

Cybersecurity Concepts

Prepared by Dr. Diaa Salama

FNT625
Introduction to Security

Lecture 4





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

Cybersecurity Concepts

Lecture 4

FNT625
Introduction to Security

Prepared by
Dr. Diao Salama

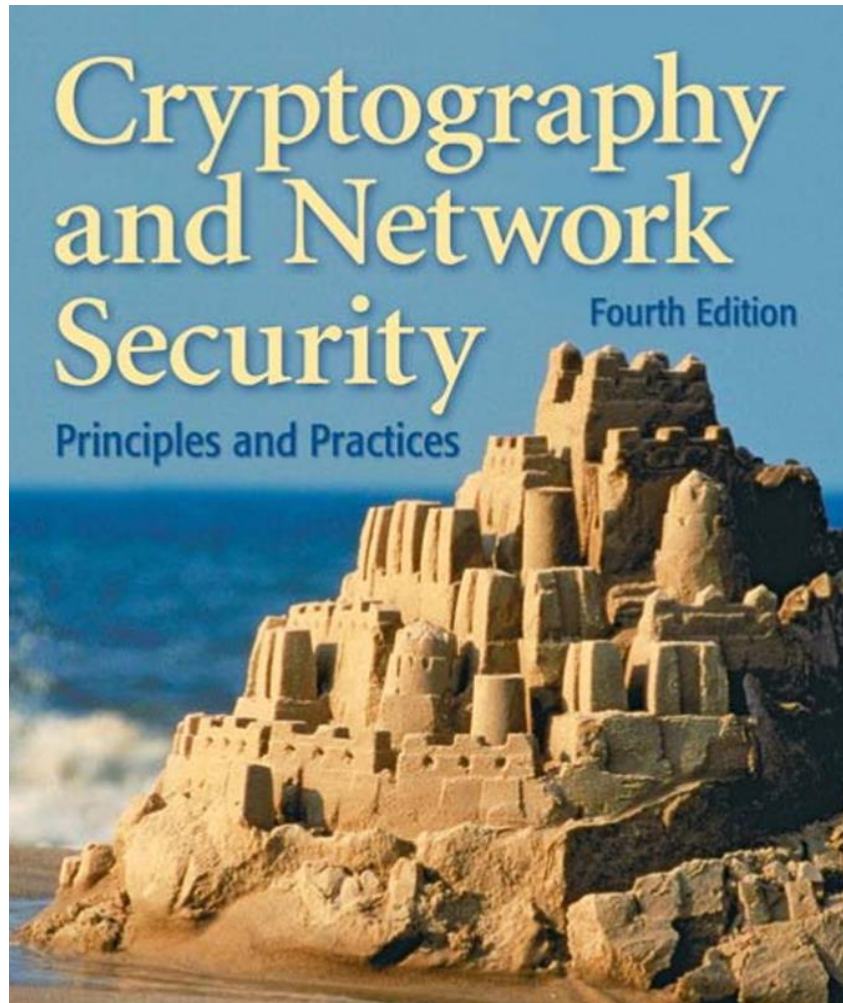
www.midocean.ae

PLEASE
BE QUIET



10





Book Title:

Cryptography and Network Security

Authors:

William Stallings

Publisher:

Pearson Education, Inc.

Edition:

