Computer Security

Lecture 1

Overview

Dr. Mohamed Loey

Lecturer, Faculty of Computers and Information

Benha University

Egypt

Table of Contents

- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- Key Properties
- Symmetric Encryption
- Asymmetric Encryption
- Book

Table of Contents

- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- Key Properties
- Symmetric Encryption
- Asymmetric Encryption
- Book

Cryptography

- ❑ Cryptography: is the science of secret writing and is an ancient art; the first documented use of cryptography in writing dates back to 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription (handwriting).

Table of Contents

- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- Key Properties
- Symmetric Encryption
- Asymmetric Encryption
- Book

Computer Security

is the protection of computer systems including hardware software and data from unauthorized access theft damage
example antivirus softawre

- ❑ **Computer Security** - generic name for the collection of tools designed to protect data

one network

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

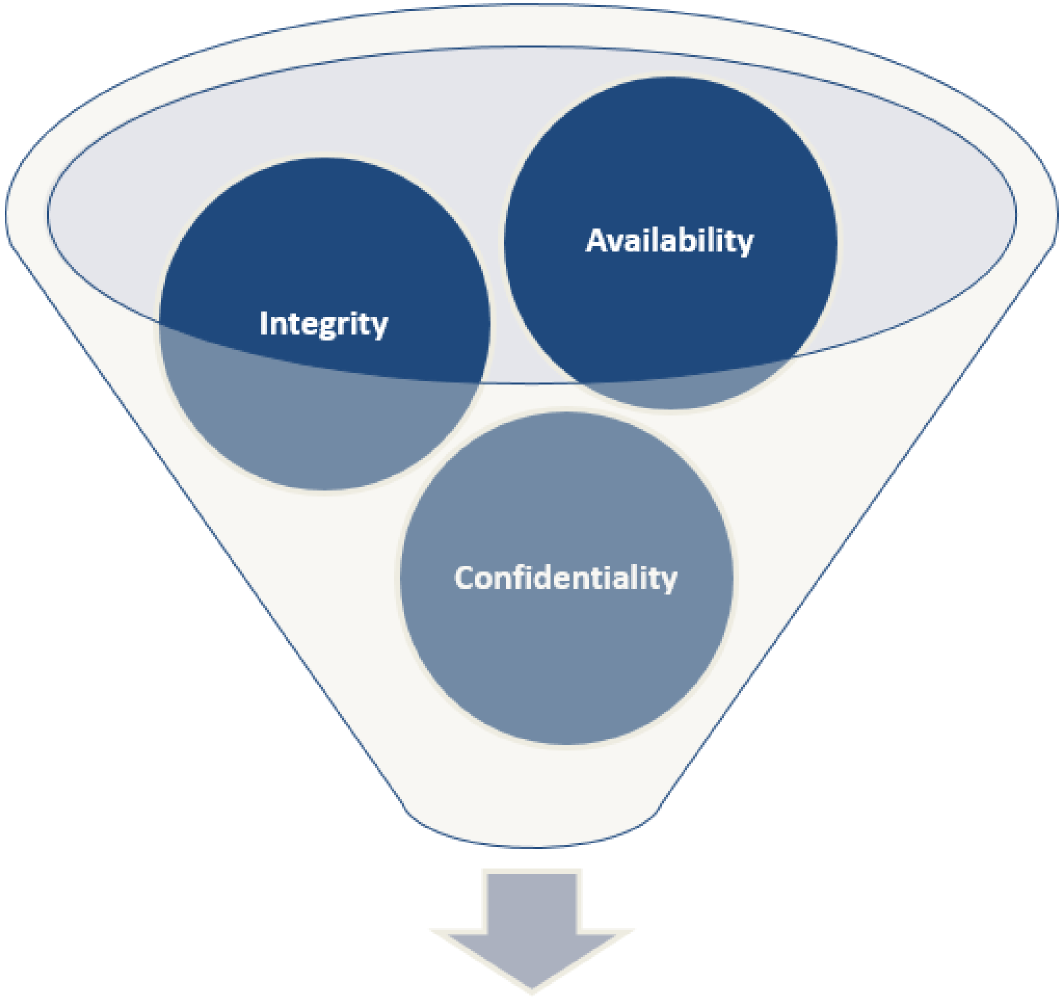
multiple networks

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

Computer Security

الاهداف التى نسعى الى تحقيقها فى مجال امن الحاسب

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability**, and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)



CIA triad

Confidentiality

اتاكد ان مفيش حد قرا الرسالة غير المستلم فقد

- Ensuring that no one can read the message except the intended receiver.

