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: $64 = 2^6$, $(2)^6 \equiv -1 \mod 65$.

\Phi(N) = (p-1)(q-1) = 4*12 = 48. d = 7 since e*d mod \Phi(N) = 7*7 = 49 mod 48 = 1.

Encrypt m = 2: c = 2^7 mod 65 = 2^6 * 2 = (-1)*2 = -2 = 63 mod 65

Decrypt c = -2: m = (-2)^7 = (-1)^7 * 2^7 = -1 * -2 = 2 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 x = 5 and y = 3. Show the messages exchanged in Diffie-Hellman key exchange, as well as the obtained shared key. Do the computations by hand and show your work.

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

First message: 2^5 mod 23 = 32 mod 23 = 9
Second message: 2^3 mod 23 = 8
Key obtained by first party: 8^5 mod 23 = 8^4 * 8 = 2 * 8 = 16
Key obtained by second party: 9^3 mod 23 = 3^3 * 3^3 = 4*4 = 16