

# Introduction to Cryptography: Homework 4

Alvin Lin

January 2018 - May 2018

## Exercise 8.5 (page 235)

Compute the two public keys and the common key for the DHKE scheme with the parameters  $p = 467$ ,  $\alpha = 2$  and

1.  $a = 3, b = 5$

$$\begin{aligned}k_{pub,a} &\equiv \alpha^a \pmod{p} \equiv 2^3 \pmod{467} \equiv 8 \\k_{pub,b} &\equiv \alpha^b \pmod{p} \equiv 2^5 \pmod{467} \equiv 32 \\k_{AB} &\equiv (k_{pub,b})^a \pmod{p} \equiv (k_{pub,a})^b \pmod{p} \\ &\equiv 8^5 \pmod{467}\end{aligned}$$

$$5 = 101_2$$

Step	Accumulated Result	Binary Exponent
1	$1^2 \times 8 \equiv 8 \pmod{467}$	1
2	$8^2 \equiv 64 \pmod{467}$	10
3	$64^2 \times 8 \equiv 78 \pmod{467}$	101

2.  $a = 400, b = 134$

$$\begin{aligned}k_{pub,a} &\equiv \alpha^a \pmod{p} \equiv 2^{400} \pmod{467} \equiv 137 \\400_2 &= 110010000\end{aligned}$$

Step	Accumulated Result	Binary Exponent
1	$1^2 \times 2 \equiv 2 \pmod{467}$	1
2	$2^2 \times 2 \equiv 8 \pmod{467}$	11
3	$8^2 \equiv 64 \pmod{467}$	110
4	$64^2 \equiv 360 \pmod{467}$	1100
5	$360^2 \times 2 \equiv 15 \pmod{467}$	11001
6	$15^2 \equiv 225 \pmod{467}$	110010
7	$225^2 \equiv 189 \pmod{467}$	1100100
8	$189^2 \equiv 229 \pmod{467}$	11001000
9	$229^2 \equiv 137 \pmod{467}$	110010000

$$\begin{aligned}k_{pub,b} &\equiv \alpha^b \pmod{p} \equiv 2^{134} \pmod{467} \equiv 84 \\134_2 &= 10000110\end{aligned}$$

Step	Accumulated Result	Binary Exponent
1	$1^2 \times 2 \equiv 2 \pmod{467}$	1
2	$2^2 \equiv 4 \pmod{467}$	10
3	$4^2 \equiv 16 \pmod{467}$	100
4	$16^2 \equiv 256 \pmod{467}$	1000
5	$256^2 \equiv 156 \pmod{467}$	10000
6	$156^2 \times 2 \equiv 104 \pmod{467}$	100001
7	$104^2 \times 2 \equiv 150 \pmod{467}$	1000011
7	$150^2 \equiv 84 \pmod{467}$	10000110

$$k_{AB} = k_{BA} \equiv (k_{pub,a})^b \pmod{p} = 84^{134} \pmod{467} = 389$$

Step	Accumulated Result	Binary Exponent
1	$1^2 \times 84 \equiv 84 \pmod{467}$	1
2	$84^2 \equiv 51 \pmod{467}$	10
3	$51^2 \equiv 266 \pmod{467}$	100
4	$266^2 \equiv 239 \pmod{467}$	1000
5	$239^2 \equiv 147 \pmod{467}$	10000
6	$147^2 \times 84 \equiv 394 \pmod{467}$	100001
7	$394^2 \times 84 \equiv 250 \pmod{467}$	1000011
7	$250^2 \equiv 389 \pmod{467}$	10000110

3.  $a = 228, b = 57$

$$k_{pub,a} \equiv \alpha^a \pmod{p} \equiv 2^{228} \pmod{467} \equiv 394$$

$$228_2 = 11100100$$

Step	Accumulated Result	Binary Exponent
1	$1^2 \times 2 \equiv 2 \pmod{467}$	1
2	$2^2 \times 2 \equiv 8 \pmod{467}$	11
3	$8^2 \times 2 \equiv 128 \pmod{467}$	111
4	$128^2 \equiv 39 \pmod{467}$	1110
5	$39^2 \equiv 120 \pmod{467}$	11100
6	$120^2 \times 2 \equiv 313 \pmod{467}$	111001
7	$313^2 \equiv 366 \pmod{467}$	1110010
8	$366^2 \equiv 394 \pmod{467}$	11100100

