

# Homework of Cryptography

Tony Zhu

December 20, 2010

## 1 Classical Cryptography

### 1.21

#### (c) Affine Cipher

*Solution:* Since in the affine cryptosystem only  $\phi(26) \times 26 = 312$  cases for key  $K = (a, b)$ , list all the cases brutally with the help of computer and scan quickly, I found only one case seems meaningful:

ocanadaterredenosaieuxtonfrontestceintdefleuronsglorieuxcartonbrassaitporterlepeeils  
aitporterlacroixtonhistoireestuneepopeedesplusbrillan tsexploitsettavaleurdefoitrem-  
peeptegeganosfoyersetnosdroits

After breaking the long sentence, I found it should be the French version of Canada national anthem:

O Canada  
Terre de nos aïeux  
Ton front est ceint de fleurons glorieux!  
  
Car ton bras sait porter l'épée  
Il sait porter la croix!  
Ton histoire est une épopée  
Des plus brillants exploits  
  
Et ta valeur, de foi trempée  
Protégera nos foyers et nos droits

### 1.22

*Proof.* (a) Obviously in the case  $p_1 \geq p_2 \geq 0$ ,  $q_1 \geq q_2 \geq 0$ , the sum  $p_1q_1 + p_2q_2$  is maximized.

Suppose  $S = \sum_{i=1}^n p_i q'_i$  is maximized, and if there exists  $i > j$  such that  $q'_i < q'_j$ , permute the positions of the two numbers and, according to the statement of last paragraph, we get  $S' = \sum_{\substack{0 \leq h \leq n \\ h \neq i, j}} p_h q'_h + p_i q'_j + p_j q'_i > S$ , contradicts. So the only arrangement for  $S$  is  $q'_1 \geq \dots \geq q'_n$ . ■

## 2 Shannon's Theory

### 2.2

*Proof.*  $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{1, \dots, n\}$ .  $\forall x \in \mathcal{P}, \forall y \in \mathcal{C}$

$$\Pr[Y = y] = \sum_{k \in \mathcal{K}} \Pr[K = k] \Pr[x = d_k(y)] = 1/n$$

so

$$\begin{aligned} \Pr[x|y] &= \frac{\Pr[x] \Pr[y|x]}{\Pr[y]} \\ &= \frac{\Pr[x] \frac{1}{n}}{\frac{1}{n}} \\ &= \Pr[x] \end{aligned}$$

that is this *Latin Square Cryptosystem* achieves perfect secrecy provided that every key is used with equal probability. ■

### 2.3

*Proof.* Similarly as (2.2). ■

### 2.5

*Proof.* According to Theorem 2.4, this cryptosystem provides perfect secrecy iff every key is used with equal probability  $1/|\mathcal{K}|$ , and for every  $x \in \mathcal{P}$  and  $y \in \mathcal{C}$ , there is unique key  $k \in \mathcal{K}$ , such that  $y = e_k(x)$ .

Due to perfect secrecy, we have

$$\begin{aligned}
& \Pr[x|y] = \Pr[x] \\
\Rightarrow & \frac{\Pr[x]\Pr[y|x]}{\Pr[y]} = \Pr[x] \\
\Rightarrow & \Pr[y] = \Pr[y|x] = \Pr_{e_k(x)=y}[K = k] = 1/|\mathcal{K}|.
\end{aligned}$$

that is every ciphertext is equally probable. ■

## 2.11

*Proof.* (Perfect secrecy  $\Rightarrow H(\mathbf{P}|\mathbf{C})=H(\mathbf{P})$ ).

$$\begin{aligned}
H(\mathbf{P}|\mathbf{C}) &= - \sum_{y \in \mathbf{C}} \sum_{x \in \mathbf{P}} \Pr[y]\Pr[x|y] \log_2 \Pr[x|y] \\
&= - \sum_{y \in \mathbf{C}} \sum_{x \in \mathbf{P}} \Pr[y]\Pr[x] \log_2 \Pr[x] \\
&= H(\mathbf{P}) \sum_{y \in \mathbf{C}} \Pr[y] \\
&= H(\mathbf{P}).
\end{aligned}$$

( $H(\mathbf{P}|\mathbf{C}) = H(\mathbf{P}) \Rightarrow$  Perfect secrecy).

According to Theorem 2.7,

$$H(\mathbf{P}, \mathbf{C}) \leq H(\mathbf{P}) + H(\mathbf{C})$$

with equality iff  $\mathbf{P}$  and  $\mathbf{C}$  are independent random variables.

so

$$\begin{aligned}
& H(\mathbf{P}|\mathbf{C}) = H(\mathbf{P}) \\
\Rightarrow & H(\mathbf{P}, \mathbf{C}) = H(\mathbf{P}) + H(\mathbf{C}) \\
\Rightarrow & \mathbf{P} \text{ and } \mathbf{C} \text{ are independent random variables} \\
\Rightarrow & \forall x \in \mathbf{P}, \forall y \in \mathbf{C}, \Pr[x|y] = \Pr[x],
\end{aligned}$$

that is the cryptosystem achieves perfect secrecy. ■

## 2.12

*Proof.* We have

$$H(\mathbf{K}, \mathbf{P}, \mathbf{C}) = H(\mathbf{P}|\mathbf{K}, \mathbf{C}) + H(\mathbf{K}, \mathbf{C}) = H(\mathbf{K}, \mathbf{C}),$$

so

$$\begin{aligned} H(\mathbf{K}, \mathbf{P}, \mathbf{C}) &\geq H(\mathbf{P}, \mathbf{C}) \\ \implies H(\mathbf{K}, \mathbf{C}) &\geq H(\mathbf{P}, \mathbf{C}) \\ \implies H(\mathbf{K}|\mathbf{C}) &= H(\mathbf{K}, \mathbf{C}) - H(\mathbf{C}) \geq H(\mathbf{P}, \mathbf{C}) - H(\mathbf{C}) = H(\mathbf{P}|\mathbf{C}). \end{aligned}$$

