

47

# Introduction to Cryptography: Homework #2

Due on May 31, 2019 at 3:10pm

*Professor Manuel*

**ShiHan Chan**

## Problem 1

**Part One** Since  $\gcd(17,101)=1$ , 17 and 101 are coprime integers. There exist two integers  $s, t$  satisfy the equation:  $17 * s + 101 * t = 1$ , and  $s$  is the inverse of 17 module 101. By applying extended euclidean algorithm, we can find  $s$  and  $t$ .

$$101=17*5+16$$

$$17=16*1+1$$

$$16=1*16$$

$$1=17-16*1$$

$$1=17-(101-17*5)*1$$

$$1=101*-1+17*6$$

$$s=6, t=-1$$

so the inverse of 17 module 101 is 6.

### Part Two

$$12x \equiv 28 \pmod{236}$$

$$12x - 28 = 236n \text{ (n is a integer)}$$

$$3x - 59n = 7$$

Since  $\gcd(3,59)=1$ , 3 and 59 are coprime, there exists a integer solution pair  $(s, t)$  to the equation  $3s+59t=1$ .

Applying extended euclidean algorithm:

$$59=3*19+2$$

$$3=2*1+1$$

$$2=1*2$$

$$1=3-2*1$$

$$1=3-(59-3*19)*1 \quad 1=3*20+59*(-1)$$

we can get  $s=20, t=-1$ .

$$3*20+59*(-1)=1$$

By multiplying 7 on both side, we can get:

$$3*(140)+59*(-7)=7$$

We can get one solution  $x=140$ .

$$\text{lcs}(3,59)=3*59=177$$

$$x=140+59*n=22+59*n' \text{ (n, n' } \in \mathbb{Z})$$

### Part Three

Since  $m \in [0, 30], c \in [0, 30]$ , we can build a relationship table between plaintext  $m$  and ciphertext  $c$ .

m	c	m	c	m	c	m	c
0	0	1	1	2	4	3	17
4	16	5	5	6	6	7	28
8	2	9	10	10	20	11	13
12	24	13	22	14	19	15	23
16	8	17	12	18	9	19	7
20	18	21	11	22	21	23	29
24	3	25	25	26	26	27	15
28	14	29	27	30	30	x	x

There is a bijection between plaintext  $m$  and ciphertext  $c$ , so we can decrypt the message by the table above.

### Part Four

$$\sqrt{4369} < \sqrt{4883} < 70$$

Find all prime integers smaller than 70, they are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67.

For 4369, we divide 4369 with each prime integer above. And we find  $4369=17*257$ . Since 2,3,5,7,11,13 are

$$c^{13} \equiv m \pmod{31}$$

not factor of 257, 257 is prime.  $4369=17 \cdot 257$ .

For 4883, we divide 4883 with each prime integer above. And we find  $4883=19 \cdot 257$ .  $4883=19 \cdot 257$ .

### Part Five

Try  $p=2, 3, 5, 7, 11$

When  $p=2$ ,

$$\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{2} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \pmod{2} \quad (1)$$

$$\det\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right) = 0 \quad (2)$$

when  $p=2$ , it is not invertible

When  $p=3$ ,

$$\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{3} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \pmod{3} \quad (3)$$

$$\det\left(\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}\right) = -2 \quad (4)$$

when  $p=3$ , it is invertible

When  $p=5$ ,

$$\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{5} = \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix} \pmod{5} \quad (5)$$

$$\det\left(\begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix}\right) = 9 \quad (6)$$

when  $p=5$ , it is invertible

When  $p=7$ ,

$$\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{7} = \begin{pmatrix} 3 & 5 \\ 0 & 3 \end{pmatrix} \pmod{7} \quad (7)$$

$$\det\left(\begin{pmatrix} 3 & 5 \\ 0 & 3 \end{pmatrix}\right) = 9 \quad (8)$$

when  $p=7$ , it is invertible

when  $p > 7 (p \in \mathbb{Z})$ ,

$$\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{p} = \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \pmod{p} \quad (9)$$

$$\det\left(\begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix}\right) = -26 \quad (10)$$

when  $p > 7 (p \in \mathbb{Z})$ , it is invertible.

Overall, it is not invertible only when  $p=2$ . Otherwise, it is invertible.

