**TRUE OR FALSE**

T F 1. Cryptography is the practice and study of techniques for secure communication and data in the presence of adversaries.

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 more critical a component or service, the higher the level of

required availability.

T F 5. 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 6. 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 7. Data origin authentication does not provide protection against the

modification of data units.

T F 8. The emphasis in dealing with active attacks is on prevention

rather than detection.

T F 9. The connection-oriented integrity service addresses both

message stream modification and denial of service.

T F 10. All the techniques for providing security have two components: a

security-related transformation on the information to be sent and some secret information shared by the two principals.

T F 11. The data integrity service inserts bits into gaps in a data stream to

frustrate traffic analysis attempts.

T F 12. 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 13. Two integers *a* and *b* are said to be congruent modulo *n*, if

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

T F 14. If *b*|*a* we say that *b* is a divisor of *a*.

T F 15. Symmetric encryption remains by far the most widely used of the

two types of encryption.

T F 16. 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 17. With the use of symmetric encryption, the principal security

problem is maintaining the secrecy of the key.

T F 18. The process of converting from plaintext to ciphertext is known

as deciphering or decryption.

T F 19. The algorithm will produce a different output depending on the

specific secret key being used at the time. The exact substitutions

and transformations performed by the algorithm depend on the

key.

T F 20. When using symmetric encryption it is very important to keep the

algorithm secret.

T F 21. On average, half of all possible keys must be tried to achieve

success with a brute-force attack.

T F 22. Ciphertext generated using a computationally secure encryption

scheme is impossible for an opponent to decrypt simply because

the required information is not there.

T F 23. Monoalphabetic ciphers are easy to break because they reflect the

frequency data of the original alphabet.

T F 24. As with Playfair, the strength of the Hill cipher is that it

completely hides single letter frequencies.

T F 25. A scheme known as a one-time pad is unbreakable because it

produces random output that bears no statistical relationship to

the plaintext.

T F 26. The one-time pad has unlimited utility and is useful primarily for

high-bandwidth channels requiring low security.

T F 27. Steganography renders the message unintelligible to outsiders by

various transformations of the text.

**MULTIPLE CHOICE**

1. \_\_\_\_\_\_\_\_\_\_ 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

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 \_\_\_\_\_\_\_\_\_\_ 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

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

A) replay B) masquerade

C) service denial D) passive attack

1. \_\_\_\_\_\_\_\_\_\_ is the protection of transmitted data from passive attacks.

A) Access control B) Data control

C) Nonrepudiation D) Confidentiality

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. \_\_\_\_\_\_\_\_\_\_ threats exploit service flaws in computers to inhibit use by legitimate users.

A) Information access B) Reliability

C) Passive D) Service

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. An integer p >1 is a \_\_\_\_\_\_\_\_\_ number if and only if its only divisors are + 1 and + p.

A) prime B) composite

C) indexed D) positive

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

A)relatively prime B) congruent modulo

C) polynomials D)residual

1. The \_\_\_\_\_\_\_\_\_\_ of two numbers is the largest integer that divides both numbers.

A)greatest common divisor B) prime polynomial

C) lowest common divisor D) integral divisor

1. An important quantity in number theory referred to as \_\_\_\_\_\_\_\_\_\_ is defined as the number of positive integers less than n and relatively prime to n.

A) CRT B) Miller-Rabin

C) Euler’s totient function D) Fermat’s theorem

1. If p is prime and a is a positive integer, then ap = a(mod p) is an alternative form of \_\_\_\_\_\_\_\_\_ theorem.

A) Rijndael’s B) Vignere’s

C) Euler’s D)Fermat’s

1. For given integers a and b, the extended \_\_\_\_\_\_\_\_\_\_ algorithm not only calculates the greatest common divisor d but also two additional integers x and y.

A) modular B)Euclidean

C) associative D)cyclic

1. For any integer b and a primitive root a of prime number p we can find a unique exponent i. This exponent i is referred to as the \_\_\_\_\_\_\_\_\_\_\_ .

A) order B) discrete logarithm

C) bijection D)primitive root

1. As a \_\_\_\_\_\_\_\_\_ relation, mod expresses that two arguments have the same remainder with respect to a given modulus.

A) finite B)monic

C) congruence D) cyclic

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

1. Restoring the plaintext from the ciphertext is \_\_\_\_\_\_\_\_\_\_ .

A) deciphering B) transposition

C) steganography D) encryption

1. A \_\_\_\_\_\_\_\_\_\_ attack involves trying every possible key until an intelligible translation of the ciphertext is obtained.

