REV-01
MSM/26/31

2023/06

SET A

M.Sc. MATHEMATICS
FOURTH SEMESTER
CRYPTOGRAPHY & CODING THEORY
MSM – 403C
[USE OMR FOR OBJECTIVE PART]

Duration: 3 hrs. **Full Marks: 70**

(Objective)

Time: 30 min. **Marks: 20**

Choose the correct answer from the following: ***1X20=20***

1. Which of the following is a decisional problem?
   a. Problems of finding generator of a cyclic group.
   b. Problem checking a number $g \in G$ is a generator or not.
   c. Both (a) and (b).
   d. None of these

2. What will be the size of a key matrix if the plaintext is "DECEMBER"?
   a. 1×8
   b. 8×1
   c. 8×8
   d. 1×1

3. The number of possible key in the Substitution cipher is
   a. 26
   b. 26!
   c. 26×26
   d. None of these

4. The function $f(n) = n^2 + 3n + 3$ is equal to
   a. $O(n^2)$
   b. $\theta(n^2)$
   c. $\psi(n^2)$
   d. None of these

5. Time required to add two binary number of length m and n is equal to:
   a. $O(\max\{m,n\})$
   b. $O(\min\{m,n\})$
   c. $O(mn)$
   d. None of these

6. Signature verification algorithm needs:
   a. Secret key of the signer.
   b. Public key of the signer.
   c. Both can be used.
   d. None of these

7. Which of the following cryptosystem has randomized encryption algorithm?
   a. RSA Cryptosystem
   b. ElGamal Cryptosystem
   c. Rabin Cryptosystem
   d. All the above

8. Which of the following algorithm is based on Birthday Paradox?
   a. Pollard's ρ method
   b. Fermat's method
   c. Pollard's $p-1$ method
   d. None of these

9. In Elliptic curve cryptography, the inverse point of $P = (r, s)$ is
   a. $(-r, -s)$
   b. $(-r, s)$
   c. $(r, -s)$
   d. (r, s)

10. The cardinality of an Elliptic curve E defined over $\mathbb{Z}_p$, for a p is a prime is:
    a. At least $p + 1 + 2\sqrt{p}$
    b. At most $p + 1 + 2\sqrt{p}$
    c. Exactly equal to $p + 1 + 2\sqrt{p}$
    d. None of these

11. C_x is the most likely codeword of x from a code C if $p(x \text{ recieved} \mid C_x \text{ sent})$ is
    a. $\max p(x \text{ recieved} \mid C \text{ sent})$
    b. $\min p(x \text{ recieved} \mid C \text{ sent})$
    c. both may be possible
    d. None of these

12. Which of the following is/are not Polynomial times algorithm
    a. Algorithm for converting decimal to binary.
    b. Algorithm to find the sum of first n natural numbers.
    c. Algorithm to find the product of first n natural numbers.
    d. All of these.

13. Let $V =< S >$ be a vector space with dimension 3, where $S = \{0001, 0010, 0100\}$. The number of distinct bases of V is
    a. 7
    b. 14
    c. 18
    d. 28

14. Let $C = \{000,101,102,010,020,011,012,021,022\}$ be the linear code and $q = 3$. The value of dim $C^{\perp}$ is
    a. 1
    b. 2
    c. 3
    d. 4

15. No of generator matrix of a linear code $C = \{0000, 1010, 0101, 1111\}$
    a. 4
    b. 6
    c. 12
    d. 24

16. The information rate of a binary code $C = \{0000,1011,0101,1110\}$ is
    a. 1/2
    b. ¼
    c. 2
    d. None of these

17. Which of the following pair of co-sets of
    $C = \{00000,10001,11011,00100,10101,01110,11111,00110\}$
    are distinct
    a. $0001 + C$ and $1000 + C$
    b. $0001 + C$ and $0100 + C$
    c. $0011 + C$ and $1000 + C$
    d. None of these

