

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

**Solution:**

$\Phi(N) = 4 \cdot 12 = 28$ . Using mental math, we can see that  $d = 7$ , since  $7 \cdot 7 = 49 = 1 \pmod{28}$ . So the secret key is  $(65, 7)$ .

To encrypt  $m = 2$ , we output  $2^7 \pmod{65} = 2^6 \cdot 2 = -1 \cdot 2$  (using the hint)  $= -2 = 63 \pmod{65}$ .

To decrypt  $c = 63$ , we output  $(63)^7 \pmod{65} = (-2)^7 \pmod{65} = (-1)^7 \cdot 2^7 = -1 \cdot 2 = 63 \pmod{65}$ .

- (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  $(23, 11, 2, x = 5)$  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  $3^3 = 4 \pmod{23}$ ,  $8^4 = 2 \pmod{23}$ ,  $4^{-1} = 6 \pmod{23}$ .

**Solution:**

The public key consists of  $(23, 11, 2, h = 2^5) = (23, 11, 2, 32 \pmod{23}) = (23, 11, 2, 9)$ .

To encrypt  $m=2$  with randomness  $r = 3$ , we need to compute  $c_1 = 2^3$ ,  $c_2 = 9^{3 \cdot 2} \pmod{23}$

So  $c_2 = 3^3 \cdot 3^3 \cdot 2 = 4 \cdot 4 \cdot 2 = 32 \pmod{23} = 9$ .

The final ciphertext is  $(8, 9)$ .

To decrypt  $(8, 9)$ , we must compute  $9/(8^5) = 9 \cdot (8^5)^{-1}$ .

We first compute  $(8^5)^{-1} = (8^4 \cdot 8)^{-1} = (2 \cdot 8)^{-1} = 16^{-1} = 4^{-1} \cdot 4^{-1} = 6 \cdot 6 = 36 \pmod{23} = 13$ .

So  $m = 9 \cdot 13 \pmod{23} = 117 \pmod{23} = 2$ .