

# T-79.5501 Cryptology      Spring 2009

## Homework 10

Tutor : Joo Y. Cho  
joo.cho@tkk.fi

23rd April 2009

Q1. Suppose that  $(y_1, y_2)$  is an encryption of message  $m$  and  $(\hat{y}_1, \hat{y}_2)$  is an encryption of message  $\hat{m}$  using ElGamal public key encryption system with the same public key. Show how, given these two encryptions, one can compute encryptions of messages  $m\hat{m} \bmod p$  and  $m/\hat{m} \bmod p$  without knowledge of the public key.

A1.

We have two ElGamal encryptions using same public key as follows:

$$e_K(m, k) = (y_1, y_2) = (\alpha^k, m\beta^k) \pmod p$$

$$e_K(\hat{m}, \hat{k}) = (\hat{y}_1, \hat{y}_2) = (\alpha^{\hat{k}}, \hat{m}\beta^{\hat{k}}) \pmod p$$

where  $k, \hat{k}$  are one-time integers,  $\alpha$  a generator, and  $\beta \equiv \alpha^a \pmod p$ .  
Combining these with multiplication we can see

$$y_1\hat{y}_1 = \alpha^{k+\hat{k}}$$

$$y_2\hat{y}_2 = m\hat{m}\beta^{k+\hat{k}}.$$

Hence the encryption of  $m\hat{m}$  is

$$e_K(m\hat{m}, k + \hat{k}) = (\alpha^{k+\hat{k}}, m\hat{m}\beta^{k+\hat{k}}) \pmod p = (y_1\hat{y}_1, y_2\hat{y}_2).$$

Similarly, the encryption of  $m/\hat{m}$  is given by the quotients  $y_1/\hat{y}_1$  and  $y_2/\hat{y}_2$ .

Q2. Using Shanks' algorithm attempt to determine  $x$  such that

$$4815^x \equiv 48794 \pmod{50101}.$$

Hint: See Problem 4 in Homework 9.

A2.

We use Shanks' algorithm with  $\alpha = 4815$ ,  $G = \langle \alpha \rangle$  in  $\mathbf{Z}_{50101}^*$ ,  
 $\beta = 48794$ .

- 4815 is of order 25 in  $\mathbf{Z}_{50101}^*$  (Problem 4 in Homework 9).  
Hence,  $m = \lceil \sqrt{25} \rceil = 5$  and  $\alpha^m = 4815^5 \equiv 46880 \pmod{50101}$ .
- Then, the first list  $L_1$  is obtained as follows:

$$\alpha^{0 \cdot m} = 46880^0 = 1 \pmod{50101}$$

$$\alpha^{1 \cdot m} = 46880^1 = 46880 \pmod{50101}$$

$$\alpha^{2 \cdot m} = 46880^2 = 3934 \pmod{50101}$$

$$\alpha^{3 \cdot m} = 46880^3 = 4139 \pmod{50101}$$

$$\alpha^{4 \cdot m} = 46880^4 = 45248 \pmod{50101}$$

- Now we calculate  $\beta\alpha^{-i}$  for  $0 \leq i < m$  until we match a  $\alpha^{mj}$ .
- First we compute  $4815^{-1} \pmod{50101}$  using the Extended Euclidean algorithm. In result, we get  $4815^{-1} \equiv -9219 \equiv 40882 \pmod{50101}$ .
- Then, the second list  $L_2$  is obtained as

$$48794 \cdot 1 = 48794 \pmod{50101}$$

$$48794 \cdot 40882 \equiv 24993 \pmod{50101}$$

$$48794 \cdot 40882^2 \equiv 4032 \pmod{50101}$$

$$48794 \cdot 40882^3 \equiv 3934 \pmod{50101}$$

$$\vdots$$

- Since  $\beta\alpha^{-3} = \alpha^{2m}$  the solution is  $i = 3$  and  $j = 2$ . Hence,  $x = m \cdot j + i = 5 \cdot 2 + 3 = 13$ .

Q3.

Solve the congruence

$$3^x \equiv 24 \pmod{31}$$

using

- a) Shanks' algorithm; and
- b) the Pohlig-Hellman algorithm.

A3-a).