Seven edition

Lecture

04

Lets Start the Fourth Lecture



Introduction to Security



Table of Content

Cryptography

Computer Security

OSI Security Architecture

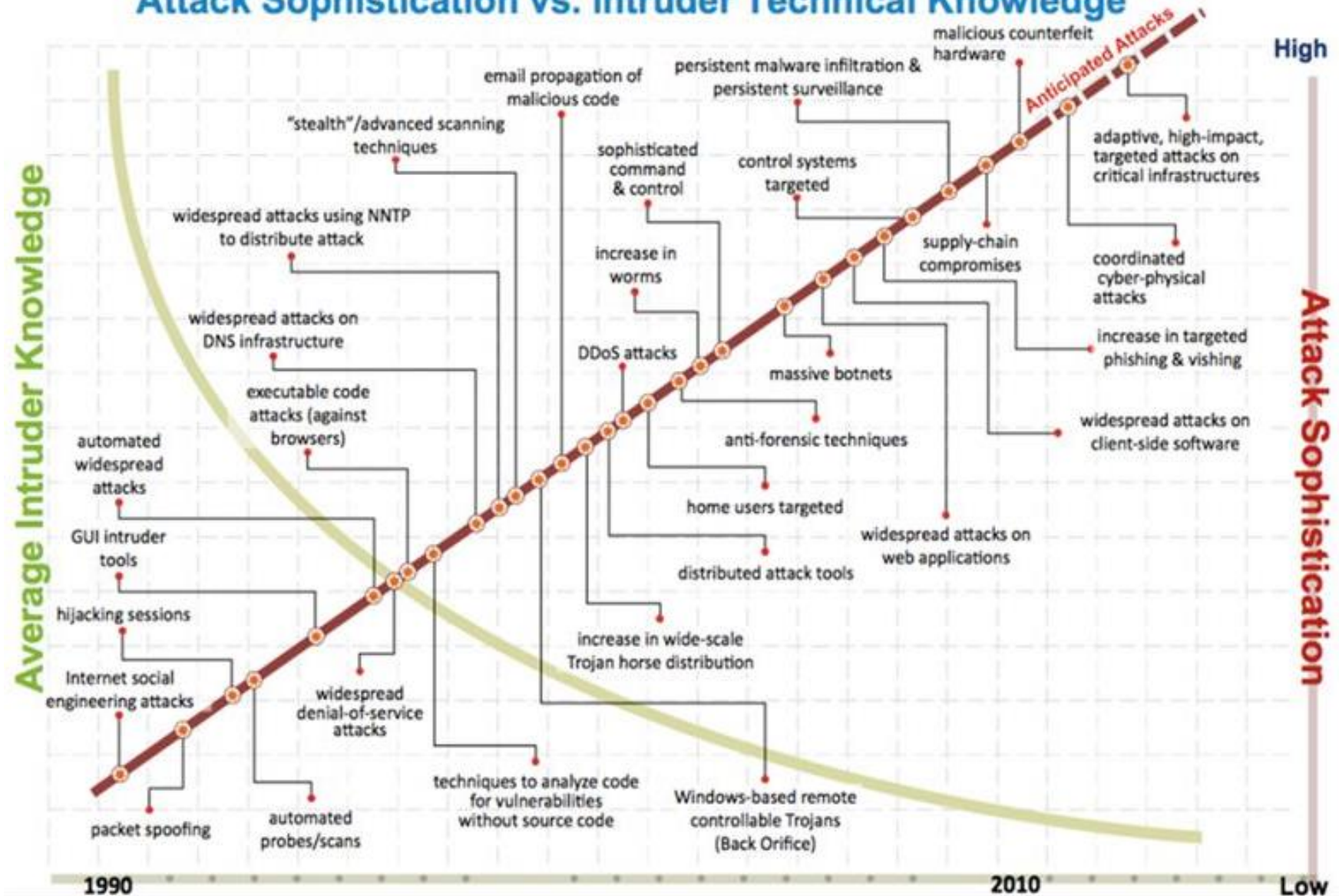
Security Structure Scheme

Key Properties

Symmetric Encryption

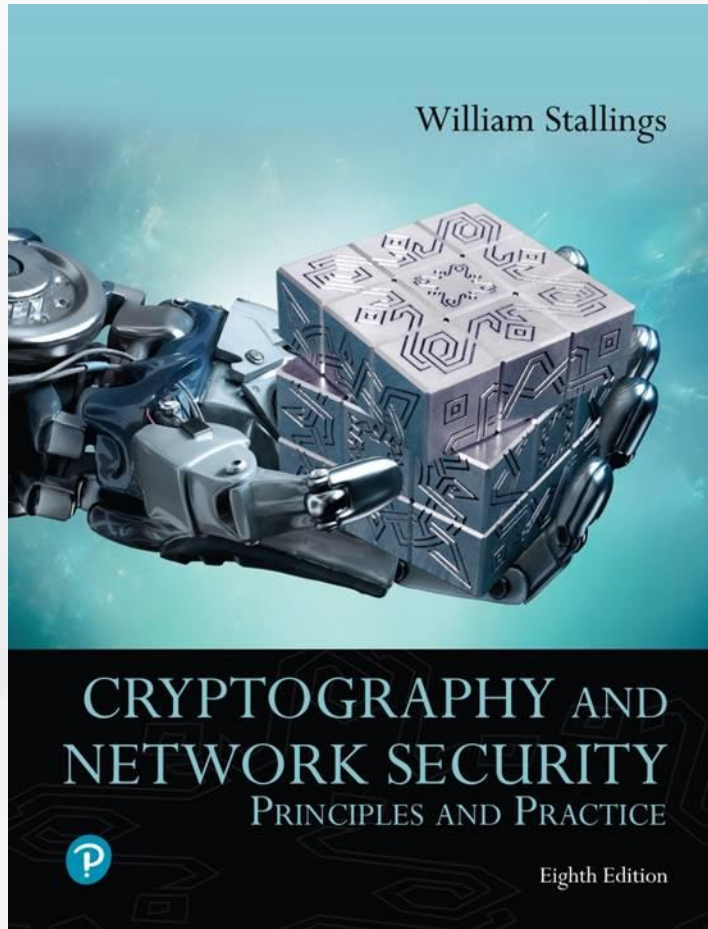
Asymmetric Encryption

Attack Sophistication vs. Intruder Technical Knowledge



Cryptography and Network Security: Principles and Practice

Eighth Edition



Chapter 1

Information and Network Security
Concepts

What is Cyber Security (Network Security) !

