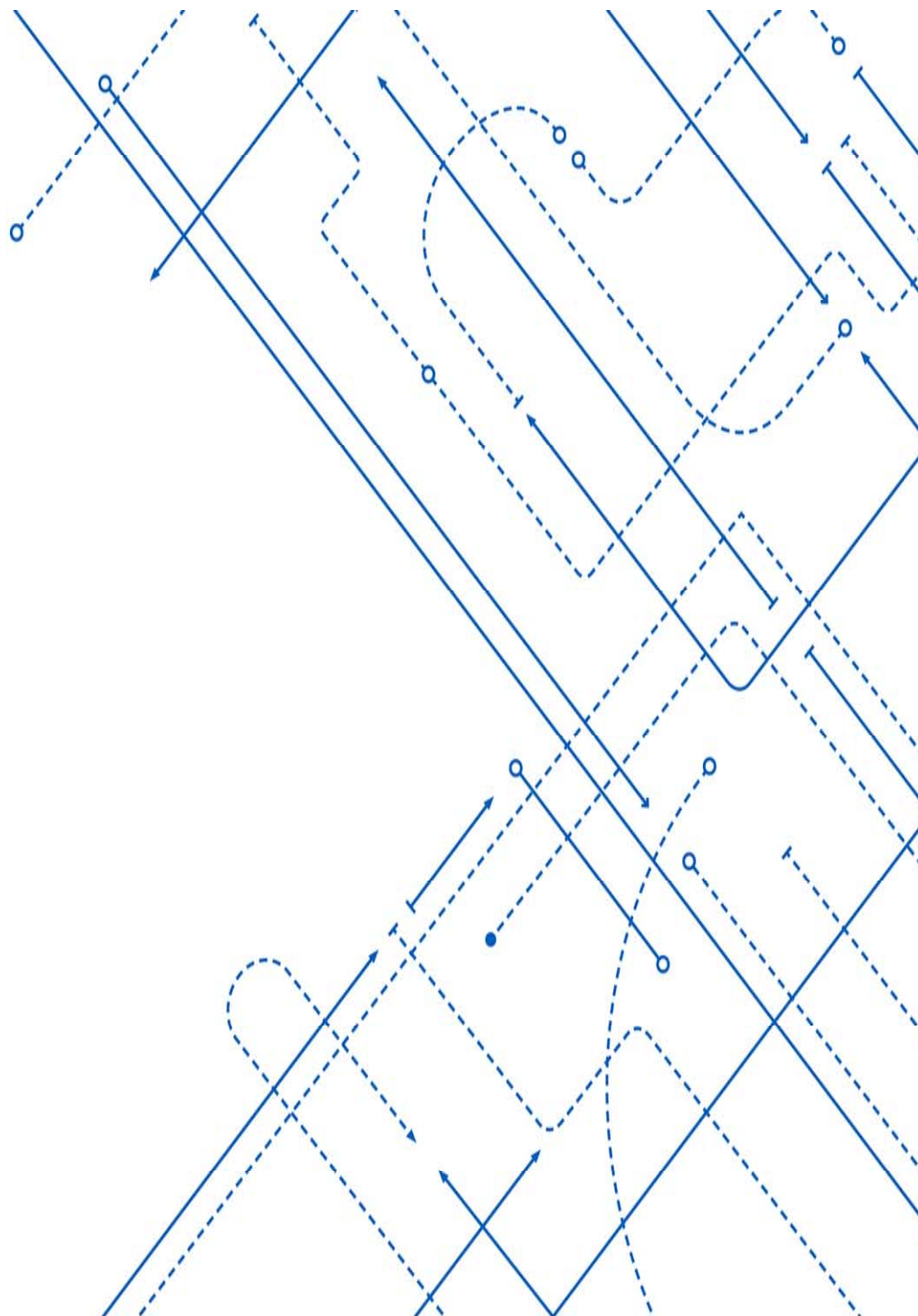


第2章 古典密码



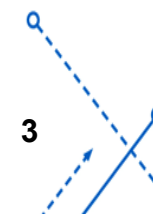
CONTENTS

1/ 单表密码

- 1.1/ 加法密码
- 1.2/ 乘法密码
- 1.3/ 仿射密码
- 1.4/ 简单替换密码

2/ 多表密码

- 2.1/ Playfair
- 2.2/ Vigenere
- 2.3/ Hill
- 2.4/ Enigma



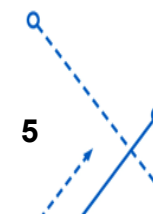
古典密码中的基本加密

- 单表密码体制:
- 对于一个密码体制, 明文字母对应的密文字母在密文中保持不变。
- 多表密码体制:
- 对于一个密码体制, 明文中不同位置的同一明文字母在密文中对应的密文字母不同。