- Since 3 is primitive modulo 31, the order of 3 is 30. Hence,  $m = \lceil \sqrt{30} \rceil = 6$  and  $\alpha^m = 3^6 \bmod 31 = 16$ .
- We run the  $j$  loop and get

$$16^0 = 1 \bmod 31$$

$$16^1 = 16 \bmod 31$$

$$16^2 = 8 \bmod 31$$

$$16^3 = 4 \bmod 31$$

$$16^4 = 2 \bmod 31$$

$$16^5 = 1 \bmod 31.$$

- For the  $i$  loop, we compute first  $3^{-1} = 21 \pmod{31}$ . Then, we get

$$24 \cdot 21^0 = 24 \bmod 31$$

$$24 \cdot 21^1 = 8 \bmod 31$$

and we find  $i = 1, j = 2$  thus  $x = mj + i = 13$ .

A3-b).

We set  $n = 30 = 2 \cdot 3 \cdot 5$ ,  $\alpha = 3$  and  $\beta = 24$ . Running Pohlig-Hellman algorithm,

- (1) we set  $q = 2$  and  $c = 1$  then  $\beta^{30/2} = 24^{15} \equiv -1 \pmod{31}$ .  
Since  $\alpha^{30/2} = 3^{15} \equiv -1 \pmod{31}$ , we get  $x = 1 \pmod{2}$ ;
- (2) we set  $q = 3$  and  $c = 1$  then  $\beta^{30/3} = 24^{10} \equiv 25 \pmod{31}$ .  
Since  $\alpha^{30/3} = 3^{10} \equiv 25 \pmod{31}$ , it follows that  $x \equiv 1 \pmod{3}$ ;
- (3) we set  $q = 5$  and  $c = 1$  then  $\beta^{30/5} = 24^6 \equiv 4 \pmod{31}$ . Since  $\alpha^{30/5} = 3^6 \equiv 16 \pmod{31}$ ,  $16^2 \equiv 8 \pmod{31}$ ,  $16^3 \equiv 4 \pmod{31}$ , it follows that  $x \equiv 3 \pmod{5}$ ;

We solve three congruences from (1),(2) and (3) by CRT. Since  $15^{-1} \equiv 1 \pmod{2}$ ,  $10^{-1} \equiv 1 \pmod{3}$  and  $6^{-1} \equiv 1 \pmod{5}$ , we get  $x = 1 \cdot 15 \cdot 1 + 1 \cdot 10 \cdot 1 + 3 \cdot 6 \cdot 1 \equiv 13 \pmod{30}$ .

Q4.

Solve the congruence

$$3^x \equiv 135 \pmod{353}$$

using the Pohlig-Hellman algorithm.

A4.

- Since 3 is a primitive element modulo 353, we get  $n = 353 - 1 = 2^5 \cdot 11$ . Also,  $\alpha = 3$  and  $\beta = \beta_0 = 135$ ,
- We set  $q = 2$  and  $c = 5$ . Then  $\alpha^{352/2} = 3^{176} \equiv -1 \pmod{353}$ .  
By Algorithm 6.3 in the textbook, we get

$$\beta_0^{352/2} = 135^{176} \equiv 1 \pmod{353}, \quad a_0 = 0, \quad \beta_1 = 135$$

$$\beta_1^{352/4} = 135^{88} \equiv 1 \pmod{353}, \quad a_1 = 0, \quad \beta_2 = 135$$

$$\beta_2^{352/8} = 135^{44} \equiv 1 \pmod{353}, \quad a_2 = 0, \quad \beta_3 = 135$$

$$\beta_3^{352/16} = 135^{22} \equiv -1 \pmod{353}, \quad a_3 = 1, \quad \beta_4 = 135 \cdot 3^{-8} \equiv 16$$

$$\beta_4^{352/32} = 16^{11} \equiv -1 \pmod{353}, \quad a_4 = 1.$$

Hence, we get  $a \equiv 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 = 24 \pmod{2^5}$ .