- **A network** is simply two or more computers linked together to share data, information or resources.
- **Security** : prevention of system Crash

Basic Terminologies

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

Cybersecurity (1 of 3)

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyberspace environment and organization and users' assets. Organization and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment.

Cybersecurity (2 of 3)

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users' assets against relevant security risks in the cyberspace environment. The general security objectives comprise the following: availability; integrity, which may include data authenticity and nonrepudiation; and confidentiality

Cybersecurity (3 of 3)

Information Security

- This term refers to preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved

Network Security

- This term refers to protection of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects

Security Objectives (1 of 2)

- The cybersecurity definition introduces three key objectives that are at the heart of information and network security:
 - Confidentiality: This term covers two related concepts:
 - Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals
 - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Security Objectives (2 of 2)

- **Integrity:** This term covers two related concepts:
 - **Data integrity:** Assures that data and programs are changed only in a specified and authorized manner. This concept also encompasses data authenticity, which means that a digital object is indeed what it claims to be or what it is claimed to be, and nonrepudiation, which is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information
 - **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- **Availability:** Assures that systems work promptly and service is not denied to authorized users

Figure 1.1 Essential Information and Network Security Objectives



Table of Content

Cryptography

Computer Security

OSI Security Architecture

Security Structure Scheme

Key Properties

Symmetric Encryption

Asymmetric Encryption

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 Content

Cryptography

Computer Security

OSI Security Architecture

Security Structure Scheme

Key Properties

Symmetric Encryption

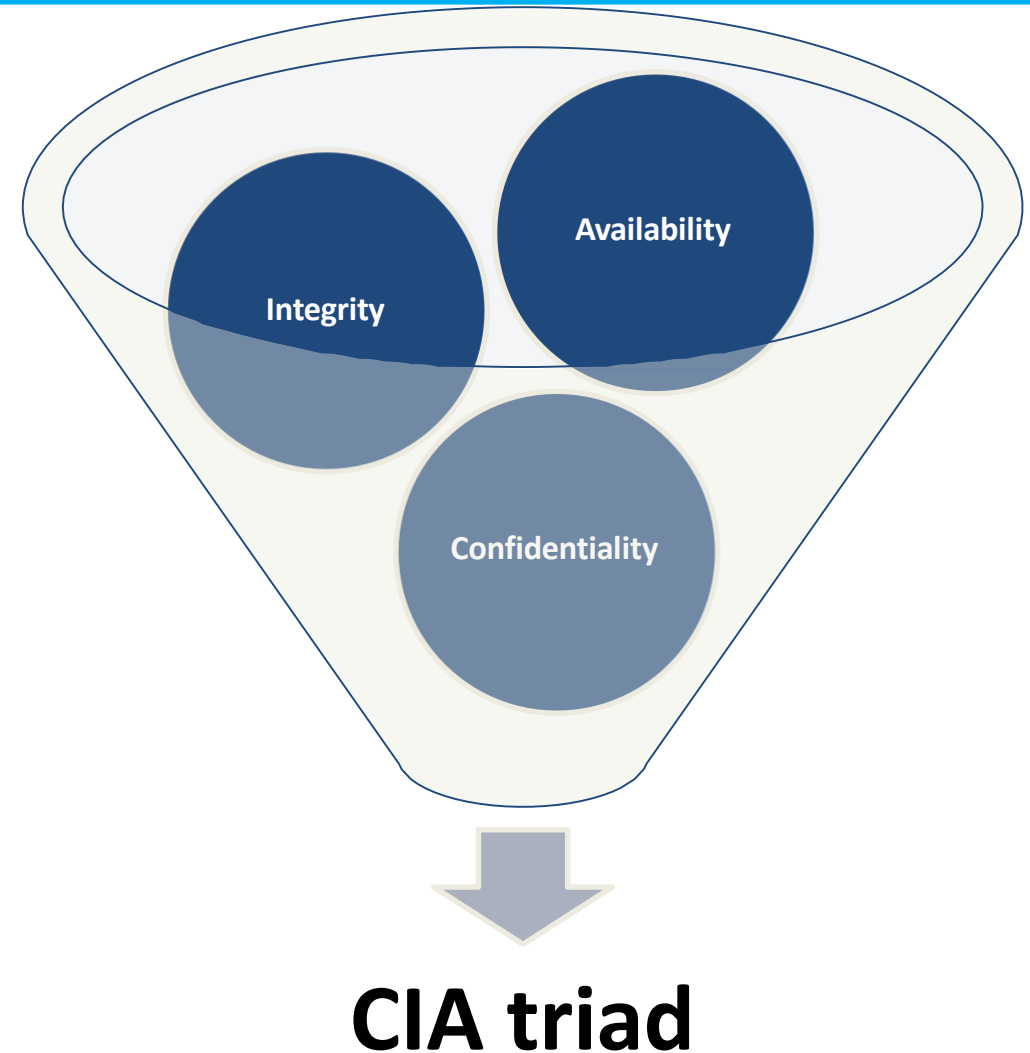
Asymmetric Encryption

Computer Security

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

Security Services

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



confidentiality

- ❑ 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.



integrity

- ❑ 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.



availability

- ❑ 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.



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 Threats

Security mechanism

- ❑ A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- ❑ no single mechanism that will support all functions required

