Reg. No.															

MINOR CERTIFICATION EXAMINATION, MAY 2024

Second Semester

18CSE011J – CRYPTOGRAPHY AND NETWORK SECURITY

(For the candidates admitted during the academic year 2018-2019 to 2021-2022)

Note:

(i) **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

(ii) **Part - B & Part - C** should be answered in answer booklet.

Time: 3 hours | Max. Marks: 100

PART – A (20 × 1 = 20 Marks)

Answer **ALL** Questions

	Marks	BL	CO	PO
1. The GCD (55, 22) is _____. (A) 11 (B) 1 (C) 0 (D) 22	1	3	1	2
2. Using CRT calculate the value of "X" for the following where $X \equiv 3(\text{Mod}5)$ and $X \equiv 1(\text{Mod}2)$ (A) 10 (B) 11 (C) 12 (D) 13	1	3	1	2
3. The $\phi(7)$ is _____. (A) 6 (B) 5 (C) 4 (D) 3	1	3	1	2
4. Which of the following is not a security service? (A) Confidentiality (B) Authentication (C) Non-repudiation (D) Encipherment	1	2	1	4
5. A cipher is one that encodes a computerized information stream as 1 bit or 1 byte in turn (A) Stream cipher (B) Block cipher (C) Ideal cipher (D) Classic cipher	1	1	2	1
6. A little change in the plaintext creates significant noteworthy changes in the ciphertext (A) Brute force attack (B) Meet in the middle (C) Avalanche effect (D) Man in the middle	1	2	2	1
7. Perform Diffie Hellman calculations for the following given primitive root $\propto = 7$ and common prime Q = 71. Given $X_A = 3$, find Y_A (A) 21 (B) 58 (C) 59 (D) 2	1	3	2	2
8. In mode of operation (block cipher principles), ECB stands for (A) Electronic code book (B) Electronic computer book (C) Electrical code book (D) Electrical computer book	1	1	2	1

9. MAC is _____ function. 1 2 3 4
   (A) Many to many (B) One to one
   (C) One to many (D) Many to one

10. Digital signature is generates from _____. 1 2 3 4
   (A) Conventional algorithm (B) Secret key encryption
   (C) Public key cryptography (D) Symmetric key algorithm

11. The primitive root of 5 is _____. 1 3 3 2
   (A) 1 (B) 2
   (C) 4 (D) 5

12. Which of the following is not a version of SHA? 1 1 3 4
   (A) SHA-0 (B) SHA-1
   (C) SHA-224 (D) SHA-288

13. _____ is a type of firewall that operates at the application layer of the OSI model. 1 2 4 4
   (A) Application firewall (B) Packet filtering firewall
   (C) Stateful inspection firewall (D) Network address translation firewall

14. Name the network device that is used to filter and forward network traffic based on MAC addresses. 1 1 4 4
   (A) Switch (B) Router
   (C) Hub (D) Repeater

15. IPS _____ the threats 1 2 4 4
   (A) Detect and prevent (B) Prevent
   (C) Detect (D) Unhandled

16. State the type of denial-of-service attack that floods a network with bogus requests? 1 2 4 4
   (A) Smurf attack (B) Spoofing
   (C) Syn flood (D) Ping of death

17. The client-key-exchange message uses a pre master key of size 1 2 5 2
   (A) 48 bytes (B) 56 bytes
   (C) 64 bytes (D) 32 bytes

18. In the handshake protocol which is the message type first sent between client and server? 1 1 5 2
   (A) Server-hello (B) Client-hello
   (C) Hello-request (D) Certificate-request

19. _____ provides either authentication or encryption, or both for packets at the IP level. 1 2 5 2
   (A) AH (B) ESP
   (C) PGP (D) SSL

20.	In the _____ mode, IPsec protects the whole IP packet, including the original IP header. (A) Transport (B) Tunnel (C) Bidirectional (D) Unidirectional	1	1	5	2

PART – B (5 × 4 = 20 Marks)
Answer **ANY FIVE** Questions

		Marks	BL	CO	PO
21.	State the Euler's totient function? Calculate $\phi(25)$.	4	3	1	2
22.	Write and prove the properties of modular arithmetic.	4	4	1	2
23.	Draw and write about Feistel cipher structure.	4	2	2	1
24.	In RSA algorithm, if e = 7, P = 11, Q = 5, then find "d". (Note: e and d are public and private key values).	4	3	2	2
25.	Discuss briefly the message authentication code.	4	2	3	4
26.	List the write bout various types of firewalls and briefly explain the package filtering firewall.	4	2	4	4
27.	Draw and write about authentication header.	4	2	5	2

PART – C (5 × 12 = 60 Marks)
Answer **ALL** Questions

		Marks	BL	CO	PO
28. a.	Encrypt the plaintext "information security" using possible polyalphabetic ciphering techniques with the key "Crypto".	12	3	1	2
	(OR)				
b.	Find the value of "X" for the given equations using Chinese remainder theorem. $X \equiv 2 \pmod 3$ $X \equiv 3 \pmod 5$ $X \equiv 2 \pmod 7$	12	3	1	2
29. a.	Calculate the ciphertext using S-DES for the following inputs. Plaintext : 0111 1111 Initial permutation: 2 6 1 3 4 7 5 8 E/P: 4 1 2 3 2 3 4 1 K1: 1010 0100 K2: 0100 0011 P4: 2 4 3 1 $S_0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix}$ $S_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$	12	3	2	2
	(OR)				
b.	Draw and explain various modes of operation in block ciphering technique.	12	2	2	1

30. a.	Explain in detail about MD5 hash algorithm with required diagrams.	12	2	3	4
	(OR)				
b.	Describe detail about Schnorr digital signature algorithm.	12	2	3	2
31. a.	Elaborate the intrusion prevention system.	12	2	4	4
	(OR)				
b.	Discuss the cloud security with neat sketch.	12	2	4	4
32. a.	With neat diagram, explain the operation of SSL.	12	2	5	2
	(OR)				
b.	What is PVN? Explain the different types of VPN.	12	2	5	2

* * * * *