VE475 Homework2

Anna Li
Student ID: 518370910048

Ex. 1

1

Since we need to find the inverse of 17 modulo 101, we need to find an integer x, which is $17x \equiv 1 \mod 101$. Therefore, according to extended Euclidean algorithm,

$$\begin{aligned} 101 &= 17 * 5 + 16 \\ 17 &= 16 + 1 \end{aligned} \tag{1}$$

Therefore,

$$1 = 17 - 16 = 17 - (101 - 17 * 5) = 17 * 6 - 101$$

Therefore, the inverse of 17 modulo 101 is 6

2

since $12x \equiv 28 \mod 236$,

$$12x + 236y = 28 \Rightarrow 3x + 59y = 7$$

First, we found that x=22 is the only integer solution for this equation when x¡59.Therefore:

$$x = 59n + 22, n \in \mathbb{R}$$

3

since plaintext=m modulo 31, we could know that $x \in [0, 30]$. $c \in [0, 30]$

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	31	0	32	1

Therefore, we can decrypt this message.

4

Since $\sqrt{4883} = 69.9 \quad \sqrt{4369} = 66.09$
Therefore, we should consider 1,2,3,5,7,9,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67
Therefore:

$$4883 = 19 * 257 \quad 4369 = 17 * 257$$

5

After calculation, we found that only when p=2, $det(A \mod p) = 0$. Therefore, when p is not equal to 2, this equation is not invertible.

6

since p is a prime, and $ab \equiv 0 \mod p$, we know that $ab = np, n \in \mathbb{Z}$. Then we prove: the statement "none of a and b is congruent to 0 mod p" is wrong.
If none of a and b is congruent to 0 mod p, which means that $a \neq xp, x \in \mathbb{Z}$ and $b \neq yp, y \in \mathbb{Z}$.Since p is a prime number, $ab \neq mp, m \in \mathbb{Z}$, which is not true. Therefore, there are at least one of a and b is congruent to 0 mod p.

7

since

$$2 \equiv 2 \mod 5 \quad 2^2 \equiv 4 \mod 5 \quad 2^3 \equiv 3 \mod 5 \quad 2^4 \equiv 1 \mod 5 \quad 2^5 \equiv 4 \mod 5$$

Therefore,

$$2^{2017} \equiv 1 \mod 5$$

$$2 \equiv 2 \mod 13 \quad 2^2 \equiv 4 \mod 13 \quad 2^3 \equiv 8 \mod 13 \quad 2^4 \equiv 3 \mod 13 \quad 2^5 \equiv 12 \mod 13$$

$$2^6 \equiv 9 \mod 13 \quad 2^7 \equiv 5 \mod 13 \quad 2^8 \equiv 10 \mod 13 \quad 2^9 \equiv 7 \mod 13 \quad 2^{10} \equiv 1 \mod 13$$

Therefore,

$$2^{2017} \equiv 7 \mod 13$$

Through the same way, we could find that

$$2^{2017} \equiv 4 \mod 31$$

Since $2015 = 5 * 13 * 31$, we could use chinese remainder thereom to solve, and get:

$$2^{2017} \equiv 717 \mod 2015$$

Ex 2

1.

The Rabin cryptosystem is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of integer factorization. However the Rabin cryptosystem has the advantage that it has been mathematically proven to be computationally

secure against a chosen-plaintext attack as long as the attacker cannot efficiently factor integers, while there is no such proof known for RSA.[1]:145 It has the disadvantage that each output of the Rabin function can be generated by any of four possible inputs; if each output is a ciphertext, extra complexity is required on decryption to identify which of the four possible inputs was the true plaintext.
For the Rabin cryptosystem, we first take two big odd prime numbers P and Q, then

$$C = (pq)^2 (\mod n)$$

In this way, if we want ot decrypto it, we will get 4 possible answers.

2.

a)

Because we are not sure which one is the correct answers, so we could only guess by choosing a meaningful answer in language.

b)

No, without knowing p and q, Eve could not solve $x \equiv m^2 \mod n$

c)

She should run CCA on it. By that equipment, she could get all four possible outputs, suppose that the outputs are a,-a,b,-b. We could get p and q by randomly minusing them.for example:

$$|a - b| = q$$

Therefore,$gcd(|a - b|, n)$is the non-trivial factor

Ex. 3

From the problems, we could list the equation that:

$$n \equiv 1 \mod 3$$

$$n \equiv 2 \mod 4$$

$$n \equiv 3 \mod 5$$

By solving this question using Chinese Remainder thereom, we get that two smallest possible numbers of people are 58 and 118.