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

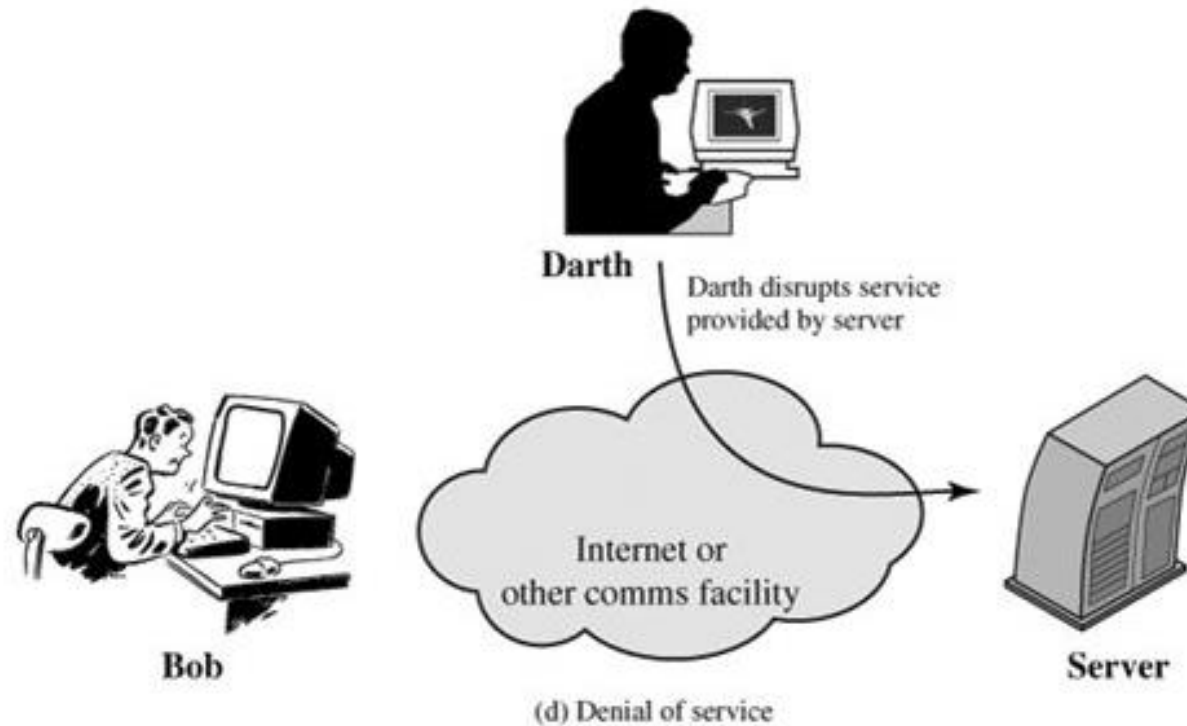
Security Attack

- ❑ 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 Attack

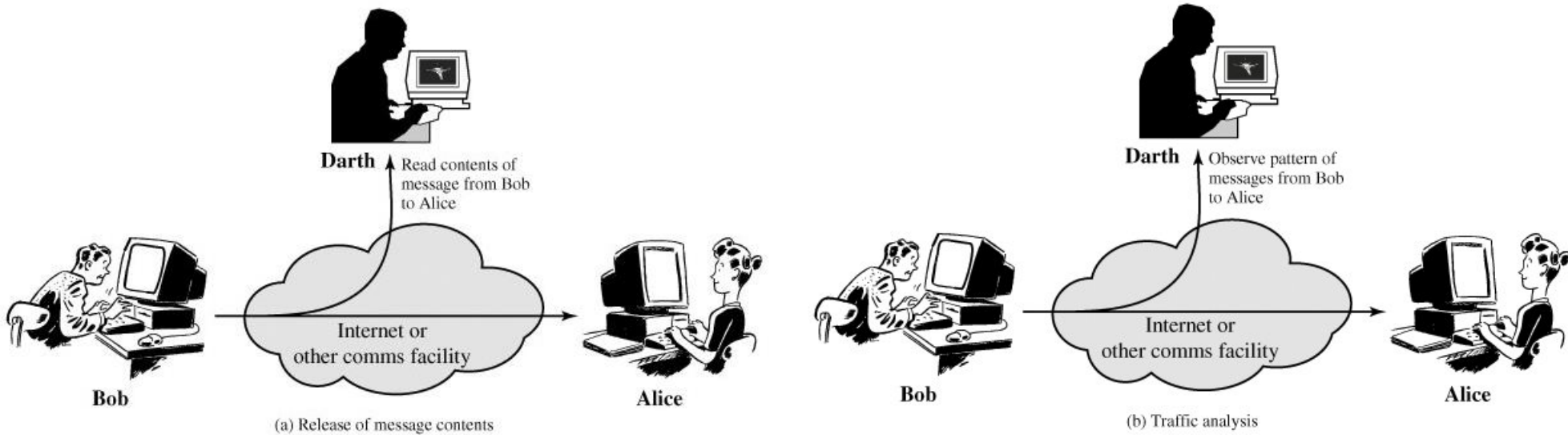
- ❑ A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- ❑ An active attack attempts to alter system resources or affect their operation.

