(b) Describe a hash function. Give three applications of the hash function, clearly specifying the role of the hash function in each application.

(c) Describe E-mail Protocols.

6. (a) Perform the Elgamal signature scheme with $q = 19$, $\alpha = 10$, $x_A = 16$, $k = 5$ and $m = 14$.

(b) Write a short note on RFC 5322 and Multipurpose Internet Mail Extensions (MIME).

(c) Write all wireless environment components. Explain wireless Network Threats.

[This question paper contains 4 printed pages.]

05.01.2024(M)

Your Roll No.....

Sr. No. of Question Paper : 4587 **G**

Unique Paper Code : 32357506

Name of the Paper : DSE-II Cryptography and Network Security

Name of the Course : **B.Sc. (H) Mathematics**

Semester : V

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. **All** questions are compulsory.
3. Attempt any **five** parts from questions **1**, each part carries **3** marks.
4. Attempt any **two** parts from questions **2** to **6**, each part carries **6** marks.

P.T.O.

1. (a) Write a short note on Active attack in computer security.

   (b) What is a transposition cipher? Write the message

   'attackpostponeduntiltwoam'

   row by row and encrypt it with the key '4 3 1 2 5 6 7'.

   (c) What is Euler's Totient function? Find $\varphi(143)$ and $\varphi(71)$.

   (d) Briefly describe MixColumns transformation of AES.

   (e) Is (5, 12) a point on the elliptic curve $y^2 = x^3 + 4x - 1$ over real numbers.

   (f) Define direct digital signature.

2. (a) Explain Symmetric Cipher model with the help of a diagram.

   (b) Encrypt the message 'CRYPTOGRAPHY' using Playfair Cipher with the key 'algorithm'. Write the rules while encrypting the message.

   (c) Explain the Feistel Decryption process with the help of a diagram.

3. (a) State the Chinese Remainder theorem and hence solve the following system of linear congruence relations :

   $x \equiv 2 (\text{mod } 5)$, $x \equiv 5 (\text{mod } 8)$ and $x \equiv 4 (\text{mod } 37)$.

   (b) State the Fermat's theorem. Find the remainder when $(300)^{3000}$ is divisible by 1001.

   (c) Explain the Data Encryption Standard (DES) with the help of a diagram.

4. (a) Find the multiplicative inverse of 550 mod (1759) where 1759 is a prime number.

   (b) Identify $GF(2^8)$ with the field of polynomial over GF(2) modulo $m(x) = x^8 + x^4 + x^3 + x + 1$. If the byte $b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0$ represent the polynomial $b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0$ in the field, find the product f(x) g(x) where f(x) = (01010011) and g(x) = (10111010) are elements of the field.

   (c) Perform encryption and decryption using the RSA algorithm for p = 3, q = 11, e = 7 and M = 14.

5. (a) On the elliptic curve over Z_{23}, $y^2 = x^3 + x + 1$, Let P = (13,7) and Q = (9,7). Find P + Q and 2P.