**Chapter 9:** **Public-Key Cryptography and RSA**

**TRUE OR FALSE**

T F 1. Asymmetric encryption utilizes only a public key for encryption

and decryption.

T F 2. Asymmetric encryption can be used for confidentiality but not for

authentication.

T F 3. Asymmetric encryption transforms plaintext into ciphertext.

T F 4. Plaintext is transformed into ciphertext using two keys and a

decryption algorithm.

T F 5. A major advance in symmetric cryptography occurred with the

development of the rotor encryption/decryption machine.

T F 6. Public-key encryption is more secure from cryptanalysis than

symmetric encryption.

T F 7. Much of the theory of public-key cryptosystems is based on

number theory.

T F 8. Asymmetric algorithms rely on one key for encryption and a

different but related key for decryption.

T F 9. The encryption algorithm performs various transformation on the

ciphertext.

T F` 10. If the authenticator is encrypted with the sender's private key, it

serves as a signature that verifies origin, content, and sequencing.

T F 11. A trap-door one-way function is easy to calculate in one direction

and infeasible to calculate in the other direction unless certain

additional information is known.

T F 12. A public-key encryption scheme is not vulnerable to a brute-force

attack.

T F 13. Before the application of the public-key cryptosystem each

participant must generate a pair of keys.

T F 14. The defense against the brute-force approach for RSA is to use a

large key space.

T F 15. Timing attacks are ciphertext attacks that are only applicable to

RSA.

**MULTIPLE CHOICE**

1. Asymmetric encryption is also known as \_\_\_\_\_\_\_\_\_\_\_ .

A. public-key encryption B. private-key encryption

C. optimal encryption D. digital-key encryption

1. Public-key encryption is also known as \_\_\_\_\_\_\_\_\_\_\_ .

A. digital-key encryption B. asymmetric encryption

C. one way time exchange encryption D. optimal-key encryption

1. Asymmetric encryption can be used for \_\_\_\_\_\_\_\_\_\_ .
2. both confidentiality and authentication
3. neither confidentiality nor authentication
4. confidentiality
5. authentication
6. Plaintext is recovered from the ciphertext using the paired key and a \_\_\_\_\_\_\_\_\_\_\_\_\_ .

A. digital signature B. recovery encryption

C. decryption algorithm D. encryption algorithm

1. The most widely used public-key cryptosystem is \_\_\_\_\_\_\_\_\_\_ .

A. optimal asymmetric encryption

B. asymmetric encryption

C. RSA

D. DES

1. Public-key algorithms are based on \_\_\_\_\_\_\_\_\_\_ .

A. permutation B. mathematical functions

C. substitution D. symmetry

1. \_\_\_\_\_\_\_\_\_\_ are two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

A. Asymmetric keys B. Key exchanges

C. Symmetric keys D. Cipher keys

1. The \_\_\_\_\_\_\_\_\_\_ indicates that the subscriber identified in the certificate has sole control and access to the private key.

A. OAEP B. Public Key Certificate

C. Digital Signature D. PKI

cabc

1. A \_\_\_\_\_\_\_\_\_\_ is a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.
2. Private Key (Symmetric) Cryptographic Algorithm
3. Key Exchange Cryptographic Algorithm
4. Public Key (Asymmetric) Cryptographic Algorithm
5. RSA Digital Cryptographic Algorithm
6. A public-key encryption scheme has \_\_\_\_\_\_\_\_\_\_ ingredients.

A. six B. four

C. eight D. two

1. The key used in symmetric encryption is referred to as a \_\_\_\_\_\_\_\_\_\_ key.

A. public B. secret

C. private D. decryption

1. The readable message or data that is fed into the algorithm as input is the \_\_\_\_\_\_\_\_\_\_\_\_ .

A. ciphertext B. exchange

C. plaintext D. encryption

1. Two issues to consider with the computation required to use

RSA are encryption/decryption and \_\_\_\_\_\_\_\_\_\_ .

A. time complexity B. trap-door one-way functions

C. key generation D. asymmetric encryption padding

1. \_\_\_\_\_\_\_\_\_\_ depend on the running time of the decryption algorithm.

A. Mathematical attacks B. Timing attacks

C. Chosen ciphertext attacks D. Brute-force attacks

1. We define the \_\_\_\_\_\_\_\_\_\_\_ of an algorithm to be f(n) if, for all n and all inputs of length n the execution of the algorithm takes at most f(n) steps. This is a common measure of the efficiency of an algorithm.

A. time complexity B. one-way function

C. timing attack D. OAEP

**SHORT ANSWER**

1. Asymmetric \_\_\_\_\_\_\_\_\_\_ encryption is a form of cryptosystem in which encryption and decryption are performed using a public key and a private key.
2. A key exchange \_\_\_\_\_\_\_\_\_\_ is when two sides cooperate to exchange a session key.
3. Asymmetric encryption transforms plaintext into \_\_\_\_\_\_\_\_\_\_ using one of two keys and an encryption algorithm.
4. The difficulty of attacking RSA \_\_\_\_\_\_\_\_\_\_ is based on the difficulty of finding the prime factors of a composite number.
5. Public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric \_\_\_\_\_\_\_\_\_\_\_ encryption, which uses only one key.
6. Public Key Certificate \_\_\_\_\_\_\_\_\_\_ is a digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key.
7. The Public Key Infrastructure (PKI)\_\_\_\_\_\_\_\_\_\_ is a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
8. The scrambled message produced as output is the ciphertext . It depends on the plaintext and the key.
9. A one-way function \_\_\_\_\_\_\_\_\_\_ is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible.
10. "The sender ‘signs’ a message with its private key. Signing is

achieved by a cryptographic algorithm applied to the message

or to a small block of data that is a function of the message," is

a description of a digital signature \_\_\_\_\_\_\_\_\_\_\_ .

1. The RSA \_\_\_\_\_\_\_\_\_\_ scheme is a block cipher in which the plaintext

and ciphertext are integers between 0 and n - 1 for some n.

1. A single algorithm that will calculate the greatest common

divisor (gcd) of two integers and, if the gcd is 1, determine the inverse of one of the integers modulo the other, is the Euclid \_\_\_\_\_\_\_\_\_\_ algorithm.

1. Four possible approaches to attacking the RSA algorithm are:

brute force, mathematical attacks, chosen ciphertext attacks, and timing attack\_\_\_\_\_\_\_\_\_\_\_ .

1. A CCA chosen ciphertext attack\_\_\_\_\_\_\_\_\_\_ is an attack in which the adversary chooses a number of ciphertexts and is then given the corresponding plaintexts, decrypted with the target's private key.
2. To counter attacks such as CCAs, RSA Security, Inc. recommends modifying the plaintext using a procedure known as optimal asymmetric encryption padding (OAEP)\_\_\_\_\_\_\_\_\_\_\_ .