Chapter 1:Clasical Cryptography

February 10,2019

1 Summary

This chapter mainly introduced 7 simple cryptosystems and cryptanalysis of these cryptosystems, as shown in the following table.

$\mathcal{L}$	$\mathcal{P}$	$\mathcal{K}$	$\mathcal{C}$
Language Alphabet	Plaintext Space	Key Space	Cyphertext Space

Cryptosystem	K	E_K
Shift Cipher	$\mathcal{K} = \mathcal{C} = \mathcal{K}$	$E_K(x) = (x + K)\ mod\ \lvert\mathcal{L}\rvert$
Substitution Cipher	$\mathcal{P} = \mathcal{C}, \mathcal{K} = Sym(\lvert\mathcal{L}\rvert)$	$E_\pi(x) = \pi(x)$
Affine Cipher	$\mathcal{P} = \mathcal{C}, \mathcal{K} \subset \mathcal{P} \times \mathcal{P}$	$E_K(x) = (ax + b)\ mod\ \lvert\mathcal{L}\rvert$
Vigenere Cipher	$\mathcal{K} = \mathcal{C} = \mathcal{K}$	$E_K(x_1, x_2, ..., x_m) = (x_1 + k_1, x_2 + k_2, ...$ $, x_m + k_m)\ mod\ \lvert\mathcal{L}\rvert$
Hill Cipher	$\mathcal{P} = \mathcal{C}, \mathcal{K} = GL(n, \mathcal{L})$	$E_K(x) = x \cdot K$
Permutation Cipher	$\mathcal{P} = \mathcal{C}, \mathcal{K} = Sym(m)$	$E_\pi(x_1, x_2, ..., x_m) = (x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(m)})$
Stream Cipher	$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L}, z_{i+m} = \sum_{j=0}^{m-1} c_j z_j$	$E_K(x_j) = x_j + z_j\ mod\ \lvert\mathcal{L}\rvert$

Cryptosystem	Cryptanalysis
Shift Cipher	frequency of occurence of letters
Substitution Cipher	frequency of occurence of letters
Affine Cipher	frequency of occurence of letters
Vigenere Cipher	Kasiski test&computation of indices of coincidence
Hill Cipher	matrx inverse(known plaintext)
Permutation Cipher	matrix inverse(known plaintext)
Stream Cipher	matrix inverse(known plaintext)

2 Excercise

1.5 $Q \to a$, Plaintext: lookupintheairitsabirditsaplaneitssuperman

1.6 $30 = 2 \cdot 3 \cdot 5, \phi(30) = (2-1)(3-1)(5-1) = 8, \lvert\mathcal{K}\rvert = 8 \cdot 30 = 240$
$100 = 2^2 \cdot 5^2, \phi(100) = (4-2)(25-5) = 40, \lvert\mathcal{K}\rvert = 40 \cdot 100 = 4000$
$1225 = 5^2 \cdot 7^2, \phi(1225) = (25-5)(49-7) = 840, \lvert\mathcal{K}\rvert = 840 \cdot 1225 = 1029000$

1.8 m=28: 1,3,5,9,11,13,15,17,19,23,25,27
m=33: 1,2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32
m=35: 1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34

1.10 $(a) : 5^{-1} = 6, d_K(y) = 6y + 1910$
$(b) : d_K(e_K(x)) = 6e_K(x) + 19 = 6(5x + 21) + 19 = 30x + 145 \equiv x\ (mod\ 29)$

1.11 (a)If an encryption function e_K is identical to the decryption function, then the key is called an invulutory key. In this question, it requires $a^{-1} \equiv a, -a^{-1} \cdot b \equiv b\ (mod\ n)$
i.e. $a^{-1} \equiv a, (a+1) \cdot b \equiv 0\ (mod\ n)$
(b) (1,0),(4,0),(4,3),(4,6),(4,9),(4,12),(11,0),(11,5),(11,10),(14,0),(14,1),(14,2),(14,3),(14,4),(14,5),(14,6),(14,7),(14,8),(14,9),(14,10),(14,11),(14,12),(14,13),(14,14)
(c) Applying (a), $a^2 \equiv 1 \Leftrightarrow pq \mid (a+1)(a-1)\ mod\ pq$

