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. Consider a Playfair Cipher where the 5×5 matrix consists of letters A to Z excluding J. The plaintext

THIS FOUR LETTER WORD DUCK IS USED TO SHOW SOME SCORED ZERO

is encrypted twice using the playfair cipher, first with use of key MOZART and then with an unknown key. The final cipher is

FNQYFAVRHSLZSRVZVIMTSTSGQYZKASCRQHVWQMIROSVIASMBIV

Find the unknown key used in the second playfair matrix.

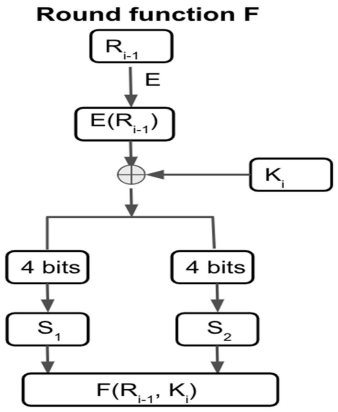
2. Consider the map $\phi : \mathbb{Z}_{60} \to \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$ defined as

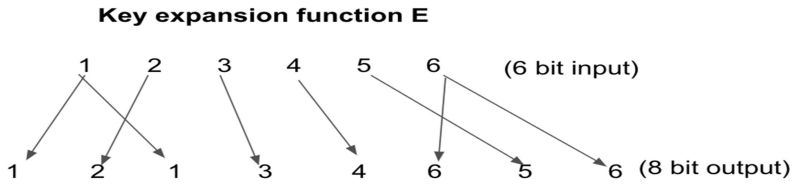
$$\phi(x) = \big(x \pmod 3, x \pmod 4, x \pmod 5\big), 0 \leq x \leq 59.$$

Show that ϕ is one-one and onto. Find the pre-image of the point $(2, 3, 3)$ under ϕ.

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





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 $(100101) = 10101101$. 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).

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. Define the basic components of a Public key cryptosystem and its encryption and decryption algorithms. What are the advantages of a Public key cryptography over Symmetric key cryptography? Define a trapdoor function and discuss its significance in the Public key cryptography. Mention the trapdoor function on which the security of RSA cryptosystem relies.

5. Let $p = 29$, $a = 4$ and $b = 20$, consider Elliptic curve $E_p(a, b): y^2 = x^3 + a\,x + b$. Show that $P = (5, 22)$ and $Q = (16, 27)$ lie on $E(F_p)$. Also, prove that $E_p(a, b)$ is nonsingular and find R & $3R$, where $R = P + Q$.

6. What components are prescribed in PGP to ensure confidentiality and integrity of an e-mail? Discuss the roles of ZIP compression and radix 64 expansion in PGP.