1. Public Key Encryption

   (a) Let (N, e) be the public key for textbook RSA, where $N = 5 \cdot 13 = 65$ and $e = 7$. Find the corresponding secret key (N, d). Then encrypt the message $m = 2 \mod 65$, obtaining some ciphertext c. Decrypt c to recover m. Do the computations by hand and show your work.

   Hint: To speed up your computations, use the following facts: $64 = 2^6$, $(2)^6 \equiv -1 \mod 65$.

   (b) Consider the subgroup of Z_{23}^* consisting of quadratic residues modulo 23. This group consists of the following elements: $\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. We choose $g = 2$ to be the generator of the subgroup. Let $(23, 11, 2, x = 5)$ be the secret key for ElGamal. Find the corresponding public key. Then encrypt the message $m = 2$, using randomness $r = 3$, obtaining some ciphertext c. Decrypt c to recover m. Do the computations by hand and show your work.

   Hint: To speed up your computations, use the fact that $3^3 = 4 \mod 23$, $8^4 = 2 \mod 23$, $4^{-1} = 6 \mod 23$.