

## Homework Set 9

### Problem 1

**Example 17.** Bob randomly generated  $N = 119$  for his public RSA key. What is the smallest possible choice for  $e$ ?

**Solution.** Recall that  $e$  must be invertible modulo  $\phi(N) = \phi(7)\phi(17) = 6 \cdot 16$ . Hence,  $e = 2, 3, 4$  are not allowed. Therefore, the smallest possible choice for  $e$  is  $e = 5$ .

### Problem 2

**Example 18.** Find  $x$  such that  $8 \equiv 3^x \pmod{19}$ .

**Solution.** We proceed by brute-force and just go through the possibilities:

$$3^2 = 9, 3^3 \equiv 8 \pmod{19}$$

Hence,  $x = 3$ .

As the next example shows, sometimes we might have to look for a while before finding the discrete logarithm.

[However, I have programmed the homework problem so that you will not have to search for long.]

**Example 19.** Find  $x$  such that  $4 \equiv 3^x \pmod{19}$ .

**Solution.** We proceed by brute-force and just go through the possibilities:

$$3^2 = 9, 3^3 \equiv 8, 3^4 \equiv 8 \cdot 3 \equiv 5, 3^5 \equiv 5 \cdot 3 \equiv -4, 3^6 \equiv -4 \cdot 3 \equiv 7, 3^7 \equiv 7 \cdot 3 \equiv 2, 3^8 \equiv 2 \cdot 3 \equiv 6, 3^9 \equiv 6 \cdot 3 \equiv -1, \\ 3^{10} \equiv -1 \cdot 3 \equiv -3, 3^{11} \equiv -3 \cdot 3 \equiv -9, 3^{12} \equiv -9 \cdot 3 \equiv -8, 3^{13} \equiv -8 \cdot 3 \equiv -5, 3^{14} \equiv -5 \cdot 3 \equiv 4 \pmod{19}$$

Hence,  $x = 14$ .

**Comment.** As a shortcut, when we observed  $3^7 \equiv 2 \pmod{19}$ , we could have concluded that  $4 = 2^2 \equiv 3^{7 \cdot 2} = 3^{14} \pmod{19}$  so that  $x = 14$ .

### Problem 3

**Example 20.** Alice and Bob select  $p = 29$  and  $g = 8$  for a Diffie-Hellman key exchange. Alice sends 13 to Bob, and Bob sends 26 to Alice. What is their shared secret?

**Solution.** If Alice's secret is  $y$  and Bob's secret is  $x$ , then  $8^y \equiv 13$  and  $8^x \equiv 26 \pmod{29}$ .

We compute  $8^2, 8^3, \dots \pmod{29}$  until we find either 13 or 26:

$$8^2 \equiv 6, 8^3 \equiv 6 \cdot 8 \equiv -10, 8^4 \equiv -10 \cdot 8 \equiv 7, 8^5 \equiv 7 \cdot 8 \equiv -2, 8^6 \equiv -2 \cdot 8 \equiv 13 \pmod{29}.$$

Hence, Alice's secret is  $y = 6$ . The shared secret is  $(8^x)^y \equiv 26^6 \equiv 4 \pmod{29}$ .

### Problem 4

**Example 21.** 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 5

**Example 22.** 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 6

**Example 23.** 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.)

### Problem 7

**Example 24.** If Bob selects  $p = 23$  for ElGamal, how many possible choices does he have for  $g$ ?

**Solution.** Since  $g$  must be a primitive root modulo  $p$ , Bob has  $\phi(\phi(p)) = \phi(p-1)$  many choices for  $g$ .

Here, Bob has  $\phi(22) = 10$  choices.