UM-SJTU JOINT INSTITUTE
VE475 Introduction to Cryptography

# Homework 2

Li Yong 517370910222

May 28, 2021

# Ex.1 Simple questions

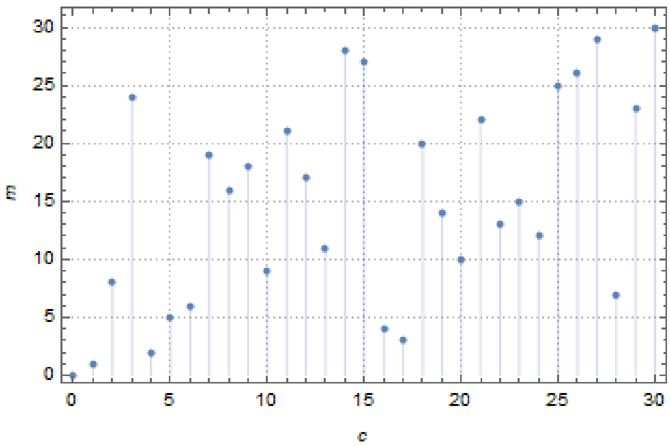
1. $$17 \cdot 6 \equiv 1 \bmod 101$$

2. $$gcd(12, 236) = 4 \Rightarrow 3x \equiv 7 \bmod 59$$
$$x \equiv 22 \bmod 59$$
$$x \equiv (22 + 59k) \bmod 236, k \in \{0, 1, 2, 3\}$$

3. We calculate the corresponding ciphertext $c$ for given plaintext $m$.

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

Plot the table, it is obviously a bijection. Hence we can decrypt the message by this table.




4. $$4883 = 19 \times 257$$
$$4369 = 17 \times 257$$

5. $$A = \begin{pmatrix} 3 & 5 \\ 7 & 3 \end{pmatrix}$$
$$\det A = -26$$
Suppose $A$ is invertible modulo $p$, then
$$\det(A) \cdot t \equiv 1 \bmod p$$
$$26t \equiv 1 \bmod p$$
So that 26 and $p$ are coprime. Hence when $p = 2$, $A$ is not invertible.

6.

$$ab \equiv 0 \bmod p$$
$$\Rightarrow p \mid ab$$

$p$ is prime so that $\gcd(a,p) = 1$ or $\gcd(a,p) = p$.

a. If $\gcd(a,p) = 1$, then $p \mid n$, *i.e.*, $b$ is congruent to 0 mod $p$[1].

b. If $\gcd(a,p) = p$, then $a$ is congruent to 0 mod $p$.

7.

$$\begin{aligned} 2^{2017} \bmod 5 &= 2 \cdot 4^{1008} \bmod 5 \\ &= 2 \cdot (-1)^{1008} \bmod 5 \\ &= 2 \bmod 5 = 2 \end{aligned}$$

$$\begin{aligned} 2^{2017} \bmod 13 &= 2 \cdot 64^{336} \bmod 13 \\ &= 2 \cdot (-1)^{336} \bmod 13 \\ &= 2 \bmod 13 = 2 \end{aligned}$$

$$\begin{aligned} 2^{2017} \bmod 31 &= 4 \cdot 32^{403} \bmod 31 \\ &= 4 \cdot (-1)^{403} \bmod 31 \\ &= 4 \bmod 31 = 4 \end{aligned}$$

According to CRT,

$$\begin{cases} 2^{2017} \equiv 2 \bmod 5 \\ 2^{2017} \equiv 2 \bmod 13 \\ 2^{2017} \equiv 4 \bmod 31 \end{cases}$$

So that

$$2^{2017} \bmod 2015 = 2 \times M_1t_1 + 2 \times M_2t_2 + 4 \times M_3t_3 \pmod{2015},$$

where

$$\begin{aligned} M_1 &= 13 \times 31 \\ M_2 &= 5 \times 31 \\ M_3 &= 5 \times 13 \end{aligned}$$

$$\begin{cases} (M_1t_1) \equiv 1 \bmod 5 \\ (M_2t_2) \equiv 1 \bmod 13 \\ (M_3t_3) \equiv 1 \bmod 31 \end{cases}$$

Hence, $2^{2017} \equiv 717 \bmod 2015$.

# Ex.2 Rabin cryptosystem

1. **Rabin cryptosystem** is an asymmetric cryptographic technique. As with all asymmetric cryptosystems, the Rabin system uses both a public and a private key.

   The keys are generated in such process:

[1] According to hw1 Ex. 1.3

- Choose two large distinct primes $p$ and $q$ as private keys.
- Then public key is $n = pq$.

For the encryption, only public key is needed, while for the decryption, private key is used.

Given a plaintext $m$ modulo $n$, its corresponding ciphertext is $c = m^2 \bmod 3n$.

2. a) According to the computation of square roots modulo introduced in Rabin cryptosystem, there are on ly four possible results. Hence, a meaningful message can be expected fairly soon.

   b) No. For decryption, she needs two private keys to calculate the square roots modulo. Even if she could factor public key to get private keys, $p$ and $q$ are large primes. So that it would take Eve much time to decrypt.

   c) CCA.
   Given ciphertext $c$, she could use this device to get 4 result. We denote them as $+r$, $-r$, $+s$ and $-s$. Then

$$gcd((+r) - (+s), n) = q$$

$$gcd((+r) - (-s), n) = p$$

# Ex.3 CRT

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 2 \bmod 4 \\ x \equiv 3 \bmod 5 \end{cases}$$

So that

$$x \bmod 60 = 1 \times M_1 t_1 + 2 \times M_2 t_2 + 3 \times M_3 t_3 \pmod{60},$$

where

$$M_1 = 4 \times 5$$
$$M_2 = 3 \times 5$$
$$M_3 = 3 \times 4$$

$$\begin{cases} (M_1 t_1) \equiv 1 \bmod 3 \\ (M_2 t_2) \equiv 1 \bmod 4 \\ (M_3 t_3) \equiv 1 \bmod 5 \end{cases}$$

Hence, $x \equiv 58 \bmod 60$. The two smallest possible numbers of people in the group are 58 and 118.

# References


1. https://cryptography.fandom.com/wiki/Rabin_cryptosystem