A) brute-force B) Caesar attack

C) ciphertext only D) chosen plaintext

1. Techniques used for deciphering a message without any knowledge of the enciphering details is \_\_\_\_\_\_\_\_\_\_\_ .

A) blind deciphering B) steganography

C) cryptanalysis D) transposition

1. If both sender and receiver use the same key, the system is referred to as:

A) public-key encryption B) two-key

C) asymmetric D) conventional encryption

1. \_\_\_\_\_\_\_\_\_\_ attacks exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

A) Brute-force B) Cryptanalytic

C) Block cipher D) Transposition

1. The \_\_\_\_\_\_\_\_\_\_ attack is the easiest to defend against because the opponent has the least amount of information to work with.

A) ciphertext-only B) chosen ciphertext

C) known plaintext D) chosen plaintext

1. \_\_\_\_\_\_\_\_\_ refer to common two-letter combinations in the English language.

A) Streamings B) Transpositions

C) Digrams D) Polyalphabetic ciphers

1. A way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is \_\_\_\_\_\_\_\_\_\_\_ .

A) rail fence cipher B) cryptanalysis

C) polyalphabetic substitution cipher D) polyanalysis cipher

1. The methods of \_\_\_\_\_\_\_\_\_\_ conceal the existence of the message in a graphic image.

A) steganography B) decryptology

C) cryptology D) cryptography

**SHORT ANSWER**

1. A \_\_\_\_\_\_\_\_\_\_\_ is any process, or a device incorporating such a process, that is designed to detect, prevent, or recover from a security attack. Examples are encryption algorithms, digital signatures and authentication protocols.

2. An \_\_\_\_\_\_\_\_\_\_ attack attempts to alter system resources or affect their operation.

3. A loss of \_\_\_\_\_\_\_\_\_\_ is the disruption of access to or use of information or an information system.

4. A loss of \_\_\_\_\_\_\_\_\_ is the unauthorized modification or destruction of information.

5. A \_\_\_\_\_\_\_\_\_ attack attempts to learn or make use of information from the system but does not affect system resources.

6. In the context of network security, \_\_\_\_\_\_\_\_\_\_\_ is the ability to limit and control the access to host systems and applications via communications links.

7. \_\_\_\_\_\_\_\_\_\_ prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message and when a message is received, the sender can prove that the alleged receiver in fact received the message.

8. An \_\_\_\_\_\_\_\_\_\_ is an assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

9.The remainder r in the division algorithm is often referred to as a \_\_\_\_\_\_\_\_\_\_ .

10.One of the basic techniques of number theory is the \_\_\_\_\_\_\_\_\_\_ algorithm which is a simple procedure for determining the greatest common divisor of two positive integers.

11. If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. The integer n is called the \_\_\_\_\_\_\_\_\_\_ .

12. Two theorems that play important roles in public-key cryptography are Fermat's theorem and \_\_\_\_\_\_\_\_\_\_ theorem.

13. \_\_\_\_\_\_\_\_\_\_ theorem states the following: If p is prime and a is a positive integer not divisible by p, then ap-1 = 1(mod p).

14. Two numbers are \_\_\_\_\_\_\_\_\_\_ if their greatest common divisor is 1.

15. The number of positive integers less than n and relatively prime to n is referred to as \_\_\_\_\_\_\_\_\_\_ function.

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

17. Two numbers are relatively prime if their greatest common divisor is \_\_\_\_\_\_.

18. An integer p > 1 is a \_\_\_\_\_\_\_\_\_\_ number if and only if its only divisors are + 1 and + p.

19. \_\_\_\_\_\_\_\_\_\_ encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.

20. An encryption scheme is said to be \_\_\_\_\_\_\_\_\_\_ if the cost of breaking the cipher exceeds the value of the encrypted information and the time required to break the cipher exceeds the useful lifetime of the information.

21. Cryptographic systems are characterized along three independent dimensions: the type of operations used for transforming plaintext to ciphertext; the way in which the plaintext is processed; and \_\_\_\_\_\_\_\_\_\_ .

22. All encryption algorithms are based on two general principles: substitution and

\_\_\_\_\_\_\_\_\_\_\_\_ .

23. A \_\_\_\_\_\_\_\_\_\_ cipher processes the input one block of elements at a time, producing an output block for each input block, whereas a stream cipher processes the input

elements continuously, producing output one element at a time.