1. 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 $g^{(ab)^r}$.

2. Implement Elgamal based on Schnorr group.

3. Implement homomorphic multiplication of two ciphertexts and homomorphic scalar multiplication of a ciphertext.

4. Suppose user has some private data $m_1, m_2, m_3$ and a company has developed a prediction function $f(x, y, z) = x^{k_1} \cdot y^{k_2} \cdot z^{k_3}$. Coefficients $k_1, k_2, k_3$ have been generated by a machine learning algorithm that company has spend a lot of time developing. Implement a protocol (using Elgamal) where user can learn $f(m_1, m_2, m_3)$, but nothing else about the coefficients and company learns nothing about users data.