(ii) Key exchange scheme using the above elliptic curve. Why is it considered hard to break this scheme? (3+4.5)

(c) Suppose you set up a (2,30) Shamir threshold scheme, working mod the prime 101. Two of the shares are (1,13) and (3,12). Another person received the share (2,*), but the part denoted by * is unreadable. What is the correct value of * ? (7.5)

6. (a) Define the XOR-based hash function. Compute the hash value for the following message blocks using the XOR operation: X_1 = 10101010, X_2 = 11001100, X_3 = 11110000, X_4 = 01011001. Also, comment on why this method is not suitable for cryptographic applications. (7.5)

(b) Describe the Schnorr Digital Signature Scheme. How does it improve efficiency compared to the ElGamal Digital Signature Scheme? Discuss its parameters and describe the key generation, signature generation, and verification steps. (7.5)

(c) Explain the following terms :

(i) Linear code
(ii) Generator matrix
(iii) Hamming distance
(iv) Orthogonal vectors
(v) Parity-check matrix (7.5)

[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 7380 **L**

Unique Paper Code : 2353010022

Name of the Paper : DSE – Cryptography

Name of the Course : **B.Sc. (H) Mathematics, UGCF-2022**

Semester : VIII

Duration : 3 Hours Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **All** questions are compulsory and carry equal marks.
3. Attempt **two** parts from each question.

1. (a) Explain the following terms :

(i) ASCII
(ii) Brute-force attack
(iii) Public key cryptography (2.5+2.5+2.5)

(b) Using the Vigenere Cipher with keyword “LOCK”, convert the following plaintext into ciphertext:

“SEND HELP SOON”

Show all steps clearly and write the final ciphertext. (7.5)

(c) Show that $f(x) = x^3 + x + 1$ and $g(x) = x^2 + 1$ are multiplicative inverses of each other in $GF(2^4)$ with irreducible polynomial $m(x) = x^4 + x + 1$. (7.5)

2. (a) State the Chinese Remainder Theorem and apply it to determine the solution of the system:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$

(7.5)

(b) Using the Blum-Blum-Shub (BBS) Pseudorandom Bit Generator, for primes 7 and 23 with initial seed 5, generate the first 4 bits b_1, b_2, b_3, $b_{4:}$. (7.5)

(c) Encrypt the plaintext "SECRET" using the Hill Cipher with key

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}.$$

Show all steps clearly and write the final ciphertext. (7.5)

3. (a) Explain the Feistel encryption structure of a block cipher with the help of a diagram. (7.5)

(b) Briefly describe ShiftRows, InvShiftRows, and rationale behind their use in AES. (7.5)

(c) Perform encryption and decryption using the RSA algorithm for p = 3, q = 11, public key b = 7 and the plaintext value X = 5. (7.5)

4. (a) What is an ideal block cipher? Explain its operation with an example for a 2-bit block size. Why it cannot be used practically? (7.5)

(b) Explain the step-by-step process of the Diffie – Hellman key exchange for q = 23 and its primitive root $\alpha = 5$ by taking $X_A = 3$ and $X_B = 4$. (7.5)

(c) Explain the concepts of diffusion and confusion in cryptography. In AES, identify which round transformations provide diffusion and which provide confusion. Justify your answer. (7.5)

5. (a) Suppose Alice and Bob use an ElGamal scheme with a common prime q = 149 and a primitive root $\alpha = 2$.

(i) If Bob has public key $Y_B = 11$ and Alice chooses the random integer k = 3, find the ciphertext for the message M = 8.

(ii) If Alice now chooses a different value of k such that the encoding of M = 7 is $C = (8, C_2)$, determine the value of C_2? (4.5+3)

(b) Explain the following :

(i) Elliptic curves over $\mathbb{Z}_p$.