18. Which of the following is/are true?
    a. Finding $\gcd(a, b)$ is polynomial time algorithm and it is a computational problem.
    b. Finding $\gcd(a, b)$ is polynomial time algorithm and it is a decisional problem
    c. Finding $\gcd(a, b)$ is not polynomial time algorithm and it is a computational problem.
    d. Finding $\gcd(a, b)$ is not polynomial time algorithm and it is a decisional problem

19. A digital signature scheme consists of which of the following algorithms?

a. Key generation, signature generation and verification algorithms.
b. Signature generation and verification algorithms.
c. Key generation algorithm
d. Key generation and signature verification algorithms.

20. Which of the following is/are not public key cryptosystem

a. *RSA* scheme
b. ElGamal scheme
c. Diffie-Helmann scheme
d. None of these

-- --- --

Descriptive

Time : 2 hrs. 30 mins. **Marks : 50**

[Answer question no.1 & any four (4) from the rest]

1. For $n=pq$, where p and q are distinct odd primes, define $(n)=(p-1)(q-1)\gcd(p-1,q-1)$. Suppose that the RSA cryptosystem is modified by considering $ed\equiv 1\ (mod\ (n))$. **10**
   a. Prove that encryption and decryption are inverse operation in the modified cryptosystem.
   b. If $p=37,=79$ and $d=7$, find e in this modified cryptosystem.
   c. If $p=37,=79$ and $d=7$, find e in RSA cryptosystem.

2. Let E be the elliptic curve defined as $y^2 = x^3 + 2x + 7$ over modulo 31. **8+2=10**
   a. Show that $\#E_{31} = 39$.
   b. Find $2P$ and its inverse.

3. **a.** Consider a memoryless binary channel probabilities **4+6=10**

$$p(0 \text{ received } | 0 \text{ sent}) = 0.07$$
$$p(1 \text{ received} | 1 \text{ sent}) = 0.8$$

   If codewords from the linear code {000, 100, 111} are being sent over this channel. Use the maximum likelihood decoding rule to decode the following received words:
   i) 010
   ii) 011

   b. Check the following whether the following code are self-orthogonal or not.
   a) C = {0000, 1010, 0101, 1111} over $F2$.
   b) C = {000, 001, 002, 010, 020, 011, 012, 021, 022} over $F3$.

4. **a.** Find the dual of the following codeword C. Also find their dimension. **6+4=10**
   i) C = {0000, 1010, 0101, 1111} over $F2$.
   ii) C = {000, 001, 002, 010, 020, 011, 012, 021, 022} over $F3$.

b. Define distance of a code. Find the distance of the following codes:

a) $C = \{00000, 00111, 11111\}$
b) $C = \{00000, 00111, 12121\}$
c) $C = \{000000, 001110, 111101\}$

5. a. Convert the decimal number -71 to binary form. **4+3+3 =10**

b. Find the upper bound, lower bound and average bound of the following functions:
(i) $f(n) = 1^2 + 2^2 + \cdots + n^2$
(ii) $f(n) = n!$
(iii) $f(n) = n \log n!$

6. Suppose Alice uses the ElGamal cryptosystem over elliptic curve $y^2 = x^3 + x + 6$ modulo 11 with public key (P, B), where the generator $B = (2, 7)$ and $P = (7, 2)$. Determine the ciphertext of the message $(10, 9)$. **10**

7. a. Find a generator matrix and a parity-check matrix for the binary code $C = \langle S \rangle$, where $S = \{11101, 10110, 01011, 11010\}$. **8+2=10**

b. Let $C = \{0000, 1011, 0101, 1110\}$ be a linear code and $q = 2$. Using cosets, decode the following received word:

$$w = 1111$$

8. a. Prove that the 5th Fermat number $F_5 = 2^{2^5} + 1$ is composite. **5+5=10**

b. Prove that the algorithm to compute $n!$ is not polynomial time algorithm.

= = *** = =