

## Homework Set 10

### Problem 1

**Example 22.** Bob's public ElGamal key is  $(p, g, h) = (47, 45, 14)$ . Encrypt the message  $m = 16$  ("randomly" select  $y = 25$ ) for sending it to Bob.

**Solution.** The ciphertext is  $c = (c_1, c_2)$  with  $c_1 = g^y \pmod{p}$  and  $c_2 = h^y m \pmod{p}$ .

Here,  $c_1 = 45^{25} \equiv 43 \pmod{47}$  and  $c_2 = 14^{25} \cdot 16 \equiv 8 \cdot 16 \equiv 34 \pmod{47}$ . Hence, the ciphertext is  $c = (43, 34)$ .

### Problem 2

**Example 23.** Your public ElGamal key is  $(p, g, h) = (23, 15, 8)$  and your private key is  $x = 12$ . Decrypt the message  $c = (5, 18)$  that was sent to you.

**Solution.** We decrypt  $m = c_2 c_1^{-x} \pmod{p}$ .

Here,  $m = 18 \cdot 5^{-12} \equiv 18 \cdot 5^{10} \equiv 18 \cdot 9 \equiv 1 \pmod{23}$ .

### Problem 3

**Example 24.** Bob's public ElGamal key is  $(p, g, h) = (41, 29, 31)$ . Determine Bob's private key.

**Solution.** We need to solve  $29^x \equiv 31 \pmod{41}$ . This yields  $x = 4$ .

(Since we haven't learned a better method (no "good" method is known!), you can just try  $x = 1, 2, 3, \dots$  until you find the right one.)