29. a. Determine the multiplicative inverse of x^3+x+1 in $GF(2^4)$ with $m(x)=x^4+x+1$. 12 4 2 1

(OR)

b. Using Chinese remainder theorem find the smallest positive integer n such that 12 3 2 1

$n \equiv 3 \bmod 5$
$n \equiv 1 \bmod 7$
$n \equiv 6 \bmod 8$

30. a. Describe DES algorithm with neat diagram and explain the steps. 12 2 3 1

(OR)

b. Explain AES algorithm with all its round functions in detail. 12 3 3 1

31. a. Find the public key of a user 'B' using elliptic curve cryptography. The parameters are E_{11} (1, 6), G(2, 7) and B's secret key $n_B = 5$. 12 4 4 1

(OR)

b.i. Find the private key and encrypt the following plain text using RSA algorithm with given inputs p = 5, q = 7, e = 11, m = 7. 6 4 4 1

ii. Find the public keys and the secret key for the following input using Diffie Hellman algorithm Q = 11, ∝ = 7, $X_A = 5$, $X_B = 3$. 6 4 4 1

32. a. Explain in detail about SHA-512 with necessary diagrams. 12 2 5 1

(OR)

b. Explain in detail about MD5 with necessary diagram. 12 2 5 1

* * * * *

Reg. No.

B.Tech. DEGREE EXAMINATION, MAY 2023

Fifth & Sixth Semester

18CSE381T – CRYPTOGRAPHY

(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. Which of the following is not a type of symmetric-key cryptography technique? 1 1 1 1
(A) Caesar cipher (B) Data encryption standard
(C) Diffie Hellman cipher (D) Play fair cipher

2. Which of the following security attacks is not an active attack? 1 1 1 1
(A) Masquerade (B) Modification of message
(C) Denial of service (D) Traffic analysis

3. Which of the following options correctly defines the brute force attack? 1 1 1 1
(A) Brutally forcing the user to share the useful information like pins and passwords (B) Trying every possible key to decrypt the message
(C) One entity pretends to be some other entity (D) The message or information is modified sending it to the receiver

4. The method of conceal the existence of the message is called 1 1 1 1
(A) Cryptography (B) Steganography
(C) Data flow (D) Encryption

5. Consider the following properties
G-i) Closure
G-ii) Associative
G-iii) Identity element
G-iv) Inverse element
G-v) Commutative
(A) G-i to G-v is an Abelian group (B) G-i to G-v is an field
(C) G-i to G-v is an ring (D) G-i to G-iii is an group

6. In modular arithmetic; (c/d) 1 2 2 1
(A) $d(a^n-1)$ (B) $d(c^n-1)$
(C) $c(d^{-1})$ (D) $d(c^{-1})$

7. If P is prime and a is a positive integer not divisible by P then 1 1 2 1

(A) $a^{P-1} \equiv 1(\bmod P)$ (B) $a^{P-1} \equiv P(\bmod P)$
(C) $a^{P} \equiv 1(\bmod P)$ (D) $a^{P+1} \equiv 1(\bmod P)$

8. Miller Robin algorithm used for 1 2 2 1

(A) Finding primitive root (B) Finding prime number
(C) Finding inverse (D) Finding GCD

9. _______ encrypts one bit or one byte at a time. 1 2 3 1

(A) Block cipher (B) Stream cipher
(C) Fiestel cipher (D) DES cipher

10. DES encrypts ______ bit blocks with ______ bit key. 1 2 3 1

(A) 64, 50 (B) 56, 64
(C) 56, 60 (D) 64, 56

11. If which mode is used to transmit a DES key securely. 1 2 3 1

(A) Electronic code book (B) Elliptic cryptography
(C) Blow fish method (D) Cipher block chaining

12. What is the minimum and maximum size of the key in blowfish algorithm? 1 2 3 1

(A) 48 bits, 256 bits (B) 64 bits, 512 bits
(C) 32 bits, 56 bytes (D) 32 bits, 48 bytes

13. In public key encryption if A wants to send an encrypted message to B 1 2 4 1

(A) A encrypts message using his private key (B) A encrypts message using B's private key
(C) A encrypts message using B's public key (D) A encrypts message using his public key

14. Which of the following ciphers uses asymmetric key cryptography? 1 2 4 1

(A) Rail Fence cipher (B) Data encryption standard
(C) Play fair cipher (D) Diffie Hellman Cipher

15. The private key in asymmetric key cryptography is kept by 1 2 4 1

(A) Sender (B) Receiver
(C) Sender and receiver (D) All the connected devices to the network

16. In RSA algorithm if p = 7, q = 11 and e = 13 then what will be the value of d = ? 1 3 4 1

(A) 37 (B) 50
(C) 55 (D) 36

17. Digital signatures authenticates the sender by appending the original message with the ______digest. 1 2 5 1

(A) Decrypted message (B) Systematic approach
(C) Encrypted message (D) Authenticated message

18. What is the output of cryptographic hash function means? 1 2 5 1

(A) A variable set of bits (B) A fixed set of bits, derived from one-way mathematical operations
(C) An output which may be easily discovered by an adversary (D) Outputs of such functions are number of importance

19. What is a one-way password file? 1 2 5 1

(A) A scheme in which the password is jumbled and stored (B) A scheme is which the password is XOR with a key and stored
(C) A scheme in which the hash of the password is stored (D) A scheme in which the password is passed through

20. In SHA-512, the size of the word is ______ bits and the number of rounds involved in the process is 1 2 5 1

(A) 80, 64 (B) 64, 80
(C) 64, 82 (D) 128, 80

PART – B (5 × 4 = 20 Marks)

Answer **ANY FIVE** Questions

Marks BL CO PO

21. Explain about OSI security in detail. 4 2 1 1

22. Using play fair cipher, encrypt the plaintext "FINAL YEARS" using key "MATRIX". 4 3 1 1

23. Find the primitive routs of prime number 23. Write the importance of primitive rout in the network security. 4 2 2 1

24. Consider the input state arrays to the add round key phase of AES algorithm are 4 3 3 1

87	F2	4D	97	47	40	A3	4C
6E	4C	90	EC	37	D4	70	9F
46	E7	4A	C3	94	E4	3A	42
A6	8C	D8	95	ED	A5	A6	BC

Find the output state array of the add round key phae.

25. Assume that Alice and Bob uses the Diffie-Hellman key management protocol. Show how the secret key is shared between them and prove that Alice and Bob obtain the same symmetric key that is K = K'. Show all works. 4 4 4 1

26. Write about the magic constants of RC5. 4 3 4 1

27. Sign the following message using Elgammal digital signature algorithm. The inputs are Q = 13, ∝ = 11, X_A = 7, K = 5 and message m = 7. Give the signature value. 4 4 5 1

PART – C (5 × 12 = 60 Marks)

Answer **ALL** Questions

Marks BL CO PO

28. a. Using Hill cipher, encrypt and decrypt the message "CAPTIVES ELEVEN" with key: $\begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix}$. 12 3 1 1

(OR)

b. Write the advantages of poly alphabetic cipher method. Encrypt and decrypt the plain text "hello" with key "dghbc" using vernam cipher method. 12 3 1 1