Reg. No															

B.Tech DEGREE EXAMINATION, NOVEMBER 2023

Fifth & Sixth Semester

18CSE381T - CRYPTOGRAPHY

(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. Encryption of the plaintext “security” using single columnar transposition with key ”2341” gives the following ciphertext 1 2 1
(A) uysreict (B) usecyrit
(C) ritysecu (D) urysetci

2. Which involves trying every possible key until a proper translation of cipher text into plain text is obtained? 1 1 1
(A) Man in the middle attack (B) Chosen Plain text Attack
(C) Brute Force attack (D) Chosen cipher text

3. ___________ is a process through which a system verifies the identity of an entity that wishes to access it. 1 1 1
(A) Integrity (B) Confidentiality
(C) Availability (D) Authentication

4. ___________ is a method which replaces each plaintext letter with another alphabetical letter. 1 1 1
(A) Transposition (B) Confusion
(C) Substitution (D) Diffusion

5. 5/3 mod 7 = 1 2 2
(A) 2 (B) 3
(C) 7 (D) 4

6. What is the identity element in the group G = {2, 4, 6, 8} under multiplication modulo 10? 1 2 2
(A) 9 (B) 6
(C) 5 (D) 12

7. _____ returns the number of integers from 1 to n, that are relatively prime to n. 1 1 2
(A) GCD (B) LCM
(C) Euler Totient function (D) Primitive root

8. ________ is a set of elements together with two binary operations addition (+) and multiplication (×) operations that satisfies six axioms, namely closure, associative, commutative, multiplication operation distribute over the addition, identity and the inverse element. 1 1 2
(A) Group (B) Ring
(C) Field (D) Finite Field

9. The number of tests required to break the DES algorithm are 1 2 3
(A) 2.8×10^{14} (B) 4.2×10^{9}
(C) 1.84×10^{19} (D) 7.2×10^{16}

10. ___ algorithm that takes an 8-bit block of plaintext and encrypts using a 10-bit key to produce an 8-bit block of the ciphertext as output 1 1 3

(A) DES (B) S-DES
(C) AES (D) RC5

11. How many round are there in AES algorithm, which uses 256 bit key? 1 1 3

(A) 10 (B) 12
(C) 14 (D) 16

12. Which of the 4 operations are false for each round in the AES algorithm 1 2 3

i) Substitute Bytes
ii) Shift Columns
iii) Mix Rows
iv) XOR Round Key

(A) only (iv) (B) (i).only
(C) (ii) (iii) and (iv) (D) (ii) and (iii)

13. The Elliptic Curve Cryptography encryption is given by the formula 1 2 4

(A) $C_m = \{kG, P_m + P_B\}$ (B) $C_m = \{G, P_m + kP_B\}$
(C) $C_m = \{kG, kP_m + kP_B\}$ (D) $C_m = \{kG, P_m + kP_B\}$

14. RSA is an _____which does not differentiate between the function of public and private keys of users. 1 1 4

(A) Exponential decipher (B) Logarithmic cipher
(C) Exponential cipher (D) Logarithmic decipher

15. The RSA encryption formula is 1 2 4

(A) $C = M^e \bmod \phi(n)$ (B) $C = M^d \bmod \phi(n)$
(C) $C = M^e \bmod n$ (D) $C = M^d \bmod n$

16. Computation of the discrete logarithm is the basis of the which cryptographic system 1 1 4

(A) Symmetric cryptography (B) Asymmetric cryptography
(C) Diffie-Hellman key exchange (D) Secret key cryptography

17. For a 150-bit message and a 10-bit MAC, how many values are the MAC value dependent on? 1 2 3

(A) 2140 (B) 2150
(C) 215 (D) 210

18. SHA-1 produces a hash value of 1 2 3

(A) 256 bits (B) 180 bits
(C) 160 bits (D) 128 bits

19. MAC is a _______ 1 1 4

(A) one-to-one mapping (B) many-to-one mapping
(C) one to many mapping (D) no mapping

20. Which can be used to preserve the integrity of a document or a message? 1 1 4

(A) message digest (B) message summary
(C) encrypted message (D) decrypted message

PART - B (5 × 4 = 20 Marks) Marks BL CO

Answer **any 5** Questions

21. Explain Play fair cipher substitution technique in detail and encrypt the message "network security" with the key “SCISSORS” (Hint: Use ‘x’ instead of space) 4 2 1

22. Illustrate the working of Vernam cipher with an example. 4 2 1

23. Apply Euclid’s algorithm to check whether 65433 and 23876 are co-primes. 4 3 2

24. Check whether the number given 56743 is a prime number or not with Miller Rabin algorithm 4 3 2

25. Outline the RC5 algorithm in detail. 4 2 3

26. Explain Elliptic curves over Z_p. 4 3 4

27. Discuss the security requirements of Cryptographic hash function. 4 3 4

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

Marks BL CO

28. (a) i. Examine the principle of Steganography (6) 12 4 1
ii. Analyze the transposition techniques of Classical Encryption with example (6)

(OR)

(b) Perform encryption and decryption using Hill Cipher. Message is "crypto" with the following key matrix

$$k = \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$$

29. (a) Examine the algebraic structures - Groups, Rings and Fields with necessary axioms. 12 4 2

(OR)

(b) State Chinese Remainder Theorem and discover x for the given set of congruent equations using Chinese Remainder Theorem
$X \equiv 1 \pmod 5$;
$X \equiv 2 \pmod 7$;
$X \equiv 3 \pmod 9$;
$X \equiv 4 \pmod{11}$;

30. (a) Demonstrate the following modes of operations with block diagrams, and state their advantages and limitations, 12 3 3
i. Cipher Block Chaining (CBC)
ii. Cipher Feedback Mode (CFB)
iii. Output Feedback Mode (OFB)
iv. Counter Mode (CTR)

(OR)

(b) Demonstrate AES algorithm with all its round function in detail with neat block diagram

31. (a) Indian Air Force at Chennai is sending a secret code M='23' to their counterpart at Mumbai. They are using RSA algorithm to perform encryption and decryption for the data. Explain the detailed processing of RSA with given specifications : p=17; q=31; e=5. 12 3 4

(OR)

(b) Infosec crypto agency is experimenting with Diffie – Hellman Key Exchange Problem with given parameters to have a secure communication between two users A and B: prime q = 11, primitive root α = 2, User A's Public key $Y_A = 7$ and User B's Public Key $Y_B = 5$.
i)Show that 2 is primitive root of 11
ii)Find User A's Private Key X_A
iii) Compute Shared Secret key K

32. (a) With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2^{128} bits and produces as output a 512-bit message digest. 12 2 4

(OR)

(b) Summarize the concepts of digital signature algorithm with key generation and verification in detail.

* * * * *