■

### 2.13

*Solution:*  $H(\mathbf{P}) = \frac{1}{2} + \frac{1}{3} \log_2 3 + \frac{1}{6} \log_2 6 \approx 1.45915$ .

$$H(\mathbf{K}) = \log_2 3 \approx 1.58496.$$

$$\begin{aligned} \mathbf{Pr}[1] &= 2/9 \\ \mathbf{Pr}[2] &= 5/18 \\ \mathbf{Pr}[3] &= 1/3 \\ \mathbf{Pr}[4] &= 1/6 \end{aligned}$$

$$H(\mathbf{C}) \approx 1.95469.$$

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C}) \approx 1.08942.$$

$\mathbf{Pr}[K_1 1] = 3/4$	$\mathbf{Pr}[K_2 1] = 0$	$\mathbf{Pr}[K_3 1] = 1/4$
$\mathbf{Pr}[K_1 2] = 2/5$	$\mathbf{Pr}[K_2 2] = 3/5$	$\mathbf{Pr}[K_3 2] = 0$
$\mathbf{Pr}[K_1 3] = 1/6$	$\mathbf{Pr}[K_2 3] = 1/3$	$\mathbf{Pr}[K_3 3] = 1/2$
$\mathbf{Pr}[K_1 4] = 0$	$\mathbf{Pr}[K_2 4] = 1/3$	$\mathbf{Pr}[K_3 4] = 2/3$

$$H(\mathbf{P}|\mathbf{C}) \approx 1.08942.$$

### 2.14

*Solution:*  $H(\mathbf{K}) = \log_2 216$ ,  $H(\mathbf{P}) = \log_2 26$ ,  $H(\mathbf{C}) = \log_2 26$ ,

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C}) = \log_2 216 \approx 7.75489.$$

It is easy to evaluate:

$$H(\mathbf{K}|\mathbf{P}, \mathbf{C}) = \log_2 12 \approx 3.58496.$$

## 2.19

*Proof.* A key in the product cipher  $\mathbf{S}_1 \times \mathbf{S}_2$  has the form  $(s_1, s_2)$ , where  $s_1, s_2 \in \mathbb{Z}_{26}$ ,

$$e_{(s_1, s_2)}(x) = x + (s_1 + s_2).$$

But this is precisely the definition of a key in the *Shift Cipher*. Further, the probability of a key in  $\mathbf{S}_1 \times \mathbf{S}_2$  equals  $\sum_{i=0}^{25} \frac{1}{26} p_i = \frac{1}{26} \sum_{i=0}^{25} 1 = \frac{1}{26}$ , which is also the probability of a key in the *Shift Cipher*. Thus  $\mathbf{S}_1 \times \mathbf{S}_2$  is the *Shift Cipher*. ■

## 2.20

*Proof.* (a) Similarly as (2.19).

(b) The number of keys in  $\mathbf{S}_3$  equals  $26^{\text{lcm}(m_1, m_2)}$ . From the following fact we can see that the keys in  $\mathbf{S}_1 \times \mathbf{S}_2$  are lesser when  $m_1 \not\equiv 0 \pmod{m_2}$ .

Notice

$$\begin{aligned} & m_2 < m_1, m_1 \not\equiv 0 \pmod{m_2} \\ \implies & m_1 + m_2 < 2m_1 \leq \frac{m_2}{\gcd(m_1, m_2)} m_2 = l, \text{ where } l \triangleq \text{lcm}(m_1, m_2) \end{aligned}$$

the equation below, which essentially gives the representation of the keys of product cryptosystem  $\mathbf{S}_1 \times \mathbf{S}_2$ , would't always has a solution  $(K_1, K_2) = (x_1, \dots, x_{m_1}, y_1, \dots, y_{m_2}) \in \mathcal{K}_1 \times \mathcal{K}_2$ , for any selected key  $K = (z_1, \dots, z_l) \in \mathcal{K}_3$ ,

$$\begin{pmatrix} I_{m_1} & I_{m_2} \\ & I_{m_2} \\ & \vdots \\ I_{m_1} & I_{m_2} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{m_1} \\ y_1 \\ \vdots \\ y_{m_2} \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_l \end{pmatrix},$$

because the coefficient matrix's column number is less than the row number. Conclusively, there must exist key  $K \in \mathcal{K}_3$  that not in  $\mathcal{K}_1 \times \mathcal{K}_2$ . ■

# 3 The RSA Cryptosystem and Factoring Integers

## 5.2

*Proof.* (a)  $r_i = q_{i+1}r_{i+1} + r_{i+2} \geq r_{i+1} + r_{i+2} \geq 2r_{i+2}$ .

