security innovation in which secret data is embedded in a cover.***


0101 0100 0110 1000
0110 1001 0111 0011
0010 0000 0110 1001
0111 0011 0010 0000
0110 0001 0010 0000
0101 0011 0100 0101
0100 0011 0101 0010
0100 0101 0101 0100

Steganography

- Deals with composing hidden messages so that only the sender and the receiver know that the message even exists.

- Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention.

Cryptography & Steganography

- *The study of hiding information is called **Cryptography**. When communicating over an untrusted medium such as internet, it is very important to protect information and Cryptography plays an important role in this.*

- *Today, Cryptography uses principles from several disciplines such as mathematics, computer science, etc.*

Cryptography & Steganography

- **Steganography** deals with composing hidden messages so that only the sender and the receiver know that the message even exists.

- **Steganography and Cryptography** are closely related. Cryptography scrambles messages so they cannot be understood.

Cryptography & Steganography

- **Steganography** on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an "invisible" message will not do so.

- Both sciences can be combined to produce better protection of the message. In this case, when the Steganography fails and the message can be detected, it is still of no use as it is encrypted using Cryptography techniques.

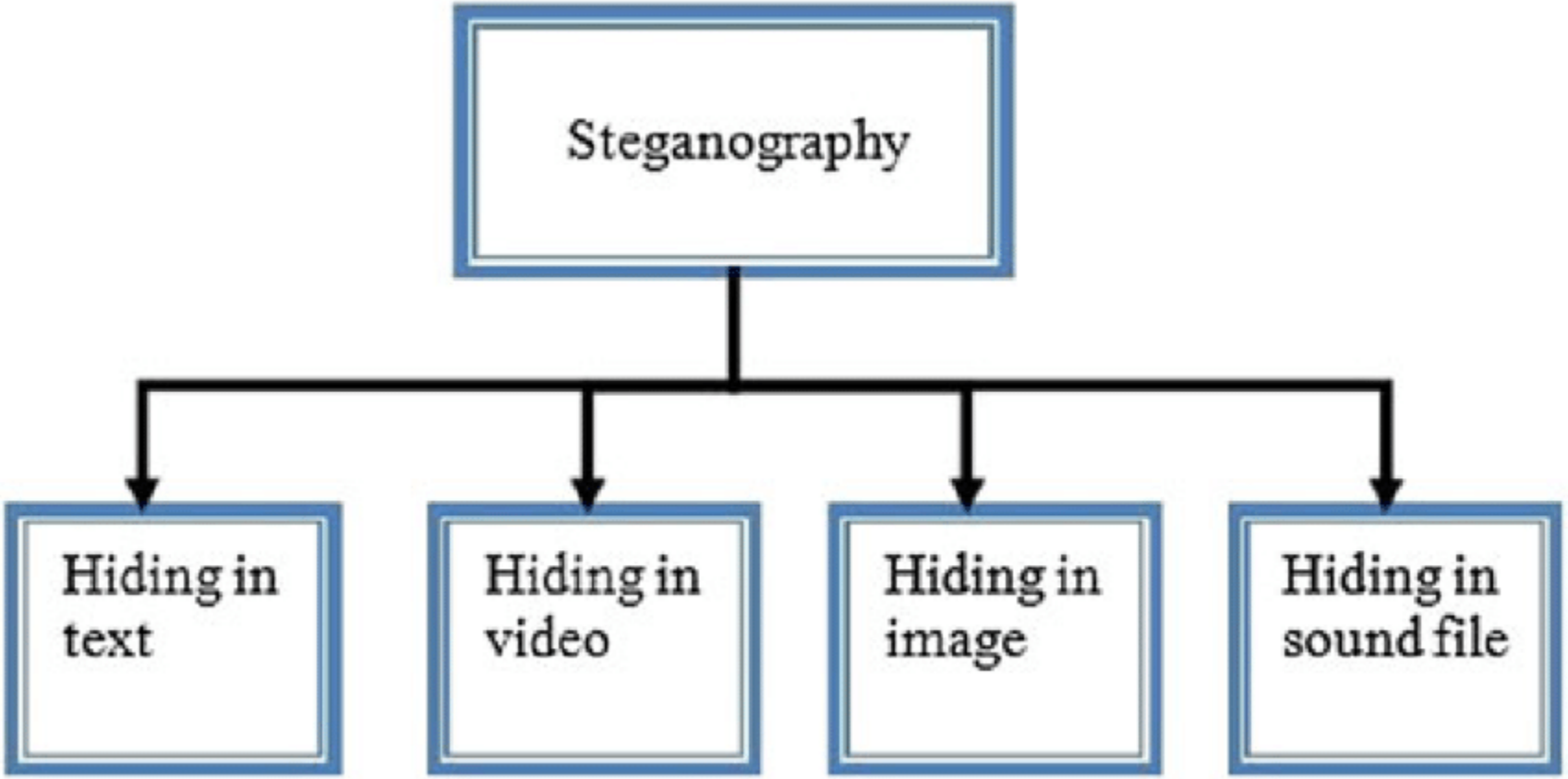
Types of materials in steganography

- There exist two types of materials in steganography:
- Message
- Carrier

- **Message** is the secret data that should be hidden.
- **Carrier** is the material that takes the message in it.

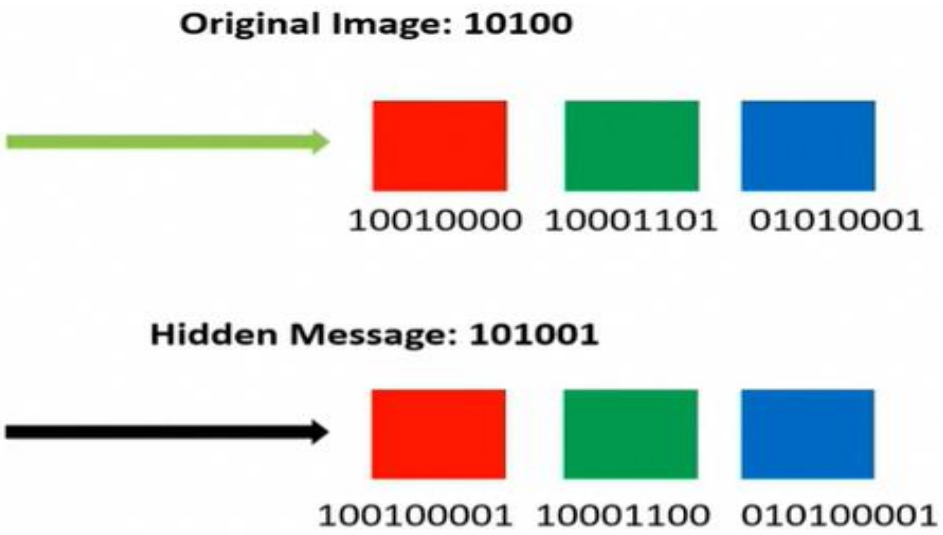
Categories of file formats

- The different categories of file formats that can be used for steganography techniques.



Types of Steganography

- **Hiding a message inside text.**
- **Hiding a message inside images.**
- **Hiding a message inside audio or video files.**

