VE475 Introduction to Cryptography
Homework 2

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

May 28, 2019

Ex. 1 - Simple questions

1. The inverse of 17 modulo 101 can be found by the extended Euclidean algorithm. Initially, $s_0 = 0$, $s_1 = 1$, $t_0 = 1$, and $t_1 = 0$.

$$\begin{array}{lllll} 101 = 5 \times 17 + 16 & s_0 = 1 & s_1 = 0 & t_0 = 0 & t_1 = 1 \\ 17 = 1 \times 16 + 1 & s_0 = -5 & s_1 = 1 & t_0 = 1 & t_1 = 0 \\ 16 = 16 \times 1 + 0 & s_0 = 6 & s_1 = -5 & t_0 = -1 & t_1 = 1 \\ 1 = 0 + 1 & s_0 = -101 & s_1 = 6 & t_0 = 17 & t_1 = -1 \end{array}$$

   So, we can see that $\gcd(17, 101) = 1$ and the multiplicative inverse of 17 modulo 101 is $s_1 = 6$.

2. Simplify the condition given, we would have

$$12x \equiv 28 \mod 236$$
$$3x \equiv 7 \mod 59$$

   So, we would have

$$3x = \begin{cases} 59 \cdot (3k + 0) + 7 \\ 59 \cdot (3k + 1) + 7 \\ 59 \cdot (3k + 2) + 7 \end{cases}, \quad \text{where } k \in Z$$
$$x = \begin{cases} 59k + 2 + \frac{1}{3} \\ 59k + 22 \\ 59k + 41 + \frac{2}{3} \end{cases}$$

   Since $x \in Z$, $x = 59k + 22$, where $k \in Z$.

3.
   - If $c \equiv 0 \equiv m^7 \mod 31$, we would also have $m \equiv 0 \mod 31$.
   - Otherwise, since 31 is a prime and in this case $m \nmid 31$, we would have $\gcd(m, 31) = 1$. So, according to Fermat's Little Theorem, we would obtain

$$m^{30} \equiv 1 \mod 31$$
$$m^{31} \equiv m \mod 31$$

Since $\gcd(7,30) = 1$, we can find the multiplicative inverse of 7 modulo 30, which is 13. We would have $7 \times 13 + 30 \times (-3) = 1$. Then, following relation would be obtained

$$\begin{aligned} c^{13} &\equiv (m^7)^{13} \mod 31 \\ &\equiv (m^{30})^3 \cdot m \mod 31 \\ &\equiv m \mod 31 \end{aligned}$$

In conclusion, to decrypt the message, we need to calculate c^{13} modulo 31. The result would gives m.

4. Since $4883 < 70^2$and $4369 < 67^2$, the smallest prime factor should be found from: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, and 67. So, we would have $4883 = 19 \times 257$. Since 19 is the smallest factor of 4883 and $257 < 17^2$, we can conclude that 257 is also a prime. Similarly, we would also have $4369 = 17 \times 257$, where 257 is also a prime. In conclusion, we have

$$\begin{aligned} 4883 &= 19 \times 257 \\ 4369 &= 17 \times 257 \end{aligned}$$

5. Assume the matrix A such that

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

is not invertible.

Since $\det(A) = -26$, we need to find prime p such that $\gcd(-26, p) \neq 1$. Or in another word, we need to find primes which are not coprime of -26. And since $|-26| = 2 \times 13$, we would have $p = 2$ or $p = 13$.

6. Since $ab \equiv 0 \mod p$, we have $ab = kp$, where $k \in Z$. Since p is a prime, we can assume that $\gcd(a,p) = 1$ or $\gcd(a,p) = p$. And when $\gcd(a,p) = p$, a is congruent to $0 \mod p$.

If $\gcd(a,p) = 1$, since $p|ab$, we would have $p|b$, which means b is congruent to $0 \mod p$.

So, in conclusion, either a or b is congruent to $0 \mod p$.

7.

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

Since $2015 = 5 \times 13 \times 31$, we could apply Chinese remainder theorem to find $2^{2017} \mod 2015$.

- Step 1: Since $\gcd(13,31) = 1$ and $13 \times 31 = 403$, we need to find the multiplicative inverse of 403 modulo 5 which is 2. With similar procedure, we would obtain

$$\begin{aligned} \text{Common\_multiple}(13,31) &\equiv 806 \equiv 1 \mod 5 \\ \text{Common\_multiple}(31,5) &\equiv -155 \equiv 1 \mod 13 \\ \text{Common\_multiple}(5,13) &\equiv -650 \equiv 1 \mod 31 \end{aligned}$$

- Step 2:

$$\begin{aligned} 806 \times 2 &= 1612 \\ -155 \times 2 &= -310 \\ -650 \times 4 &= -2600 \\ 1612 - 310 - 2600 &= -1298 \end{aligned}$$

- Step 3:

$$\begin{aligned} 2^{2017} &\equiv -1298 \mod 2015 \\ &\equiv 717 \mod 2015 \end{aligned}$$

Ex. 2 - Rabin cryptosystem

1. The Rabin cryptosystem uses a private key and a public key at the same time. The system works as followed.

   First, choose two large different primes p and q. The primes p and q are the private key and let $n = pq$ be the public key. The public key is used in the encryption while the private key is required in the decryption.

   Then in the encryption part, let $m \in \{0, \cdots, n-1\}$ be the plaintext. And the ciphertext c is determined by

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

   And for most of the ciphertexts, there are exactly four possible plaintexts could lead to the same ciphertext.

   To efficiently decrypt the ciphertext, the private key is necessary. We can use the Chinese remainder theorem to solve for m. We have to calculate the square roots

$$\begin{aligned} m_p &= \sqrt{c} \mod p \\ m_q &= \sqrt{c} \mod q \end{aligned}$$

   By applying the extended Euclidean algorithm, we can find y_p and y_q such that $y_p \cdot p + y_q \cdot q = 1$.

Ex. 3 - CRT

Assume there are at least x people in the group, we then have

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 4 \\ x &\equiv 3 \mod 5 \end{aligned}$$

To solve x, we need to apply the Chinese remainder theorem

- Step 1:

$$\begin{aligned} \text{Common\_multiple}(4,5) &\equiv 40 \equiv 1 \mod 3 \\ \text{Common\_multiple}(5,3) &\equiv 45 \equiv 1 \mod 4 \\ \text{Common\_multiple}(3,4) &\equiv 36 \equiv 1 \mod 5 \end{aligned}$$

- Step 2:

$$\begin{aligned} 40 \times 1 &= 40 \\ 45 \times 2 &= 90 \\ 36 \times 3 &= 108 \\ 40 + 90 + 108 &= 238 \end{aligned}$$

- Step 3:

$$\begin{aligned} x &\equiv 238 \mod \text{Lowest\_common\_multiple}(3, 4, 5) \\ &\equiv 58 \mod 60 \\ &\equiv 118 \mod 60 \end{aligned}$$

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