- Preserving authorized restrictions on information access and disclosure (detection), including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Confidentiality

IODQNHDVW

DWWDFNDWGDZQ

Integrity

اتاكد من ان المستلم قام باستلام الرسالة ولم يتم تعديلها فى الطريق للوصول اليه عن الرسالة الاصلية

- Assuring the receiver that the received message has not been altered in any way from the original.

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Integrity

□ An unbroken wax seal on an envelop ensures integrity.

حل المشكلة يضمن عدم قراءة اي شخص للمحتويات الخاصة بالرسالة فى طريقها للوصول اليه

□ The unique unbroken seal ensures no one has read the contents

Availability

التاكد من انه يمكننى الوصول اللى البيانات الخاصة فى الوقت المطلوب فيه

- □ Ensuring timely and reliable access to and use of information. A loss of availability is the disruption (confusion) of access to or use of information or an information system.

Table of Contents

- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- Key Properties
- Symmetric Encryption
- Asymmetric Encryption
- Book

OSI Security Architecture

- The Open System Interconnect (OSI) security architecture was designated by the ITU-T (International Telecommunication Union - Telecommunication). The ITU-T decided that their standard "X.800" would be the ISO security architecture.

- The OSI security architecture focuses on:
  - Security mechanism
  - Security service
  - Security attack

Security mechanism

هى عملية مصممة للتحقق او اتجنب او استرجاع من هجوم امنى حدث

❑ A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

لا يمكن ان يوجد ميكانزم يدعم كل الفانكشن المطلوبة

❑ no single mechanism that will support all functions required

Security service

هى خدمة معالجة او خدمة اتصال معززة بامان البيانات ونقل المعلومات لمنظمة ويستخدم اكتر من ميكانزم ليقوم بتقديم الخدمة

- 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.
- Make use of one or more security mechanisms to provide the service

Security attack

اى اجراء يمكن ان يمس بامن المعلومات التى تمتلكها المؤسسة

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

- □ Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems

Security Attacks

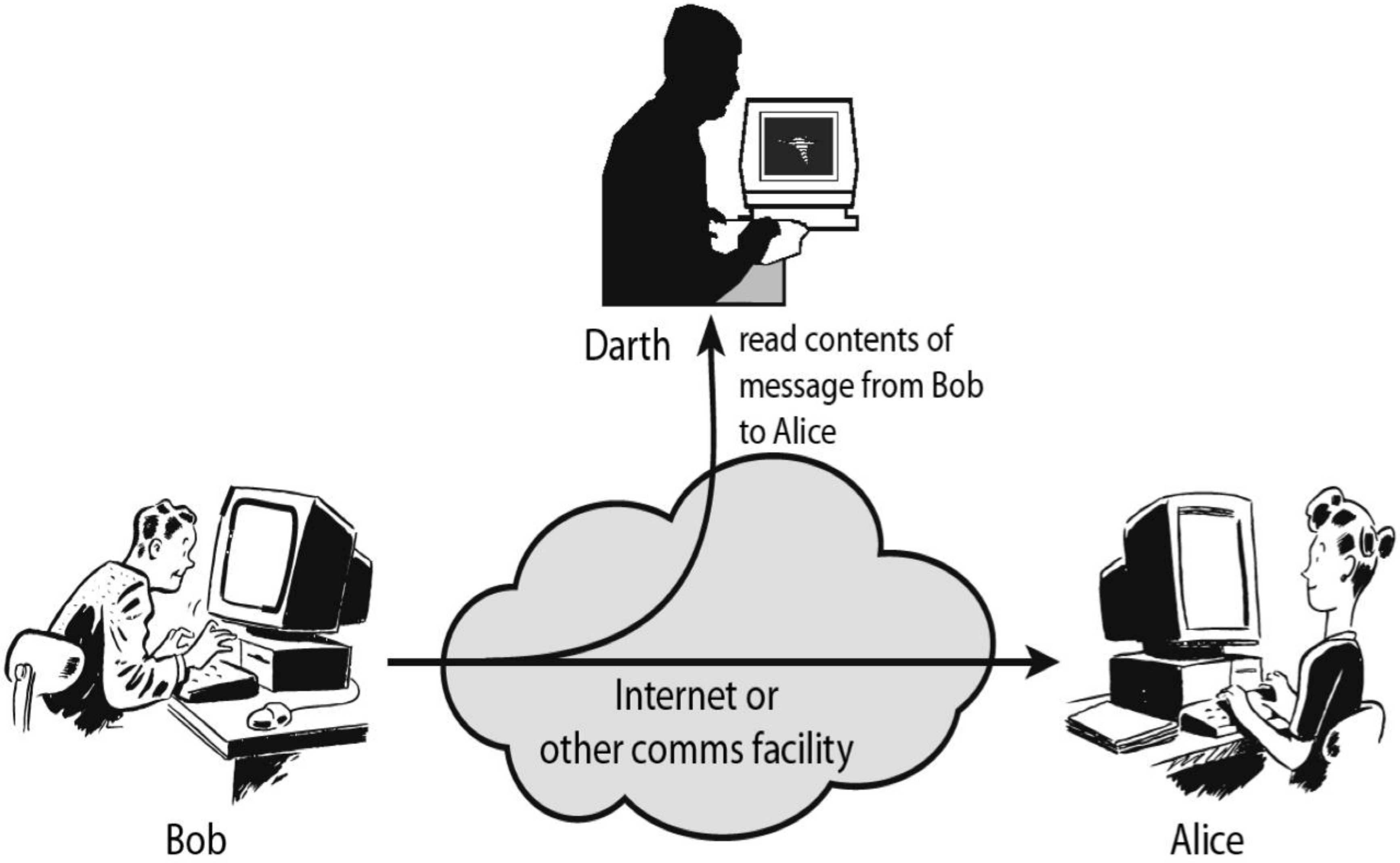
التعلم او استغلال المعلومات ولا يوثر هذا على الموارد

