1. Exercise 7.16

2. Exercise 7.18

3. Exercise 9.2

4. Exercise 9.3

5. Consider the following key-exchange protocol: Common input: The security parameter $1^n$. The protocol:

   (a) Alice runs $\mathcal{G}(1^n)$ 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 $h_3 = g^{x_2 x_3}$ 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).