Problem 1. Simple questions

1. We first apply Extended Euclidean Algorithm to find the greatest common diviser and Bezout coefficient.

$$\begin{aligned} 101 &= 5 \times 17 + 16 & 1 &= 5 \times 0 + 1 & 0 &= 5 \times 1 - 5 \\ 17 &= 1 \times 16 + 1 & 0 &= 1 \times 1 - 1 & 1 &= 1 \times (-5) + 6 \\ 16 &= 16 \times 1 \end{aligned}$$

   Then we have

$$17 * 6 + 101 * (-1) = gcd(17, 101) = 1$$

   Therefore, 6 is the inverse of 17 modulo 101.

2.

$$\begin{aligned} 12x &\equiv 28 \mod 236 \\ 3x &\equiv 7 \mod 59 \\ 3x &= 59n + 7 \quad n \in \mathbb{Z} \\ x &= \frac{59n+7}{3} = \frac{59(n-1)+59+7}{3} = \frac{59(n-1)}{3} + 22 \end{aligned}$$

   Let $n - 1 = 3k$ ($k \in \mathbb{Z}$), then we have $x = 59k + 22$, $k \in \mathbb{Z}$.

3. Given plaintext m and corresponding ciphertext c $\in (0, 1, ..., 30)$ have the same size, we can verify that for m = 0 to 30 that $gcd(m^7, 31) = 1 \longrightarrow c = m^7 \mod 31$ has an inverse. Therefore, we can decrypt the message using the key inverse. Using the generated table below, it's easy to decrypt the message by transforming letter.

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		

Table 1: Bijection between m and c

4. Since $\sqrt{4883} = 69.88$, $\sqrt{4369} = 66.1$, so the factors smaller than 70 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67. We can simply start by dividing the largest factor, and we will find that $4883 = 19 \times 257$, and we have proven 257 is a prime in homework 1. In a similar way, we will find $4369 = 17 \times 257$.

5. Given prime p and matrix

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

If the matrix A is not invertible, we have

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

$$gcd(det(A), p) \neq 1$$

Therefore, we can easily find that only when $p = 2$ and $p = 13$ the matrix is not invertible.

6. As is proved in the last homework, we know that given three positive integers a,b and n, if $n|ab$ and $gcd(a, n) = 1$, we can prove that $n|b$.
Now we have a prime p, then we know $gcd(a, p) = 1$ or p. If $gcd(a, p) = 1$, since $p|ab$, then $b|p$, $b \equiv 0 \mod p$. If $\gcd(a, p) = p$, then $a \equiv 0 \mod p$, therefore at least one of a or b is congruent to 0 mod p.

7.

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

Using Chinese Remainder Theorem, we can express 2^{2017} in another way. We have

$$M = 5 \times 13 \times 31 = 2015$$

$$M_1 = 403, M_2 = 155, M_3 = 65$$

Let t_i be the inverse of M_i, such that $t_i M_i \equiv 1 \mod m_i (i \in 1, 2, 3)$

$$\begin{aligned} t_1 \times 403 \equiv 1 \bmod 5 &\Rightarrow t_1 = 2 \\ t_2 \times 155 \equiv 1 \bmod 155 &\Rightarrow t_2 = -1 \\ t_3 \times 65 \equiv 1 \bmod 65 &\Rightarrow t_3 = -10 \end{aligned}$$

Therefore, we have the solution

$$\begin{aligned} 2^{2^{2017}} \bmod 2015 &= kM + \sum_{i=1}^{3} a_i t_i M_i = 2015k - 1298 \ (k \in \mathbb{Z}) \bmod 2015 \\ &= -1298 \bmod 2015 \\ &= 717 \bmod 2015 \\ &= 717 \end{aligned}$$

Problem 2. Rabin cryptosystem

1. The Rabin cryptosystem is an asymmetric cryptographic technique. It uses a key pair: a public key for encryption and a private key for decryption. The public key is published for anyone to use, while the private key remains known only to the recipient of the message.
   For the key generation, there are two steps:

   (a) Choose two large distinct prime numbers p and q, such that

   $$\begin{aligned} p &\equiv 3 \mod 4 \\ q &\equiv 3 \mod 4 \end{aligned}$$

   (b) Compute $n = pq$, and then we have the public key n and private key pair (p, q)

   To encrypt the plaintext M, first we can convert it into a number $m < n$ using reversible mapping, and then compute the ciphertext $c \equiv m^2 \mod n$.
   To decrypt the ciphertext c, we will do the following:

   (a) Compute the square root of c modulo p and q by

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

   (b) Use the extended Euclidean algorithm to find y_p and y_q such that $y_p p + y_q q = 1$

   (c) Use the Chinese remainder theorem to find the four square roots of c modulo n, and one of these four values is the original plaintext m

   $$\begin{aligned} r_1 &= (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \mod n \\ r_2 &= n - r_1 \\ r_3 &= (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \mod n \\ r_4 &= n - r_3 \end{aligned}$$

2. (a) Everytime the device has an output, it has 25% chance to get a meaningful message, this is because there are four possible answers for the square root of x, and one of them is the plaintext m.

(b) No. Eve has to solve $m \equiv \sqrt{x} \mod n$, since n is a relative large number, its security related to the integer factorization, which is known to be an NP and co-NP problem.

(c) Eve should use Chosen Ciphertext Attact(CCA). To find the factorization of n, Eve can use any message m to calculate $c = m^2$, and send c to the machine to calculate the roots. The four square roots r_1, r_2, r_3, r_4 can be denoted as $r, -r, s, -s$. Therefore, one root should the message m and the other one is -m, for the rest, either of one minus m and apply gcd with n will give p or q. The detailed calculation is listed below.

$$\begin{aligned} |r-(-s)| &= |(-r)-s| \\ &= 2|y_p \cdot p \cdot m_q| \mod n \\ &= 2|y_p m_q| p - kpq \\ &= 2(|y_p m_q| - kq)p, k \in \mathbb{Z} \\ \gcd(|r-s|, n) &= \gcd(2(|y_p m_q| - kq)p, pq) = p \end{aligned}$$

$$\begin{aligned} |r-s| &= |(-r)-(-s)| \\ &= 2|y_q \cdot q \cdot m_p| \mod n \\ &= 2|y_q m_p| p - kpq \\ &= 2(|y_q m_p| - kp)q, k \in \mathbb{Z} \\ \gcd(|r-s|, n) &= \gcd(2(|y_q m_p| - kp)q, pq) = q \end{aligned}$$

Problem 3. CRT

Assume there are n people in the group, we have

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

According to the Chinese Remainder Theorem, we have

$$M = 3 \times 4 \times 5 = 60$$

$$M_1 = 20, M_2 = 15, M_3 = 12$$

Let t_i be the inverse of M_i, such that $t_i M_i \equiv 1 \mod m_i (i \in 1, 2, 3)$

$$\begin{aligned} t_1 \times 20 &\equiv 1 \bmod 3 \Rightarrow t_1 = 5 \\ t_2 \times 15 &\equiv 1 \bmod 4 \Rightarrow t_2 = 3 \\ t_3 \times 12 &\equiv 1 \bmod 5 \Rightarrow t_3 = 3 \end{aligned}$$

Therefore, we have the solution

$$n = kM + \sum_{i=1}^{3} a_i t_i M_i = 60k + 298 \ (k \in \mathbb{Z})$$

Since the number of people in the group have to be positive number, two smallest solutions are 58 and 118.