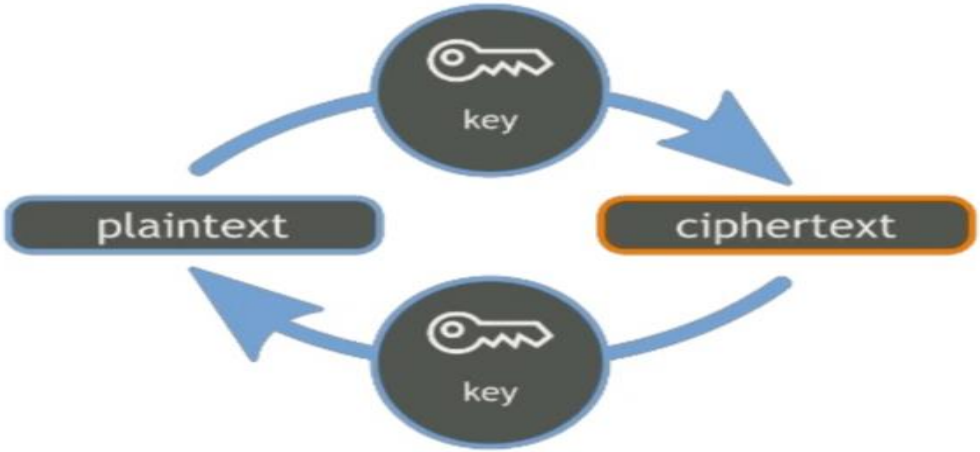



original image


stegnographic
image

Differences between Steganography and Cryptography

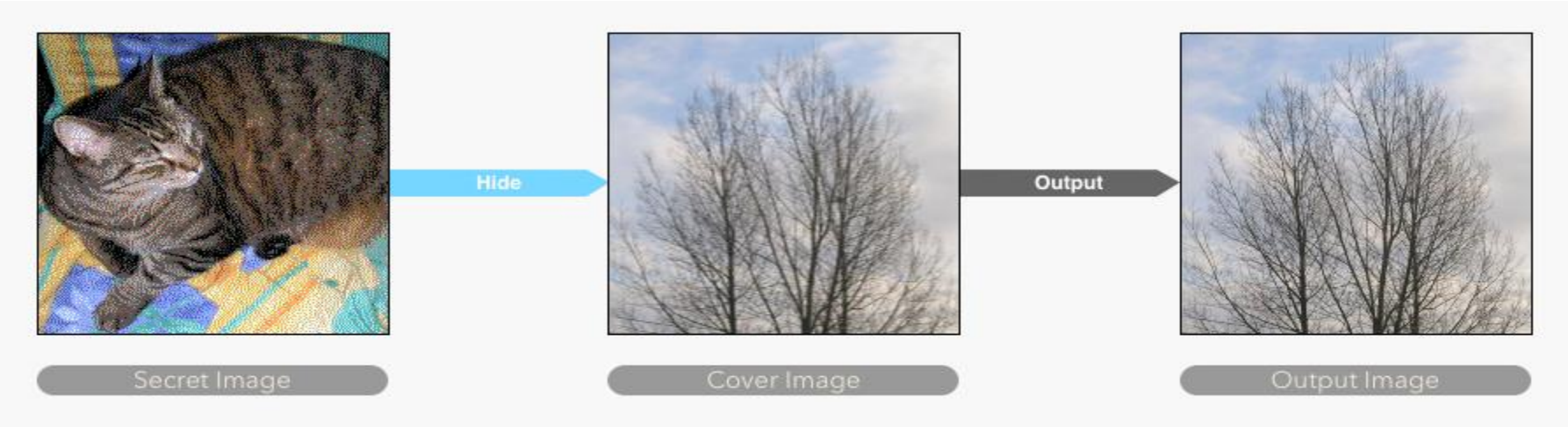
- ***Cryptography*** *is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists.*



- *In* ***Steganography****, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message.*

Differences between Steganography and Cryptography

- ***Steganography*** *hides a message within another message normally called as a cover and looks like a normal graphic, video, or sound file. In cryptography, encrypted message looks like meaningless jumble of characters.*



- ***Cryptographic*** *methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.*

Differences between Steganography and Cryptography

- ***Steganography*** *requires caution when reusing pictures or sound files.*

- *In* ***cryptography*** *caution is required when reusing keys.*

- *By* ***combining*** *Steganography and Cryptography one can achieve better security.*