$$k_{pub,b} \equiv \alpha^b \pmod{p} \equiv 2^{57} \pmod{467} \equiv 313$$

Step	Accumulated Result	Binary Exponent
1	$1^2 \times 2 \equiv 2 \pmod{467}$	1
2	$2^2 \times 2 \equiv 8 \pmod{467}$	11
3	$8^2 \times 2 \equiv 128 \pmod{467}$	111
4	$128^2 \equiv 39 \pmod{467}$	1110
5	$39^2 \equiv 120 \pmod{467}$	11100
6	$120^2 \times 2 \equiv 313 \pmod{467}$	111001

$$k_{AB} = k_{BA} \equiv (k_{pub,a})^b \pmod{p} = 394^{57} \pmod{467} = 206$$

Step	Accumulated Result	Binary Exponent
1	$1^2 \times 394 \equiv 394 \pmod{467}$	1
2	$394^2 \times 394 \equiv 461 \pmod{467}$	11
3	$461^2 \times 394 \equiv 174 \pmod{467}$	111
4	$174^2 \equiv 388 \pmod{467}$	1110
5	$388^2 \equiv 170 \pmod{467}$	11100
6	$170^2 \times 394 \equiv 206 \pmod{467}$	111001

### Exercise 8.6 (page 235)

We now design another DHKE scheme with the same prime  $p = 467$  as in Problem 8.5. This time, however, we use the element  $\alpha = 4$ . The element 4 has order 233 and generates thus a subgroup with 233 elements. Compute  $k_{AB}$  for:

1.  $a = 400, b = 134$

Work is the same as above.

$$k_{pub,a} = \alpha^a \pmod{p} \equiv 4^{400} \pmod{467} = 89$$

$$k_{AB} = (k_{pub,a})^b \pmod{p} \equiv 89^{134} \pmod{467} = 161$$

2.  $a = 167, b = 134$

Work is the same as above.

$$k_{pub,a} = \alpha^a \pmod{p} \equiv 4^{167} \pmod{467} = 89$$

$$k_{AB} = (k_{pub,a})^b \pmod{p} \equiv 89^{134} \pmod{467} = 161$$

Why are the session keys identical?

Both 167 and 400 are solutions to the discrete logarithm problem  $4^x \equiv 89 \pmod{467}$ .

### Exercise 8.7 (page 235)

In the DHKE protocol, the private keys are chosen from the set

$$\{2, \dots, p - 2\}$$

Why are the values 1 and  $p - 1$  excluded? Describe the weakness of those two values.

1 is a weak value to use as a private key because the published public key will be equal to  $\alpha$ , which allows an attacker to infer the private key.  $p - 1$  is also a weak value because  $\alpha^{p-1} \pmod{p} \equiv 1$  for any  $\alpha$  since  $p$  is a prime number, which would also allow an attacker to infer the private key.

### Exercise 9.5 (page 256)

Let  $E$  be an elliptic curve defined over  $\mathbb{Z}_7$ :

$$E : y^2 = x^3 + 3x + 2$$

1. Compute all points on  $E$  over  $\mathbb{Z}_7$ .

$$P = (0, 3)$$

$$P = (0, 4)$$

$$P = (2, 3)$$

$$P = (2, 4)$$

$$P = (4, 1)$$

$$P = (4, 6)$$

$$P = (5, 3)$$

$$P = (5, 4)$$

2. What is the order of the group?

$$P = (2, 4)$$

$$2P = P + P = (4, 1)$$

$$3P = 2P + P = (5, 4)$$

$$4P = 3P + P = (0, 3)$$

$$5P = 4P + P = (0, 4)$$

$$6P = 5P + P = (5, 3)$$

$$7P = 6P + P = (4, 6)$$

$$8P = 7P + P = (2, 3)$$

$$9P = 8P + P = \text{neutral element}$$

This group has order 9.

