北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

《现代密码学》第二讲

古典密码学

BUPT ISC 信息安全中心

上讲内容回顾

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 密码学安全属性
- 密码学分类

加密术语

- 明文(plaintext/message)：是加密之前的字符、符号；
- 密文(ciphertext)：是加密之后的字符、符号；
- 密钥(key)：是在明文转换为密文或将密文转换为明文的算法中输入的参数；
- 加密(encryption)：以某种特殊的算法改变原有的（明文）信息数据过程；
- 解密(decryption)：是从密文恢复出原有的（明文）信息数据的过程。

字母数字对照表

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

本章主要内容

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 代换密码
- 置换密码
- Hill密码
- 转轮密码
- 代换密码的惟密文攻击

本章主要内容

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 代换密码
- 置换密码
- Hill密码
- 转轮密码
- 代换密码的惟密文攻击方法

密码分类

- 代换密码（ substitution ）：代换是古典密码中用到的最基本的处理技巧之一。所谓代换，就是将明文中的一个字母由其它字母、数字或符号替代的一种方法。又分为：
  - 移位(凯撒)密码
  - 仿射密码
  - 单表代换
  - 多表代换

移位（凯撒）密码

- 数学描述

明文p $\in Z_{26}$，密文c $\in Z_{26}$，密钥k取[1,25]

$$加密：c = E(p) = (p + k) \bmod 26$$

$$解密：p = D(c) = (c - k) \bmod 26$$

- 代换表（密钥） k=3

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
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

凯撒密码

例:令k=3，或使用上述代换表加解密

明文：meet me after the party

密文：PHHW PH DIWHU WKH SDUWB

仿射密码

- 数学描述

明文$p \in Z_{26}$，密文$c \in Z_{26}$，

密钥$k=(a, b) \in Z_{26}^{*} \times Z_{26}$ 且$\gcd(a, 26)=1$.

加密：$c = E(p) = (a \times p + b) \bmod 26$

解密：$p = D(c) = (c - b) \times a^{-1} \bmod 26$

仿射密码

例：令密钥$k=(7, 3)$， 且gcd(7, 26)=1.

明文hot=(7, 14, 19)

加密：

$(7 \times 7 + 3) \bmod 26 = 0$

$(7 \times 14 + 3) \bmod 26 = 23$

$(7 \times 19 + 3) \bmod 26 = 6$

密文为(0, 23, 6)=(a, x, g)

解密：$7^{-1}=15=-11 \bmod 26$

$(0- 3) \times 15 \bmod 26 = 7$

$(23- 3) \times 15 \bmod 26 = 14$

$(6- 3) \times 15 \bmod 26 = 19$

明文为(7, 14, 19)=(h, o, t)

单表代换密码

- 数学描述

明文$p \in Z_{26}$，密文$c \in Z_{26}$，

密钥$k \in$ {Π | 定义在0, 2, …, 25上的置换}

加密

$$c = k(p)$$

解密

$$p = k^{-1}(c).$$

单表代换密码

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

例：

加密函数：

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

解密函数：

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
s	g	m	a	k	e	x	o	f	h	b	v	q	z	u	j	d	w	l	p	t	c	i	n	r	y

明文: **if we wish to replace letters**

密文: **WI RF RWAJ UH YFTSDVF SFUUFYA**

BUPT ISC 信息安全中心

多表代换密码

- 简化多表代换密码-维吉尼亚密码(Vigenère Cipher):由26个类似 Caesar密码的代换表组成

- 维吉尼亚密码数学描述:

  明文$p \in Z_{26}$，密文$c \in Z_{26}$，密钥$k \in (Z_{26})^m$

  加密

  $c=(p_1+k_1, p_2+k_2, \ldots, p_m+k_m, p_{m+1}+k_1, \ldots) \bmod 26;$

  解密

  $p=(c_1-k_1, c_2-k_2, \ldots, c_m-k_m, c_{m+1}-k_1, \ldots) \bmod 26.$

多表代换密码

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

例：

	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

Key:
GOOGLE
Plaintext:
BUYYOUTUBE
Ciphertext:
HIMEZYZIPK

本章主要内容

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 代换密码
- 置换密码
- Hill密码
- 转轮密码
- 代换密码的惟密文攻击

置换密码

- 置换密码（permutation）：是古典密码中用到的另一个最基本的处理技巧。将明文字符按照某种规律重新排列而形成密文的过程。
- 数学描述

明文$p \in (Z_{26})^m$，密文$c \in (Z_{26})^m$，

密钥$k \in \{\Pi \mid$定义在$1, 2, \ldots, m$上的置换$\}$

加密

$c = (p_{\Pi(1)}, p_{\Pi(2)}, \ldots, p_{\Pi(m)})$；

解密

$p = (c_{\Pi^{-1}(1)}, c_{\Pi^{-1}(2)}, \ldots, c_{\Pi^{-1}(m)})$.

