Reg. No

B.Tech. DEGREE EXAMINATION, JUNE 2023

Fifth / Sixth Semester

18ECE224T - 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 40 minutes.
ii. **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours **Max. Marks: 100**

Part - A (20 × 1 Marks = 20 Marks)

Answer **All** Questions

		Marks	BL	CO
1.	Authentication, access control and availability are (A) Security services (B) Security attacks (C) Encryption techniques (D) Cipher models	1	1	1
2.	Trying every possible key on a piece of ciphertext to get the plaintext is (A) Torjan horse attack (B) Brute force attack (C) Known plaintext attack (D) Ciphertext-only attack	1	1	1
3.	The maximum possible number of keys in Playfair cipher is (A) 26! (B) 26 (C) 25! (D) 25	1	2	1
4.	________ is the only unconditionally secure algorithm. (A) One-time pad (B) RSA (C) Triple DES (D) Blowfish	1	2	1
5.	In RSA plaintext(M) is obtained by decrypting ciphertext(C) using ________. (A) $M= C^d \bmod n$ (B) $M= C^{-1} \bmod n$ (C) $M= C^d \bmod \Phi(n)$ (D) $M= C \bmod n$	1	1	2
6.	Find the GCD of (2740, 1760). (A) 40 (B) 05 (C) 20 (D) 10	1	3	2
7.	Public key certificate of a user is verified using _______. (A) CA's private key (B) CA's public key (C) User's private key (D) User's public key	1	2	2
8.	Find the value of $\Phi(49)$. (A) 48 (B) 36 (C) 42 (D) 49	1	2	2
9.	______ is vulnerable to birthday attack. (A) DSA (B) DAA (C) SHA (D) Digital signature	1	1	3
10.	The size of SHA -1 digest is ________. (A) 16 bytes (B) 08 bytes (C) 20 bytes (D) 24 bytes	1	1	3
11.	Digital signature includes __________. (A) Access Control (B) Message Authentication (C) Data Confidentiality (D) Data integrity	1	2	3

12. The size of one message block in MD5 is ________. 1 1 3

(A) 128 bits (B) 512 bits
(C) 160 bits (D) 256 bits

13. Kerberos authentication service uses _______. 1 1 4

(A) Public key encryption (B) Private key encryption
(C) Symmetric key encryption (D) Asymmetric key encryption

14. A one-way relationship between sender & receiver that affords security for IP traffic flow is called 1 1 4

(A) Security Parameters Index (B) Security Protocol Identifier
(C) Security Assistance (D) Security Association

15. ___________ is used to encrypt and authenticate the entire IP packet. 1 2 4

(A) Transport mode ESP (B) Tunnel mode ESP
(C) Transport mode AH (D) Tunnel mode AH

16. SSL uses _______ to provide a reliable end to end secure service. 1 1 4

(A) SIP (B) UDP
(C) HTTP (D) TCP

17. _________ is a method of externally opening ports on a firewall. 1 2 5

(A) Port scanning (B) Port Knocking
(C) Port sweeping (D) Port pinging

18. Basic firewall protects only against the following. 1 1 5

(A) Internal threats (B) External threats
(C) Transfer of virus (D) Threats raised by dial up/in connections

19. Which is of the following encryption algorithm is used in WEP of WLAN? 1 2 5

(A) RC4 (B) RC5
(C) DES (D) AES

20. Identify the authentication algorithm used in GSM. 1 1 6

(A) EK74 (B) A3
(C) A4 (D) A5

Part - B (5 × 4 Marks = 20 Marks)

Answer **any 5** Questions

Marks BL CO

21. Define Security attacks and mechanisms. Give examples. 4 2 1

22. Explain the operation of single round of DES with neat sketches. 4 3 1

23. Illustrate pictorially public key authority and write the properties of publicly available directory. 4 1 2

24. Draw the X.509 public key certificate format. 4 2 3

25. Sketch the public key cryptosystem for authentication and secrecy. 4 2 2

26. Diagrammatically summarize the Kerberos v4 authentication dialogue. 4 4 4

27. Discover the working of distributed intrusion detection system with neat sketches. 4 2 5

Part - C (5 × 12 Marks = 60 Marks)

Answer **All** Questions

Marks BL CO

28. a. Sketch the models for Network Security considering the place of encryption and write the basic tasks required in designing a particular security service. 12 2 1

(OR)

b.i. Encrypt the plain text "Safe messages" with key "ciphering" in 3*3 matrix using Hill cipher.

ii. Encrypt the message "Test" using f(p) = (p+8) mod 26. Decrypt the message "MIAG" using f(p) = (p-8) mod 26.

29. a. Enumerate key exchange between user A and user B to be accomplished using Elliptic curve cryptography? 12 3 2

(OR)

b. Two parties A and B wish to setup a common secret key between themselves using DHKE algorithm. They agree on 7 as modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their private values. Find their common secret key?

30. a. Illustrate the overall operation of HMAC and define the following terms and give its expression. 12 2 3

(OR)

b. Sketch the compression function of any one cryptographic hash function that is reputable and competent in using it in a context where collision-resistance is important, overview.

31. a. Define SSL connection and session.Explain with neat diagrams the operation of SSL record protocol. 12 2 4

(OR)

b. Create a Virtual Private Network using suitable IPSec protocol and mode. Illustrate its working with appropriate packet formats.

32. a. Evaluate Firewall types that inserted between premises network and internet to establish an outer security perimeter which can effectively protects network of local systems from network-based security threat. 12 2 5

(OR)

b. Draw the screened subnet configuration and analyze its security strength by presenting the merits of the firewalls involved.

* * * * *