(b) (c) From (a),  $m \leq \log_2 a + 1 \sim \log a \sim \log b$ . ■

### 5.3

*Solution:* (a)  $17^{-1} \equiv 6 \pmod{101}$ .

(b)  $357^{-1} \equiv 1075 \pmod{1234}$ .

(c)  $3125^{-1} \equiv 1844 \pmod{9987}$ .

### 5.4

*Solution:*  $8 \times 93 - 13 \times 57 = 3$ .

### 5.5

*Solution:* It's easy to see that

$$\chi^{-1}(x, y, z) = 70x + 21y + 15z \pmod{105}.$$

So

$$\chi^{-1}(2, 2, 3) = 17.$$

### 5.6

*Solution:* Similarly we have

$$\chi^{-1}(x, y, z) = (13 \times 26 \times 27)x + (25^2 \times 27)y + (14 \times 25 \times 26)z \pmod{25 \times 26 \times 27}.$$

So

$$\chi^{-1}(12, 9, 23) = 470687.$$

### 5.7

*Solution:* Similarly we have

$$\chi^{-1}(x, y) = (50 \times 101)x + (51 \times 99)y \pmod{99 \times 101}.$$

$13^{-1} \equiv 61 \pmod{99}$ ,  $15^{-1} \equiv 27 \pmod{101}$ . So

$$\begin{cases} 13x \equiv 4 \pmod{99} \\ 15x \equiv 56 \pmod{101} \end{cases}$$

$$\iff \begin{cases} x \equiv 46 \pmod{99} \\ x \equiv 98 \pmod{101} \end{cases}$$

$$\implies x = 7471.$$

## 5.9

*Proof.*

$$\begin{aligned}
 & \alpha \not\equiv \pm 1 \pmod{p}, \alpha \text{ is primitive element modulo } p \\
 \iff & \text{the order of } \alpha \in \mathbb{Z}_p^* \text{ is } 2q. \\
 \iff & \alpha \not\equiv \pm 1 \pmod{p}, \alpha^q \equiv -1 \pmod{p}. \\
 & \text{(Because the order of } \alpha \text{ could only be } 2, q \text{ or } 2q.)
 \end{aligned}$$

■

## 5.11

*Proof.* By showing  $x^{\lambda(n)} = 1 \pmod{n}$ ,  $\forall x \in \mathbb{Z}_n$ , we can prove the encryption and decryption are still inverse operations in this modified cryptosystem.

Since we have

$$\mathbb{Z}_n \cong \mathbb{Z}_p \oplus \mathbb{Z}_q,$$

and the isomorphism is  $\Psi(h) = (h \pmod{p}, h \pmod{q})$ , it only needs to show  $x^{\lambda(n)} = 1 \pmod{p}$ , and  $x^{\lambda(n)} = 1 \pmod{q}$ .

$$\begin{aligned}
 x^{\lambda(n)} & \equiv (x^{p-1})^{\frac{q-1}{\gcd(p-1, q-1)}} \pmod{p} \\
 & \equiv (1)^{\frac{q-1}{\gcd(p-1, q-1)}} \pmod{p} \\
 & \equiv 1 \pmod{p}.
 \end{aligned}$$

For  $q$  is the same. So complete the proof.

■

*Solution:* (b)  $p = 37$ ,  $q = 79$ ,  $b = 7$ .

*Modified cryptosystem.*  $\lambda(n) = 468$ ,  $a = 67$ .

*Original cryptosystem.*  $\phi(n) = 2808$ ,  $a = 2407$ .

## 5.13

*Proof.* (a) Again use the isomorphism

$$\mathbb{Z}_n \cong \mathbb{Z}_p \oplus \mathbb{Z}_q,$$

and note that  $x^{p-1} \equiv 1 \pmod{p}$  and  $x^{q-1} \equiv 1 \pmod{q}$  for all  $x \neq 0$ , we get

$$\begin{aligned}
 \mathbb{Z}_n & \rightarrow \mathbb{Z}_p \oplus \mathbb{Z}_q \rightarrow \mathbb{Z}_n \\
 y^d \pmod{n} & \rightarrow (y^d \pmod{p}, y^d \pmod{q}) \rightarrow M_p q x_p + M_q p x_q \pmod{n} \\
 & = (y^{d_p} \pmod{p}, y^{d_q} \pmod{q}) \\
 & = (x_p, x_q)
 \end{aligned}$$

so complete the proof.

(b)  $p = 1511$ ,  $q = 2003$ , and  $d = 1234577$ .

After some calculation, we get  $d_p = 907$ ,  $d_q = 1345$ ,  $M_p = 777$ , and  $M_q = 973$ .

(c)  $y = 152702$ ,  $y^{d_p} = 242 \pmod{1511}$ ,  $y^{d_q} = 1087 \pmod{2003}$ ,  $y^d = 1443247 \pmod{n = 3026533}$ . ■

### 5.14

*Solution:* If  $\gcd(y, n) \neq 1$ , we get a factor  $p = \gcd(y, n)$  of  $n$ , and another factor  $q = \frac{n}{\gcd(y, n)}$ , consequently,  $d_K$  and  $x = d_K(y)$  can be calculated explicitly.