单表密码

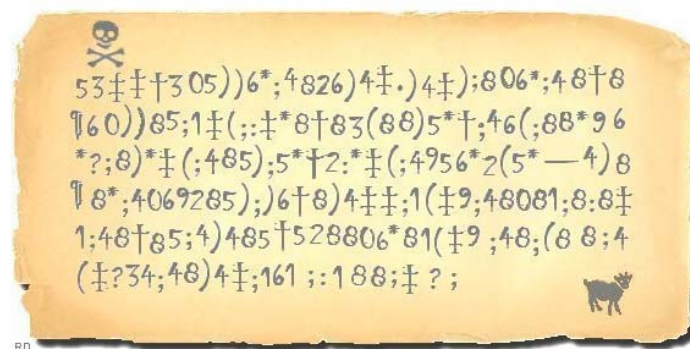
- 单表密码只使用一张密码字母表（Alphabet），且明文字母与密文字母有固定的对应关系。
- 频率分析法可以对付单表密码。
- 小说中出现的单表密码：
 - Edgar Allan Poe "The Gold-Bug"
 - Arthur Conan Doyle "The Dancing Men"



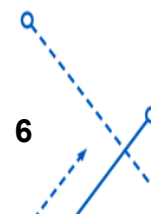
The Gold-Bug

- 《金甲虫》使用了对字母的频率分析来破解简单的换字式密码。
- 文中的密码为：

53†††305))6*;4826)4†.)4†);806*;48†8
 ¶60))85;1†(:;†*8†83(88)5*†;46(;88*96
 ?;8)†(;485);5*†2:*†(;4956*2(5*—4)8
 ¶8*;4069285);)6†8)4††;1(†9;48081;8:8†
 1;48†85;4)485†528806*81(†9;48;(88;4
 (†?34;48)4†;161;;188;†?;



- 在英文中，最频繁出现的字母为e，因此故事中假设密码出现次数最多的8为e。其次，英文中最经常出现的字词为the，基于8等于e的假设，又可以从密码里发现;48共出现了五次之多，故并解读出;等于t及4等h。根据以上的假设及英文特定的语法，便可以解读其他密码的意思。



The Gold-Bug

53‡‡†305))6*;4826)4‡.)4‡);80
agoodglassinthebishopshostel

6*;48†8¶60))85;1‡(;:‡*8†83(88)
inthedevilsseatfortyonedegrees

5*†;46(;88*96*?;8)*‡(;485);5*†
andthirteenminutesnortheastand

2:*‡(;4956*2(5*-4)8¶8*;40692
bynorthmainbranchseventhlimb

85);)6†8)4‡‡;1(‡9;48081;8:8‡1
eastsideshootfromthelifteyeof

;48†85;4)485†528806*81(‡9;48
thedeathshheadabeelinefromthe

; (88;4(‡?34;48)4‡;161;;188;‡?;
treethroughtheshotfiftyfeetout

- A good glass in the bishop's hostel in the devil's seat
- forty-one degrees and thirteen minutes northeast and by north
- main branch seventh limb east side
- shoot from the left eye of the death's-head
- a bee line from the tree through the shot fifty feet out.



The Dancing Men

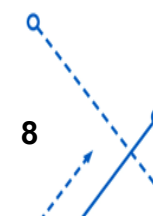
➤ Sherlock Holmes - Arthur Conan Doyle

见犯人扔在桌上的纸团，那就是福尔摩斯曾经用来诱捕他的信。

“华生，你看上面写的是什么？”福尔摩斯笑着说。
信上没有字，只有这样一排跳舞的人：



“如果你使用我解释过的那种密码，”福尔摩斯说，“你会发现它的意思不过是‘马上到这里来’。我相信，他决不会拒绝邀请，因为他想不到除了埃尔茜以外，还有别人能写这样的信。所以，我亲爱的华生，结果，”



希尔顿给福尔摩斯的信

① 

两星期后，在工具间的门上发现

② 

两天后

③ 

三天后

④ 





















































希尔顿发来的另一封信

⑤ 

知乎 @FOUNDC

The Dancing Men

➤ Sherlock Holmes - Arthur Conan Doyle

A	B	C	D	E	F	G	H	I	J	K	L	M
												
												
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
												
												