- □ A passive attack attempts to learn or make use of information from the system but does not affect system resources.

استبدال موارد النظام معناها التعديل على البيانات او التاثير على العمليات التى يقوم بها النظام

- □ An active attack attempts to alter system resources or affect their operation.

Passive Attack


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Active Attack

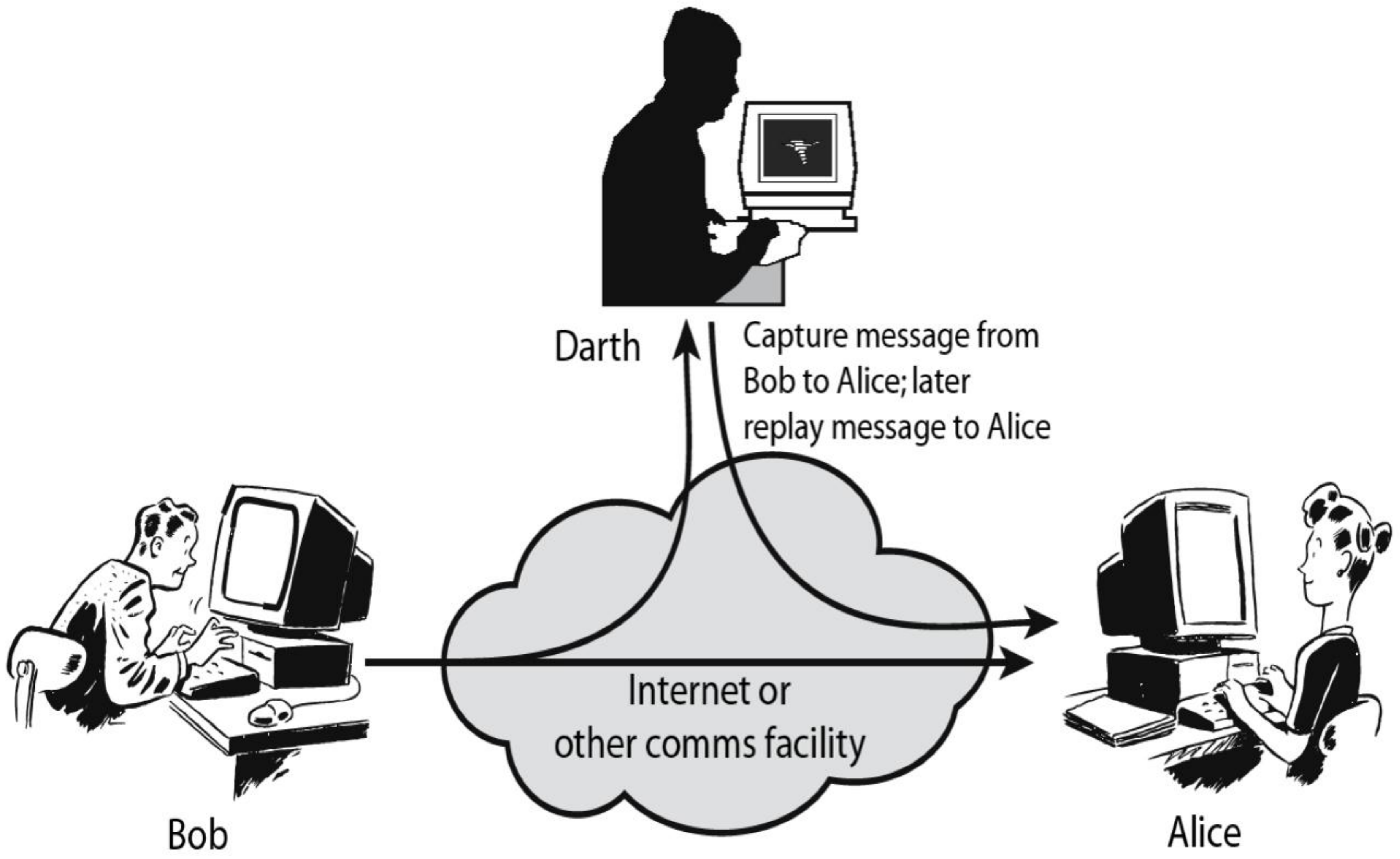
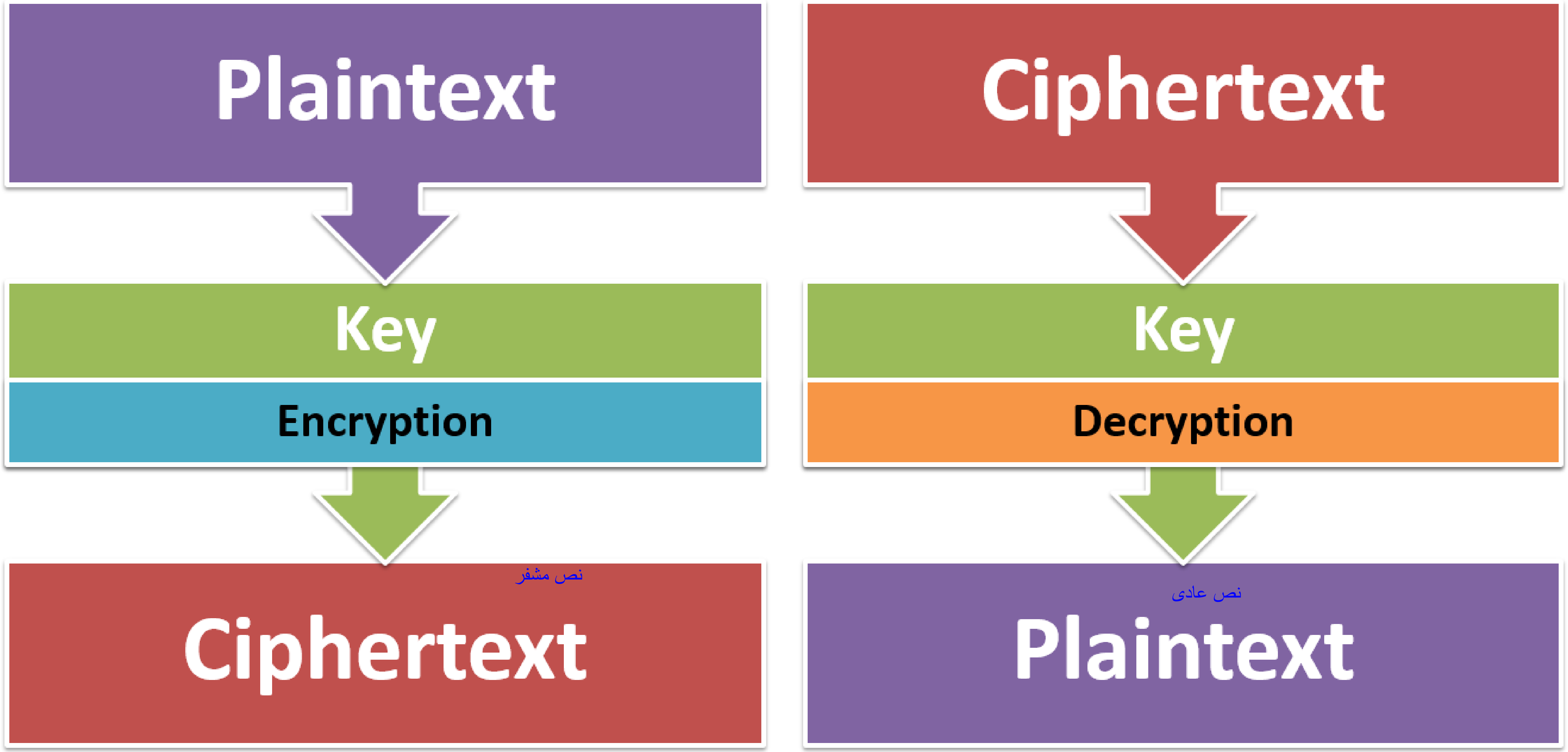

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Table of Contents

- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- Key Properties
- Symmetric Encryption
- Asymmetric Encryption
- Book

Security Structure Scheme



Plaintext

Key

Encryption

نص مشفر

Ciphertext

Ciphertext

Key

Decryption

نص عادى

Plaintext

Security Structure Scheme

- ❑ **Plaintext** is the original message or data

- ❑ **Secret Key** is a value independent of the plaintext and of the algorithm.

