53 (CS 717) CPNS

2021

CRYPTOGRAPHY AND NETWORK SECURITY

Paper : CS 717

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

*Answer **any ten** questions.*

1. *(a)* Compute GCD (6622, 645).

   (b) Find the inverse of 77 in module of 411. 5+5=10

2. Consider the field $GF(2^4)$. Let field multiplication be performed, module the irreducible polynomial $x^4 + x + 1$. Compute each of the following— 5+5=10

   (a) (1100) + (1001)

   (b) (1011) * (0111)

3. *(a)* Explain the Chinese remainder theorem.

(b) Given an integer n, $0 \leq n < 210$ satisfies the following set of congruences :

$$n \bmod 5 = 4$$

$$n \bmod 6 = 3$$

$$n \bmod 7 = 2$$

Using CRT find n? 4+6=10

4. *(a)* What are the differences between polyalphabetic cipher and monoalphabetic cipher ?

(b) Consider a Hill Cipher with $m = 3$ (block size = 3) with the key k shown below —

$$\begin{pmatrix} 25 & 3 & 7 \\ 5 & 9 & 21 \\ 11 & 8 & 13 \end{pmatrix}$$

What is the ciphertext corresponding to the plaintext (VOW) ? 4+6=10

5. *(a)* What do you understand by security threat and security attack ?

(b) Explain different cryptanalysis technique with example. 4+6=10

6. *(a)* What do you understand by Discrete Logarithm ?

(b) Explain the Diffie-Hellman key exchange protocol using discrete logarithm.

(c) Given $p = 131$, $g = 2$; two entities trying to agree upon a common secret using DH key exchange protocol. One entity A chooses a random number 24 and another entity B chooses the random number 17. Find the common secret. 2+5+3=10

7. 10

(a) Explain the ElGamal Encryption algorithm using Discrete Logarithm.

(b) Given $p = 131$ and $g = 2$. Let A's private key is $a = 97$. B wants to send a message ($m = 75$) encrypted using A's public key for which he chooses a random number $r = 33$. Find the Ciphertext encrypted using ElGamal encryption algorithm.

8. (a) What do you understand by Elliptic curve ?

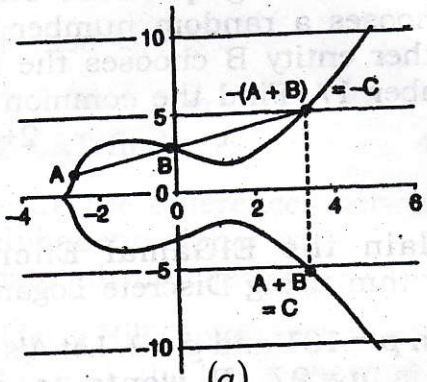
(b) Explain *any two* benefits of using Elliptic curve in Crytography.

(c) Find whether the following elliptic curve self intersect or not

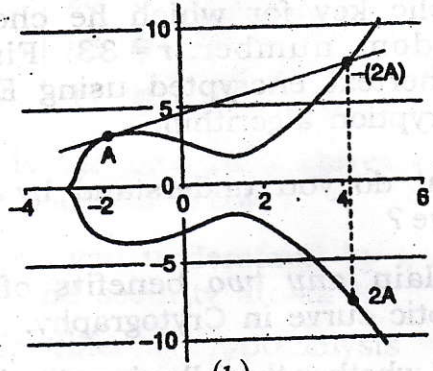
(i) EC (−5, 8)

(ii) EC (−3, 2). 2+2+6=10

9. Consider the geometric interpretation of adding two points $A=(x_1, y_1)$ and $B=(x_2, y_2)$ on elliptic curve as shown in the figure to obtain the point $C=(x_3, y_3)$.



(a)



(b)

Explain the point addition and point doubling for the EC over real numbers as shown in the *Figures (a)* and *(b)*. 10

10. 10

Consider the EC, $y^2 = x^3 + 3x^2 + 1$ over $F(19)$ compute —

(a) (8, 9) + (12, 13)

(b) $2 \times (17, 14)$

11. *(a)* Explain Discrete Logarithm problem on ECs.

(b) Explain EC based Digital Signature scheme. 4+6=10

12. Consider EC, $y^2 + xy = x^3 + gx^2 + g^4$ over $F(2^4)$. Let g = 0010 be generator of the group where field multiplication is defined using the irreducible polynomial $x^4 + x^3 + 1$. Find $\left(g^{13}, g^{12}\right) + \left(g^6, g^2\right)$. 10