VE475 Intro to Cryptography Homework 2

Taoyue Xia, 518370910087

2020/05/25

1 Ex1

1. To find the inverse of of 17 modulo 101, we just need to find the solution to the equation: $17x + 101y = 1$
   Firstly, construct a matrix to show the equation set when $x = 0$, $y = 0$ and $x = 0$, $y = 1$

$$\begin{pmatrix} 0 & 1 & 101 \\ 1 & 0 & 17 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 17 \\ -5 & 1 & 16 \end{pmatrix} \Rightarrow \begin{pmatrix} -5 & 1 & 16 \\ 6 & -1 & 1 \end{pmatrix}$$

   From above, we can have $\begin{cases} x = 6 \\ y = -1 \end{cases}$ that satisfies $17x + 101y = 1$, so the inverse of 17 modulo 101 is 6.

2. For 12, 28 and 136, all of them can be divided by 4, so the original equation is congruent with:

$$3x = 7 \ mod \ 59$$

   Note that 20 is the inverse of 3 *mod* 59, so we multiply 20 to both sides of the equation:

$$x = 7 \times 20 = 140 = 22 \ mod \ 59$$

   So we get the solution that $x = 59t + 22$, where $t \in \mathbb{Z}$

3. For m from 0 to 30, use the table below to demonstrate:

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

   We can obviously find that there is a bijection between the plaintext and ciphertext, so we just need to refer to the table above to decrypt the message.

4. Firstly, we calculate the square root of 4883 and 4369, which is about 70. Then if the two numbers can be divided by some number, it must be the prime number in range $[2, 70)$.
   According to the program "ex1_4.cpp", we can see that:

$$4883 = 19 \times 257 \qquad and \qquad 4369 = 17 \times 257$$

5. Firstly, we are going to calculate the determinant of matrix A.

$$det(A) = det \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} = -26$$

   We know that if the matrix is invertible modulo p, then its determinant should be coprime with p. For the prime numbers 2, 3, 5, 7, 11, 13, 17, 19, 23, we have $26 = -(2 \times 13)$, which means that -26 is not coprime with 2 and 13, for the others, $gcd(-26, p) = 1$.
   So p is 2 and 13.

6. As is proved in Homework 1 Ex1.3 that given $n|ab$ and $gcd(a, n) = 1$, we know that $n \mid b$. Let $n = p$ here, as p is a prime number, we know that $gcd(a, p) = 1$ or $gcd(a, p) = p$. If $gcd(a, p) = 1$, we can get $p \mid b$ which means $b \equiv 0 \ mod \ p$. If $gcd(a, p) = p$, it obviously show that $a \equiv 0 \ mod \ p$. Proof done.

7. First, calculate 2^{2017} modulo 5:

$$2^{2017} \equiv 2 \times 4^{1008} \ mod \ 5$$

It is common sense that $4 \equiv -1 \ mod \ 5$, so

$$2^{2017} \equiv 2 \times (-1)^{1008} \ mod \ 5 \equiv 2 \ mod \ 5$$

Next, use the same method to calculate modulo to 13 and 31:

$$2^{2017} \equiv 2 \times 64^{336} \ mod \ 13$$
$$2^{2017} \equiv 2 \times (-1)168 \ mod \ 13$$
$$2^{2017} \equiv 2 \ mod \ 13$$

$$2^{2017} \equiv 4 \times 32^{403} \ mod \ 31$$
$$2^{2017} \equiv 4 \times 1^{403} \ mod \ 31$$
$$2^{2017} \equiv 4 \ mod \ 31$$

Find that $2015 = 5 \times 13 \times 31$, so use the Chinese Remainder Theorem to calculate the answer:

$$5 \times 13 \equiv 65 \equiv 3 \ mod \ 31$$
$$65 \times 21 \equiv 1365 \equiv 1 \ mod \ 31$$

$$5 \times 31 \equiv 155 \equiv -1 \ mod \ 13$$
$$155 \times 12 \equiv 1860 \equiv 1 \ mod \ 13$$

$$13 \times 31 \equiv 403 \equiv 3 \ mod \ 5$$
$$403 \times 2 \equiv 806 \equiv 1 \ mod \ 5$$

Then we can have the result:

$$2^{2017} \equiv 1365 \times 4 + 1860 \times 2 + 806 \times 2 \ mod \ 2015$$
$$2^{2017} \equiv 10792 \equiv 717 \ mod \ 2015$$

So we have the conclusion that $2^{2017} \equiv 717 \ mod \ 2015$.

