1. Describe in detail a man-in-the-middle attack on the Diffie-Hellman key-exchange protocol whereby the adversary ends up sharing a key \( k_A \) with Alice and a different key \( k_B \) with Bob, and Alice and Bob cannot detect that anything has gone wrong.

What happens if Alice and Bob try to detect the presence of a man-in-the-middle adversary by sending each other (encrypted) questions that only the other party would know how to answer?

2. Consider the following key-exchange protocol:

   (a) Alice chooses \( k, r \leftarrow \{0, 1\}^n \) at random, and sends \( s := k \oplus r \) to Bob.
   (b) Bob chooses \( t \leftarrow \{0, 1\}^n \) at random and sends \( u := s \oplus t \) to Alice.
   (c) Alice computes \( w := u \oplus r \) and sends \( w \) to Bob.
   (d) Alice outputs \( k \) and Bob outputs \( w \oplus t \).

Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).

3. Consider the following key-exchange protocol:

   Common input: The security parameter \( 1^n \).
   (a) Alice runs \( G(1^n) \) to obtain \( (G, q, g) \).
   (b) Alice chooses \( x_1, x_2 \leftarrow \mathbb{Z}_q \) and sends \( \alpha = x_1 + x_2 \) to Bob.
   (c) Bob chooses \( x_3 \leftarrow \mathbb{Z}_q \) and sends \( h_2 = g^{x_3} \) to Alice.
   (d) Alice sends \( h_3 = g^{x_1 x_3} \) to Bob.
   (e) Alice outputs \( h_2^{x_1} \). Bob outputs \( (g^\alpha)^{x_3} \cdot (h_3)^{-1} \).

Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).

4. Show that any 2-round key-exchange protocol (that is, where each party sends a single message) can be converted into a CPA-secure public-key encryption scheme.

5. Fix an RSA public key \( \langle N, e \rangle \) and assume we have an algorithm \( A \) that always correctly computes \( \text{lsb}(x) \) given \( [x^e \mod N] \). Write full pseudocode for an algorithm \( A' \) that computes \( x \) from \( [x^e \mod N] \).