VE475 Homework 2

Liu Yihao 515370910207

Ex. 1 — Simple questions

1.

	q_i	r_i	s_i	t_i
0		17	1	0
1		101	0	1
2	$17 \div 101 = 0$	$17 - 0 \times 101 = 17$	$1 - 0 \times 0 = 1$	$0 - 0 \times 1 = 0$
3	$101 \div 17 = 5$	$101 - 5 \times 17 = 16$	$0 - 5 \times 1 = -5$	$1 - 5 \times 0 = 1$
4	$17 \div 16 = 1$	$17 - 1 \times 16 = 1$	$1 - 1 \times -5 = 6$	$0 - 1 \times 1 = -1$

$$17 \cdot 6 \equiv 1 \bmod 101$$

So the inverse of 17 modulo 101 is 6.

2.

$$12x \equiv 28 \bmod 236$$

$$3x \equiv 7 \bmod 59$$

$$3x = 59k + 7 \quad k \in Z$$

First, we can find the solutions in $[0, 58]$, try $k = 0, 1, 2$
When $k = 0$, $x = \frac{7}{3}$. When $k = 1$, $x = 22$. When $k = 1$, $x = \frac{125}{3}$.
So $x = 59k + 22$, $k \in Z$.

3. Suppose $m \in [0, 30]$ and $c \in [0, 30]$, we know

$$c \equiv m^7 \bmod 31$$

Then we can generate a table from m to 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		

Obviously there is a bijection between the plaintext m and the ciphertext c, and we can simply decrypt the message according to the table above.

4.

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

Consider all of the primes in $[2, 70]$, they are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67.
For 4883, first, try to divide 4883 by them one by one, we can find that $4883 = 19 \times 257$. Then, try to divide 257 by 2, 3, 5, 7, 11, 13, all of them have a reminder, so 257 is a prime, $4883 = 19 \times 257$.
For 4369, it's interesting because $4883 = 4369 + 2 \times 257$, so $4369 = 17 \times 257$, where 17 and 257 are primes.

5.

$$A = \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \bmod p$$

When $p = 2$,

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \bmod 2$$

$$\det \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = 0$$

It is not invertible.

When $p = 3$,

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \bmod 3$$

$$\det \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = -2$$

It is invertible.

When $p = 5$,

$$A = \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix} \bmod 5$$

$$\det \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix} = 9$$

It is invertible.

When $p = 7$,

$$A = \begin{pmatrix} 3 & 5 \\ 0 & 3 \end{pmatrix} \bmod 7$$

$$\det \begin{pmatrix} 3 & 5 \\ 0 & 3 \end{pmatrix} = 9$$

It is invertible.

When $p > 7$,

$$A = \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix} \bmod 7$$

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

It is invertible.

So when $p = 2$, it is not invertible.

6.

$$\begin{aligned} 2^{2017} &\equiv 2 \cdot 4^{1008} \bmod 5 \\ &\equiv 2 \cdot (-1)^{1008} \bmod 5 \\ &\equiv 2 \bmod 5 \\ 2^{2017} &\equiv 2 \cdot 64^{336} \bmod 13 \\ &\equiv 2 \cdot (-1)^{336} \bmod 13 \\ &\equiv 2 \bmod 13 \\ 2^{2017} &\equiv 4 \cdot 32^{403} \bmod 31 \\ &\equiv 4 \cdot 1^{403} \bmod 31 \\ &\equiv 4 \bmod 31 \end{aligned}$$

Then we can apply the Chinese remainder theorem to solve 2^{2017} modulo 2015.

$$\begin{aligned} 5 \cdot 13 &\equiv 3 \bmod 31 \\ 65 \cdot -10 &\equiv 1 \bmod 31 \\ 13 \cdot 31 &\equiv 3 \bmod 5 \\ 403 \cdot 2 &\equiv 1 \bmod 5 \\ 5 \cdot 31 &\equiv -1 \bmod 13 \\ 155 \cdot -1 &\equiv 1 \bmod 13 \end{aligned}$$

$$\begin{aligned} 2^{2017} &\equiv 65 \cdot -10 \cdot 4 + 403 \cdot 2 \cdot 2 + 155 \cdot -1 \cdot 2 \bmod 2015 \\ &\equiv -1298 \bmod 2015 \\ &\equiv 717 \bmod 2015 \end{aligned}$$

7. According to Assignment 1/Ex. 1/3, let a, b and n be three positive integers such that $n \mid ab$ and $\gcd(a, n) = 1$, we can prove that $n \mid b$.
Now let $n = p$, since p is a prime, we know $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. If $\gcd(a, p) = 1$, according to the conclusion above, $p \mid b$, so $b \equiv 0 \bmod p$. If $\gcd(a, p) = p$, we can simply get $a \equiv 0 \bmod p$, so it is proved.