Security Threats



- ❑ Interruption Threats

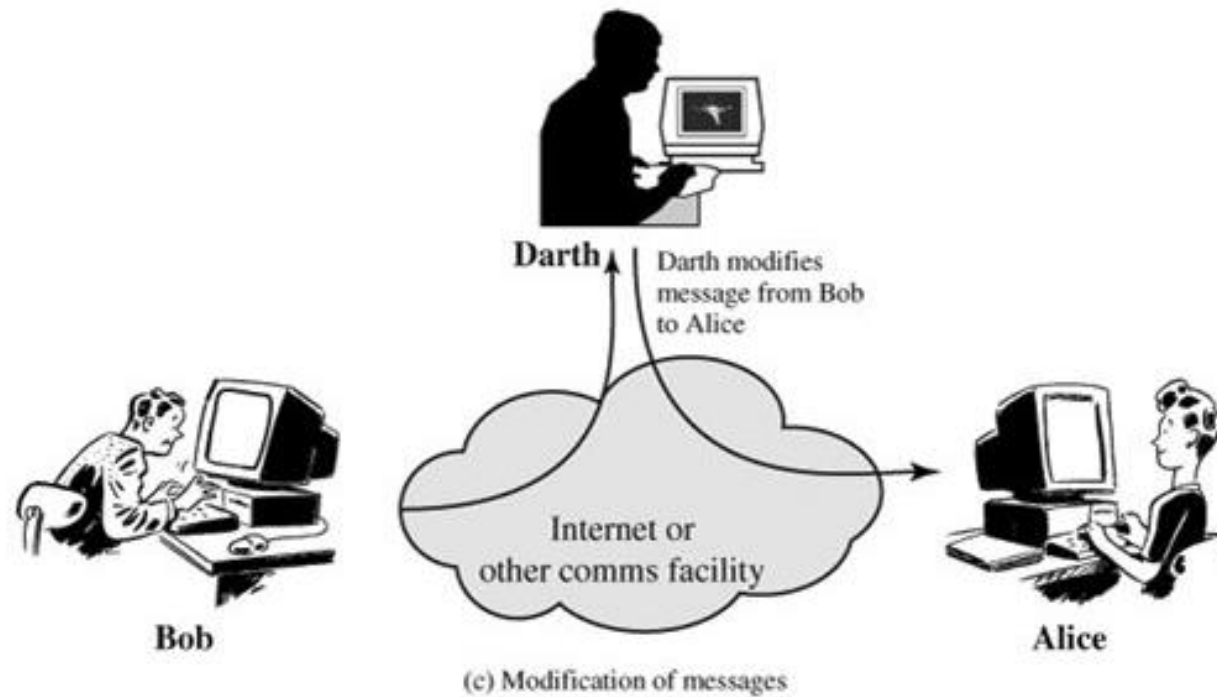
Security Threats



❑ Interception Threats

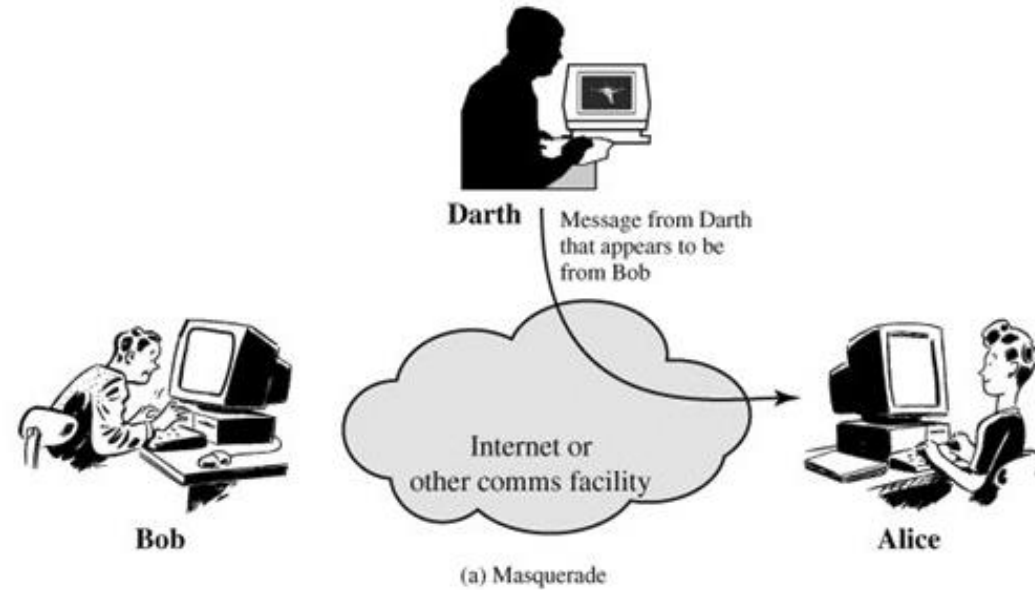


Security Threats



- ❑ Modification Threats

Security Threats



- ❑ Fabrication Threats

Table of Content

Cryptography

Computer Security

OSI Security Architecture

Security Structure Scheme

Key Properties

Symmetric Encryption

Asymmetric Encryption

Plaintext



Key

Encryption



Ciphertext

Ciphertext



Key

Decryption



Plaintext

- ❑ **Plain text** is the original message or data
- ❑ **Secret Key** is a value independent of the plaintext and of the algorithm.
- ❑ **Cipher text** This is the scrambled message produced as output.
- ❑ **Encryption Algorithm** is a mathematical procedure for performing encryption on data.
- ❑ **Decryption Algorithm** is a mathematical procedure for performing decryption on data.