- ❑ **Ciphertext** This is the scrambled message produced as output.

Security Structure Scheme

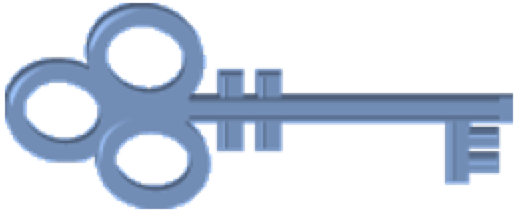
- ❑ **Encryption Algorithm** is a mathematical procedure for performing encryption on data.

- ❑ **Decryption Algorithm** is a mathematical procedure for performing decryption on data.

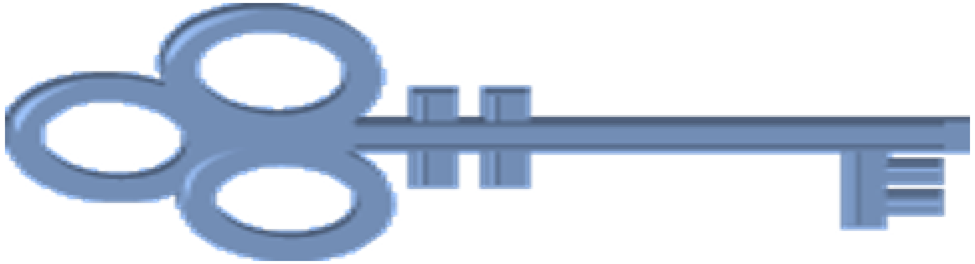
Table of Contents

- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- **Key Properties**
- Symmetric Encryption
- Asymmetric Encryption
- Book

Key Properties



Shorter keys = faster processing, but less secure



Longer keys = slower processing, but more secure

Key Properties

Single use key: (one time key)

- Key is only used to encrypt one message
  - encrypted email: new key generated for every email

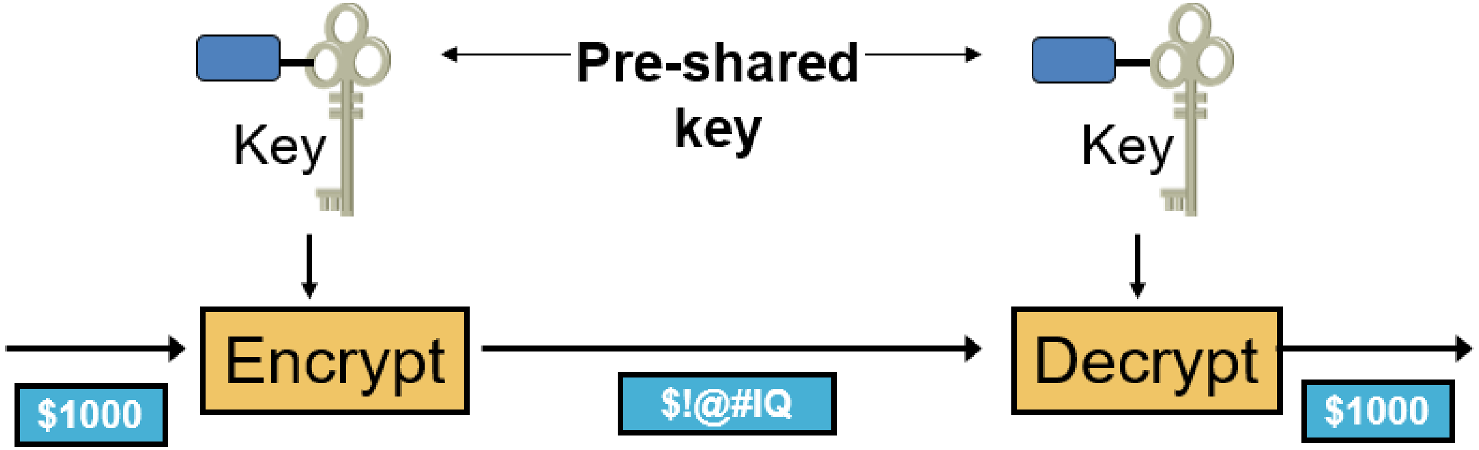
Multi use key: (many time key)

- Key used to encrypt multiple messages
  - encrypted files: same key used to encrypt many files

