Name of Course	: **CBCS B.Sc. (H) Mathematics**
Unique Paper Code	: **32357506**
Name of Paper	: **DSE-II Cryptography and Network Security**
Semester	: **V**
Duration	: **3 hours**
Maximum Marks	: **75 Marks**

Attempt any four questions. All questions carry equal marks.

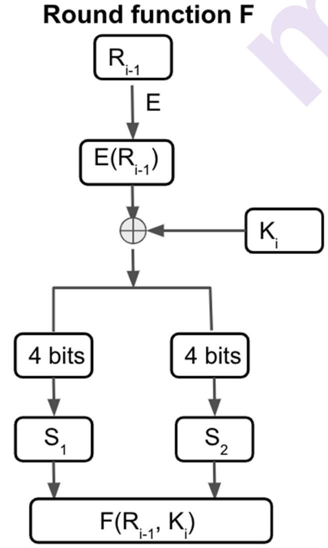
1. Let p be a prime such that $\frac{p-1}{2}$ is an odd integer. Let m and n be integers such that p divides m^2+n^2. Show that if $p \nmid m$ and $p \nmid n$ then use of Euler's theorem leads to a contradiction on the choice of p and hence conclude that p must divide both m and n.

2. Describe the encryption technique of a Hill-Cipher. Show that the matrix $A = \begin{bmatrix} 4 & 23 \\ 2 & 18 \end{bmatrix}$ can not be used as a Hill-Cipher encryption matrix. Find two different plaintexts that map to the same cipher if encrypted using A.

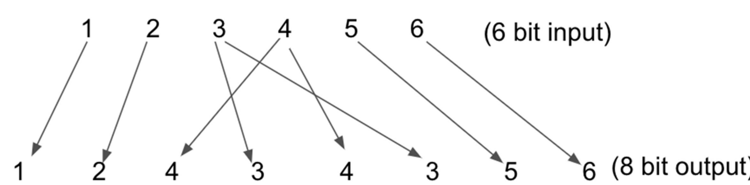
3. Consider a cryptosystem based on the Feistel structure, where plaintext m is divided into two equal parts say $m = L_0R_0$ and L_iR_i are generated in various rounds during encryption process as follows:

$L_i = R_{i-1}$ and $R_i = F(R_{i-1}) \oplus L_{i-1}$, where F is the round function defined as:

Round function F



Key expansion function E



S_1	100	010	011	101	110	001	000	111
	011	100	111	110	000	101	010	001

S_2	100	110	000	001	101	010	111	011
	010	111	011	000	110	100	001	101

E is a key expansion function that takes 6 bit input and produces 8 bit output. For example $(100101) = 10101101$. S_i are S-boxes that take 4 bit input and produce 3 bit output. The first bit of the input gives the row number and the last three bits of the input gives the column number. For example, to calculate $S_1(0101)$, we will take the cell value at 0^{th} row and 5^{th} column of S_1, so $S_1(0101) = 001$. Similarly $S_1(1010) = 000$ (cell value at 1^{st} row and 2^{nd} column).

4. State the Prime factorization problem. Mention and describe the public key cryptosystem whose security relies on this problem. Suppose Alice and Bob decide to use a symmetric key encryption scheme for secure communication. But as they live apart, they cannot meet physically to share the secret key for symmetric key encryption. Alice generated a secret key K and encrypted it with the Bob's RSA cryptosystem public key $(d, n) = (13, 77)$, which is calculated as 64. On receiving the encrypted K, that is 64, Bob decrypts it using his private key and recovers the secret key K. Find the secret key K.

5. Let $E_p(a, b)$ be an elliptic curve, and let g be chosen global base point. Let H be a fixed Hash taking values in $E_p(a, b)$. Alice calculates private key $X_A \in \mathbb{N}$ and computes public key $P_A = X_A g$. To sign a message M:

Step 1. Alice selects a random positive integer α and computes the signature

$$S_1 = H(M) - \alpha X_A g, \text{ and } S_2 = \alpha X_A.$$

The pair (S_1, S_2) is sent to Bob.

Step 2. Bob computes $V = S_1 + S_2 g$. If $V = H(M)$ then the signature is verified.

Show that this digital signature protocol works. What may be the issue if instead of taking the Hash value, the original plaintext M is used.

6. Let a message M be expressed as the tuple $(a_1, a_2, \dots, a_t)$ with $a_i \in \mathbb{Z}_{11}$. Let $H(M) = \sum_{i-1}^{t} a_i$ be used as a Hash function. Does it satisfy the required properties of a Hash function? Justify your answer with explanation or illustrative example, as the case may be.