- **Next lecture**
- **Caesar Cipher**

Thank you

جامعة الموصل
كلية التربية للعلوم الصرفة
قسم علوم الحاسوب
Fourth Class

Data Security

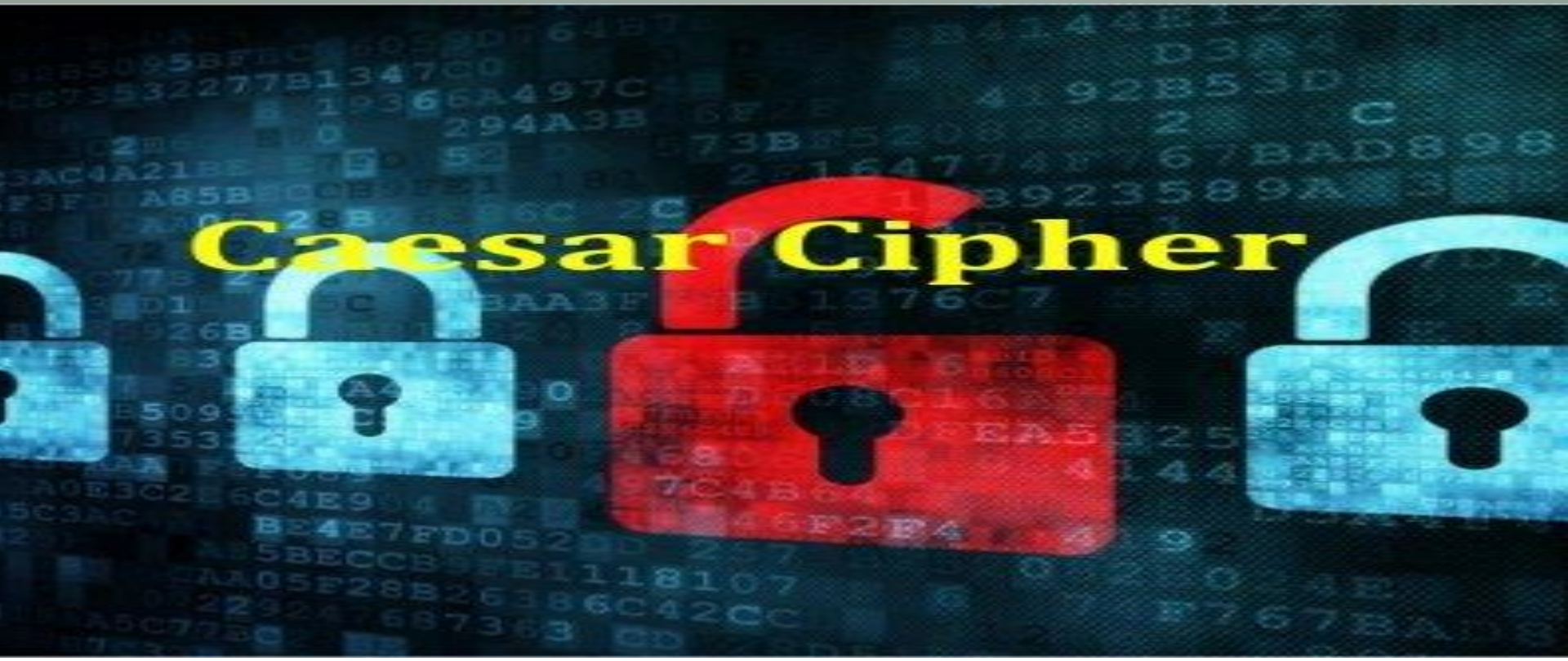
أستاذ المادة:
د. ثامر عبدالحافظ جرجيس

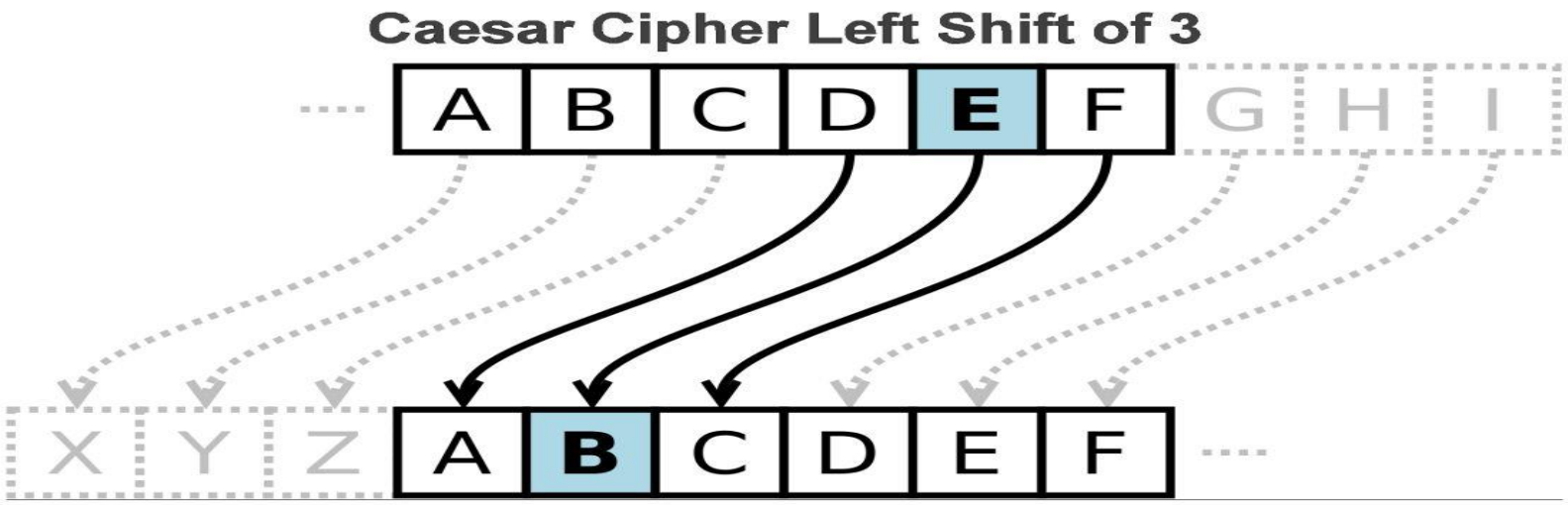
Lecture 13

Caesar Cipher

