What is cryptography(التشفير)?

Is the science of secret writing and it is an ancient art

هو علم الكتابة السرية وهو فن قديم

Give the Definitions of:

Computer security: generic name for the collection of tools designed to protect data. هو اسم عام لمجموعة الادوات المصممة لحماية البيانات

Network Security: measures to protect data during their transmission (1 network) الاجراءات المتخذة لحماية البيانات اثناء نقلها.

Internet Security: measures to protect data during their transmission over a collection of interconnected networks الاجراءت المتخذة لحماية البيانات اثناء نقلها عبر مجموعة من الشبكات المتصلة.

What are The goals that we seek to achieve in the field of computer security

- **Integrity (التأكد من سلامة البيانات)**
- **Availability (التوافر التأكد من انه يمكن الوصول الى البيانات)**
- **Confidentiality(السرية)**

What is meant by integrity?

Assuring the message that the receiver has received not been altered in any way from the original التأكد من الرسالة التي استلمها المستلم لم يتم تبديلها عن الهيئة الاصلية.

What is meant by Availability?

Ensuring timely and reliable access to and use of information
التأكد من انه يمكن الوصول الى البيانات واستخدمها في الوقت المطلوب فيه

What is meant by Confidentiality?

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

التأكد من عدم قراءة أي شخص للرسالة غير المستلم

what OSI security architecture focuses on write brief about each one:

Security mechanisms: a process that is designed to detect, prevent, or recover from a security attack.

we can say security service is deployment security mechanisms

هي عمليه مصممة للتعرف او تجنب او الاسترجاع من أي هجوم امنى

Security service: a processing or communication service that enhances the security of the data processing systems and the information transfers. The services are intended to use one or more security mechanisms to provide service.

هي خدمة تواصل تقوم بتحسين الامن اثناء نقل البيانات وتقوم باستخدام اكتر من ميكانزيم امان لتوفير الخدمة

Security attack: any action that can effect on the security of information owned by an organization

أي اجراء يوثر على امن البيانات المملوكة بواسطة منظمة

Mention two types of security attacks:

Passive attack: attempts to learn or make use of information from the system but does not affect system resources.

تهدف الى استغلال المعلومات من النظام ولكن لا يؤثر على موارد النظام

Active attack: to alter system resources or affect their operation.استبدال موارد النظام او التأثير على العمليات

What are elements of security structure scheme?

Plaintext(P): is the original message or data. الرسالة

Secret key(K): is a value independent of plaintext and algorithms.غير معتمد على النص او الالجروزم التشفير

Ciphertext(C): this is encrypted message produced as output رسالة مشفرة

What mean by Encryption algorithm and Decryption algorithm?

is a mathematical procedure for performing encryption on dataاجراءات حسابيه لإجراء تشفير للبيانات

// Decryption on data

Mention key properties?

Shorter Keys: faster processing but less secure

أسرع في المعالجة ولكن اقل منا

Longer Keys: slower processing but more secure

اقل في وقت المعالجة ولكن اقل امنا

Single use key (one time key): used only to encrypt one message. مفتاح يستخدم مرة واحده فقط لرسالة واحده فقط

Multi use key (many times key): key used to encrypt multiple messages. مفاتيح مختلفة لأكثر من رسالة

Compare Between Symmetric Encryptions Vs Asymmetric Encryption?

Symmetric:

Known as shared-secret key algorithm.

Key length 80-256 bits

A sender and receiver must share a secret key.

Faster processing using simple mathematical operation.

Including DES, AES,etc.

Encryption Techniques:

Block Cipher-Encryption: cryptographic key and algorithm are applied to a block of data. (64 bit)

Stream cipher: plaintext digit is combined with a pseudorandom cipher digit stream. (bit by bit)

Asymmetric:

public key algorithm called public because each person share one of their keys

key length: 512-4096

sender and receiver do not share a secret key.

slow because difficult computational

include RSA, etc.

Cryptoanalysis: is the science of analyzing and breaking encryption.

Cryptology: is the term referring to the wide study of secret writing and covered both cryptography and cryptoanalysis