Question 1: (12 Marks)

If exists, calculate multiplicative inverse of 7, 12, 22, 23, 66, 93, and 129 in Z_{164}. If does not exists explain why? Note that gcd(164, X) =1, otherwise no multiplicative inverse possible.

Formulas:

x * d mod 164=1

d= (1+k *164)/e, k= 1… upto x, should be an integer number

Question 2: (12 Marks)

If exists, find the determinant and the multiplicative inverse of the residue matrix M_1 and M_2 over $\mathbf{Z_{26}}$

$$M_1 = \begin{pmatrix} 21 & 6 & 22 \\ 5 & 23 & 25 \\ 7 & 3 & 9 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 23 & 6 & 3 \\ 25 & 21 & 22 \\ 9 & 5 & 7 \end{pmatrix}$$

Question 3: (12 Marks)

If we want to use above matrices (M_1 and/ or M_2) of Question 5 as a key for constructing a Hill Cipher cryptosystem, then which one between M_1 and M_2 you recommend to use as a key, and why?

Using your recommended key decrypt the following ciphertext.

Ciphertext: **TJFKBSXXW**

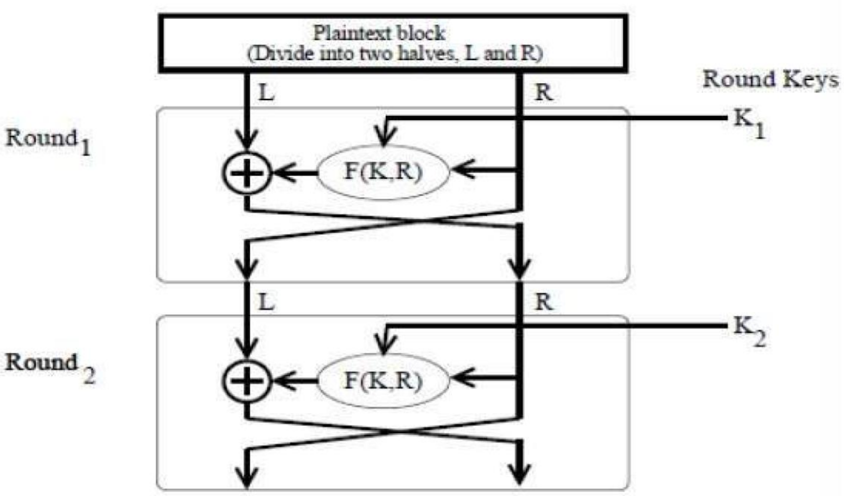
Question 4: (20 Marks)

Using Feistel Block Cipher Encryption technique with two rounds, encrypt the following plaintext .

Plaintext: be (01100010 01100101)

K_1 : 10101011

K_2 : 11001101



F is defined as follows:

$F(K, R) = K \oplus$ [4-bit left circular shift of R]

Question 5: (20 Marks)

Ahmed is using RSA crypto-system with the following setup:

- p = 11 and q = 3
- n = pq = 11 × 3 = 33.
- Φ(n) = (p − 1)(q − 1) = 10 × 2 = 20.
- Ahmed publish his Public Key:
  (n, e) = (33, 3).

A. Calculate Ahmed's private key.
B. Charlie wants to send the message M = 13 to Ahmed. Using Ahmed's public and private keys, calculate the ciphertext C, and the value for Message R, when Alice recovers the message.
C. Dixit wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find his private and public keys.

Question 6: (12 Marks)

In a RSA cryptanalysis, you intercept the ciphertext C = 10 sent to a user whose public key is (*e* = 7, *n* = 35). What is the plaintext M?

Question 7: (12 Marks)

In a Deffie-Hellman key exchange setup, for simplicity, consider the large prime **P = 53** and the primitive root of ***P*** is ***a = 5.*** A sender generates his random secret $X_A = 12$ and the receiver generates his random secret $Y_B = 18$. Calculate the session key.