Jiayuan Ye, Email:yuan74@mail.ustc.edu.cn
School of Mathematics, University of Science and Technology of China, Hefei, Anhui, 230026, China

$\Leftrightarrow a \equiv \pm 1\ or\ p|(a-1)\&q|(a+1)\ or$ q|(a-1)&p|(a+1)
If $a \equiv 1$, applying (a),we get $2b \equiv 0\ mod\ pq\ \ \because p\ and\ q\ are\ primes, \therefore b \equiv 0\ mod\ pq$, resulting in 1 solutions
If $a \equiv -1, (a+1)b \equiv 0$ always holds, resulting in pq solutions
If $p|(a-1)\&q|(a+1)$, then applying (a), we get p|b$\Rightarrow b = kp, k = 0, 1, ..., q-1$, resulting in q solutions
If $q|(a-1)\&p|(a+1)$, then applying (a), we get q|b$\Rightarrow b = kq, k = 0, 1, ..., p-1$, resulting in p solutions
There are p+q+pq+1 involutary keys in total in total.

1.12 (a) First column is a 2-element vector. It only need to be non-zero vector, resulting in p^2-1 choices.
Second column is a 2-element vector independent of the first column, resulting in p^2-p choices
Combined, we get $(p^2-1)(p^2-p)$ invertible matrices.
(b)# of invertible $m \times m$ matrices over $Z_p = \prod_{k=0}^{m-1}(p^m - p^k)$

1.13 If $n = pq(p\ and\ q\ are\ primes, p \neq q)$, then $\phi(n) = n - p - q + 1$. The first column is a 2-element non-zero vector.Assume $first\ column = (a,b)^T$. Second column can't be linear combination of it.
(1)If $(a,b) \nmid n\ and\ ab \neq 0$, then there're n^2-n choices for the second column,and there're $n^2-(p-1)^2-(q-1)^2-2-2-1 = n^2-(p-1)^2-(q-1)^2-5$ choices of (a,b),resulting in $(n^2-n)[n^2-(p-1)^2-(q-1)^2-5]$ invertible matrices.
(2) if (a,b)=p, then there are n^2-q choices for the second column, resulting in $(q^2-1)(n^2-q)$ invertible matrices.
(3) if (a,b)=q, then there are n^2-p choices for the second column, resulting in $(p^2-1)(n^2-p)$ invertible matrices.
n=6: $6 = 2 \cdot 3,\ (6^2-6)(6^2-1^2-2^2-5)+(3^2-1)(6^2-3)+(2^2-1)(6^2-2) = 1146$
n=9: $9 = 3^2,\ (9^2-9)(9^2-2^2-2^2-5)+(3^2-1)(9^2-3)+(3^2-1)(9^2-3) = 6144$
n=26: $26 = 2 \cdot 13,\ (26^2-26)(26^2-1^2-12^2-5)+(2^2-1)(26^2-2)+(13^2-1)(26^2-13) = 455306$

1.14 (a) calculating determinant both sides$\Rightarrow det(A) = det(A)^{-1} \Rightarrow det(A)^2 \equiv 1\ mod\ 26$
$\Rightarrow det(A) \equiv \pm 1\ mod\ 26$
(b) Applying (a) and Corollary 1.4, we get
If $det(A) \equiv 1$, then $a_{22} = a_{11} = a,\ a_{12} = -a_{21} = b \Rightarrow a^2+b^2 \equiv 1\ mod\ 26$
$\Rightarrow\ 22\ solutions\ for\ (a,b) : (0,1),(1,0),(0,25),(25,0),(2,7),(7,2),(2,19),(19,2),(6,11),(11,6),(6,15),(15,6),(7,24),(24,7),(11,20),(20,11),(12,13),(13,12),(13,14),(14,13),(15,20),(20,15)$
If $det(A) \equiv -1$, then $a_{11} = -a_{22} = a,\ a_{12} = a_{21} = b \Rightarrow a^2+b^2 \equiv 25\ mod\ 26$
$\Rightarrow\ 24\ solutions\ for\ (a,b) : (0,5),(5,0),(0,21),(21,0),(3,4),(4,3),(3,22),(22,3),(4,23),(23,4),(8,13),(13,8),(9,10),(10,9),(9,16),(16,9),(10,17),(17,10),(13,18),(18,13),(16,17),(17,16),(22,23),(23,22)$
So there are 46 involutary keys.

