اسم الطالب الثلاثي (عربي):

الأجوبة النموذجية

Q1)) ANSWER all of the following: (16*3=48-points)

T F **1)** OSI security architecture provides a systematic framework for defining security attacks, mechanisms, and services.

T F **2)** Security attacks are classified as either passive or aggressive.

T F **3)** Authentication protocols and encryption algorithms are examples of security mechanisms.

T F **4)** The field of network and Internet security consists of measures to deter, prevent, detect and correct security violations that involve the transmission of information.

T F **5)** Symmetric encryption is used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords.

T F **6)** A prime number can have a remainder when divided by positive or negative values of itself.

T F **7)** The number 37 is prime so therefore all of the positive integers from 1 to 36 are relatively prime to 37.

8) ____ is the most common method used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.

A) Symmetric encryption B) Data integrity algorithms

C) Asymmetric encryption D) Authentication protocols

9) A common technique for masking contents of messages or other information traffic so that opponents can not extract the information from the message is ____.

A) integrity B) encryption C) analysis D) masquerade

10) A loss of _____is the unauthorized disclosure of information.

A) authenticity B) confidentiality C) reliability D) integrity

11) A _____ is any action that compromises the security of information owned by an organization.

A) security attack B) security service C) security alert D) security mechanism

12) _ Nonrepudiation _ prevents either sender or receiver from denying a transmitted message.

13) The __Notarization__ is the use of a trusted third party to assure certain properties of a data exchange.

14) The _____ algorithm is typically used to test a large number for primality.

A. Rijndael B. Fermat C. Miller-Rabin D. Euler

15) Two numbers are _ relatively prime _ if their greatest common divisor is 1.

16) The _ greatest common divisor _ of integers *a* and *b*, expressed (gcd a, b), is an integer *c* that divides both *a* and *b* without remainder and that any divisor of *a* and *b* is a divisor of *c*.

Q2)) Describe using Figure the Essential Network and Computer Security Requirements? What is FIPS PUB 199, Describe the levels of impact on organizations or individuals should there be a breach of security by FIPS? (26-points)
ANSWER

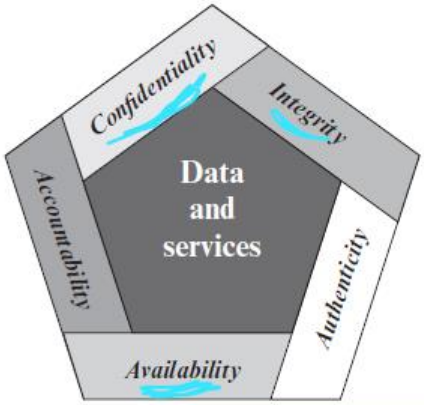

Figure 1.1 Essential Network and Computer Security Requirements

These levels are defined in FIPS PUB 199 as follow:

- **Low:** The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
- **Moderate:** The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.
- **High:** The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries.

Q3)) What is Euclidian Algorithm? Describe using Table the Properties of Modular Arithmetic for Integers?

Prove That $\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$ **Where n=21? (26-points)**

ANSWER:

One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. First, we need a simple definition: Two integers are **relatively prime** if and only if their only common positive integer factor is 1.

Table 2.3 Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Proving Euler (21):

$$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$$
where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.