كلية الرشيد الجامعة
قسم هندسة تقنيات الحاسوب

المرحلة الرابعة

أمنية الحاسوب و شبكاتها

المحاضرة رقم (١)

مدرس المادة : م.م تميم محمد

SECURITY OF COMPUTER AND NETWORKS

REFERENCE

CRYPTOGRAPHY AND NETWORK SECURITY

PRINCIPLES AND PRACTICE 5TH EDITION

وزارة التعليم العالي والبحث العلمي
الجامعة التقنية الوسطى
قسم الشؤون العلمية
الدراسات العليا

وزارة التعليم العالي والبحث العلمي / الجامعة التقنية الوسطى
كلية التقنيات الهندسية الكهربائية والالكترونية / قسم هندسة تقنيات الحاسوب
المرحلة: الرابعة / الفرع: شبكات اتصالات الحاسوب

اسم المادة		عدد الساعات الاسبوعية			
باللغة العربية	باللغة الانكليزية	ن	ع	م	عدد الوحدات
امنية الحاسوب وشبكاتها	Security of computer & Networks	2	2	4	6

أهداف المادة:تهدف المادة الى:
تهدف المادة الى بيان الوسائل والطرق التي يجب اتباعها لحماية الحاسوب من الدخول اليها من غير المخولين والعبث فيها كذلك حماية البيانات وقواعد البيانات من المتطفلين كذلك حماية شبكة الحاسوب وخصوصا الشبكات الخاصة من هجمات المتطفلين من خلال تفعيل واستثمار بروتوكولات حماية الشبكات.

Weeks	Syllabus
1st, 2nd, 3rd	Introduction ,Symmetric Ciphers model: plaintext, encryption algorithm, secret key, cipher text, decryption algorithm, A Model of conventional encryption. Cryptography, Cryptanalysis, block and stream cipher
4th	Caeser Cipher The affine Cipher
5th, 6th	Mono alphabetic substitution ciphers Shift ciphers
7th	Hill cipher
8th	Playfair cipher
9th	Polyalphabetic ciphers Vigenere cipher
10th	The Transposition cipher
11th	Affine cipher
12th	One time pad
13th, 14th , 15th	Cryptanalysis of a Symmetric key
16th	Euclid's Algorithm
17th, 18th , 19th	SYMMETRIC-KEY ALGORITHMS -DES—The Data Encryption Standard, hers -16 round Feistel system
20st , 21nd	PUBLIC-KEY ALGORITHMS, -RSA, - Other Public-Key Algorithms,
22nd ,2 3rd, 24th ,25th	AUTHENTICATION PROTOCOLS, -Authentication Based on a Shared Secret Key, -Establishing a Shared Key: The Diffie -Hellman Key Exchange, -Authentication Using a Key Distribution Center, -Authentication Using Kerberos, - Authentication Using Public-Key Cryptography,
26th, 27th	OSI security Architecture , a model for network security,EMAIL SECURITY -PGP—Pretty Good Privacy, S/MIME
28th , 29th ,30th	Protocols of computer networks PROTECTION SERVICES: • OS protection service: protected objects and methods of OS protection, security of OS, memory and addressing protection, fence protection • Database protection service: • Network protection service: IP and E-Commerce protection, VPN and next generation networks protection