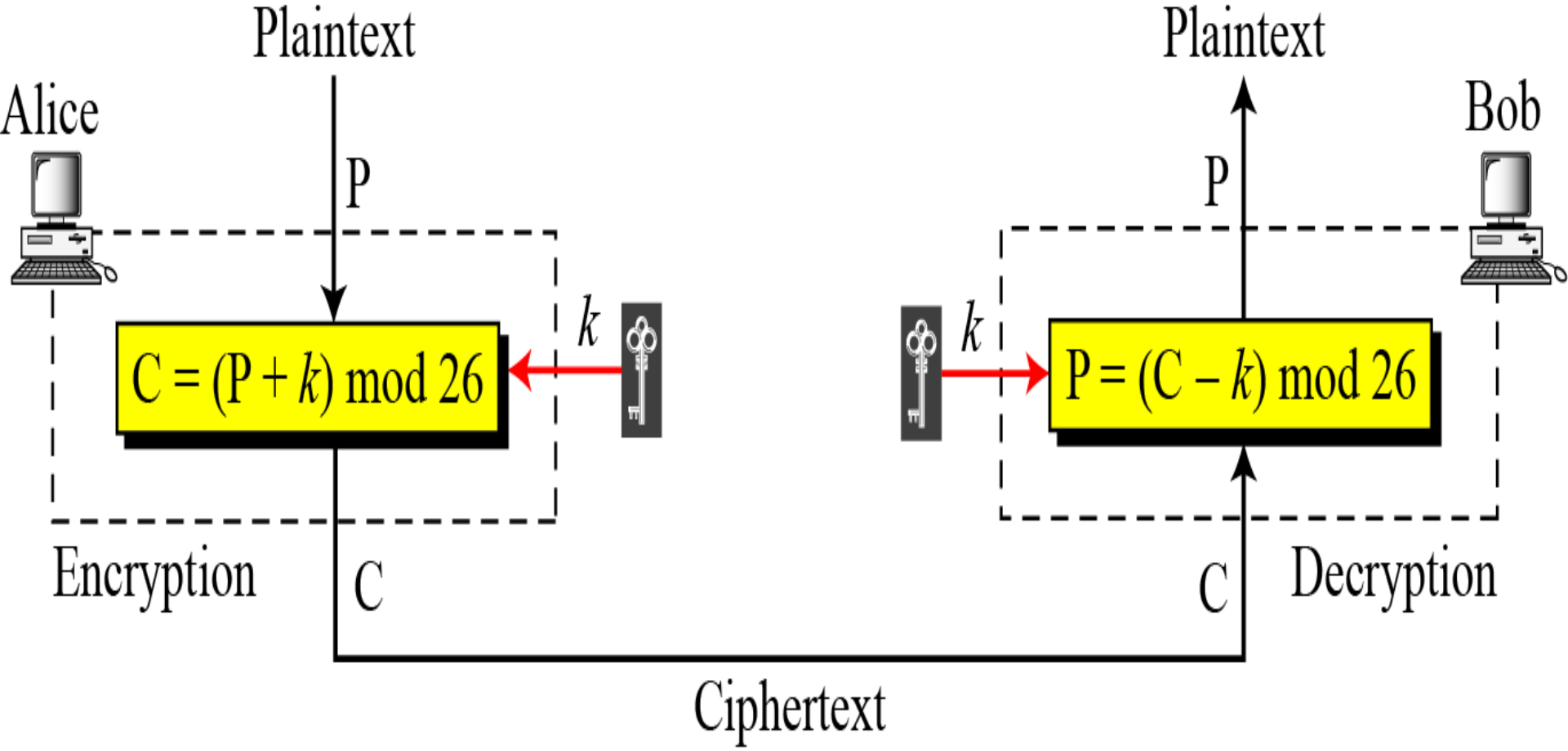
- is the simplest monoalphabetic cipher. It is sometimes called a shift cipher and sometimes **a Caesar cipher**, but the term additive cipher better reveals its mathematical nature. When the cipher is additive, the plaintext, ciphertext, and key are integers.

