

5. (a) Define a cryptographic hash function. Give three applications of cryptographic hash function in cryptography. (6.5)
- (b) Suppose Alice chooses two primes $p = 7$, $q = 11$ and she wants to use the RSA cryptosystem. Can he choose $e = 13$ as his public key? If no, give the reason. If yes, find his private key and encrypt the message $m = 15$. (6.5)
- (c) Describe the key differences between Elliptic Curve Cryptosystem and RSA Algorithm for as public key cryptosystems. (6.5)
6. (a) Describe the SHA-512 round function technique with the help of a diagram. (6.5)
- (b) State ElGamal digital signature scheme and verify with the help of an example. Also, explain existential forgery in this method. (6.5)
- (c) Let $q = 29$, $a = 4$ and $b = 20$, consider Elliptic curve $E_q(a, b): y^2 = x^3 + ax + b \pmod{q}$. Show that $A = (5, 22)$ and $B = (16, 27)$ lie on $E_q(a, b)$. Also, prove that $E_q(a, b)$ is nonsingular and find W , where $W = A + B$. (6.5)

(500)

[This question paper contains 4 printed pages.]

26.12.2024 (M)
Your Roll No.....

Sr. No. of Question Paper : 6087

Unique Paper Code : 32357506

Name of the Paper : Cryptography and Network Security

Name of the Course : CBCS / LOCF B.Sc. (H) Mathematics

Semester : V - DSE-II

Duration : 3 Hours

Maximum Marks : 75

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. Attempt all questions by selecting **two** parts from each question.
3. Parts of the questions to be attempted together.
4. Marks are indicated after each question.
5. Use of a simple calculator is allowed.

P.T.O.

1. (a) Explain the three key objectives Confidentiality, Integrity and Availability of computer security. (6)
- (b) Define Euler's totient function. Prove that if $n = pq$, where p and q are primes, then $\phi(n) = \phi(p)\phi(q)$. Also, find Euler's totient function $\phi(72)$. (6)
- (c) Encrypt the following message using Vigenere Cipher system using HUMOR as the keyword.
THE PEPSI IS IN THE REFRIDGERATOR (6)
2. (a) Given that 5 is a primitive root for the prime 1223, solve the discrete logarithm problem $5^x \equiv 3 \pmod{1223}$. Given that $3^{611} \equiv 1 \pmod{1223}$, determine whether x is even or odd. (6)
- (b) Illustrate the Feistel cipher structure with the help of a diagram. (6)
- (c) Describe the Blum-Blum Shub pseudorandom bit generator and use it to generate a sequence of six random bits with $p = 5$, $q = 7$, $x = 2$. (6)

3. (a) Write a binary representation of the elements of the field $GF(2^4)$ modulo the irreducible polynomial $m(x) = x^4 + x + 11$. Find the multiplicative inverse of $x^2 + 1$ modulo $m(x)$. (6)
- (b) List any six threats to a wireless network with a brief description of each. (6)
- (c) Describe MIME content types with the details of possible subtypes in each content type. (6)
4. (a) Give an overview of the AES key expansion algorithm with a short description of the function g . (6.5)
- (b) Given the entries of the first column of a state matrix in hexadecimal form $\begin{matrix} 1B \\ 23 \\ 45 \\ 86 \end{matrix}$, compute the outcome of the MixColumns transformation on 1B. Describe the rationale behind MixColumn Transformation. (6.5)
- (c) Compute the substitution for the byte 10 in AES SubByte transformation. (6.5)