1. Implement the A5/1 algorithm. Suppose that, after a particular step, the values in the registers are

$$X = (x_0, x_1, \ldots, x_{18}) = (1010101010101010101)$$
$$Y = (y_0, y_1, \ldots, y_{21}) = (1100110011001100110011)$$
$$Z = (z_0, z_1, \ldots, z_{22}) = (11100001111000011110000)$$

2. Consider a Feistel cipher with four rounds. Then the plaintext is denoted as $P = (L_0, R_0)$ and the corresponding ciphertext is $C = (L_4, R_4)$. What is the ciphertext C, in terms of L_0, R_0, and the subkey, for each of the following round functions?

a. $F(R_{i-1}, K_i) = 0$
b. $F(R_{i-1}, K_i) = R_{i-1}$
c. $F(R_{i-1}, K_i) = K_i$
d. $F(R_{i-1}, K_i) = R_{i-1} \oplus K_i$

3. Suppose that Alice's RSA public key is $(N, e) = (33, 3)$ and her private key is $d = 7$.

a. If Bob encrypts the message $M = 19$ using Alice's public key, what is the ciphertext C? Show that Alice can decrypt C to obtain M.
b. Let S be the result when Alice digitally signs the message $M = 25$. What is S? If Bob receives M and S, explain the process Bob will use to verify the signature and show that in this particular case, the signature verification succeeds.

4. **For (N, e) = (33,3) and d = 7, show in which message (m) values the cube root attack works?**