27. a. In a RSA cryptosystem, 'A' uses two prime numbers p =13, q =11 to generate his public and private keys. Calculate 'n' $\phi(n)$, e and d. Encrypt the plain text M=8 and decrypt the cipher text to verify your calculation. 10 3 2 1

(OR)

b.i. In a Diffie-Hellman key exchange, Alice and Bob have chosen prime value q =17, primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6. What is the secret key they exchanged? 5 3 2 1

ii. Enumerate the methods of public key distribution. 5 2 2 1

28. a.i. With neat sketch of HMAC explain its operation. 5 3 3 3

ii. Specify the signing and verifying process in digital signature algorithm. 5 3 3 3

(OR)

b.i. Analyze the message authentication technique that uses a secret key to generate a fixed size code that is appended to the message with neat sketch. 6 3 3 3

ii. Compare MD5 and SHA-1. 4 2 3 3

29. a. Give the Kerberos V4 dialogues. Analyze and identify their environmental shortcomings and technical deficiencies. 10 3 4 7

(OR)

b. How to create a virtual private network using tunnel mode ESP? Explain with neat frame and payload formats. 10 3 4 7

30. a. Explain the working of distributed intrusion detection system with neat sketches. 10 3 5 7

(OR)

b.i. Illustrate with neat sketch how GSM messages are protected from eavesotropping attack. 6 3 6 7

ii. Evaluate the security strength of screened subnet firewall configuration. 4 3 5 7

* * * * *

Reg. No. □□□□□□□□□□□□□□□

B.Tech. DEGREE EXAMINATION, NOVEMBER 2022
Sixth and Seventh Semester

18ECE224T – CRYPTOGRAPHY AND NETWORK SECURITY
(For the candidates admitted from the academic year 2018-2019 to 2019-2020)

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** should be answered in answer booklet.

Time: 2½ Hours Max. Marks: 75

PART – A (25 × 1 = 25 Marks)
Answer **ALL** Questions

Marks BL CO PO

1. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of _________ 1 1 1 1
(A) Cryptography (B) Cryptanalysis
(C) Cryptology (D) Steganography

2. A __________processes the input elements continuously producing output one element at a time. 1 1 1 1
(A) Stream cipher (B) Deciphering
(C) Enciphering (D) Block cipher

3. ________________is designed to overcome meet-in-the middle attack. 1 1 1 1
(A) Double DES (B) Triple DES
(C) DES (D) δ-DES

4. The main motive for using steganography is hiding a secret message behind a __________ 1 1 1 1
(A) Special file (B) Encrypted file
(C) Program file (D) Ordinary file

5. Vigenere cipher is an example of __________cipher. 1 1 1 1
(A) Monoalphabetic (B) Product
(C) Polyalphabetic (D) Transposition

6. In asymmetric key cipher, the sender uses __________for confidentiality. 1 1 2 1
(A) Sender's private key (B) Sender's public key
(C) Recipient's public key (D) Recipient's private key

7. Find the value of $\phi(35)$ 1 2 2 1
(A) 34 (B) 24
(C) 14 (D) 28

8. Zero point of an elliptic curve is not the __________ 1 1 2 1

(A) Point of infinity (B) Additive identity
(C) Inverse element (D) Base point

9. Find 4 mod 13 1 2 2 1

(A) 2 (B) 3
(C) 4 (D) 1

10. Find the multiplicative inverse of 13mod220 1 2 2 1

(A) 17 (B) 13
(C) 221 (D) 1

11. MAC does not support 1 1 3 3

(A) Integrity (B) Authentication
(C) Non-repudiation (D) Confidentiality

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

(A) 128 bits (B) 512 bits
(C) 164 bits (D) 256 bits

13. Digital signature includes 1 1 3 3

(A) Access control (B) Message authentication
(C) Data confidentiality (D) Availability

14. Public key certificate of a user is verified using__________ 1 1 3 1

(A) CA's private key (B) User's private key
(C) User's public key (D) CA's public key

15. The size of SHA-1 digest is 1 1 3 3

(A) 16 bytes (B) 20 bytes
(C) 24 bytes (D) 12 bytes

16. SSL uses __________to provide a reliable end to end secure services. 1 1 4 7

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

17. ____________is a method of externally opening ports on a firewalls. 1 1 4 7

(A) Port scanning (B) Payment gateway
(C) Port knocking (D) Port sweeping

18. A one way relationship between sender and receiver that affords security for IP traffic flow is called as __________ 1 1 4 7

(A) Security parameters index (B) Security protocol identifier
(C) Security association (D) Security assistance

19. Which of the following checks, if proposed purchase does not exceed the card limit? 1 1 4 7

(A) Merchant (B) Payment gateway
(C) Acquirer (D) Certificate authority

20. A random value to be repeated in message to assure that the response is fresh and has not been replayed by an opponent. 1 1 4 7

(A) Realm (B) Nonce
(C) Options (D) rtime

21. Which layers filters the proxy firewalls? 1 1 5 7

(A) Application (B) Network
(C) Transport (D) Data link

22. ____________ web threat is used to fake one's identity. 1 1 6 7

(A) Sniffing (B) Spoofing
(C) Pharming (D) Phishing

23. SPI stands for 1 1 5 7

(A) Scalable payload index (B) Scalable parameter index
(C) Security physical index (D) Security parameters index

24. A computer __________is a malicious code which self-replicates by copying itself to other programs. 1 1 5 7

(A) Virus (B) Worms
(C) Program (D) Torjan-horse

25. Choose the right statements regarding multilevel security 1 2 6 7

(A) It is obtained by enforcing "No read down" and "No write down" rules
(B) It is obtained by enforcing "No read up" and "No write down" rules
(C) A low-level subject should permitted to access information owned by high-levels subject
(D) A high level subject may convey information to a low-level subject

PART – B (5 × 10 = 50 Marks)

Answer **ALL** Questions

Marks BL CO PO

26. a.i. Encrypt the plain text "EXAM FOR INFORMATION SECURITY" with keyword "EFFECTIVENESS" using play fair cipher. 5 3 1 1

ii. Illustrates the classical feistel cipher structure and list the design elements. 5 2 1 1

(OR)

b.i. Enumerate the operation of DES encryption standards with neat sketch. 5 3 1 1

ii. Encrypt the plain text "SHORT EXAMPLE" using the keyword "HILL" using 2×2 matrix Hill cipher. Assume A-Z from 0-25. 5 3 1 1