Student Number :

Name, Surname :

Signature :

**TRUE OR FALSE**

T F 1. Security attacks are classified as either passive or aggressive.

T F 2. Thanks to years of research and development, it is now possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions.

T F 3. The emphasis in dealing with active attacks is on prevention

rather than detection.

T F 4. Two integers *a* and *b* are said to be congruent modulo *n*, if

(*a* mod *n*) = (*b* mod *n*).

T F 5. If *b*|*a* we say that *b* is a divisor of *a*.

T F 6. Symmetric encryption is a form of cryptosystem in which

encryption and decryption are performed using different keys. It is

also known as non-conventional encryption.

T F 7. With the use of symmetric encryption, the principal security

problem is maintaining the secrecy of the key.

T F 8. When using symmetric encryption it is very important to keep the

algorithm secret.

T F 9. (*ax* mod *n*)y = (*ay* mod *n*)x.

T F 10. If p is prime and a is a positive integer, then ap-1 = p(mod p).

**MULTIPLE CHOICE**

1. 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

1. \_\_\_\_\_\_\_\_\_\_ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

A) Disruption B) Replay C) Service denial D) Masquerade

1. A loss of \_\_\_\_\_\_\_\_\_\_ is the unauthorized disclosure of information.

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

1. Verifying that users are who they say they are and that each input arriving at the system came from a trusted source is \_\_\_\_\_\_\_\_\_ .

A) authenticity B) credibility C) accountability D) integrity

1. A \_\_\_\_\_\_\_\_\_\_ takes place when one entity pretends to be a different entity.

A) replay B) masquerade C) service denial D) passive attack

1. A(n) \_\_\_\_\_\_\_\_\_\_ service is one that protects a system to ensure its availability and addresses the security concerns raised by denial- of- service attacks.

A) replay B) availability C) masquerade D) integrity

1. A(n) \_\_\_\_\_\_\_\_\_\_ is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.

A) threat B) attack C) risk D) attack vector

1. Two integers are \_\_\_\_\_\_\_\_\_\_ if their only common positive integer factor is 1.

A)relatively prime B) congruent modulo C) polynomials D)residual

1. Gcd(517,238) =?

A) 1 B) 11 C) 3 D) 55

1. An original intelligible message fed into the algorithm as input is known as \_\_\_\_\_\_\_\_\_ , while the coded message produced as output is called the \_\_\_\_\_\_\_\_\_\_ .

A) decryption, encryption B) plaintext, ciphertext C) ciphertext, plaintext D) encryption, decryption