Now suppose  $\gcd(y, n) = 1$ , computer  $\hat{y} = y^{-1} \pmod{n}$ , which is chosen as the attack allows to know the plaintext  $\hat{x}$ , it is easy to see that  $x = \hat{x}^{-1} \pmod{n}$ .

### 5.18

*Proof.* The isomorphism

$$\mathbb{Z}_n \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$$

is used again to show

$$e_K(x) = x^a = x \iff (x^a \pmod{p}, x^a \pmod{q}) = (x \pmod{p}, x \pmod{q}).$$

And

$\mathbb{F}_p^*$  is multiplicative cyclic group of order  $p - 1$ ,

$\mathbb{F}_q^*$  is multiplicative cyclic group of order  $q - 1$ ,

deduce that

$$\#S_p = \#\{x \in \mathbb{F}_p^* | x^a = x\} = \gcd(a - 1, p - 1),$$

$$\#S_q = \#\{x \in \mathbb{F}_q^* | x^a = x\} = \gcd(a - 1, q - 1),$$

so

$$\begin{aligned} \#S &= \#\{x \in \mathbb{Z}_n | x \neq 0, (x^a \pmod{p}, x^a \pmod{q}) = (x \pmod{p}, x \pmod{q})\} \\ &= \#(S_p \times S_q) \\ &= \gcd(a - 1, p - 1) \times \gcd(a - 1, q - 1) \\ &= \gcd(b - 1, p - 1) \times \gcd(b - 1, q - 1), \end{aligned}$$

the last equation can be easily seen from the equality

$$ab \equiv 1 \pmod{(p - 1)(q - 1)}, \text{ i.e. } (a - 1)b \equiv -(b - 1) \pmod{(p - 1)(q - 1)}.$$



## 5.22

*Proof.* (a)  $G(n)$  is a subgroup of  $\mathbb{Z}_n^*$ , because  $1 \in G(n)$ , and  $\forall x, y \in G(n)$ ,

$$\left(\frac{x^{-1}}{n}\right) \equiv \left(\frac{x}{n}\right)^{-1} \equiv a^{(-1)(n-1)/2} \pmod{n},$$

$$\left(\frac{xy}{n}\right) \equiv \left(\frac{x}{n}\right)\left(\frac{y}{n}\right) \equiv x^{(n-1)/2}y^{(n-1)/2} \equiv (xy)^{(n-1)/2} \pmod{n},$$

i.e.  $x^{-1} \in G(n)$ ,  $xy \in G(n)$ .

If  $G(n) \neq \mathbb{Z}_n^*$ , obviously we have

$$|G(n)| \leq \frac{|\mathbb{Z}_n^*|}{2} \leq \frac{n-1}{2}.$$

(b) On one hand,

$$\left(\frac{a}{n}\right) \equiv \left(\frac{1+p^{(k-1)}q}{p^k}\right)\left(\frac{1+p^{(k-1)}q}{q}\right) \equiv 1 \pmod{n},$$

on the other hand,

$$a^{(n-1)/2} \equiv (1+p^{(k-1)}q)^{(n-1)/2} \equiv 1 + \frac{(p^kq-1)p^{(k-1)}q}{2} \equiv 1 + \frac{p^{(k-1)}q}{2} \not\equiv 1 \pmod{n},$$

so

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}.$$

(c) On one hand, we have

$$\left(\frac{a}{n}\right) \equiv \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2p_3 \dots p_s}\right) \equiv (-1) \times 1 \equiv 1 \pmod{n},$$

on the other hand, from the definition of  $a$ , we have

$$a^{(n-1)/2} \equiv 1 \pmod{p_2p_3 \dots p_s}$$

so  $a^{(n-1)/2} \not\equiv -1 \pmod{n}$ , because otherwise we can deduce that  $a^{(n-1)/2} \equiv -1 \pmod{p_2p_3 \dots p_s}$ , contradicts.

(d) If  $n$  is odd and composite, suppose its factorization is  $n = p_1^{k_1}p_2^{k_2} \dots p_s^{k_s}$ , then there must exist  $n_1$  of the form  $p^kq$  or the form  $p_1 \dots p_s$  for some primes  $p, q, p_1, \dots, p_s$ , such that  $n = n_1n_2$ . Now if  $G(n) = \mathbb{Z}_n^*$ , i.e.  $\forall a \in \mathbb{Z}_n^*, \left(\frac{a}{n}\right) \equiv a^{(n-1)/2}$

(mod  $n$ ), so we have  $\forall a \in \mathbb{Z}_n^*, \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n_1}$ , which contradicts the results of (b) and (c). Thus we must have  $G(n) \neq \mathbb{Z}_n^*$ , and, resulting from (a),  $G(n) \leq (n-1)/2$ .