- **Additive Cipher**


Caesar Cipher


Caesar Cipher Left Shift of 3
A B C D E F G H I
X Y Z A B C D E F

Caesar cipher



- **Caesar Cipher: -** Named for Julious Caesar.
- Caesar used a key of 3 for his communications.

- **Plaintext**

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

d e f g h i j k l m n o p q r s t u v w x y z a b c

- **Ciphertext**

- Plaintext : computer

  ciphertext : FRPSXWHU

Caesar cipher

- **K= number of shift**

$$C=Ek(m)= (m+k) \text{ mode } 26$$

The nubmer of accept keys is 26

Example

- Use the additive cipher with key = 15 to encrypt the plain text (hello).

- We apply the encryption algorithm to the plaintext, character by character:

- Plaintext : h e l l o

7 4 11 11 14

Encryption

- (7+15) mod 26=22→ W
- (4+15) mod 26=19 →T
- (11 +15) mod 26=0 →A
- (11+15) mod 26=0 →A
- (14+15) mod 26=3 →D
- Ciphertext WTAAD

Decryption

- We apply the decryption algorithm to the plaintext character by character:

- Ciphertext: W T A A D
  22 19 0 0 3

(22-15) mod 26=7→ h
(19-15) mod 26=4 →e
(0-15) mod 26=11 →l
(0-15) mod 26=11 →l
(3-15) mod 26=14 →0

plaintext: h e l l o

شكرا

لكم

جامعة الموصل
كلية التربية للعلوم الصرفة
قسم علوم الحاسوب
Fourth Class

Data Security

أستاذ المادة:
د. ثامر عبدالحافظ جرجيس

Lecture 14

- **Multiplicative Cipher**

- While using Caesar cipher technique, encrypting and decrypting symbols involves converting the values into numbers with a simple basic procedure of addition or subtraction.

- Let us think up a different method of enciphering a message. Instead of adding a key number to the equivalents of the plain text letters, we shall multiply by the key number.

- **Multiplicative Cipher**

Multiplicative Cipher

- is the simplest monoalphabetic cipher. It is sometimes called a **Multiplicative Cipher**.