$q = 11$  and  $c = 1$ . Then,  $\beta^{352/11} = 135^{32} \equiv 337 \pmod{353}$ . Now

$$\alpha^{0 \cdot 353/11} = 3^0 = 1 \pmod{353}$$

$$\alpha^{1 \cdot 353/11} = 3^{32} = 140$$

$$\alpha^{2 \cdot 353/11} = 3^{64} = 185$$

$$\alpha^{3 \cdot 353/11} = 3^{128} = 131$$

$$\alpha^{4 \cdot 353/11} = 3^{256} = 337$$

Hence we get  $a \equiv 4 \pmod{11}$ .

Using the Chinese Remainder Theorem that

$$a = 4 \cdot 32 \cdot (-1) + 24 \cdot 11 \cdot 3 \equiv 312 \pmod{352}.$$

We verify the result by checking that

$$3^{312} = 3^{2^8} \cdot 3^{2^5} \cdot 3^{2^4} \cdot 3^{2^3} = 256 \cdot 140 \cdot 136 \cdot 207 \equiv 135 \pmod{353}.$$

Q5. Let  $E$  be the elliptic curve  $y^2 = x^3 + 2x + 7$  defined over  $\mathbf{Z}_{31}$ .

- a) Determine the quadratic residues modulo 31.
- b) Determine the points on  $E$ .

A5.

- a) The 15 quadratic residues modulo 31 are:  $1 = 1^2$ ,  $4 = 2^2$ ,  
 $9 = 3^2$ ,  $16 = 4^2$ ,  $25 = 5^2$ ,  $5 = 6^2$ ,  $18 = 7^2$ ,  $2 = 8^2$ ,  $19 = 9^2$ ,  
 $7 = 10^2$ ,  $28 = 11^2$ ,  $20 = 12^2$ ,  $14 = 13^2$ ,  $10 = 14^2$ ,  $8 = 15^2$ .
- b) We find the points using the same procedure as in the textbook,

Table 6.1.

$x$	$x^3 + 2x + 7$ mod31	in $QR(31)$ ?	$y$	$x$	$x^3 + x + 13$ mod31	in $QR(31)$ ?	$y$
0	7	yes	$\pm 10$	16	11	no	
1	10	yes	$\pm 14$	17	25	yes	$\pm 5$
2	19	yes	$\pm 9$	18	16	yes	$\pm 4$
3	9	yes	$\pm 3$	19	15	no	
4	17	no		20	18	yes	$\pm 7$
5	18	yes	$\pm 7$	21	10	yes	$\pm 14$
6	18	yes	$\pm 7$	22	4	yes	$\pm 2$
7	23	no		23	22	no	
8	8	yes	$\pm 15$	24	22	no	
9	10	yes	$\pm 14$	25	27	no	
10	4	yes	$\pm 2$	26	27	no	
11	27	no		27	28	yes	$\pm 11$
12	23	no		28	5	yes	$\pm 6$
13	3	no		29	26	no	
14	20	yes	$\pm 12$	30	4	yes	$\pm 2$
15	2	yes	$\pm 8$				

Q6.

Let  $E$  be the elliptic curve defined in Problem 5. Then the point  $P = (2, 9) \in E$ . Compute  $3P$ ,  $8P$  and  $13P$ .

A6.

We use the addition method on Elliptic Curve in Section 6.5.2 of text book. Given  $P = (2, 9)$  and  $a = 2$ ,

- $2P = P + P = (2, 9) + (2, 9)$

$$\lambda = (3 * 2^2 + 2)(2 * 9)^{-1} = 14 \cdot 18^{-1} = 14 \cdot 19 \equiv 18 \pmod{31},$$

$$x_3 = \lambda^2 - x_1 - x_2 = 18^2 - 4 \equiv 10 \pmod{31}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 18 \cdot (2 - 10) - 9 \equiv 2 \pmod{31}$$

It follows that  $2P = (10, 2)$ .

- $3P = 2P + P = (10, 2) + (2, 9): 3P = (28, 6)$ .
- $4P = 2P + 2P = (10, 2) + (10, 2): 4P = (15, 8)$ .
- $8P = 4P + 4P = (15, 8) + (15, 8): 8P = (8, 15)$ .
- $12P = 8P + 4P = (8, 15) + (15, 8): 12P = (9, 17)$ .
- $13P = 12P + P = (9, 17) + (2, 9): 13P = (27, 20)$ .