Ex. 2 — Rabin cryptosystem

1. Rabin cryptosystem is an asymmetric cryptosystem, which uses both a public key and a private key. The public key is necessary for later encryption and can be published, while the private key must be possessed only by the recipient of the message.

The keys can be generated by this method: choose two large distinct primes p and q as the private keys, and $n = p \cdot q$ as the public key.

For the encryption, suppose the plaintext $m \in [0, n-1]$, the ciphertext c is determined by

$$c = m^2 \bmod n$$

For the decryption, the private keys are necessary. We can find the plaintext m by

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

There is no efficient method known for the finding of m if we don't have the private keys. However, if we know p and q, the Chinese remainder theorem can be applied to solve for m.

$$m_p = \sqrt{c} \bmod p$$
$$m_q = \sqrt{c} \bmod q$$

By applying the the extended Euclidean algorithm, we can find y_p and y_q such that

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

Now, by invocation of the Chinese remainder theorem, the four square roots $+r$, $-r$, $+s$, $-s$ can be found by the following formulas. They are all possible values of m.

$$+r = (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \bmod n \quad -r = n - r$$
$$+s = (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \bmod n \quad -s = n - s$$

2. a) As is mentioned above, the calculation of $m \equiv \sqrt{x} \bmod n$ will give at most four different answers, and one of them is the plaintext, which is meaningful. If we choose one at random, we will have at least 25% chance to get a meaningful message, which can be expected fairly soon.

   b) No. If Eve only have the ciphertext x and the public key n, she will have two choices: directly solve $m \equiv \sqrt{x} \bmod n$ or factorize n into private keys p and q and use the decryption method above. However there is no efficient method known for solving $m \equiv \sqrt{x} \bmod n$ if we don't have the private keys. And the integer factorization problem of the product of two big primes is also very difficult. So Eve can't easily determine the original message.

   c) Eve can try to break the system with a chosen ciphertext attack.
   Suppose that she uses a certain x to compute the result with the device for many many times, such that she'll get all of the four different results (if failed, she can change the ciphertext x and retry). According to the explanation above, they are four square roots $+r$, $-r$, $+s$, $-s$, and $(+r) + (-r) = n$, $(+s) + (-s) = n$. So Eve can sort these four roots to two sets, r and s, with the public key n. Then, she can randomly choose one root from each of two sets.
   If she chooses $+r$ and $+s$, or $-r$ and $-s$

$$|r - s| = |2y_q \cdot m_p| q \bmod n = |2y_q \cdot m_p| q - kpq = (|2y_q \cdot m_p| - kp)q, k \in Z$$
$$\gcd(|r - s|, n) = \gcd((|2y_q \cdot m_p| - kp)q, pq) = q$$

   If she chooses $+r$ and $-s$, or $-r$ and $+s$

$$|r - s| = |2y_p \cdot m_q| p \bmod n = |2y_p \cdot m_q| p - kpq = (|2y_p \cdot m_q| - kq)p, k \in Z$$
$$\gcd(|r - s|, n) = \gcd((|2y_p \cdot m_q| - kq)p, pq) = p$$

   Since calculating $\gcd(|r - s|, n)$ is efficient, Eve will simply find either of p and q, then the factorization of n is successfully recovered.

Ex. 3 — CRT

According to the problem, suppose there are at least n people in the group, we know

$$\begin{aligned} n &\equiv 1 \bmod 3 \\ n &\equiv 2 \bmod 4 \\ n &\equiv 3 \bmod 5 \end{aligned}$$

Then, we should calculate these

$$\begin{aligned} 3 \cdot 4 &\equiv 2 \bmod 5 \\ 12 \cdot 3 &\equiv 1 \bmod 5 \\ 4 \cdot 5 &\equiv 2 \bmod 3 \\ 20 \cdot 2 &\equiv 1 \bmod 3 \\ 3 \cdot 5 &\equiv 3 \bmod 4 \\ 15 \cdot 3 &\equiv 1 \bmod 4 \end{aligned}$$

Applying the Chinese remainder theorem, we know

$$\begin{aligned} n &\equiv 12 \cdot 3 \cdot 3 + 20 \cdot 2 \cdot 1 + 15 \cdot 3 \cdot 2 \bmod 3 \cdot 4 \cdot 5 \\ &\equiv 238 \bmod 60 \\ &\equiv 58 \bmod 60 \end{aligned}$$

So the two smallest possible number of people in the group is 58 and 118.