VE475 Homework 2

Yiwen Yang 519370910053

Ex.1 - Simple Questions

1.

$$\begin{aligned}
101 &= 5 \times 17 + 16 \\
17 &= 1 \times 16 + 1 \\
16 &= 16 \times 1 \\
1 &= 17 - 1 \times 16 \\
&= 6 \times 17 - 101
\end{aligned}$$

   So the inverse of 17 modulo 101 is 6.

2. To solve $12x \equiv 28 \bmod 236$, is equivalent to solve $12x + 236y = 28 \Leftrightarrow 3x + 59y = 7$.

$$\begin{aligned}
59 &= 19 \times 3 + 2 \\
3 &= 1 \times 2 + 1 \\
2 &= 2 \times 1 \\
1 &= 3 - 1 \times 2 \\
&= 20 \times 3 - 59 \\
7 &= 140 \times 3 + (-7) \times 59
\end{aligned}$$

   So $x = 140 + 59t$, $t \in \mathbb{Z}$.

3. From Euclidean algorithm, one can infer that

$$\begin{cases} gcd(c, 31) = 1 \\ gcd(7, \phi(31)) = gcd(7, 30) = 1 \end{cases}$$

   Using extended Euclidean algorithm to find p such that $7p \equiv 1 \bmod 30$, one can get $p = 13 + 30t$, $t \in \mathbb{Z}$. Assume $t = 0$, then the plain text $m \equiv c^p \equiv c^{13} \bmod 31$.

4.

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

5. Let $M = \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix}$.

   M is not invertible modulo p implies that $det(M \bmod p) = 0$.

   When $p > 7$, $det(M \bmod p) = det(M) = -26$, M is invertible.

   Try all $p \leq 7$: $p = 2, 3, 5, 7$, one can get that $det(M \bmod 2) = 0$. So when $p = 2$, M is not invertible.

6. Suppose a and p are coprime, *i.e.*, $gcd(a,p) = 1$. Then according to Bézout's identity, $\exists r, s \in \mathbb{Z}$ such that $ra + sp = 1$. Multiply both sides by b, one can get $rab + spb = b$. Since $p \mid rab, p \mid spb$, then $p \mid b$, *i.e.*, $b \equiv 0 \bmod p$.

   Similarly, if b and p are coprime, then $a \equiv 0 \bmod p$. So at least one of a, b should be divisible by p.

7.

$$\begin{aligned} 2^{2017} &\equiv (2^2)^{1008} \times 2 \\ &\equiv (-1)^{1008} \times 2 \\ &\equiv 2 \bmod 5 \end{aligned}$$

$$\begin{aligned} 2^{2017} &\equiv (2^6)^{336} \times 2 \\ &\equiv (-1)^{336} \times 2 \\ &\equiv 2 \bmod 13 \end{aligned}$$

$$\begin{aligned} 2^{2017} &\equiv (2^5)^{403} \times 4 \\ &\equiv 1^{403} \times 4 \\ &\equiv 4 \bmod 31 \end{aligned}$$

   Since $2015 = 5 \times 13 \times 31$, Chinese Remainder Theorem may be used to calculated $2^{2017} \bmod 2015$.

$$\begin{aligned} (-161) \times 5 + 2 \times 403 = 1 \\ 12 \times 13 + (-1) \times 155 = 1 \\ 21 \times 31 + (-10) \times 65 = 1 \end{aligned}$$

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

Ex.2 - Rabin Cryptosystem

1. Find two big prime number p and q, and $p, q \equiv 3 \bmod 4$. Rabin Cryptosystem takes $n = pq$ as public key, (p, q) as private key.

   To encrypt plain text m, cipher text c is calculated as

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

   To decrypt cipher text, solve the simultaneous congruence equations

   $$\begin{cases} m_p \equiv c^{\frac{p+1}{4}} \bmod p \\ m_q \equiv c^{\frac{q+1}{4}} \bmod q \end{cases}$$

   Where m_p and m_q are defined as

   $$\begin{cases} m \equiv \pm m_p \bmod p \\ m \equiv \pm m_q \bmod q \end{cases}$$

   Apply the Chinese Remainder Theorem, one can get four different solutions for the plain text.

2. (a) Since at most four different solutions can be found, there is 25% of chance to observe a meaningful message when feeding random numbers.

   (b) No, since if Eve only has x and public key n, he cannot solve like above. Whether to factorize n, or to solve $m \equiv \sqrt{x} \bmod n$ are as the same difficulty.

   (c) Eve should run a chosen cipher attack. Eve can then use the device to get the four different solutions as $\pm a, \pm b$. Since $gcd(|a - b|, n)$ is a non-trivial factor of n, then Eve can factorize n by calculating $|a - b|$, which is either p or q.

Ex.3 - CRT

Assume there are x people in the group, then x satisfies that

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

Since $3, 4, 5$ are coprime to each other, one can use Chinese Remainder Theorem to solve x.

$$7 \times 3 + (-1) \times 20 = 1$$
$$4 \times 4 + (-1) \times 15 = 1$$
$$5 \times 5 + (-2) \times 12 = 1$$

$$\begin{aligned} x &\equiv 1 \times (-1) \times 20 + 2 \times (-1) \times 15 + 3 \times (-2) \times 12 \\ &\equiv -122 \\ &\equiv 58 \bmod 60 \end{aligned}$$

Then the two smallest possible x are 58 and 118.