1. **Square-And-Multiply, Efficient Modular Exponentiation**: Exercise B.3 in [KL]. Argue why your algorithm is efficient. **Corrected hint**: Let $y = [a^b \mod N]$ denote the answer. Use auxiliary variables $x$ (initialized to $a$) and $t$ (initialized to 1), and maintain the invariant $t \cdot x^b = y \mod N$ while decreasing $b$ and squaring $x$. The algorithm terminates when $b = 0$ and $t$ is equal to the answer.

2. **Interactive Secure Encryption**: Exercise 9.1 in [KL]

3. **Man-In-The-Middle Attacks**: Exercise 9.2 in [KL]

4. **Key Exchange with Bit Strings**: Exercise 9.3 in [KL]

5. **CDH and DDH**:

   (a) Give an example of a (not necessarily multiplicative) group $G$ relative to which the CDH-Problem is easy.

   (b) Prove formally that the hardness of the CDH problem relative to a group $G$ implies the hardness of the discrete logarithm problem relative to $G$. (Exercise 7.15 in [KL])

   (c) Prove formally that the hardness of the DDH problem relative to a group $G$ implies the hardness of the CDH problem relative to $G$. (Exercise 7.16 in [KL])

---

**Diffie-Hellman Key Exchange Using Buckets of Paint**

Image credit: [wikimedia.org](https://commons.wikimedia.org/wiki/File:Diffie-Hellman_key_exch.png).