置换密码

例：密钥

x	1	2	3	4	5	6
Π(x)	3	5	1	6	4	2
x	1	2	3	4	5	6
Π^{-1}(x)	3	6	1	5	2	4

明文：she sells sea shells by the shore

分组：shesel lsseas hellsb ythesh

ore ‘z’ ‘z’ ‘z’

置换：EESLSH SALSES LSHBLE HSYHET E ‘z’ O ‘z’ ‘z’ R

本章主要内容

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 代换密码
- 置换密码
- Hill密码
- 转轮密码
- 代换密码的惟密文攻击

希尔密码（Hill cipher）

1929年，LesterS. Hill提出

明文$p \in (Z_{26})^m$，密文$c \in (Z_{26})^m$，
密钥$K \in$ {定义在Z_{26}上$m \times m$的可逆矩阵}

加密

$$c = p * K \bmod 26$$

解密

$$p = c * K^{-1} \bmod 26$$

希尔密码

例:令明文为hi=(7, 8)

密钥:

$$K=\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix} \qquad K^{-1}=\begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}$$

加密:

$$\begin{pmatrix}7 & 8\end{pmatrix}\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}=(77+24 \quad 56+56)=(23 \quad 8)=(x \quad i)$$

解密:

$$\begin{pmatrix}23 & 8\end{pmatrix}\begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}=(161+184 \quad 414+88)=(7 \quad 8)=(h \quad i)$$

希尔密码（Hill cipher）

课堂练习：

- WE(22 4)　---移位→ ？
- HE(7 4)　---移位→ ？

- WE(22 4) ---Hill → ？
- HE(7 4)　---Hill → ？

本章主要内容

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 代换密码
- 置换密码
- Hill密码
- **转轮密码**
- 代换密码的惟密文攻击

