TERNA ENGINEERING COLLEGE
NERUL, NAVI MUMBAI
AN ISO 9001 : 2000 | NBA ACCREDITATION

TEC 237
FH 2021 EXAMINATION

MCQ_TE-B_CSS_R16_Block2

* Required

MCQ

Q1 *

1.	_____ defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.
Option A:	X.800
Option B:	X.809
Option C:	X.832
Option D:	X.802

- (●) A
- ( ) B
- ( ) C
- ( ) D

Q2 *

2.	_____are fundamental to a number of public-key algorithms, including and the digital signature algorithm (DSA).
Option A:	Discrete logarithms
Option B:	Chinese remainder theorem
Option C:	Fermat's theorem
Option D:	Miller and Rabin algorithm

- (●) A
- ( ) B
- ( ) C
- ( ) D

Q3 *

3.	Plain text message is: "meet me after the toga party" with a rail fence of depth 2. Compute cipher text.
Option A:	MEMATRHTGPRYETEFETEOAAT
Option B:	MEMATRHTGPRYETEFETFOAAT
Option C:	MEMATRHTHPRYETEFETEOAAT
Option D:	MEMATRHTGPRYETEFFTEOAOT

- (●) A
- ( ) B
- ( ) C
- ( ) D

Q4 *

4.	In_____ mode, the same plaintext value will always result in the same cipher text value.
Option A:	Cipher Block Chaining
Option B:	Cipher Feedback
Option C:	Electronic code book
Option D:	Output Feedback

- ○ A
- ○ B
- ◉ C
- ○ D

Q5 *

5.	DES encrypting the plaintext as block of _____ bits.
Option A:	64
Option B:	56
Option C:	128
Option D:	32

- ◉ A
- ○ B
- ○ C
- ○ D

Q6 *

6.	_____ is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications.
Option A:	AES
Option B:	RSA
Option C:	MD5
Option D:	RC5

- (●) A
- ( ) B
- ( ) C
- ( ) D

Q7 *

7.	The number of rounds in RC5 can range from 0 to _____
Option A:	127
Option B:	63
Option C:	31
Option D:	255

- ( ) A
- ( ) B
- ( ) C
- (●) D

Q8 *

8.	How many rounds does the AES-192 perform?
Option A:	10
Option B:	14
Option C:	16
Option D:	12

- ○ A
- ○ B
- ○ C
- ◉ D

Q9 *

9.	For the Knapsack: {1 6 8 15 24}, Find the cipher text value for the plain text 10011.
Option A:	40
Option B:	15
Option C:	14
Option D:	39

- ◉ A
- ○ B
- ○ C
- ○ D

Q10 *

10.	Which of the following is not possible through hash value?
Option A:	Password check
Option B:	Data integrity check
Option C:	Data retrieval
Option D:	Digital signature

- ○ A
- ○ B
- ○ C
- ◉ D

Q11 *

11.	Which of the following is not an element/field of the X.509 certificates?
Option A:	Issuer Name
Option B:	Serial Modifier
Option C:	Issue unique identifier
Option D:	Signature

- ○ A
- ◉ B
- ○ C
- ○ D

Q12 *

12.	_____ is responsible for distributing keys to pairs of users (hosts, processes, applications) as needed
Option A:	Key distribution center
Option B:	Key analysis center
Option C:	UKey storing center
Option D:	HKey storing center

- (●) A
- ( ) B
- ( ) C
- ( ) D

Q13 *

13.	A digital certificate system is _____.
Option A:	uses third-party CAs to validate a user's identity
Option B:	uses digital signatures to validate a user's identity
Option C:	uses tokens to validate a user's identity
Option D:	are used primarily by individuals for personal correspondence

- (●) A
- ( ) B
- ( ) C
- ( ) D

Q14 *

14.	Hashed message is signed by a sender using
Option A:	His public key
Option B:	His private key
Option C:	Receivers public key
Option D:	Receivers private key

- ○ A
- ◉ B
- ○ C
- ○ D

Q15 *

15.	The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
Option A:	Authenticated
Option B:	Joined
Option C:	Submit
Option D:	Separate

- ◉ A
- ○ B
- ○ C
- ○ D

Q16 *

16.	Which of the following does authorization aim to accomplish?
Option A:	Restrict what operations/data the user can access
Option B:	Determine if the user is an attacker
Option C:	Flag the user if he/she misbehaves
Option D:	Determine who the user is

- (●) A
- ( ) B
- ( ) C
- ( ) D

Q17 *

17.	_____ operates in the transport mode or the tunnel mode.
Option A:	IPSec
Option B:	SSL
Option C:	PGP
Option D:	BGP

- (●) A
- ( ) B
- ( ) C
- ( ) D

Q18 *

18.	When a hash function is used to provide message authentication, the hash function value is referred to as
Option A:	Message Field
Option B:	Message Digest
Option C:	Message Score
Option D:	Message Leap

- ○ A
- ◉ B
- ○ C
- ○ D

Q19 *

19.	Which of the following tool would NOT be useful in figuring out what spyware or viruses could be installed on a client's computer?
Option A:	Wireshark
Option B:	Malware Bytes
Option C:	HighjackThis
Option D:	HitmanPro

- ◉ A
- ○ B
- ○ C
- ○ D

Q20 *

20.	What is honey pot attack?
Option A:	dummy device put into the network to attract attackers
Option B:	single line threat
Option C:	Ip spoofing bypass
Option D:	recognition attack

- (●) A
- ( ) B
- ( ) C
- ( ) D

Back Submit