Started on   Wednesday, 28 April 2021, 4:00 PM
State   Finished
Completed on   Wednesday, 28 April 2021, 4:43 PM
Time taken   42 mins 37 secs
Grade   **21.00** out of 30.00 (**70**%)

Question **1**
Correct
Mark 1.00 out of 1.00

Hash length of SHA-1 is

○ a. 64 bits

◉ b. 160 bits   ✔

○ c. 256 bits

○ d. 128 bits

Your answer is correct.

The correct answer is:
160 bits

Question **2**
Correct
Mark 1.00 out of 1.00

Public-key cryptography is also known as

○ a. block cipher

◉ b. asymmetric key cryptography   ✔

○ c. symmetric key cryptography

Your answer is correct.

The correct answer is:
asymmetric key cryptography

Question 3
Correct

Mark 1.00 out of 1.00

Hash functions must have collision resistance properties.

Select one:
- ◉ True ✔
- ○ False

The correct answer is 'True'.

Question 4
Correct

Mark 1.00 out of 1.00

PGP compresses files using ----------------- algorithm

- ○ a. SHA-1
- ◉ b. ZIP ✔
- ○ c. RAR
- ○ d. RSA

Your answer is correct.

The correct answer is:
ZIP

Question 5
Correct

Mark 1.00 out of 1.00

---------------------- is a key distribution and authentication service.

- ○ a. X.509
- ○ b. PKI
- ◉ c. Kerberos ✔
- ○ d. PXI

Your answer is correct.

The correct answer is:
Kerberos

Question 6

Incorrect

Mark 0.00 out of 1.00

Distribution of public keys can be done by

- ○ a. public key authority   ✖
- ○ b. All of the options given
- ○ c. Publicly available directory
- ○ d. certificate authority

Your answer is incorrect.

The correct answer is:
All of the options given

Question 7

Correct

Mark 1.00 out of 1.00

S/MIME adds security to internet e-mail based on

- ○ a. TCP
- ○ b. FTP
- ◉ c. SMTP   ✔
- ○ d. UDP

Your answer is correct.

The correct answer is:
SMTP

Question 8

Correct

Mark 1.00 out of 1.00

S/MIME can provide

- ◉ a. All of the options given   ✔
- ○ b. integrity checking
- ○ c. authentication
- ○ d. privacy

Your answer is correct.

The correct answer is:
All of the options given

Question 9

Correct

Mark 1.00 out of 1.00

PKI stands for

- ○ a. public key infrastructure ✔
- ○ b. private key instance
- ○ c. public key instance
- ○ d. private key infrastructure

Your answer is correct.

The correct answer is:
public key infrastructure

Question 10

Correct

Mark 1.00 out of 1.00

Firewall is a type of

- ○ a. worm
- ○ b. none of the options given ✔
- ○ c. threat
- ○ d. virus

Your answer is correct.

The correct answer is:
none of the options given

Question 11

Correct

Mark 1.00 out of 1.00

Set of documents which describe key management schemes for IPSec is

- ○ a. key authority
- ○ b. internet key exchange ✔
- ○ c. secret key exchange
- ○ d. public key exchange

Your answer is correct.

The correct answer is:
internet key exchange

Question 12

Incorrect

Mark 0.00 out of 1.00

Payload length of authentication header is

- ○ a. 8 bits
- ● b. 32 bits ✖
- ○ c. 16 bits
- ○ d. 24 bits

Your answer is incorrect.

The correct answer is:
8 bits

Question 13

Correct

Mark 1.00 out of 1.00

Digital signatures provide the ability to

- ○ a. authenticate message contents
- ● b. all of the options given ✔
- ○ c. verify author, date & time of signature
- ○ d. be verified by third parties to resolve disputes

Your answer is correct.

The correct answer is:
all of the options given

Question **14**

Incorrect

Mark 0.00 out of 1.00

Which is the public key distribution scheme?

○ a. Diffie-Hellman Key Exchange

○ b. RSA

○ c. Public Key Cryptography

◉ d. DES ✖

Your answer is incorrect.

The correct answer is:
Diffie-Hellman Key Exchange

Question **15**

Correct

Mark 1.00 out of 1.00

$$K_{AB} = a^{x_A \cdot x_B} \bmod q \quad \text{where} \quad K_{AB} \quad \text{is}$$

○ a. public key of A

◉ b. shared secret key ✔

○ c. private key of A and B

○ d. public key of B

Your answer is correct.