转轮密码（Rotor Machine）

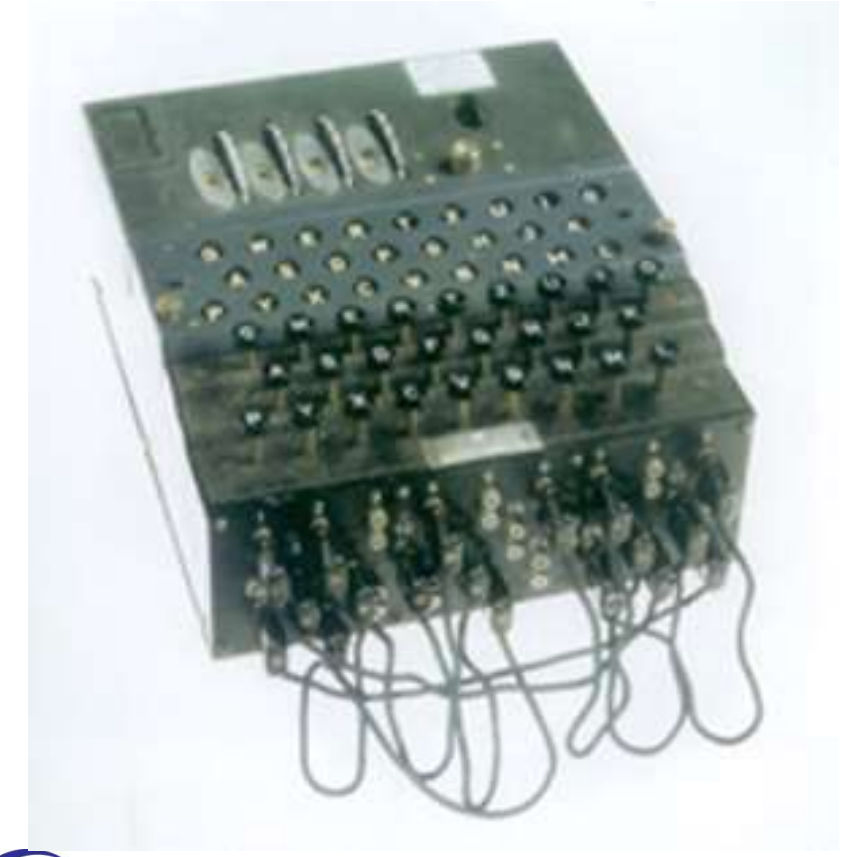
- 19世纪20年代，开始出现机械加解密设备，最典型的是转轮密码机

- 1918年Arthur Scherbius发明的EIGMA，瑞典Haglin发明的Haglin，和日军发明的“紫密”和“兰密”都属于转轮密码机。

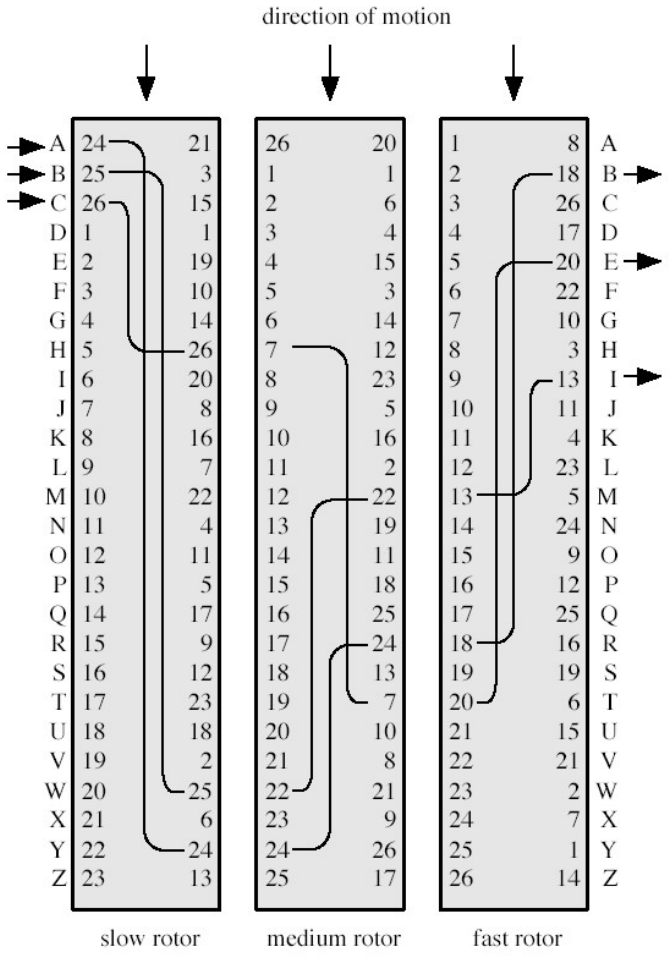
转轮密码

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

