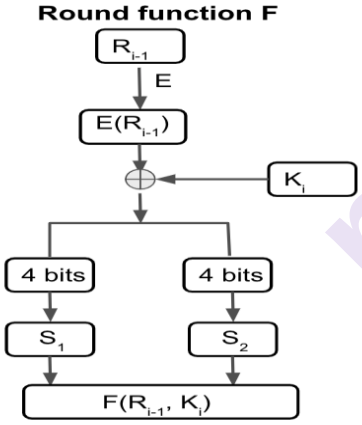
Name of Course	: **CBCS B.Sc. (H) Mathematics**
Unique Paper Code	: **32357506**
Name of Paper	: **DSE-II Cryptography and Network Security**
Semester	: **V**
Duration	: **3 hours**
Maximum Marks	: **75 Marks**

Attempt any four questions. All questions carry equal marks.

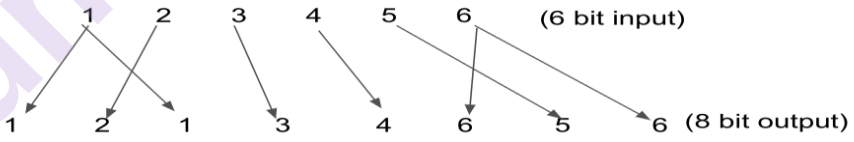
1. Show that the polynomial $f(x) = 3x^3 + 2x + 1$ has no zeros in $\mathbb{Z}_5$. Is f irreducible over $\mathbb{Z}_5$ (answer with justification)? Use an irreducible factor of f to construct a finite filed of order 5^n for some n. What are the possible values of n? Find the multiplicative inverse of $2x^2 + 4x + 3$ in the field you have constructed.
2. In order to obtain confidentiality, why does the PGP use a symmetric key block cipher to encrypt the content of the email and not a public key encryption? Discuss the role of compression of the message in PGP. Explain why it is not wise to compress the message before putting the digital signature?

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 the encryption process as follows:

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



Key expansion function E



S_1	010	100	011	101	110	001	111	000
	001	100	000	110	111	101	010	011
S_2	011	110	000	001	101	010	111	100
	010	000	011	111	110	100	001	101

E is a key expansion function that takes 6-bit input and produces 8-bit output. For example $E(100101) = 10101101$. Si 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 give the column number. For example, to calculate S1(0101), we will take the cell value at 0th row and 5th column of S1 , so S1(0101) = 001. Similarly S1(1010) = 000 (cell value at 1st row and 2nd column).

The Shift function circular shifts the bits to two places towards the left. For example Shift(100101) = 010110.

Suppose the plaintext $m = 101101001101$ (12 bits) and the first two rounds keys are $K_1 = 10011010$ and $K_2 = 01101101$. Perform two iterations of the above-described encryption scheme.

4. Describe the main components and working of a Public Key cryptosystem (PKC). Describe the RSA cryptosystem and identify the main components, as that of a PKC. Suppose under the RSA cryptosystem, Alice chooses $p = 13, q = 17$ and her public key is 77. Suppose she received the ciphertext $c = 5$ from Bob. Find the corresponding plaintext.

5. Consider the following Key exchange protocol known as Diffie Hellman Key exchange between User U and Sever S:

   Step I: U and S choose a cyclic group $G = Z_q^* \text{ or } U(q)$, where q is prime and P be a generator of G.

   Step II: U chooses secret value $\alpha < q$ and sends P^{α} to S.

   Step III: S chooses secret value β and sends P^{β} to U.

   Step IV: U computes $\left(P^{\beta}\right)^{\alpha} = P^{\alpha\beta}$.

   Step V: S calculates $(P^{\alpha})^{\beta} = P^{\alpha\beta}$. Thus, U and S have same shared secret key $P^{\alpha\beta}$.

   Suppose $q = 11$, generator $P = 5$, U and S secret keys are $\alpha = 3, \beta = 5$ respectively. Find the secret key shared by U and S. Also, find public keys of U and S.

6. Let q be a prime and let α be an integer such that q does not divide α. Let $h(x) = \alpha^x (mod\ q)$. Explain why $h(x)$ not a good cryptographic hash function. Again let $m = p.q$ be the product of two distinct large primes and let $h(x) = x^2 (mod\ m)$. Why is h preimage resistant?