The correct answer is:
shared secret key

Question 16

Correct

Mark 1.00 out of 1.00

IPSec is designed to provide security at the

○ a. Application layer

○ b. Session layer

○ c. Transport layer

◉ d. Network layer   ✔

Your answer is correct.

The correct answer is:
Network layer

Question 17

Correct

Mark 1.00 out of 1.00

PGP is used in

○ a. Browser security

○ b. FTP security

○ c. Wifi security

◉ d. Email security   ✔

Your answer is correct.

The correct answer is:
Email security

Question 18

Correct

Mark 1.00 out of 1.00

Who can modify X.509 certificate?

◉ a. certification authority   ✔

○ b. user

○ c. application server

○ d. authentication server

Your answer is correct.

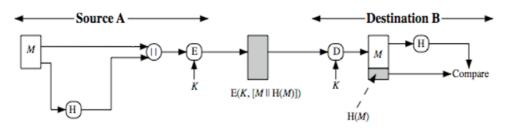The correct answer is:
certification authority

Question **19**

Correct

Mark 1.00 out of 1.00

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

○ a. unique key

◉ b. private key ✔

○ c. secret key

○ d. public key

Your answer is correct.

The correct answer is:
private key

Question **20**

Incorrect

Mark 0.00 out of 1.00

Notation CA<<X>> denotes

○ a. certificate for X signed by CA

◉ b. certificate for A signed by CA ✖

○ c. certificate for CA signed by X

○ d. certificate for X signed by A

Your answer is incorrect.

The correct answer is:
certificate for X signed by CA

Question 21

Incorrect

Mark 0.00 out of 1.00

Unique identifiers are not available in X.509 certificate

○ a. version 3

○ b. version 1

◉ c. version 2   ✖

○ d. version 2 and version 3

Your answer is incorrect.

The correct answer is:
version 1

Question 22

Incorrect

Mark 0.00 out of 1.00

SET is a network layer security mechanism

Select one:

◉ True ✖

○ False

The correct answer is 'False'.

Question 23

Correct

Mark 1.00 out of 1.00

HMAC refers

◉ a. Hash based MAC   ✔

○ b. None of the options given

○ c. Heuristic MAC

○ d. Highest MAC

Your answer is correct.

The correct answer is:
Hash based MAC

Question 24

Correct

Mark 1.00 out of 1.00

A Kerberos realm is a set of managed nodes that share the same Kerberos database

Select one:

○ True ✔

○ False

The correct answer is 'True'.

Question 25

Correct

Mark 1.00 out of 1.00

Examples of hash functions are

○ a. S/MIME

◉ b. MD-5 ✔

○ c. PGP

○ d. RSA

Your answer is correct.

The correct answer is:
MD-5

Question 26

Incorrect

Mark 0.00 out of 1.00

Identify the usage of hash function in the figure shown below.

○ a. authentication and confidentiality

○ b. confidentiality

○ c. authentication

◉ d. confidentiality, integrity and availability ✖

Your answer is incorrect.

The correct answer is:
authentication and confidentiality

Question 27

Incorrect

Mark 0.00 out of 1.00

firewalls can protect against access via WLAN

Select one:

◉ True ✖

○ False

The correct answer is 'False'.

Question 28

Incorrect

Mark 0.00 out of 1.00

Padding 5 bits in hash algorithm means appending

- ⦿ a. 11111　　　　　　　　　　　　　　　　　✖
- ○ b. 10000
- ○ c. 00000
- ○ d. 10101

Your answer is incorrect.

The correct answer is:
10000

Question 29

Correct

Mark 1.00 out of 1.00

X.509 certificate is issued by

- ○ a. application server
- ○ b. authentication server
- ○ c. public key authority
- ⦿ d. certification authority　　　　　　　　　　✔

Your answer is correct.

The correct answer is:
certification authority

Question 30

Correct

Mark 1.00 out of 1.00

TGS provides ticket to access application server

Select one:
- ⦿ True ✔
- ○ False

The correct answer is 'True'.

◄ Quiz-1

Jump to...

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Sathyabama Learning Management System ~Developed by [Cognibot](#)

💻📚 **e-Resources**

INFO

[Facebook](#)

[Twitter](#)

[Instagram](#)

[YouTube](#)

GET SOCIAL

Copyright © 2020 - cognibotrobotics.com