**Part Six**

Show that either  $a$  or  $b$  is congruent to  $0 \pmod{p}$  means that we only need to prove either  $p|a$  or  $p|b$ .

From assignment 1 ex1.3, we show that if  $a, b, n$  are three integers,  $n|ab$ ,  $\gcd(a, n) = 1$ , then  $n|b$ .

Let  $n=p$ ,  $p|ab$ , since  $p$  is prime,  $\gcd(p, a)=1$  or  $\gcd(p, a)=p$ . If  $\gcd(p, a)=1$ , then  $p|b$  according to above theorem, and  $b \equiv 0 \pmod{p}$ . If  $\gcd(p, a)=p$ , then  $p|a$ , and  $a \equiv 0 \pmod{p}$ .

**Part Seven**

$$2^{2017} \equiv 2^{2017} \pmod{5} \equiv 2 * 4^{1008} \pmod{5} \equiv 2 * (-1)^{1008} \pmod{5} \equiv 2 \pmod{5}$$

$$2^{2017} \equiv 2^{2017} \pmod{13} \equiv 2 * 64^{336} \pmod{13} \equiv 2 * (-1)^{336} \pmod{13} \equiv 2 \pmod{13}$$

$$2^{2017} \equiv 2^{2017} \pmod{31} \equiv 4 * 32^{403} \pmod{31} \equiv 4 * (1)^{334} \pmod{31} \equiv 4 \pmod{31}$$

Since  $5*13*31=2015$ , we apply chinese remainder theorem to solve  $2^{2017} \pmod{2015}$

$M=2015$

$$M_1 = \frac{M}{m_1} = \frac{2015}{5} = 403$$

$$M_2 = \frac{M}{m_2} = \frac{2015}{13} = 155$$

$$M_3 = \frac{M}{m_3} = \frac{2015}{31} = 65$$

$$403 * t_1 \equiv 1 \pmod{5} \quad t_1 = 2 + 5 * n \quad \forall n \in \mathbb{Z}$$

$$155 * t_2 \equiv 1 \pmod{13} \quad t_2 = -1 + 13 * n \quad \forall n \in \mathbb{Z}$$

$$65 * t_3 \equiv 1 \pmod{31} \quad t_3 = -10 + 31 * n \quad \forall n \in \mathbb{Z}$$

(Solve  $t_1, t_2, t_3$  by extended euclidean algorithm.)

We calculate  $x = (\sum_1^3 a_i t_i M_i) + M * k (k \in \mathbb{Z}) = 2 * 2 * 403 + 2 * (-1) * 155 + 4 * (-10) * 65 + 2015 * k = -1298 + 2015 * k = 717 + 2015 * k$

$$2^{2017} \equiv 717 \pmod{2015}$$

$$2^{2017} \pmod{2015} = 717$$

## Problem 2

1.

Rabin cryptosystem is an asymmetric cryptosystem. It contains public key and private key: public key is used to encrypt the plaintext and it is known by everybody. While the private key is used to decrypt the ciphertext and it is only known by text recipient and owner of plaintext.

Choose two random large prime numbers  $p, q$  as the private keys, and  $n=p*q$  is the public key. For encryption, if the plaintext  $m \in [0, n-1]$ , the ciphertext  $c$  could be generated by

$$c \equiv m^2 \pmod{n}$$

Proposition:

Suppose  $p$  is a prime that  $p \equiv 3 \pmod{4}$ . If  $y$  has a square root  $(r) \pmod{p}$  ( $y \equiv r^2 \pmod{p}$ ), let  $x \equiv y^{(p+1)/4} \pmod{p}$ , then  $r \equiv \pm x \pmod{p}$ .

If  $y$  has not a square root  $(r) \pmod{p}$  ( $-y \equiv r^2 \pmod{p}$ ), let  $x \equiv y^{(p+1)/4} \pmod{p}$ , then  $r \equiv \pm x \pmod{p}$ .

For decryption, the private key is necessary to help us decrypt efficiently by applying proposition above.

$c \equiv m^2 \pmod{n}$ , we can find corresponding plaintext  $m$  efficiently only if we know  $p$  and  $q$ .

Since  $n=p*q$ , we know that  $c \equiv m^2 \pmod{p}$

$$c \equiv m^2 \pmod{q}$$

Because of the process of encryption,  $c$  has a square root mod  $n$ , and  $c$  has a square root mod  $p$  or  $q$ .

