1. Implement Schnorr group, that is, generate primes $p$, $q$, and a group element $g$, such that $p = kq + 1$ and $g$ generates an order $q$ multiplicative subgroup of $\mathbb{Z}_p^*$.

2. Is the following assumption secure? If yes, reduce it to a known assumption (DLOG, DDH, CDH), otherwise find an attack. Adversary gets $g^a$ and $g^b$ as an input (like in CDH) and it should be computationally hard to output group elements $A \neq 1$ and $B \neq 1$ such that $A^a \cdot B^b = 1$.

3. For a fixed security parameter $\kappa$, assume we have algorithm $\mathcal{A}$ that runs in time $T$ and solves discrete logarithm with probability 0.01.
   (a) Construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ to solve CDH with the same parameter $\kappa$.
   (b) How to increase the success probability?
   (c) Give a lower bound for the success probability of $\mathcal{B}$.
   (d) If all group operations take time 1, how much time does $\mathcal{B}$ take in total?

4. Is the following assumption secure? If yes, reduce it to a known assumption (DLOG, DDH, CDH), otherwise find an attack. Adversary gets $g^a$ and $g^b$ as an input (like in CDH) and it should be computationally hard to output $g^{(ab)^2}$.