2 Ex2

1. The Rabin cryptosystem is an asymmetric cryptographic technique, which uses a key pair: a public key for encryption and a private key for decryption. Furthermore, The private key should only be possessed by the receiver.

   For generation of the key, we first choose two distinct prime numbers p and q, which is large and should satisfy:

   $$p \equiv 3 \ mod \ 4 \qquad and \qquad q \equiv 3 \ mod \ 4$$

   Then compute $n = pq$.

   Thus n is the public key, and the pair $(p,\ q)$ is the private key.

   For the encryption, we first convert the message to a number m, which satisfies $m < n$. Then compute $c = m^2 \ mod \ n$ to get the ciphertext.

   For the decryption, if we only have the public key n, we can only compute like:

   $$m^2 \equiv c \ mod \ n$$
   $$m \equiv \sqrt{c} \ mod \ n$$

   so that we will never get a specific plaintext message as there exists infinite examples of m.

   However, if we have the private key p and q, the decryption would be possible. Firstly, we need to calculate the square root of c modulo p and q.

   Since $p \equiv 3 \ mod \ 4$, then $\frac{1}{4}(p+1)$ is an integer, as $m^2 \equiv c \ mod \ pq$, then we can tell $m^2 \equiv c \ mod \ p$, so c is a quadratic residue modulo p. From the Euler's criterion, we have:

   $$x^{\frac{k-1}{2}} \equiv 1 \ mod \ p \qquad if \ there \ exists \ an \ integer \ a \ that \ x \equiv a^2 \ mod \ k$$

   where k here is an odd prime number and x is an integer coprime to k. Then we can apply the criterion to the equation below:

$$c^{\frac{1}{2}(p+1)} \equiv c \cdot c^{\frac{1}{2}(p-1)} \equiv c \cdot 1 \ mod \ p$$

Then we can assign $m_p^2 \equiv c^{\frac{1}{2}(p+1)} \equiv c \ mod \ p$. Finally we get:

$$m_p = c^{\frac{1}{4}(p+1)} \ mod \ p$$
$$m_q = c^{\frac{1}{4}(q+1)} \ mod \ q$$

After we get m_p and m_q, we can apply the Extended Euclidean Algorithm to find y_p and y_q such that:

$$y_p \cdot p + y_q \cdot q = 1$$

Finally, we can use the Chinese Remainder Theorem to calculate the four square roots of c modulo n:

$$r_1 = y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p \ mod \ n$$
$$r_2 = n - r_1$$
$$r_3 = y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p \ mod \ n$$
$$r_4 = n - r_3$$

Then we can know that one of the four square roots stands for the plaintext m.

2. a) As is shown above, we can get four possible answers of $\sqrt{x} \ mod \ n$, which means that each time we have a 25% chance to get the right plaintext, so we can expect a meaningful message fairly soon.

   b) No, Eve cannot easily determine the original message. If she only knows the ciphertext x and the public key n, she will just be able to use the equation $m = \sqrt{c} \ mod \ n$. However, it is comparatively impossible to solve the equation without the private key pair. Also, as p and q are two quite large prime numbers, it is very hard to factorize n into $p \cdot q$, thus it is not easy to determine the original message.

c) Eve can run the chosen ciphertext attack to recover the factorization of n.

Firstly, she randomly choose an m and compute $c \equiv m^2 \ mod \ n$, then it will given her the decryption d, which is one of the four square roots of c. As it is a probability of $\frac{1}{2}$ that $d \neq \pm m$, we can calculate:

$$gcd(m - d, n) = p \ or \ q$$

Then after a large number of attacks, she will finally get the factorial p and q.

3 Ex3

From the question, suppose that there are at least x people in the parade, we can generate the equations below:

$$x \equiv 1 \ mod \ 3$$
$$x \equiv 2 \ mod \ 4$$
$$x \equiv 3 \ mod \ 5$$

Then we can apply the Chinese Remainder Theorem:

$$3 \times 4 \equiv 12 \equiv 2 \ mod \ 5$$
$$12 \times 3 \equiv 36 \equiv 1 \ mod \ 5$$

$$3 \times 5 \equiv 15 \equiv 3 \ mod \ 4$$
$$15 \times 3 \equiv 45 \equiv 1 \ mod \ 4$$

$$4 \times 5 \equiv 20 \equiv 2 \ mod \ 3$$
$$20 \times 2 \equiv 40 \equiv 1 \ mod \ 3$$

Then we can calculate x as:

$$x \equiv 36 \times 3 + 45 \times 2 + 40 \times 1 \; mod \; 60$$
$$x \equiv 238 \equiv 58 \; mod \; 60$$

Thus, the two smallest possible numbers of people are 58 and 118.