Table of Contents

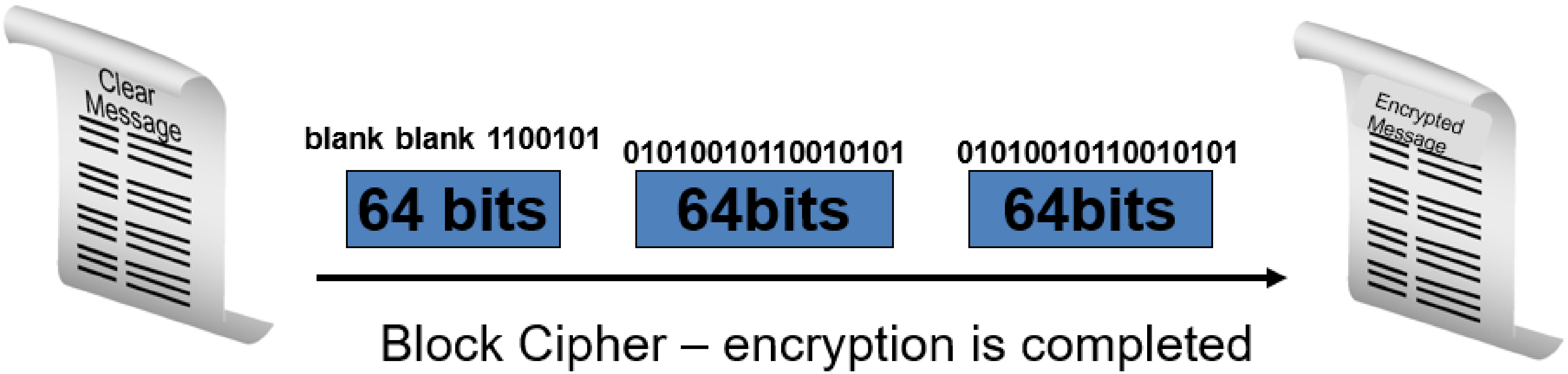
- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- Key Properties
- Symmetric Encryption
- Asymmetric Encryption
- Book

Symmetric Encryption

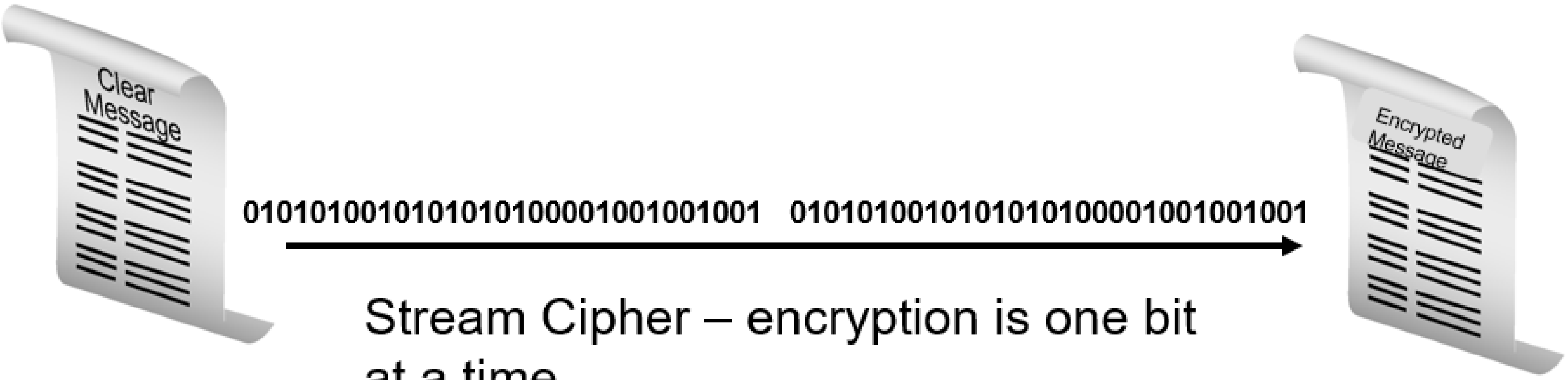


- ❑ Best known as shared-secret key algorithms
- ❑ The usual key length is 80 - 256 bits
- ❑ A sender and receiver must share a secret key
- ❑ Faster processing because they use simple mathematical operations.
- ❑ Examples include DES, 3DES, AES, IDEA, RC2/4/5/6, and Blowfish.

