Reg. No															

B.Tech DEGREE EXAMINATION, DECEMBER 2023

Fifth Semester

18ECE224T - CRYPTOGRAPHY AND NETWORK SECURITY

(For the candidates admitted during the academic year 2020 - 2021 & 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** and **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

1. _______is the process of transforming plain text into unreadable text 1 1 1
(A) Decryption (B) Encryption
(C) Network security (D) Information hiding

2. The DES Algorithm Cipher System consists of ___________rounds (iterations) each with a round key 1 1 2
(A) 12 (B) 18
(C) 9 (D) 16

3. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via __________ 1 1 1
(A) Scaling of the existing bits (B) Duplication of the existing bits
(C) Addition of zeros (D) Addition of ones

4. How many S-boxes are present in the blowfish algorithm? 1 1 1
(A) 2 (B) 4
(C) 6 (D) 8

5. A group that satisfies the commutative property is called______ group. 1 1 2
(A) Cyclic (B) Abelian
(C) Finite (D) Rational

6. In RSA algorithm private key 1 1 2
(A) $d \equiv e^{-1} \pmod{\varphi(n)}$ (B) $d = e^{-1} \pmod{\varphi(n)}$
(C) $d \neq e^{-1} \pmod{\varphi(n)}$ (D) $d \equiv e \pmod{\varphi(n)}$

7. The key exchange protocol is vulnerable to a __________ attack because it does not authenticate the participants. 1 1 2
(A) One way function (B) Time Complexity
(C) Chosen Ciphertext (D) Man in the middle attack

8. The Diffie Hellman key exchange formula for calculation of a secret key by User A is 1 1 2
(A) K = nB x PA (B) K = nA x PB
(C) K = nP x BA (D) K = nA x PA

9. Message authentication is a service beyond........ 1 1 3
(A) Message Confidentiality (B) Message Integrity
(C) Message Splashing (D) Message Sending

10. When does the collision occurs in a hash function? 1 1 3
(A) $x \neq y$ and $H(x) = H(y)$ (B) $x = y$ and $H(x) = H(y)$
(C) $x \neq y$ and $H(x) \neq H(y)$. (D) $x = y$ and $H(x) \neq H(y)$.

11. The Digest created by hash function is normally called a........ 1 1 3

(A) Modification detection code (B) Modify authentication connection
(C) Message authentication control (D) Message authentication cipher

12. What is the maximum length of the message (in bits) that can be taken by SHA-512? 1 1 3

(A) 2^{128} (B) 2^{256}
(C) 2^{64} (D) 2^{192}

13. ___________ ensures the integrity and security of data that are passing over a network. 1 1 4

(A) Firewall (B) Antivirus
(C) Pentesting Tools (D) Network-security protocols

14. Which of the following is not a secured mail transferring methodology? 1 1 4

(A) POP3 (B) SSMTP
(C) Mail using PGP (D) S/MIME

15. In tunnel mode, IPSec protects the ______ 1 1 4

(A) Entire IP packet (B) IP header
(C) IP payload (D) IP trailer

16. Extensible authentication protocol is authentication framework frequently used in ______ 1 1 4

(A) Wired personal area network (B) Wireless networks
(C) Wired local area network (D) Wired metropolitan area network

17. Password cracking in system hacking is of ________ types. 1 1 5

(A) 2 (B) 3
(C) 4 (D) 5

18. Which of the following is not a type of virus? 1 1 5

(A) Boot sector (B) Polymorphic
(C) Multipartite (D) Trojans

19. _________________ is the kind of firewall is connected between the device and the network connecting to internet. 1 1 5

(A) Hardware Firewall (B) Software Firewall
(C) Stateful Inspection Firewall (D) Microsoft Firewall

20. Firewall examines each ____________ that are entering or leaving the internal network. 1 1 5

(A) emails users (B) updates
(C) connections (D) data packets

PART - B (5 × 4 = 20 Marks)

Answer **any 5** Questions

	Marks	BL	CO
21. Compare block cipher and stream cipher .	4	1	1
22. Write a short note on Euler's totient function.	4	1	2
23. List the properties of congruence.	4	1	3
24. Briefly explain the requirements of authentication.	4	1	3
25. Explain the Encapsulating Security payload.	4	1	4
26. Define Port Scanning and Knocking.	4	1	4
27. Firewall Types.	4	1	5

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

Marks BL CO

28.	(a) (i) Explain Hill Cipher (ii) Obtain ciphertext of "Fire Rocket" by using a Polyfair cipher (Key:Monk) **(OR)** (b) Build a Feistel structure and explain DES algorithm	12	1	1
29.	(a) Explain Elliptic curve cryptography. **(OR)** (b) Perform encryption and decryption using RSA Algorithm for the following. Plain text=123, e=17, p=61, q=53	12	1	2
30.	(a) Discuss the message authentication codes and requirements of MAC in detail. **(OR)** (b) Explain in detail about the operation of SHA-512.	12	1	3
31.	(a) Explain the working of ESP under tunnel mode. **(OR)** (b) Discuss in detail about PGP email security architecture.	12	1	4
32.	(a) Explain in detail about IDS. **(OR)** (b) Classify malwares. Explain in detail about virus types and their structures.	12	1	5

* * * * *