(e) Summarize the above: we finally prove that the error probability of the Solovay-Strassen primality test is at most  $1/2$ . ■

### 5.23

*Proof.* (b) The average number of trials to achieves success is

$$\sum_{n=1}^{\infty} (n \times p_n),$$

now apply the following identity

$$\begin{aligned} \frac{1}{(1-x)^2} &= \frac{d}{dx} \left( \frac{1}{1-x} \right) \\ &= \frac{d}{dx} \left( \sum_{n=0}^{\infty} x^n \right) \\ &= \sum_{n=1}^{\infty} n x^{n-1} \quad \text{for } |x| < 1, \end{aligned}$$

we have

$$\begin{aligned} \sum_{n=1}^{\infty} (n \times p_n) &= \sum_{n=1}^{\infty} (n \times \epsilon^{n-1} (1 - \epsilon)) \\ &= (1 - \epsilon) \sum_{n=1}^{\infty} n \epsilon^{n-1} \\ &= \frac{1}{1 - \epsilon}. \end{aligned}$$

(c) Suppose  $n$  is the number of iteraitons required in order to reduce the possibility of failure to at most  $\delta$ , so we have

$$\epsilon^n \leq \delta,$$

i.e.

$$\begin{aligned} n &\leq \log_{\epsilon} \delta \\ &\leq \left\lceil \frac{\log_2 \delta}{\log_2 \epsilon} \right\rceil \end{aligned}$$

■

## 5.24

*Proof.* (a)

**Algorithm:** Lifting( $a, b, n$ )

$$b_0 \leftarrow b \pmod{p}$$

$$b_1 \leftarrow b_0^{-1} \pmod{p}$$

$$h \leftarrow b^2 - a \pmod{p^{i-1}}$$

$$x \leftarrow -h \frac{p+1}{2} b_1 \pmod{p}$$

**return**( $x$ )

The reason for the algorithm is following: suppose the lift of  $b$  to  $\mathbb{Z}_{p^i}$  is  $b + xp^{i-1}$ , then

$$\begin{aligned} & (b + xp^{i-1})^2 \equiv a \pmod{p^i} \\ \implies & b^2 + 2bxp^{i-1} \equiv a \pmod{p^i} \\ \implies & 2bxp^{i-1} \equiv -h \pmod{p^i} \\ \implies & x \equiv -h 2^{-1} b^{-1} \pmod{p^i} \\ \implies & x \equiv -h \frac{p+1}{2} b_1 \pmod{p} \end{aligned}$$

(b)

$$\begin{aligned} 6^2 & \equiv 17 \pmod{19} \\ (6 + 11 \cdot 19)^2 & = 215^2 \equiv 17 \pmod{19^2} \\ (6 + 11 \cdot 19 + 2 \cdot 19^2) & = 937^2 \equiv 17 \pmod{19^3} \end{aligned}$$

(c) This result can be directly deduced from Hensel's Lemma. ■

## 5.29

*Proof.* (a)

$$\begin{aligned} n + d^2 & = pq + d^2 \\ & = p(p + 2d) + d^2 \\ & = (p + d)^2 \end{aligned}$$

(b) Let  $h^2 = n + d^2$ , then  $(h + d)(h - d) = h^2 - d^2 = n$ .

(c)

$$n = 2189284635403183,$$

$$d = 9,$$

$$h = 46789792,$$

$$h^2 = 2189284635403264 = n + 81,$$

so

$$(h + d)(h - d) = 46789783 \cdot 46789801 = 2189284635403183 = n.$$

■

### 5.30

*Solution:*

$$n = 36581, a = 14039, b = 4679,$$

$$ab - 1 = 65688481 = 2^5 \cdot 2052765$$

$$r = 2052765.$$

When  $w = 9983$ ,  $\gcd(w, n) = 1$ ,

$$w^r \equiv 35039 \pmod{n}$$

$$w^{2r} \equiv 36580 \equiv -1 \pmod{n}. \quad \textbf{Fail.}$$

When  $w = 13461$ ,  $\gcd(w, n) = 1$ ,

$$w^r \equiv 11747 \pmod{n}$$

$$w^{2r} \equiv 8477 \pmod{n}$$

$$w^{4r} \equiv 14445 \pmod{n}$$

$$w^{8r} \equiv 1 \pmod{n}$$

$$\gcd(14444, n) = 157, \gcd(14446, n) = 233,$$

$$233 \cdot 157 = 36581 = n$$

### 5.32

*Solution:*

$$n = 317940011, b = 77537081,$$

the continued fraction expansion of  $b/n$  is

$$[0, 4, 9, 1, 19, 1, 1, 15, 3, 2, 3, 71, 3, 2].$$

The partial convergents of this continued fraction are as follows:

$$\begin{aligned} [0, 4] &= 1/4 \\ [0, 4, 9] &= 9/37 \\ [0, 4, 9, 1] &= 10/41 \end{aligned}$$

The  $n'$  and equations are listed:

$$\begin{aligned} 1/4 \quad n' &= 310148323 & X^2 - 7791689X + 317940011 &= 0, \text{ No integer solutions.} \\ 9/37 \quad n' &= 2868871996/9 \\ 10/41 \quad n' &= 317902032 & X^2 - 37980X + 317940011 &= 0, X_1 = 12457, X_2 = 25523 \end{aligned}$$

Finally we have the factors of  $n = 12457 \cdot 25523$ .

### 5.33

*Solution:* (a)  $n = 41989$ ,  $y = e_K(32767) = 16027$ .