Symmetric Encryption Techniques



Block Cipher – encryption is completed in 64 bit blocks



Stream Cipher – encryption is one bit at a time

Symmetric Encryption Techniques

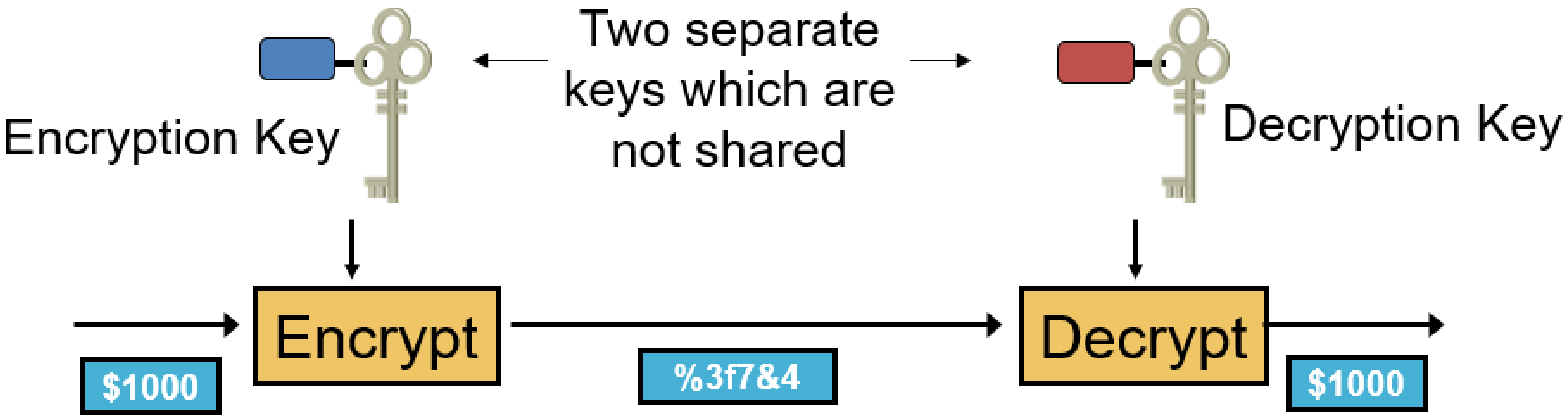
- A **stream cipher** is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream).

- A **block cipher** is a symmetric key cipher in which a cryptographic key and algorithm are applied to a **block** of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time.

Table of Contents

- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- Key Properties
- Symmetric Encryption
- Asymmetric Encryption
- Book

Asymmetric Encryption



- ❑ Also known as public key algorithms
- ❑ The usual key length is 512–4096 bits
- ❑ A sender and receiver do not share a secret key
- ❑ Relatively slow because they are based on difficult computational algorithms
- ❑ Examples include RSA, ElGamal, elliptic curves, and DH.

Cryptanalysis & Cryptology

- ❑ Cryptanalysis: is the science of analyzing and breaking encryption schemes.

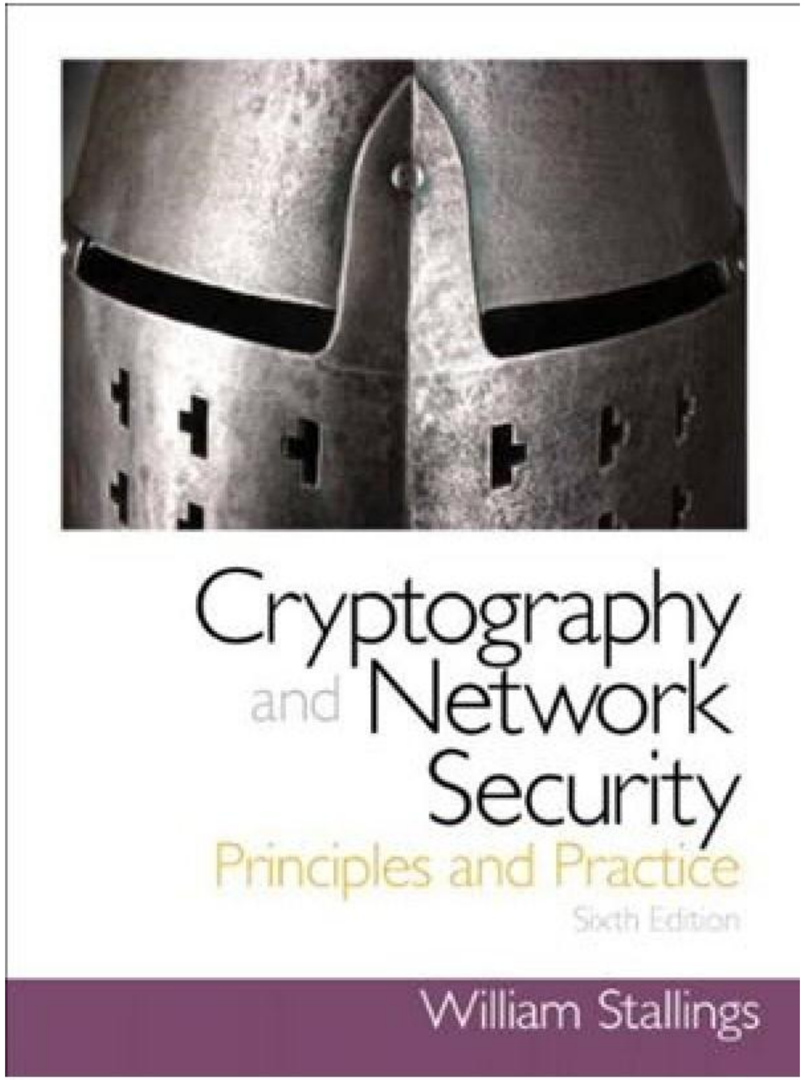
- ❑ Cryptology: is the term referring to the wide study of secret writing, and covered both cryptography and cryptanalysis.