By applying the proposition, we can get:

$$m \equiv \pm c^{(p+1)/4} \pmod{p} \text{ and } m \equiv \pm c^{(q+1)/4} \pmod{q}$$

Now we can apply Chinese remainder theorem to solve four simultaneous equations.

$$m \equiv c^{(p+1)/4} \pmod{p} \text{ and } m \equiv c^{(q+1)/4} \pmod{q}$$

$$m \equiv c^{(p+1)/4} \pmod{p} \text{ and } m \equiv -c^{(q+1)/4} \pmod{q}$$

$$m \equiv -c^{(p+1)/4} \pmod{p} \text{ and } m \equiv c^{(q+1)/4} \pmod{q}$$

$$m \equiv -c^{(p+1)/4} \pmod{p} \text{ and } m \equiv -c^{(q+1)/4} \pmod{q}$$

$M = n = p * q$ ,  $M1 = \frac{M}{p}$ ,  $M2 = \frac{M}{q}$ , and use extended euclidean theorem to find  $t1, t2$  such that  $M1 * t1 \equiv 1 \pmod{m1}$  and  $M2 * t2 \equiv 1 \pmod{m2}$ , and finally we can get four  $m \equiv M1 * a1 * t1 + M2 * a2 * t2 \pmod{n}$  ( $m \equiv a \pmod{M}$ ). However, only one of them is correct(meaningful) plaintext.

2.

a. Through the decryption method above, it would generate four answers, and only one of them is correct(meaningful) answer. Meaningful message can be expected fairly soon since there is at least 25 percent chance to get the correct answer if we choose one at random.

b. No. If Eve only has ciphertext  $x$  and public key  $n$  without private keys  $p$  and  $q$ , she needs to solve  $x \equiv m^2 \pmod{n}$  ( $m$  is the plaintext). There is no known method to solve this without private keys. Although she can factorize  $n$  to any two prime numbers and try to use method above, since  $p$  and  $q$  are all big prime numbers, the factorization problem is also hard. So it is hard for Eve to determine the original message.

c. Eve can try to use CCA to break the system.

If Eve use a ciphertext  $c$  to compute the output of the system (possible  $x$ ) for many times, she would get all four possible outputs  $\pm r1, \pm r2$ . Randomly choose  $\pm r1$  to minus  $\pm r2$

If we pick  $+r1$  and  $+r2$  or  $-r1$  and  $-r2$ , then  $|r1 - r2| = q$ , if we pick  $+r1$  and  $-r2$  or  $-r1$  and  $+r2$ , then  $|r1 - r2| = p$ . So we can calculate  $\gcd(|r1 - r2|, n)$  to get one non-trivial factor, and get another non-trivial factor. Then we finish factorization.

### Problem 3

Let  $n$  be numbers of people in the group, we know that  $n$  satisfies three equations below at the same time:

$$n \equiv 1 \pmod{3}$$

$$n \equiv 2 \pmod{4}$$

$$n \equiv 3 \pmod{5}$$

we can solve  $n$  by applying Chinese Remainder theorem:

$$M = 3 \cdot 4 \cdot 5 = 60$$

$$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$$

$$M_2 = \frac{M}{m_2} = \frac{60}{4} = 15$$

$$M_3 = \frac{M}{m_3} = \frac{60}{5} = 12$$

$$20 * t_1 \equiv 1 \pmod{3} \quad t_1 = -1 + 3 * n \quad \forall n \in \mathbb{Z}$$

$$15 * t_2 \equiv 1 \pmod{4} \quad t_2 = -1 + 4 * n \quad \forall n \in \mathbb{Z}$$

$$12 * t_3 \equiv 1 \pmod{5} \quad t_3 = 3 + 5 * n \quad \forall n \in \mathbb{Z}$$

(Solve  $t_1, t_2, t_3$  by extended euclidean algorithm.)

$$\text{We calculate } n = \left( \sum_{i=1}^3 a_i t_i M_i \right) + M * k \quad (k \in \mathbb{Z}) = 1 * (-1) * 20 + 2 * (-1) * 15 + 3 * (3) * 12 + 60 * k = 58 + 60 * k$$

$$n \equiv 58 \pmod{60}$$

We choose  $n$  as two smallest positive integer: 58, 118.

Two smallest possible numbers of people in group are 58 and 118.