Cryptography

Computer Security

OSI Security Architecture

Security Structure Scheme

Key Properties

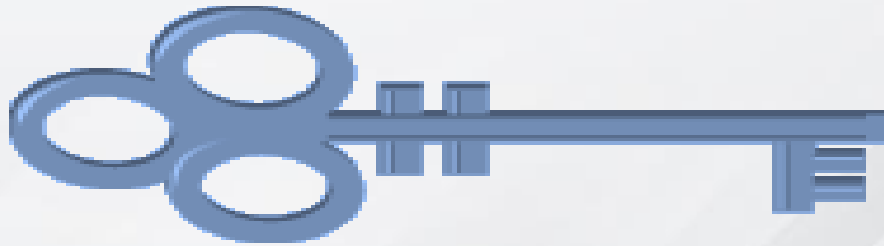
Symmetric Encryption

Asymmetric Encryption

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 Content

Cryptography

Computer Security

OSI Security Architecture

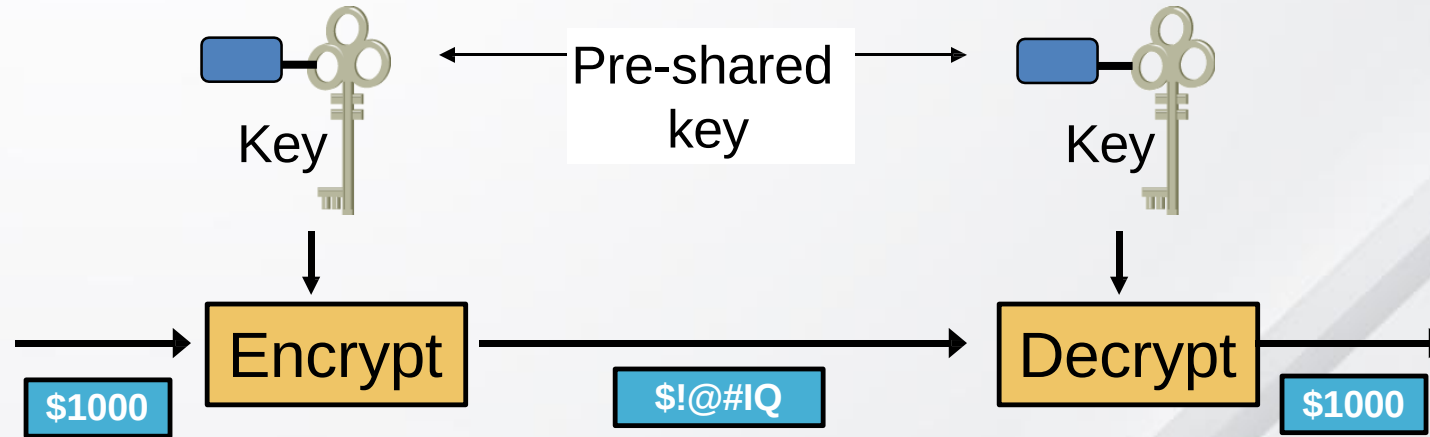
Security Structure Scheme

Key Properties

Symmetric Encryption

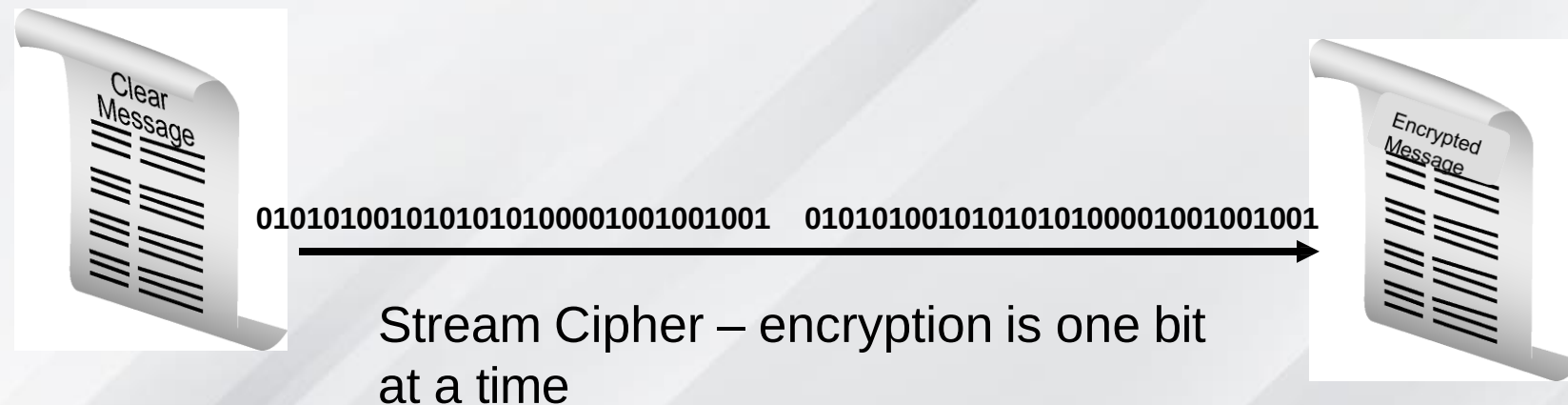
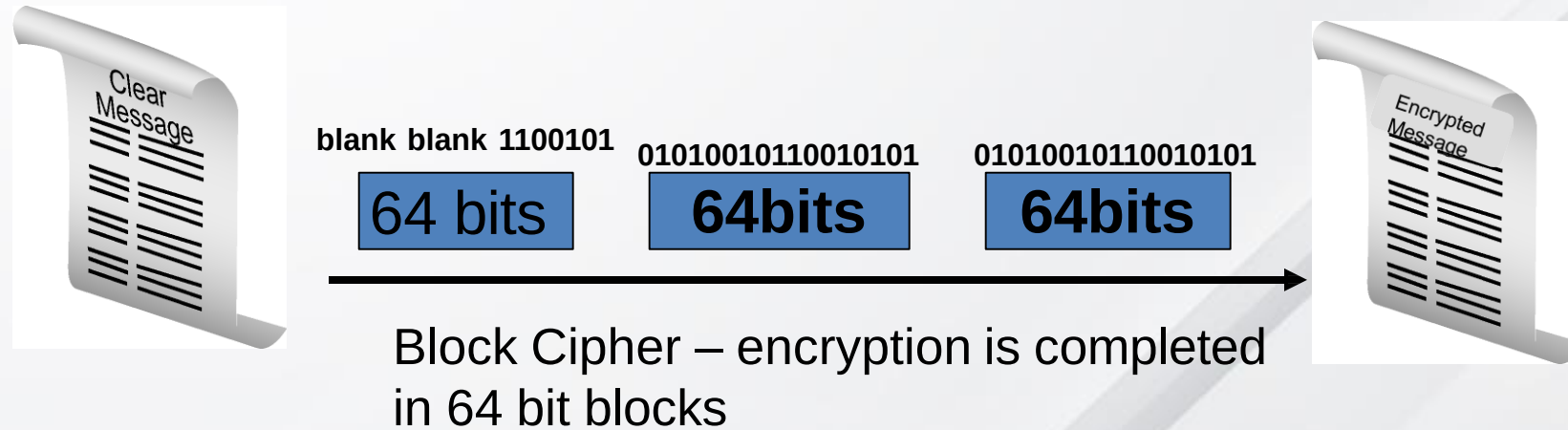
Asymmetric Encryption