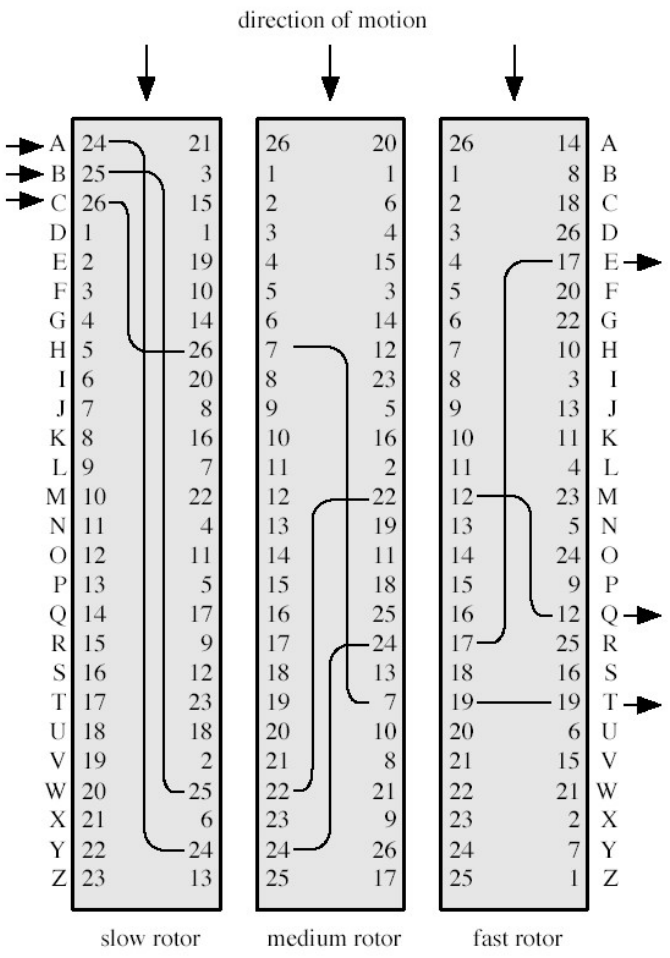
Enigma密码机



转轮密码



(a) Initial setting



(b) Setting after one keystroke

本章主要内容

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

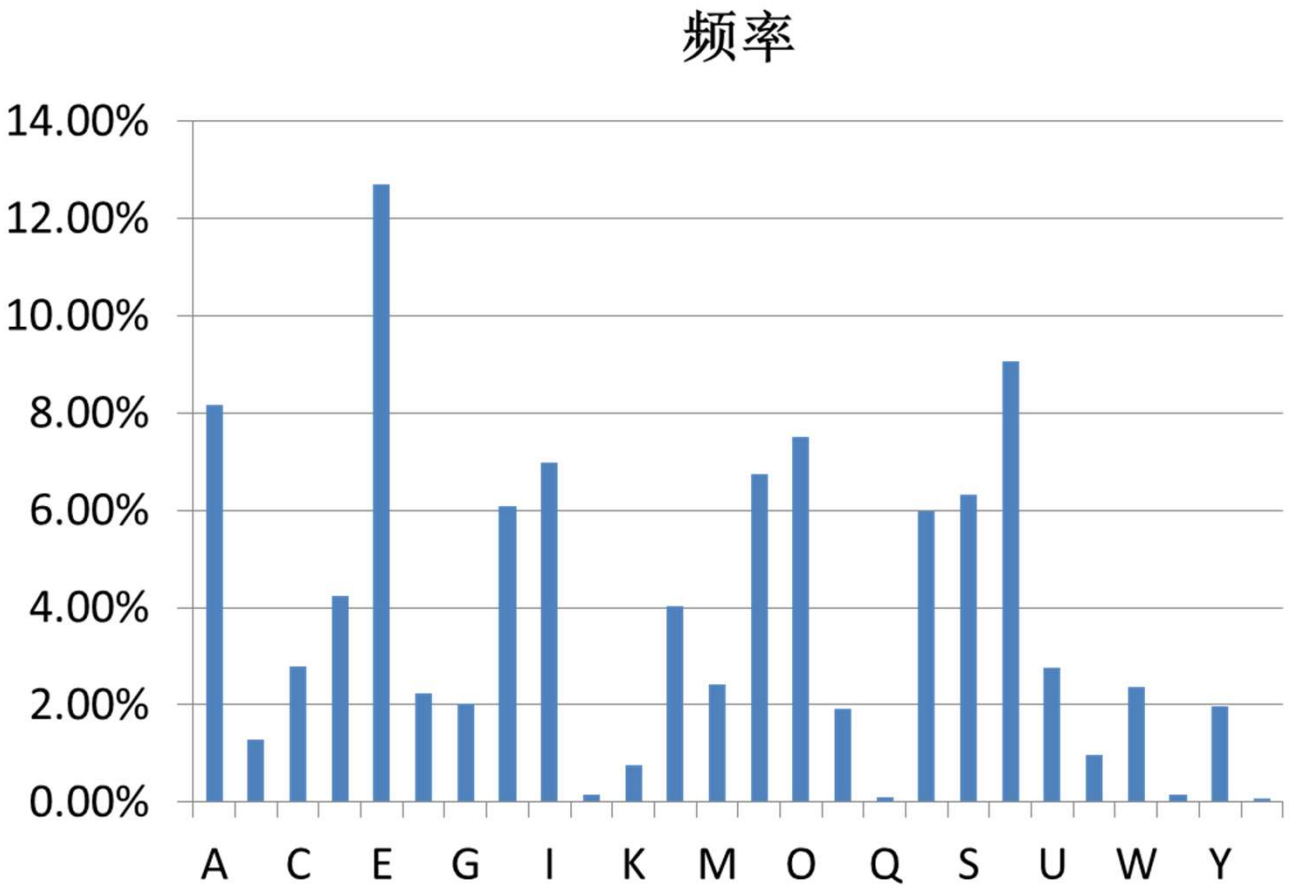
- 代换密码
- 置换密码
- Hill密码
- 转轮密码
- 代换密码的惟密文攻击

