REV-01
MSM/12/17

2022/07

M.Sc. MATHEMATICS
FOURTH SEMESTER
CRYPTOGRAPHY AND CODING THEORY
MSM-403C

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

(PART-A: Objective)

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

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

1. The four primary security services of a security system are:
   a. Confidentiality, Access control, Integrity, Non-repudiation
   b. Confidentiality, Access control, Authorization, Non-repudiation.
   c. Confidentiality, Integrity, Non-repudiation, Authentication
   d. Confidentiality, Access control, Authentication, Authorization.

2. Which of the following is a decisional problem?
   a. Problems of finding factors of a composite number
   b. Problems of checking a number is prime or not.
   c. Both (a) are (b)
   d. None of these

3. Which of the following is a trapdoor one-way function
   a. RSA function
   b. DLP function
   c. Both (a) and (b).
   d. None of these

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

5. In a non-singular elliptic curve $y^2 = x^3 + ax + b$, the equation $x^3 + ax + b = 0$ has
   a. all the three solutions are distinct
   b. all are same
   c. does not have distinct solution
   d. none of these

6. The number of possible key in the Affine cipher is
   a. 312
   b. 313
   c. 675
   d. 676

7. 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

8. 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.

9. Let A be an alphabet and x, y be the words of length n. Then

a. $d(x, y) \geq n$ b. $d(x, y) \leq n$
c. $d(x, y) = n$ d. None of these

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

11. Let $S = \{0100,0101\}$ and $q = 2$. Then S^+ is
a. $\{(0,0,0,0),(0,1,1,0),(1,0,0,0),(1,0,1,0)\}$ b. $\{(0,0,0,0),(0,0,1,0),(1,0,0,0),(1,0,1,0)\}$
c. $\{(0,0,0,0),(0,0,1,0),(1,0,0,1),(1,0,1,0)\}$ d. None of these

12. **Which of the following is/are 7-smooth number?**
a. 961 b. 972
c. Both of these d. None of these

13. **Suppose** $C = \{0000,0011,1000,1100,0001,1001\}$ and $x = 0111$. **Then by nearest neighbor decoding rule,** x **is decoded to**
a. 0111 b. 1010
c. 0101 d. 0011

14. Dimension of the linear code $C = \{000,101,102,010,020,011,012,021,022\}$
a. 1 b. 3
c. 2 d. 9

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

16. The number of different co-sets of
$C = \{00000,10001,11011,00100,10101,01110,11111,00110\}$
Are
a. 8 b. 9
c. 10 d. None of these.

17. A key matrix used for encryption in hill cipher must be
a. Invertible matrix b. Non-invertible matrix
c. Square matrix 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. No of generator matrix of a linear code $C = \{0000, 1010, 0101, 1111\}$

a. 3

b. 6

c. 12

d. None of these.

20. Which of the following cryptosystem has randomized encryption algorithm:

a. RSA cryptosystem

b. Rabin cryptosystem

c. ElGamal cryptosystem

d. All of these.

-- --- -

(PART-B : Descriptive)

Time: 2 HRS 40 MINS **Marks : 50**

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

1. Let E be the elliptic curve defined as $y^2 = x^3 + 2x + 7$ over modulo 31. 10

a. Show that $\#E_{31} = 39$ and $P = (2, 9)$ is an element of order 39 in E_{31}.

b. Find $8P$ and its inverse.

2. **a.** Suppose that $\pi = (142)(36)(578)$. Compute 5+5=10

(i) the permutation π^{-1} .

(ii) Decrypt the following ciphertext, for a permutation cipher with $m = 8$, which was encrypted using the key π:

"TGEEMNELNNTDROEOAAHDOETCSHAEIRLM"

b. Show that, for the RSA cryptosystem, the number of fixed plaintext $x \in \mathbb{Z}_n^*$ is equal to $\gcd(e-1, p-1) \times \gcd(e-1, q-1)$, where e is an encryption key.

3. a. Describe Pollard's $p-1$ algorithm for integer factorization. 5+5=10
b. Using Pollard's $p-1$ algorithm find the factors of 1403.

4. 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

5. **a.** Suppose that codewords from the binary code $\{000, 100, 111\}$ are being sent over a BSC with crossover probability $p = 0.03$. Suppose that the following words 6+4=10

a) 010
b) 011
c) 001

are received. Find the more likely codeword sent by the sender.

b. Find the dual of the following codeword C. Also find their dimension.

a) $C = \{0000, 1010, 0101, 1111\}$ over F_2.
b) $C = \{000, 001, 002, 010, 020, 011, 012, 021, 022\}$ over F_3.

6. a. Convert -71 to binary form. 4+3×2=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) $f(n) = n \log n!$

7. 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:
a) 010
b) 011

b. Let $q = 3$, and
$C = \{0000, 1010, 2020, 0101, 0202, 1111, 1212, 2121\}$. Decode the following two words by Syndrome decoding procedure:
(i) 2100
(ii) 0111

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.

= = *** = =