1.15 (a) $det(A) \equiv 17, 17^{-1} \equiv 23, A^{-1} \equiv \begin{pmatrix} 11 & 25 \\ 11 & 20 \end{pmatrix}$
(b) $det(A) \equiv 5, 5^{-1} \equiv 21, A^{-1} \equiv \begin{pmatrix} 25 & 11 & 22 \\ 10 & 13 & 4 \\ 17 & 24 & 1 \end{pmatrix}$

1.16 (a)

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$	2	4	6	1	8	3	5	7

(b) gentlemendonotreadeachothersmail

1.17 (a) represent permutation π by matrix A,$\Rightarrow A = A^T$, then π is involutary, $\Leftrightarrow A = A^{-1} = A^T$
$\Leftrightarrow if\ \pi(i) = (j), then\ \pi(j) = (i)$
(b) Choosing 2j elements to form j pairs that are changed by π, and other elements are not changed.
If m=2k: there are $1 + \sum_{j=1}^{k}\binom{m}{2j}(2j-1)!!$ symmetric matrices
If m=2k+1: there are $1 + \sum_{j=1}^{k}\binom{m}{2j}(2j-1)!!$ symmetric matrices
So, m=2: 2 keys, m=3: 4 keys, m=4: 10 keys, m=5: 41 keys, m=6: 76 keys

1.18 0000: period 1; other keys: period 5

1.19 0000: period 1; other keys: period 6

1.20 K is fixed, so σ_i only depends on σ_{i-1}, z_i only depends on σ_i,since Σ is finite set. According to pegionhole principle, there are at least two elements of the same value in $\{\sigma_0, ..., \sigma_{|\Sigma|}\}$,$\Rightarrow \exists i \neq j, s.t. \sigma_i = \sigma_j$
$\Rightarrow$ sequence σ_i has period at most $|\Sigma|$, keystream z_i has period at most $|\Sigma|$

Jiayuan Ye, Email:yuan74@mail.ustc.edu.cn
School of Mathematics, University of Science and Technology of China, Hefei, Anhui, 230026, China

1.22 (a)If $\exists\ q_i \le q_j$ and $i \le j$, then let $q_i' = q_j, q_j' = q_i \Rightarrow p_iq_i + p_jq_j - p_iq_i' - p_jq_j' = p_iq_i + p_jq_j - p_iq_j - p_jq_i$ $= (p_i - p_j)(q_i - q_j) < 0$, $\therefore \sum_{i=1}^{n} p_iq_i'$ is maximized when $q_1' \ge ... \ge q_n'$

(b) Applying (a), Equation(1.1) is maximized when $\frac{f_{i+g}}{n'} = p_i \Leftrightarrow g = k_i$

1.23 By testing we get m=3, $e_K((x_1,x_2,x_3)) = (x_1,x_2,x_3) \cdot \begin{pmatrix} 3 & 21 & 20 \\ 4 & 15 & 23 \\ 6 & 14 & 5 \end{pmatrix}$

1.24 In number form, we write 0 3 8 18 15 11 0 24 4 3 4 16 20 0 19 8 14 13 $\to$ 3 18 17 12 18 8 14 15 11 23 11 9 1 25 20 11 11 12, subtracting the last 3 number from the first 15 number(3 in a group), we get 18 15 21 10 1 24 18 10 17 21 16 3 12 12 6 $\to$ 18 7 5 1 7 22 3 4 25 12 0 23 16 14 8