علم التشفير وعلم فك التشفير

Table of Contents

- Cryptography
- Computer Security
- OSI Security Architecture
- Security Structure Scheme
- Key Properties
- Symmetric Encryption
- Asymmetric Encryption
- **Book**

Book

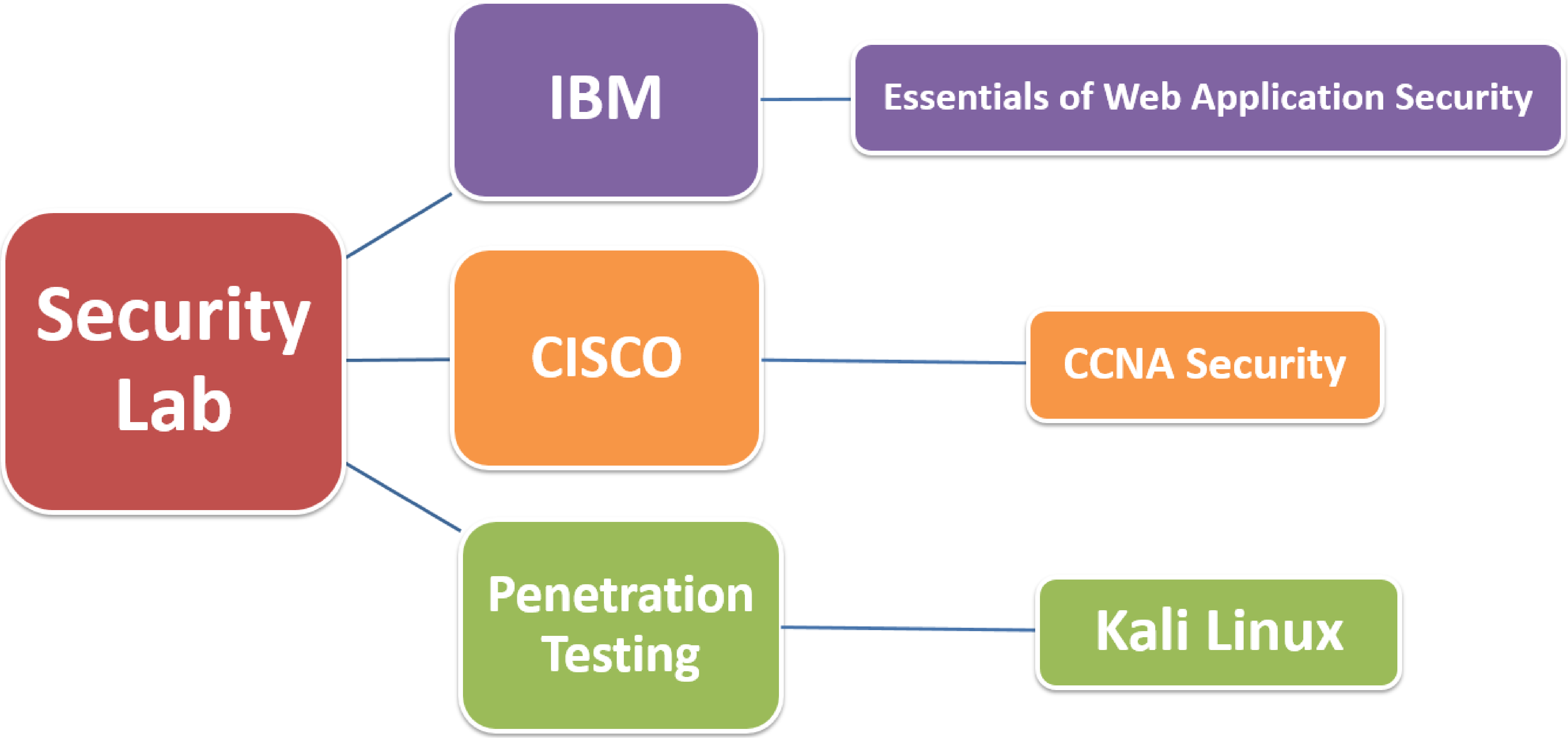


Cryptography and Network Security

Principles and Practice

Sixth Edition

William Stallings



Security Lab

IBM

Essentials of Web Application Security

CISCO

CCNA Security

Penetration Testing

Kali Linux

THANKS FOR YOUR TIME