(b) The four possible decryption of this ciphertext  $y$  is

$$\begin{aligned} x_1 &= 32767, & x_2 &= 7865, \\ x_3 &= 18837, & x_4 &= 21795. \end{aligned}$$

## 4 Public-key Cryptography and Discrete Logarithms

### 6.4

*Solution:* (a) Suppose  $\alpha$  is a primitive element modulo  $p$ , since  $\text{ord}(\alpha) | p(p-1)$ , to show  $\alpha$  is a primitive element modulo  $p^2$  is equivalent to show  $\alpha^{p-1} \not\equiv 1 \pmod{p^2}$ , and  $\alpha^p \not\equiv 1 \pmod{p^2}$ . And we already have

$$\alpha \text{ is a primitive element modulo } p \implies \alpha^p \not\equiv 1 \pmod{p^2}.$$

If  $\alpha^{(p-1)} \equiv (\alpha + p)^{(p-1)} \equiv 1 \pmod{p^2}$ , then we can get  $p | \alpha$ , contradicted with the choice of  $\alpha$ , so at least one of  $\alpha$  or  $\alpha + p$  is a primitive element modulo  $p^2$ .

(b) We only need to check there is no such non-trivial factor  $h$  of  $p - 1$  that  $3^h \equiv 1 \pmod{29}$  to confirm 3 is a primitive element modulo 29, and to check  $3^{28} \not\equiv 1 \pmod{29^2}$  to confirm 3 is a primitive element modulo  $29^2$ .

(c) 14.

$$(d) 24388 = 2^2 \cdot 7 \cdot 13 \cdot 67$$

$$\log_3 3344 = 18762 \text{ in } \mathbb{Z}_{24389}^*.$$

## 6.6

*Solution:* (a)  $\alpha = 2$ ,  $p = 227$ ,

$$\begin{aligned} \alpha^{32} &\equiv 176 \pmod{227} \equiv 2^4 \cdot 11 \pmod{227} \\ \alpha^{40} &\equiv 110 \pmod{227} \equiv 2 \cdot 5 \cdot 11 \pmod{227} \\ \alpha^{59} &\equiv 60 \pmod{227} \equiv 2^2 \cdot 3 \cdot 5 \pmod{227} \\ \alpha^{156} &\equiv 28 \pmod{227} \equiv 2^2 \cdot 7 \pmod{227} \end{aligned}$$

(b)

$$\begin{aligned} \log 3 &= 46, & \log 5 &= 11, \\ \log 7 &= 154, & \log 11 &= 28. \end{aligned}$$

(c)

$$\begin{aligned} 173 \cdot 2^{177} &\equiv 168 \pmod{227} \equiv 2^3 \cdot 3 \cdot 7, \\ \log 173 &= 26. \end{aligned}$$

## 6.7

*Proof.* (a) From the following isomorphism

$$\mathbb{Z}_n \cong \mathbb{Z}_p \oplus \mathbb{Z}_q,$$

directly we have

$$\text{ord}_n(\alpha) = \text{lcm}(\text{ord}_p(\alpha), \text{ord}_q(\alpha)).$$

(b) Suppose  $\alpha_p, \alpha_q$  be generators of  $\mathbb{Z}_p, \mathbb{Z}_q$  respectively. Chinese Remainder Theorem assures the existence of the follow equations

$$\begin{cases} x \equiv \alpha_p \pmod{p} \\ x \equiv \alpha_q \pmod{q} \end{cases},$$

denote the solution by  $\alpha$ , now applying (a),

$$\text{ord}_n(\alpha) = \text{lcm}(\text{ord}_p(\alpha), \text{ord}_q(\alpha)) = \frac{\phi(n)}{d}.$$

(c)

$$\begin{aligned}\alpha^a &\equiv \alpha^n \pmod{n} \\ \implies \alpha^{n-a} &\equiv 1 \pmod{n} \\ \implies \exists k \in \mathbb{N}^*, \text{ s.t. } k \frac{\phi(n)}{2} &= (n-a),\end{aligned}$$

from  $k \frac{\phi(n)}{2} \leq n$ ,  $p > 3$ ,  $q > 3$ , we get  $k \leq 2$ , and from  $0 \leq a \leq \phi(n)/2 - 1$ , we get  $k = 2$ , i.e.  $n - a = \phi(n)$ .

(d) The roots of the equation

$$x^2 + (n - \phi(n) + 1)x + n = 0$$

are  $p$ ,  $q$ . ■

### 6.10

*Solution:*  $x^5 + x^3 + 1$  is irreducible,

$$\begin{aligned}x^5 + x^4 + 1 &= (1 + x + x^2)(1 + x + x^3), \\ x^5 + x^4 + x^2 + 1 &= (1 + x)(1 + x + x^4).\end{aligned}$$

### 6.11

*Solution:* (a)  $(x^4 + x^2)(x^3 + x^2 + 1) \equiv 1 + x + x^2 + x^3 + x^4$ , in  $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$ .

(b)  $(x^3 + x^2)^{-1} \equiv 1 + x + x^2$ , in  $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$ .

(c)  $x^{25} \equiv 1 + x^3 + x^4$ , in  $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$ .

### 6.12

*Solution:* The plaintext is “GaloisField”.

### 6.13

*Solution:* (a)  $\#E(\mathbb{F}_{71}) = 72$ .

