

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 $m = 2 \pmod{65}$, 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: $64 = 2^6$, $(2)^6 \equiv -1 \pmod{65}$.

- (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 $3^3 = 4 \pmod{23}$, $8^4 = 2 \pmod{23}$, $4^{-1} = 6 \pmod{23}$.