3. Given the element  $\alpha = (0, 3)$ , determine the order of  $\alpha$ . Is  $\alpha$  a primitive element?

$$\begin{aligned}
P &= (0, 3) \\
2P &= P + P \\
s &= \frac{3(x_1)^2 + a}{2y_1} \pmod{p} \equiv \frac{3(0)^2 + 3}{6} \pmod{7} \equiv \frac{3}{6} \pmod{7} \equiv 4 \\
2P &= (s^2 - x_1 - x_2 \pmod{p}, s(x_1 - x_3) - y_1 \pmod{p}) = (2, 3) \\
3P &= 2P + P \\
s &= \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{0}{2} \pmod{7} \equiv 0 \\
3P &= (s^2 - x_1 - x_2 \pmod{p}, s(x_1 - x_3) - y_1 \pmod{p}) = (5, 4) \\
4P &= 3P + P \\
s &= \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{1}{5} \pmod{7} \equiv 3 \\
4P &= (s^2 - x_1 - x_2 \pmod{p}, s(x_1 - x_3) - y_1 \pmod{p}) = (4, 6) \\
5P &= 4P + P \\
s &= \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{3}{4} \pmod{7} \equiv 6 \\
5P &= (s^2 - x_1 - x_2 \pmod{p}, s(x_1 - x_3) - y_1 \pmod{p}) = (4, 1) \\
6P &= 5P + P \\
s &= \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{-2}{4} \pmod{7} \equiv 3 \\
6P &= (s^2 - x_1 - x_2 \pmod{p}, s(x_1 - x_3) - y_1 \pmod{p}) = (5, 3) \\
7P &= 6P + P \\
s &= \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{0}{5} \pmod{7} \equiv 0 \\
7P &= (s^2 - x_1 - x_2 \pmod{p}, s(x_1 - x_3) - y_1 \pmod{p}) = (2, 4) \\
8P &= 7P + P \\
s &= \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{1}{2} \pmod{7} \equiv 3 \\
8P &= (s^2 - x_1 - x_2 \pmod{p}, s(x_1 - x_3) - y_1 \pmod{p}) = (0, 4) \\
9P &= 8P + P \\
s &= \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{1}{0} \pmod{7} \equiv \emptyset \\
9P &= (s^2 - x_1 - x_2 \pmod{p}, s(x_1 - x_3) - y_1 \pmod{p}) = \text{neutral element}
\end{aligned}$$

$\alpha$  has order 9 and is a primitive element.

### Exercise 9.7 (page 256)

Given an elliptic curve  $E$  over  $\mathbb{Z}_{29}$  and the base point  $P = (8, 10)$ :

$$E : y^2 = x^3 + 4x + 20 \pmod{29}$$

Calculate the following point multiplication  $k \cdot P$  using the Double-and-Add algorithm. Provide the intermediate results after each step.

1.  $k = 9$

$$\begin{aligned}9P &= (1001_2)P \\P &= (1_2)P = (8, 10) \\2P &= P + P = (10_2)P = (0, 22) \\4P &= 2P + 2P = (100_2)P = (6, 17) \\8P &= 4P + 4P = (1000_2)P = (13, 6) \\9P &= 8P + P = (1001_2)P = (4, 10)\end{aligned}$$

2.  $k = 20$

$$\begin{aligned}20P &= (10100_2)P \\P &= (1_2)P = (8, 10) \\2P &= P + P = (10_2)P = (0, 22) \\4P &= 2P + 2P = (100_2)P = (6, 17) \\5P &= 4P + P = (101_2)P = (20, 3) \\10P &= 5P + 5P = (1010_2)P = (17, 19) \\20P &= 10P + 10P = (10100_2)P = (19, 3)\end{aligned}$$

### Exercise 9.9 (page 256)

Your task is to compute a session key in a DHKE protocol based on elliptic curves. Your private key is  $a = 6$ . You receive Bob's public key  $B = (5, 9)$ . The elliptic curve being used is defined by:

$$y^2 \equiv x^3 + x + 6 \pmod{11}$$

$$\begin{aligned}T_{AB} &= aB = 6B = (110)_2B \\B &= (1_2)B = (5, 9) \\2B &= B + B = (10_2)B = (10, 9) \\3B &= 2B + B = (11_2)B = (7, 2) \\6B &= 3B + 3B = (110_2)B = (2, 7)\end{aligned}$$

If you have any questions, comments, or concerns, please contact me at [alvin@omgimanagerd.tech](mailto:alvin@omgimanagerd.tech)