The Dancing Men

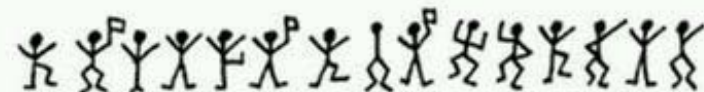


图 1

A M H E R E A B E S L A N E 我已到达。阿贝·斯兰尼



图 2 住在埃尔里奇

A T E L R I G E S



图 3 来，埃尔西

C O M E E L S I E



图 4 绝不

N E V E R

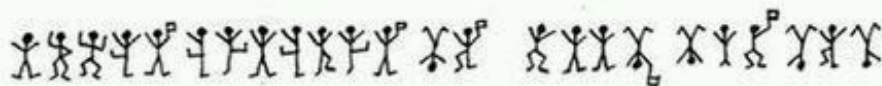


图 5

E L S I E P R E P A R E T O M E E T T H E G O D 埃尔西准备见上帝



图 6 E



加法密码

- 恺撒加密法：替换加密，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。
- 加密时会将明文中的每个字母都按照其在字母表中的顺序向后（或向前）移动固定数目（循环移动）作为密文。例如，当偏移量是左移3的时候（解密时的密钥就是3）：

- 加密算法: $y = (x - 'a' + 3) \% 26 + 'a'$;
- 解密算法: $x = (y - 'a' + 23) \% 26 + 'a'$;

举例：

- 明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
- 密文：WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

序号	加密前		加密后
0	A	→	D
1	B	→	E
2	C	→	F
...
23	X	→	A
24	Y	→	B
25	Z	→	C



恺撒加密法

➤ 根据偏移量的不同，还存在若干特定的恺撒密码名称：

- 偏移量为 10: Avocat (A→K)
- 偏移量为 13: ROT13
- 偏移量为 -5: Cassis (K 6)
- 偏移量为 -6: Cassette (K 7)

➤ 破解：

- 遍历 26 个偏移量，适用于普遍情况。
- 利用词频分析，适用于密文较长的情况。



乘法密码

- 乘法密码需要预先知道消息元素的个数，加密的过程其实是相当于对明文消息所组成的数组下标进行加密，然后用明文消息中加密后位置所对应的明文字符代替。
- 加密过程
 - 设明文消息元素个数为 n ，密钥为 k 。
 - 密钥 k 在选取的时候应满足两个条件：
 - (1) $0 < k < n$
 - (2) k 与 n 互素
 - 设明文消息为 M ，消息元素为 m ;
 - 则密文消息为 C ，密文元素为 $c = m * k \bmod n$;
- 解密过程
 - 首先要得到解密密钥，就是要求得加密密钥 k 模 n 的逆元；
 - 具体求法为 $k * k^{-1} \bmod n = 1$;
 - 然后计算 $m = c * k^{-1} \bmod n$ 即可得到明文消息 M 。



乘法密码-举例

➤ 过程举例

- 英文字母有26个，即 $n=26$;
- $M=m[26]=\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}$;
- 我们选取密钥 $k=5$ ，对hello进行加密：hello所对应的数组为 $[8, 5, 12, 12, 15]$;
- 由于 $8 \times 5 \pmod{26} = 40 \pmod{26} = 14$;
- 依次类推，可得到加密后的数组为 $[14, 25, 8, 8, 23]$ ，对应的密文消息就是nyhhw
- 对nyhhw解密：
- 首先要求得解密密钥 k^{-1} ;
- 由于 $5 \times 21 \pmod{26} = 105 \pmod{26} = 1$ ；所以 $k^{-1} = 21$;
- nyhhw所对应的数组为 $[14, 25, 8, 8, 23]$
- 由于 $14 \times 21 \pmod{26} = 294 \pmod{26} = 8$;
- 依次类推，可得到解密后的数组为 $[8, 5, 12, 12, 15]$ ；对应的明文消息就是hello。



仿射密码

- ▶ 仿射密码为单表加密的一种，字母系统中所有字母都藉一简单数学方程加密，对应至数值，或转回字母。
- ▶ 仿射密码的加密函数是 $E(x) = (ax + b) \pmod{m}$ ，其中
 - ▶ x 表示明文按照某种编码得到的数字
 - ▶ a 和 m 互质
 - ▶ m 是编码系统中字母的数目
- ▶ 解密函数是 $D(x) = a^{-1}(x - b) \pmod{m}$ ，其中 a^{-1} 是 a 在 Z_m 群的乘法逆元。
(其中 $Z_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$)