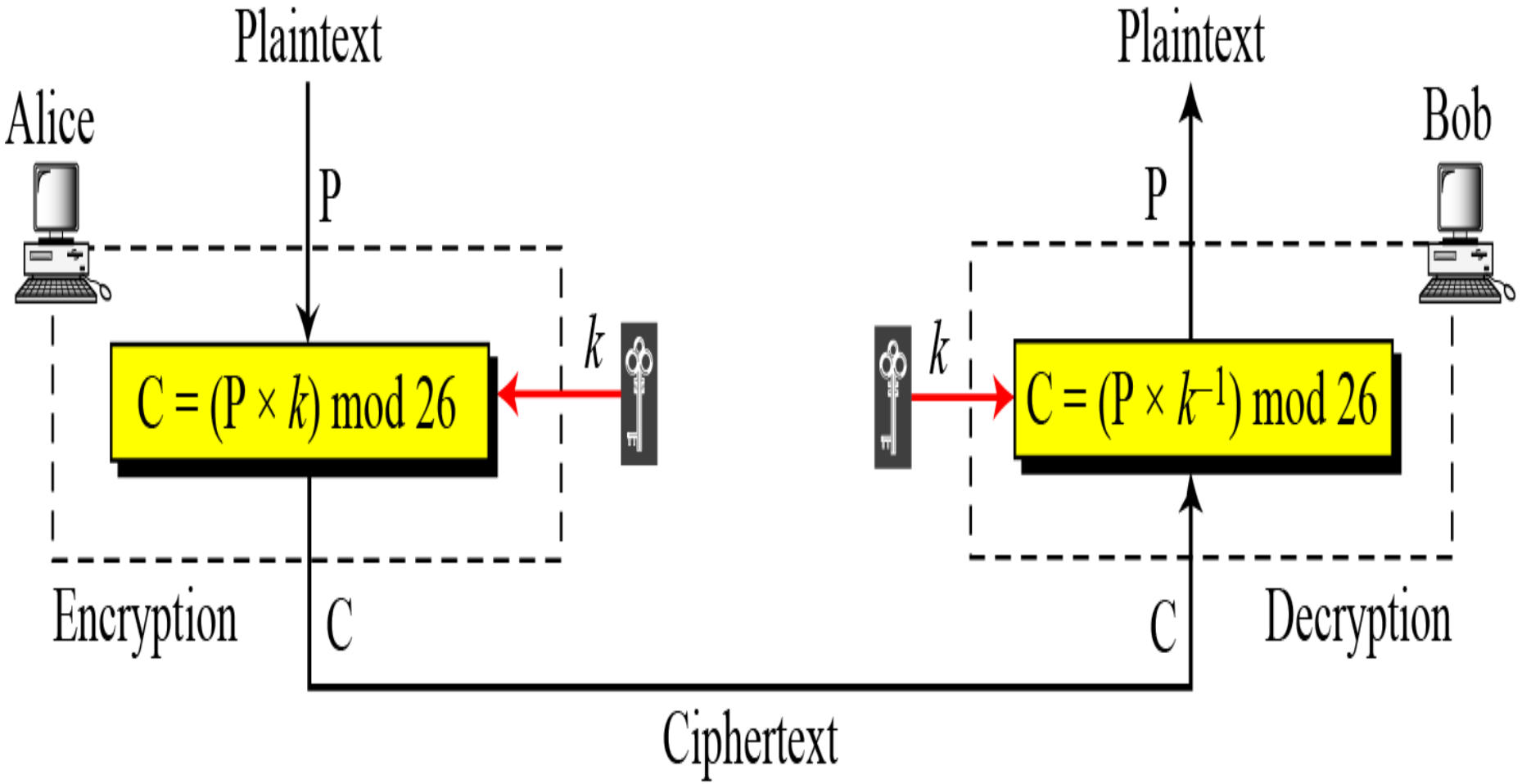
- If multiplication is used to convert to cipher text, it is called a wrap-around situation.

Accepted keys

- Number of accepted keys for any multiplicative cipher which must be is the set that has only 12 key:

[1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]

Multiplicative Cipher



Encryption using the Multiplication Cipher

$$C=Ek(m)= (m* k) \text{ mode } 26$$

The nubmer of accept keys is 12

Alphabetic

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Example

- We use a multiplicative cipher to encrypt the message “**hello**”
- with a key of 7.

Encryption

Plaintext: h → 07	Encryption: (07 x 07) mod 26	ciphertext: 23 → X
Plaintext: e → 04	Encryption: (04 x 07) mod 26	ciphertext: 02 → C
Plaintext: l → 11	Encryption: (11 x 07) mod 26	ciphertext: 25 → Z
Plaintext: l → 11	Encryption: (11 x 07) mod 26	ciphertext: 25 → Z
Plaintext: o → 14	Encryption: (14 x 07) mod 26	ciphertext: 20 → U

The ciphertext is “XCZZU

Example 2

- **plaintext [Computer] by using Multiplicative cipher by equations with key [5]**

- **Computer**
- **C1= 2*5 mod 26**= 10= K

- Homework:
- Write the decryption equation?

شكرا لكم