Taking the middle 9 elements we get $\begin{pmatrix} 1 & 7 & 22 \\ 3 & 4 & 25 \\ 12 & 0 & 23 \end{pmatrix} = \begin{pmatrix} 10 & 1 & 24 \\ 18 & 10 & 17 \\ 21 & 16 & 3 \end{pmatrix} \cdot L$, where right mat is invertible

$\Rightarrow L = \begin{pmatrix} 3 & 6 & 4 \\ 5 & 15 & 18 \\ 17 & 8 & 5 \end{pmatrix}$

For b part,take the first 3 plaintext $\Rightarrow \begin{pmatrix} 0 & 3 & 18 \end{pmatrix} \cdot L + b \equiv \begin{pmatrix} 3 & 18 & 17 \end{pmatrix} \Rightarrow b = \begin{pmatrix} 20 & 11 & 3 \end{pmatrix}$

1.25 Frequent ciphertext diagram: TX:4, LM:3

Frequent plaintext diagram:th,he,in,er,an,re,ed,on,es,st,en,at,to,nt,ha,nd,ou,ea,ng,as,or,ti,is,et,it,ar,te,se, hi,of.Trough programming, we get in$\to$ TX, th$\to$ LM

plaintext ='thekingwasinhiscountinghousecountingouthismoneythequeenwasintheparloureatingbreadand honeyz'

1.26 (a)ommitted

(b) 42 letters divided into 7 groups(6 letters a group), then for each group, apply this method m=2,n=6

plaintext: marymaryquitecontraryhowdoesyourgardengrow

1.27 (a)(b)ommitted

(c)Applying (b) and evaluate the i-th element of v_h, we get $z_{h+i-1} = \sum_{j=0}^{h-2} \alpha_j z_{j+1+i-1}, i = 1,..,m$

$\Rightarrow z_{h+i-1} = \sum_{j=0}^{h-2} \alpha_j z_{j+i}, i = 1,..,m.$

If i>m, assume $z_{h+k-1} = \sum_{j=0}^{h-2} \alpha_j z_{j+k}\ when\ k < i$

$\Rightarrow z_{h+i-1} = \sum_{j=0}^{m-1} c_j z_{h+i+j-m-1} = \sum_{j=0}^{m-1} c_j \sum_{l=0}^{h-2} \alpha_l z_{l+i+j-m} = \sum_{l=0}^{h-2} \alpha_l \sum_{j=0}^{m-1} c_j z_{l+i+j-m} = \sum_{l=0}^{h-2} \alpha_l z_{l+i}\ mod\ 2$

(d)If $h \le m$, consider initial vector (0,...,0,1), applying (c), we get $z_m = \sum_{l=0}^{h-2} \alpha_l z_{l+m+1-h} = 0\ mod\ 2$

Contradiction to $z_m = 1\ mod\ 2$! $\therefore h = m+1$, the matrix is invertible.

1.28 Testing K from A to Z, we get K=19, plaintext: thereisnotimelikethepresent

1.29 (a) m letters a row, and for i=2,3..., replace the i-th row by: mod($i^{th}\ row - i + 1$,26), then use computation of indices of coincidence just like in vigenere cipher to determine key length and keyword.

(b) 246 characters, (Reminder: key length doesn't have to divide 246)

keylength:5 Using the same method as p.35(textbook), we can get key is PRIME

plaintext:themostfamouscryptologistinhistoryoweshisfamelesstowhathedidthantowhathesaidandtothe sensationalwayinwhichhesaditandthiswasmostperfectlyincharacterforherbertosborneyardleywasperhapsthe mostengagingarticulateandtechnicoloredpersonalityinthebusiness

1.30 K=k, plaintext:thefirstdepositconsistedofonethousandandfourteenpoundsofgold

Jiayuan Ye, Email:yuan74@mail.ustc.edu.cn
School of Mathematics, University of Science and Technology of China, Hefei, Anhui, 230026, China