仿射密码-举例

- 例如 $E(x) = (5x + 8) \bmod 26$ ，加密字符串为 **AFFINE CIPHER**，采用字母表 26 个字母作为编码系统。

明文	A	F	F	I	N	E	C	I	P	H	E	R
x	0	5	5	8	13	4	2	8	15	7	4	17
$y = 5x + 8$	8	33	33	48	73	28	18	48	83	43	28	93
$y \bmod 26$	8	7	7	22	21	2	18	22	5	17	2	15
密文	I	H	H	W	V	C	S	W	F	R	C	P

- 对应的加密结果是 **IHHWVCSWFRCP**



仿射密码-举例

► 解密时，可以计算得到 a^{-1} 为 21，所以解密函数是 $D(x) = 21(x - 8)(\text{mod } 26)$

密文	I	H	H	W	V	C	S	W	F	R	C	P
y	8	7	7	22	21	2	18	22	5	17	2	15
$x = 21(y - 8)$	0	-21	-21	294	273	-126	210	294	-63	189	-126	147
$x \text{ mod } 26$	0	5	5	8	13	4	2	8	15	7	4	17
明文	A	F	F	I	N	E	C	I	P	H	E	R

► 解密得到 AFFINE CIPHER



简单替换密码

- 简单替换密码 (Simple Substitution Cipher) 加密时, 将每个明文字母替换为与之唯一对应且不同的字母。
- 它与恺撒密码之间的区别是其密码字母表的字母不是简单的移位, 而是完全是混乱的, 这也使得其破解难度要高于凯撒密码 (几乎无法暴力破解)。一般采用词频分析破解。
- 举例:
 - 明文字母: abcdefghijklmnopqrstuvwxyz
 - 密钥字母: phqgiumeaylnofdxjkrcvstzwb
- a 对应 p, d 对应 h, 以此类推。
 - 明文: the quick brown fox jumps over the lazy dog
 - 密文: cei jvaql hkdtf udz yvoxr dsik cei npbw gdm



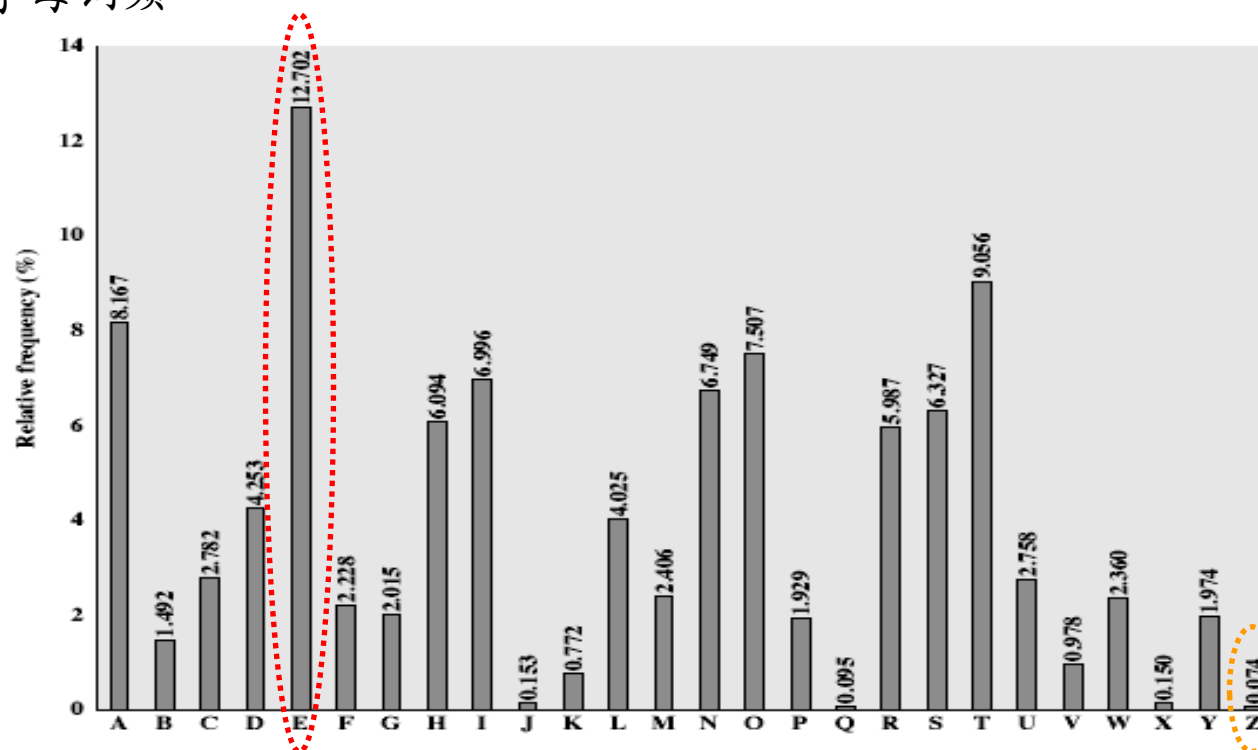
单表古典密码的统计分析

- 单表古典密码体制的密文字母表实际上是明文字母表的一个排列。
- 因此, 明文字的统计特性在密文中能够反映出来。
- 当截获的密文足够多时, 可以通过统计密文字母的出现频率来确定明文字母和密文字母之间的对应关系。



