1. Consider the Diffie-Hellman protocol. Let $p = 11$ and $g = 3$. Let $x_a = 5$ and $x_b = 2$. (5 pts)
   a) Compute
      $$y_a = g^{x_a} \mod p$$
      $$y_b = g^{x_b} \mod p$$
   b) Compute
      $$K_a = y_b^{x_a} \mod p$$
      $$K_b = y_a^{x_b} \mod p$$

2. Consider the RSA encryption system with public keys $n = 55$ and $e = 7$. (5 pts)
   a) Encipher the plaintext $M = 10$.
   b) Break the cipher by finding $p$, $q$, and $d$. Then decipher the ciphertext $C = 35$.

3. Suppose there are three users in a network, say Bob, Bart and Bert, all having public encryption exponent $b = 3$. Let their moduli be denoted by $n_1$, $n_2$, $n_3$. Now suppose Alice encrypts the same plaintext $x$ to send to Bob, Bart and Bert. That is Alice computes $y_1 = x^3 \mod n_1$, $y_2 = x^3 \mod n_2$, $y_3 = x^3 \mod n_3$. Describe how Oscar can compute $x$, given $y_1$, $y_2$ and $y_3$, without factoring any of the moduli. (10 points)