(b) According to Theorem 6.1,  $E(\mathbb{F}_{71})$  could only be isomorphism to either  $\mathbb{Z}_{72}$  or  $\mathbb{Z}_{36} \times \mathbb{Z}_2$ . Now from the fact that  $E(\mathbb{F}_{71})$  has four points of order 2—they are  $(27, 0)$ ,  $(53, 0)$ ,  $(62, 0)$  and the special point  $O$ , we can conclude that

$$E(\mathbb{F}_{71}) \cong \mathbb{Z}_{36} \times \mathbb{Z}_2.$$

(c) From the above discussion we know the maximum order of a point on  $E$  is 36, and the point  $(3, 22)$  has this order.

### 6.14

*Proof.* Let the three distinct roots of  $x^3 + ax + b \equiv 0 \pmod{p}$  be  $x_1, x_2, x_3$ . Hence points  $(x_1, 0), (x_2, 0), (x_3, 0)$  and the special point  $\mathcal{O}$  are the only four points of order 2 on  $E$ , and according to the group theory, they must be isomorphism to  $\mathbb{Z}_2 \times \mathbb{Z}_2$  as groups. Therefore, group  $E(\mathbb{F}_p)$  containing the above four points as a subgroup can not be cyclic. ■

### 6.15

*Solution:* (a) Directly from the calculation.

(b) Obviously.

(c)  $(1, 20), (1, 53), (2, 21), (2, 52), (71, 17), (71, 56), (72, 29), (72, 44)$  and the special point  $\mathcal{O}$ .

### 6.17

*Solution:* (a)  $Q = mP = (8, 15)$ .

(b)

Ciphertext	$((18, 1), 21)$	$((3, 1), 18)$	$((17, 0), 19)$	$((28, 0), 18)$
Step 1 ( $kP$ )	$((18, 17), 21)$	$((3, 3), 18)$	$((17, 26), 19)$	$((28, 6), 18)$
Step 2 ( $kQ$ )	$(15, 8)$	$(2, 9)$	$(30, 29)$	$(14, 19)$
Plaintext	20	9	12	5

(c) TILE.

### 6.18

*Solution:* (a)  $87 = (-1) \cdot 2^0 + (-1) \cdot 2^3 + (-1) \cdot 2^5 + 2^7$ .

(b)  $87P = (102, 88)$ .

### 6.20

*Solution:*  $\log_5 896 = 147$  in  $\mathbb{Z}_{1103}$

### 6.21

*Proof.* (a) Since  $a^{(p-1)/2} \equiv 1 \pmod{p}$ , as square root  $a^{(p-1)/4} \equiv \pm 1 \pmod{p}$ .



(b)

$$\begin{aligned}
a &\equiv 1 \cdot a \pmod{p} \\
&\equiv a^{(p-1)/4} \cdot a \pmod{p} \\
&\equiv a^{(p+3)/4} \pmod{p} \\
&\equiv (a^{(p+3)/8})^2 \pmod{p}.
\end{aligned}$$

(c) Since  $p \equiv 5 \pmod{8}$ , we have  $\left(\frac{2}{p}\right) = -1$ , i.e.  $2^{(p-1)/2} \equiv -1 \pmod{p}$ .

$$\begin{aligned}
a &\equiv (-1) \cdot (-1) \cdot a \pmod{p} \\
&\equiv 2^{(p-1)/2} \cdot a^{(p-1)/4} \cdot a \pmod{p} \\
&\equiv 2^{-2} \cdot 4^{(p+3)/4} \cdot a^{(p+3)/4} \pmod{p} \\
&\equiv (2^{-1}(4a)^{(p+3)/8})^2 \pmod{p}.
\end{aligned}$$

(d) Based on above discussions, it's known that it is possible to compute square root modulo  $p$ . Furthermore, since  $p \equiv 5 \pmod{8}$ , we have  $\left(\frac{-1}{p}\right) = 1$ , that is  $L_1(\beta) = L_1(-\beta)$  for all  $\beta \in \mathbb{Z}_p^*$ . So  $L_2(\beta) = L_1(\pm \sqrt{\beta/\alpha^{L_1(\beta)}})$  can be computed efficiently. ■

## 5 Signature Schemes

**7.1**  $p = 31847$ ,  $\alpha = 5$ ,  $\beta = 25703$ ,  $x_1 = 8990$ ,  $(\gamma_1, \delta_1) = (23972, 31396)$ ,  $x_2 = 31415$ ,  $(\gamma_2, \delta_2) = (23972, 20481)$ .

*Solution:* Notice that  $\gamma_1 = \gamma_2$ , and further calculation shows

$$(\delta_1 - \delta_2)^{-1} \equiv 22317 \pmod{p-1},$$

thus

$$\begin{aligned}
a\gamma_1 &= x_2 - \delta_2(x_1 - x_2)/(\delta_1 - \delta_2) \pmod{p-1} \\
&\equiv 23704 \pmod{p-1},
\end{aligned}$$

$a$  has two solutions to this equation, but only one satisfies the equation  $\alpha^a \equiv \beta \pmod{p}$ , that is

$$a \equiv 7459 \pmod{p-1},$$

for  $k$ , we have

$$\begin{aligned} k &= (x_2 - a\gamma_1)\delta_2 \pmod{p-1} \\ &\equiv 1165 \pmod{p-1}, \end{aligned}$$

#### 7.4

*Solution:* (a) All the notations in this exercise are in accordance with those in Section 7.3.

