1. **Answer the following questions about S-boxes in DES:**

a. Show the result of passing 110111 through S-box 3.

b. Show the result of passing 001100 through S-box 4.

c. Show the result of passing 000000 through S-box 7.

d. Show the result of passing 111111 through S-box 2.

1. **Let us consider an RSA Public Key Crypto System**

Alice selects 2 prime numbers :p=5, q=11

1. Compute n, and Φ(n)
2. Alice selects her public exponent e = 3 , Is this choice for “e” valid here? Is this choice always valid ?
3. Compute d , the private exponent of Alice
4. Encrypt your plaintext M=4 using Alice public exponent. What is the resulting ciphertext C?
5. Now Alice receives C. Verify that Alice can obtain M from C, using her private decryption exponent.
6. **Alice publishes the following data n = pq = 221 and e = 13. Bob receives the message P = 65 and the corresponding digital signature S = 182. Verify the signature.**
7. **Encrypt the following message M=9 knowing that : p= 5 , q= 11 and e=3 .**