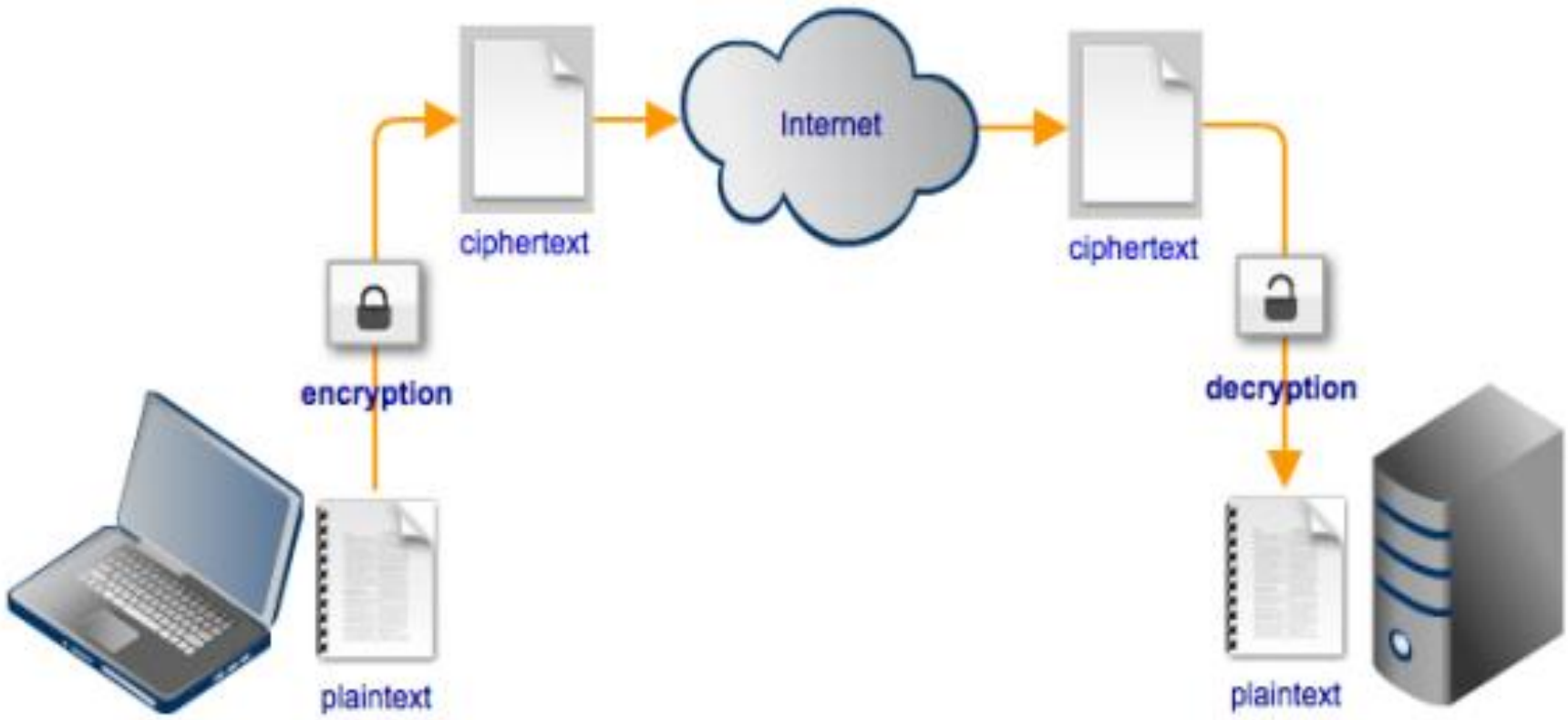
INTRODUCTION

Data security

Refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites.

Data security also protects data from corruption.

INTRODUCTION



CRYPTOGRAPHY

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

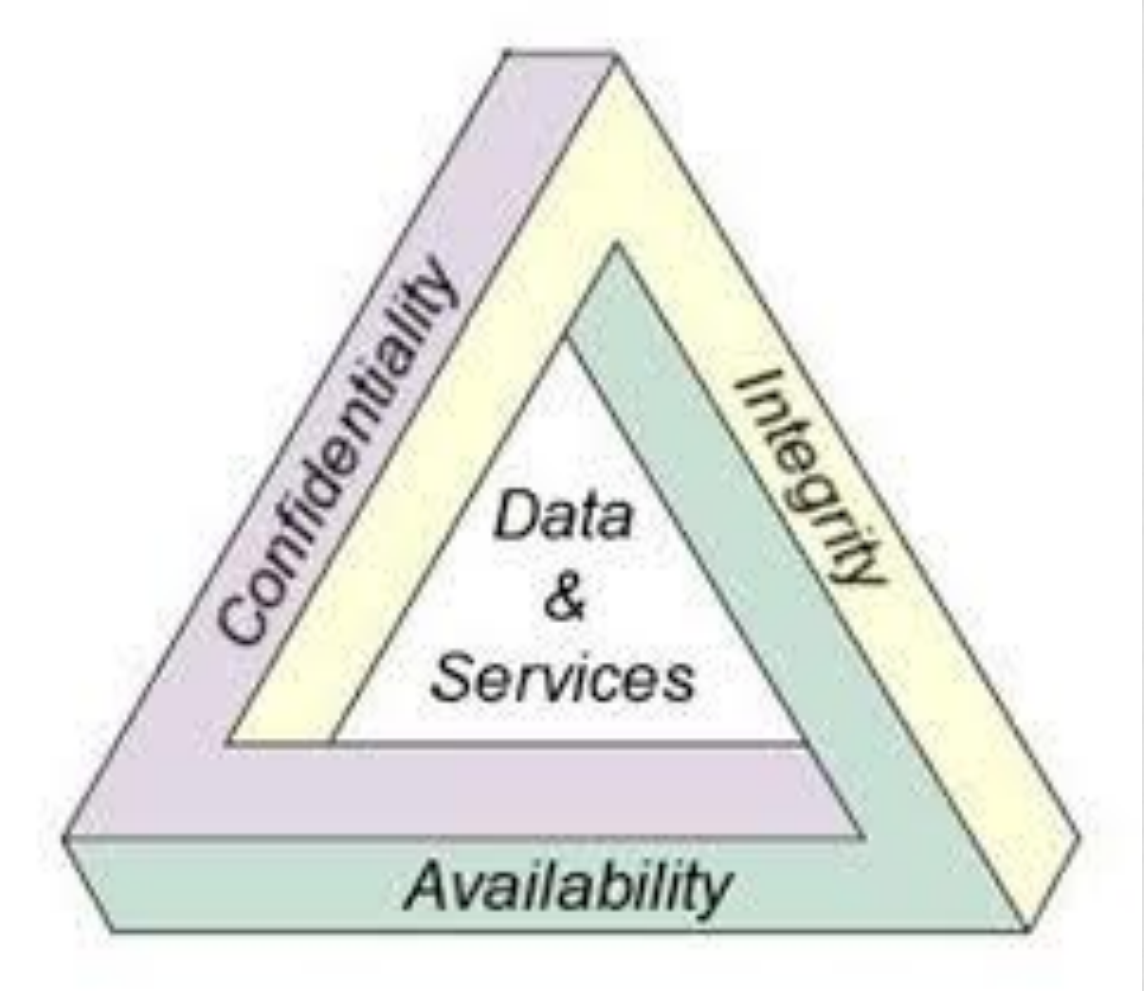
SECURITY OBJECTIVES

- **Confidentiality**: Preserving authorized restrictions on information, including means for protecting personal privacy and proprietary information.

A loss of confidentiality is the unauthorized disclosure of information.

- **Integrity:** 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 of access to or use of information or an information system.

CIA TRIANGLE



CRYPTANALYSIS

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