Started on	Wednesday, 23 February 2022, 7:00 PM
State	Finished
Completed on	Wednesday, 23 February 2022, 7:35 PM
Time taken	35 mins 14 secs
Grade	**27.00** out of 30.00 (**90**%)

Question 1

Correct

Mark 1.00 out of 1.00

In public key cryptosystem ____ keys are used for encryption and decryption.

- a. Same
- b. Different ✔
- c. shared key

Your answer is correct.

The correct answer is:
Different

Question 2

Correct

Mark 1.00 out of 1.00

In public key cryptosystem which is kept as public?

- a. Both
- b. Encryption keys ✔
- c. Decryption keys

Your answer is correct.

The correct answer is:
Encryption keys

Question 3

Correct

Mark 1.00 out of 1.00

Public-key cryptography is also known as

- a. Both a and b
- b. Asymmetric Cryptography ✔
- c. symmetric cryptography

Your answer is correct.

The correct answer is:
Asymmetric Cryptography

Question 4

Correct

Mark 1.00 out of 1.00

Which of the following keys are known only to the owner?

- a. protected key
- b. private key ✔
- c. public key

Your answer is correct.

The correct answer is:
private key

Question 5

Correct

Mark 1.00 out of 1.00

Using Rivest, Shamir, Adleman cryptosystem with p=7 and q=9. Encrypt M=24 to find ciphertext. The Ciphertext is:

- a. 114 ✔
- b. 35
- c. 20

Your answer is correct.

The correct answer is:
114

Question 6

Correct

Mark 1.00 out of 1.00

RSA algorithm is ___ cryptography algorithm.

- a. asymmetric ✔
- b. systematic
- c. symmetric

Your answer is correct.

The correct answer is:
asymmetric

Question 7

Correct

Mark 1.00 out of 1.00

RSA is named after the researchers (____) who proposed it.

- a. Rivest Shamir Adleman ✔
- b. Rivest Shameet, Adam
- c. 1. River, Shamir, Adleman

Your answer is correct.

The correct answer is:
Rivest Shamir Adleman

Question 8

Correct

Mark 1.00 out of 1.00

Public key algorithms are computationally _____ to find decryption key knowing only algorithm & encryption key

- a. infeasible ✔
- b. difficult
- c. feasible

Your answer is correct.

The correct answer is:
infeasible

Question 9

Correct

Mark 1.00 out of 1.00

The public key of user A will be denoted _____

- a. KRA
- b. KURB
- c. KUA ✔

Your answer is correct.

The correct answer is:
KUA

Question 10

Correct

Mark 1.00 out of 1.00

One entity pretends to be another entity is _____

- a. unauthorized acecess
- b. Brute force
- c. Masquerading ✔

Your answer is correct.

The correct answer is: Masquerading

Question 11

Incorrect

Mark 0.00 out of 1.00

Sender "signs" the message) using his private key ensures_____

- a. integrity
- b. confidentiality ✖
- c. Digital Sign

Your answer is incorrect.

The correct answer is:
Digital Sign

Question 12

Correct

Mark 1.00 out of 1.00

In RSA, the public key KU of the recipient is

- a. e,n ✔
- b. p,n
- c. d,n

Your answer is correct.

The correct answer is:
e,n

Question 13

Correct

Mark 1.00 out of 1.00

Trying all possible private keys is _____

- a. sniffing attack
- b. insider attack
- c. brute force attack ✔

Your answer is correct.

The correct answer is:
brute force attack

Question 14

Correct

Mark 1.00 out of 1.00

_____is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

- a. DES
- b. RSA
- c. Diffie Hellman ✔

Your answer is correct.

The correct answer is:
Diffie Hellman

Question 15

Incorrect

Mark 0.00 out of 1.00

Primitive root of a prime number p, is one whose powers generate all the integers from _____

- a. 0 to q
- b. 0 to p-1 ✖
- c. 1 to p-1

Your answer is incorrect.

The correct answer is:
1 to p-1

Question 16

Correct

Mark 1.00 out of 1.00

Public Announcement of Public key is done by_____

- a. Unicast
- b. Anycast
- c. broadcast ✔

Your answer is correct.

The correct answer is:
broadcast

Question 17

Correct

Mark 1.00 out of 1.00

Public available directory maintains a directory with a _____entry for each participant

- a. public key
- b. name, secret key, public key
- c. {name, public key} ✔

Your answer is correct.

The correct answer is:
{name, public key}

Question 18

Incorrect

Mark 0.00 out of 1.00

In public key authority, timestamp is used to_____

- a. propagation time
- b. mark the moment of the request
- c. mark the time expiration of the request ✖

Your answer is incorrect.

The correct answer is:
mark the moment of the request

Question 19

Correct

Mark 1.00 out of 1.00

In public key certificates, For any communication between any two users, the ____ must be consulted by both users to get the newest public keys

- a. public authority
- b. directory
- c. central authority ✔

Your answer is correct.

The correct answer is:
central authority

Question 20

Correct

Mark 1.00 out of 1.00

Which technique is used for data protection

- a. Data piracy
- b. Authentication
- c. Encryption ✔

Your answer is correct.

The correct answer is:
Encryption

Question 21

Correct

Mark 1.00 out of 1.00

The art and science of breaking the cipher text is known as

- a. cryptology
- b. cryptanalysis ✔
- c. cryptography

Your answer is correct.

The correct answer is:
cryptanalysis

Question 22

Correct

Mark 1.00 out of 1.00

Which of the following is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key?

- a. plaintext
- b. encryption
- c. ciphertext ✔

Your answer is correct.

The correct answer is:
ciphertext

Question 23

Correct

Mark 1.00 out of 1.00

The encryption process where same keys are used for encrypting and decrypting the information is known as ?

- a. ASymmetric Key Encryption
- b. Symmetric Key Encryption ✔
- c. None of the above

Your answer is correct.

The correct answer is:
Symmetric Key Encryption

Question 24

Correct

Mark 1.00 out of 1.00

The main goal of a _____ is to obtain unauthorized access to the information

- a. acive attack
- b. internet attack
- c. passive attack ✔

Your answer is correct.

The correct answer is:
passive attack

Question 25

Correct

Mark 1.00 out of 1.00

___ is a weakness in the security system

- a. theft
- b. virus
- c. vulnerability ✔

Your answer is correct.

The correct answer is:
vulnerability

Question 26

Correct

Mark 1.00 out of 1.00

___ means that assets can be modified only by authorized parties or only in authorized ways.

- a. Authentication
- b. Confidentiality
- c. Integrity ✔

Your answer is correct.

The correct answer is:
Integrity

Question 27

Correct

Mark 1.00 out of 1.00

Ciphertext depends on the original plaintext message, the algorithm, and the ___.

- a. latency
- b. key ✔
- c. network size

Your answer is correct.

The correct answer is:
key

Question 28

Correct

Mark 1.00 out of 1.00

___ can be used to distribute other keys.

- a. private keys
- b. shared secret key
- c. public keys ✔

Your answer is correct.

The correct answer is:
public keys

Question 29

Correct

Mark 1.00 out of 1.00

___ are mutually agreed-upon code words, assumed to be known only to the user and the system.

- a. passwords ✔
- b. key
- c. signature

Your answer is correct.

The correct answer is:
passwords

Question 30

Correct

Mark 1.00 out of 1.00

Encrypted e-mail messages always carry a digital signature, so the ___ of the sender are assured.

- a. confidentiality
- b. integrity
- c. Authenticity ✔

Your answer is correct.

The correct answer is:
Authenticity

◄ CAE 1 Question Sheet

Jump to...