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



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 Content

Cryptography

Computer Security

OSI Security Architecture

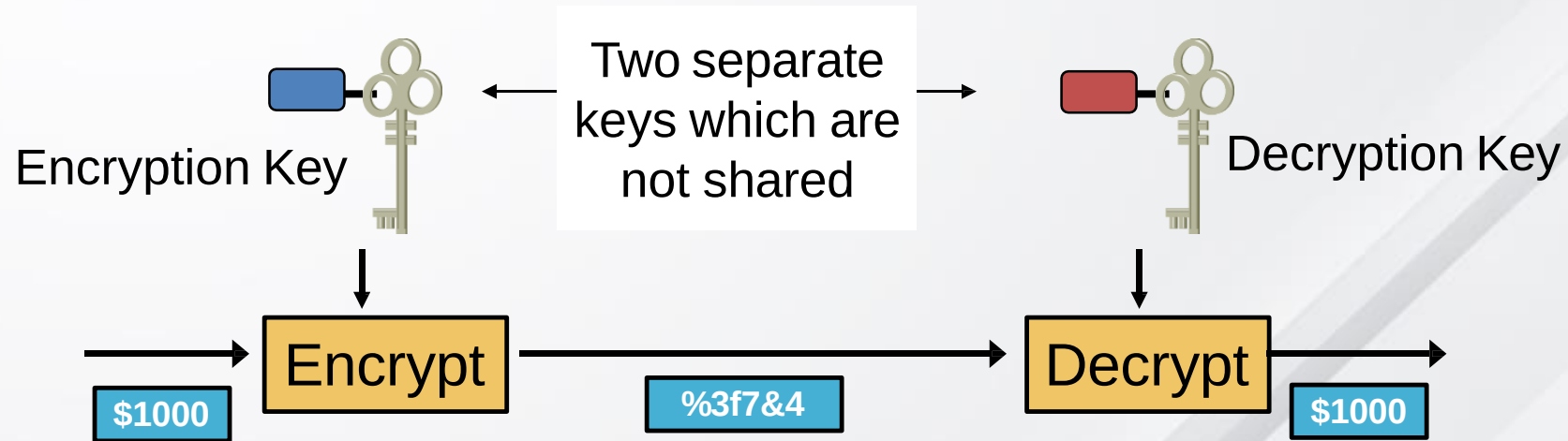
Security Structure Scheme

Key Properties

Symmetric Encryption

Asymmetric Encryption

Asymmetric Encryption Techniques



- ❑ 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.

References

- Kumar, Rajesh, and Pinky Ramchandra Shinde. "Computer Network-IP Address & Subnetting." *International Journal of Engineering and Advanced Technology (IJEAT)* 5, no. 4 (2016): 242-246.
- Singh, Dr Anil Kumar. "Internet Protocol (IP) Address-Subnetting and Supernetting." *Int. J. Emerg. Trends Technol. Comput. Sci* 4 (2015): 87-90.
- Sisat, Shailesh N., Prajkta S. Bhopale, and Vishwajit K. Barbudhe. "IP Subnetting." *International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCE)* 2, no. 5 (2012): 5.
- Cheon, SeongKwon, DongXue Jin, and ChongGun Kim. "A VLSM address management method for variable IP subnetting." In *International Conference on Computational Science and Its Applications*, pp. 73-83. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