$$\begin{aligned} \beta^\lambda \lambda^\mu &\equiv \beta^\lambda (\gamma^h \alpha^i \beta^j)^{\delta \lambda (h\gamma - j\delta)^{-1}} \pmod{p} \\ &\equiv (\beta^{(h\gamma - j\delta)} \gamma^{h\delta} \alpha^{i\delta} \beta^{j\delta})^{(h\gamma - j\delta)^{-1} \lambda} \pmod{p} \\ &\equiv (\beta^{h\gamma} \gamma^{h\delta} \alpha^{i\delta})^{\lambda (h\gamma - j\delta)^{-1}} \pmod{p} \\ &\equiv (\alpha^{xh} \alpha^{i\delta})^{\lambda (h\gamma - j\delta)^{-1}} \pmod{p} \\ &\equiv \alpha^{x'} \pmod{p}. \end{aligned}$$

(b)

$$\begin{aligned} \lambda &= 363, \\ \mu &= 401, \\ x' &= 385. \end{aligned}$$

#### 7.5

*Solution:* (a)  $\delta = 0$  means  $x \equiv a\gamma \pmod{p-1}$ , and since  $x, \gamma$  are public, it's easy to compute  $a$ .

(b)  $\gamma = 0$  means  $k\delta \equiv x \pmod{q}$ ,  $k$  is thus determined. Using this  $k$  any forgery can be made.

(c) In the ECDSA,  $r = 0$  makes  $k$  is available,  $s = 0$  yields the secret key  $m$ .

#### 7.6

*Solution:* (a)

$$\text{ver}_K(x, (\gamma, \delta)) = \text{true} \Leftrightarrow \beta^\delta \gamma^\gamma \equiv \alpha^x \pmod{p}.$$

(b) One inversion operation in finite field is saved in each procedure of signing.

### 7.10

*Proof.* (a) We only need to show

$$(\alpha^{e_1} \beta^{e_2} \pmod{p}) \pmod{q} = \gamma,$$

where

$$\begin{aligned} e_1 &= x\delta^{-1} \pmod{q} \\ e_2 &= \gamma\delta^{-1} \pmod{q}. \end{aligned}$$

$$\begin{aligned} (\alpha^{e_1} \beta^{e_2} \pmod{p}) \pmod{q} &= (\alpha^{x\delta^{-1}} \beta^{\gamma\delta^{-1}} \pmod{p}) \pmod{q} \\ &= (\alpha^{\lambda^{-1}} \beta^{\gamma x^{-1} \lambda^{-1}} \pmod{q} \pmod{p}) \pmod{q} \\ &= (\alpha \beta^{\gamma x^{-1}})^{\lambda^{-1}} \pmod{q} \pmod{p} \pmod{q} \\ &= ((\alpha \epsilon^\gamma)^{\lambda^{-1}} \pmod{q}) \pmod{p} \pmod{q} \\ &= \gamma \end{aligned}$$

■

### 7.13

*Solution:* (a) The public key  $B = mA = (24, 44)$ .

(b)  $q = 131$ ,  $x = 10$ ,  $k = 75$ ,  $kA = (88, 55)$ ,  $r = 88$ ,  $s = 60$ .

(c)  $w = 107$ ,  $i = 22$ ,  $j = 115$ ,  $iA = (91, 18)$ ,  $jB = (18, 62)$ ,  $iA + jB = (88, 55)$ ,  $u = 88 = r$ .

### 7.14

*Proof.* Obviously.

■

**7.15**  $p = 467$ ,  $\alpha = 4$ ,  $\beta = 449$ ,  $a = 101$ ,  $y = 25$ ,  $x = 157$ ,  $e_1 = 46$ ,  $e_2 = 123$ ,  $f_1 = 198$ ,  $f_2 = 11$ .

*Solution:* Bob's challenges:

$$c = 280$$

$$C = 17.$$

Alice's responses:

$$d = 193$$

$$D = 21.$$

Verification:

$$x^{e_1} \alpha^{e_2} \equiv 22 \not\equiv d \pmod{p}$$

$$x^{f_1} \alpha^{f_2} \equiv 276 \not\equiv D \pmod{p}$$

$$(d\alpha^{-e_2})^{f_1} \equiv 137 \equiv (D\alpha^{-f_2})^{e_1} \pmod{p}. \quad \text{Forgery.}$$

### 7.17

*Solution:* (a)

$$\begin{cases} a_1 = 1118 - 42b_1 \pmod{p} \\ a_2 = 1449 - 42b_2 \pmod{p} \end{cases}$$

(b)

$$\begin{cases} a_1 + 42b_1 = 1118 \pmod{p} \\ a_2 + 42b_2 = 1449 \pmod{p} \\ a_1 + 969b_1 = 899 \pmod{p} \\ a_2 + 969b_2 = 471 \pmod{p} \end{cases}$$

$$\Rightarrow \begin{cases} a_1 = 724 \pmod{p} \\ a_2 = 3109 \pmod{p} \\ b_1 = 2816 \pmod{p} \\ b_2 = 2602 \pmod{p}. \end{cases}$$

### 7.18

*Solution:* (a)

$$\gamma_1 \gamma_2^x \equiv 1943 \pmod{p},$$

$$\alpha^{y_1} \beta^{y_2} \equiv 1943 \pmod{p},$$

so, this signature is valid.

(b)

$$y_1 = 917,$$

$$y_2 = 1983,$$

$$a_0 = 2187.$$