单表古典密码的统计分析

► 英文字母词频



多表密码

- 针对单表代替密码容易被频率分析法破解的缺点，人们提出多表代换密码。
- 多表密码是对每个明文字母采用不同的单表代换，即同一明文字母对应多个密文字母。
- 对于多表替换加密来说，加密后的字母几乎不再保持原来的频率。



Playfair (Playfair cipher or Playfair square)

- 1. 选取一串英文字母，除去重复出现的字母，将剩下的字母逐个逐个加入 5×5 的矩阵内，剩下的空间由未加入的英文字母依 a-z 的顺序加入。注意，将 q 去除，或将 i 和 j 视作同一字。
- 2. 将要加密的明文分成两个一组。若组内的字母相同，将 X（或 Q）加到该组的第一个字母后，重新分组。若剩下一个字，也加入 X。
- 3. 在每组中，找出两个字母在矩阵中的地方。
 - 若两个字母不同行也不同列，在矩阵中找出另外两个字母（第一个字母对应行优先），使这四个字母成为一个长方形的四个角。
 - 若两个字母同行，取这两个字母右方的字母（若字母在最右方则取最左方的字母）。
 - 若两个字母同列，取这两个字母下方的字母（若字母在最下方则取最上方的字母）。
- 新找到的两个字母就是原本的两个字母加密的结果。



Playfair-举例

➤ 例如以 playfair example 为密钥，得

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

➤ 要加密的讯息为 Hide the gold in the tree stump

HI DE TH EG OL DI NT HE TR EX ES TU MP

➤ 就会得到

BM OD ZB XD NA BE KU DM UI XM MO UV IF

Playfair-举例

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

HI

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

BM

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

EG

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

XD

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

DE

Shape: Column
Rule: Pick Items Below Each
Letter, Wrap to Top if Needed

OD

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

OL

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

NA

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

TH

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

ZB

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

EX

Shape: Row
Rule: Pick Items to Right of Each
Letter, Wrap to Left if Needed

XM



维吉尼亚 (Vigenere) 密码

➤ 维吉尼亚密码 (Vigenere) 是使用一系列凯撒密码组成密码字母表的加密算法，属于多表密码的一种简单形式。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



维吉尼亚密码-举例

- 明文: come greatwall
- 密钥: crypto
- 首先, 对密钥进行填充使其长度与明文长度一样。

明文	c	o	m	e	g	r	e	a	t	w	a	l	l
密钥	c	r	y	p	t	o	c	r	y	p	t	o	c

- 其次, 查表得密文

维吉尼亚密码-举例

- 明文: come greatwall
- 密钥: crypto
- 密文: efkt zferrltzn

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	明文
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	

密钥



维吉尼亚密码-举例

- 加密算法: $y = (x + k_i) \% n$;
 - 解密算法: $x = (y - k_i) \% n$;
 - 明文=this crypto system is not secure
(19,7,8,18,2,17,24,15,19,14,...)
 - 密钥=cipher cipher cipher ...
(2,8,15,7,4,17)
 - 密文=vpxzgixiv...
(21,15,23,25,6,8,0,23,8,21,...)
- 't'-'a'=19 明文
 - 'c'-'a'=2 密钥 +)
 - 21
 - $(19+2) \% 26 = 21$
 - $21+'A' = 'v'$ 密文



Hill密码

- 希尔密码 (Hill) 使用每个字母在字母表中的顺序作为其对应的数字, 即 $A=0$, $B=1$, $C=2$ 等。
- 然后将明文转化为 n 维向量, 跟一个 $n \times n$ 的矩阵相乘, 再将得出的结果模 26。
- 注意用作加密的矩阵 (即密钥) 在 \mathbb{Z}_{26}^n 必须是可逆的, 否则就不可能解码。只有矩阵的行列式和 26 互质, 才是可逆的。



Hill密码-举例

➤ 假设明文为 ACT

➤ 将明文化为矩阵:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

➤ 假设密钥为:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

➤ 加密过程为:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \equiv \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

➤ 密文即 POH

Thank you!