惟密文攻击

人类的语言存在冗余，以英文文档为例：

- 字母 e 是使用频率最高的
- 其次是 T, R, N, I, O, A, S
- Z, J, K, Q, X 很少使用
- A、I、U很少用在词尾，E、N、R常出现在词尾。E、S、D作为字母结尾字母的单词超过一半，T、A、S、W为起始字母的单词约占一半。

惟密文攻击



a	8.17%
b	1.49%
c	2.78%
d	4.25%
e	12.70%
f	2.23%
g	2.02%
h	6.09%
i	6.97%
j	0.15%
k	0.77%
l	4.03%
m	2.41%
n	6.75%
o	7.51%
p	1.93%
q	0.10%
r	5.99%
s	6.33%
t	9.06%
u	2.76%
v	0.98%
w	2.36%
x	0.15%
y	1.97%
z	0.07%

惟密文攻击

对于双字母组合，三字母组合：

Single Letter	Double Letter	Triple Letter
E	TH	THE
T	HE	AND
R	IN	TIO
N	ER	ATI
I	RE	FOR
O	ON	THA
A	AN	TER
S	EN	RES

惟密文攻击

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 统计攻击（频率攻击）
  - 假设：根据统计规律分析假设某些结论。
  - 推断：在假设的前提下，推断出一些结论。
    - ✓双频
    - ✓字母跟随关系
    - ✓构词规则
    - ✓词义
  - 验证发展：填上破译出的字母，根据词义、构词规则不断发展 。

惟密文攻击

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 移位密码、仿射密码和单表代换密码都没有破坏明文的频率统计规律，可以直接用统计分析法
- 例：

  截取一段仿射密码的密文 $c=ap+b \mod 26$

  FMXVEDKAPHFERBNDKRXRSREFMOR

  UDSDKDVSHVUFEDKAPRKDLYEVLRHHRH

惟密文攻击

统计得到R(8),D(7),E,H,K(5),S,F,V(4)

密文出现字母频率统计

字母	频率	字母	频率	字母	频率	字母	频率
A	2	H	5	O	1	U	2
B	1	I	0	P	2	V	4
C	0	J	0	Q	0	W	0
D	7	K	5	R	8	X	2
E	5	L	2	S	3	Y	1
F	4	M	2	T	0	Z	0
G	0	N	1				

惟密文攻击

- 令R=E(e)，D=E(t)，得到方程组

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$\begin{cases} 4a + b = 17 \\ 19a + b = 3 \end{cases}$$

解得a=6 ， b= 19 ；

其中gcd(6, 26)=2>1，故猜测错误。

惟密文攻击

1、令R=E(e)， E=E(t)？ a=13

2、R=E(e)， H=E(t)？ a=8

3、R=E(e)， K=E(t)， a=3,b=5,

第3组解有效，则解密函数$p=(c-5)*3^{-1}=9c-19$

解密得明文：algorithms are quite general definitions of arithmetic processes.

惟密文攻击

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

练习：

已知用户用移位密码加密，密文为“KHOOR,HYHUB RQH”，用统计法求密钥和对应明文

- 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
- 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

H(4),O,R(2),K(1),Q(1),Y(1),U(1),B(1)

H-------e，也就是e+x=h得4+x=7，密钥为3

解密：hello, every one

惟密文攻击

维吉尼亚密码由m个移位密码构成，移位密码不改变字符的分布，故若能确定m，则可以找到每个移位密码的位移量k

- 克思斯基测试（Kasiski ）
  - 若用给定的m个密钥表周期地对明文字母加密，则当明文中有两个相同字母组(长度大于3)在明文序列中间隔的字母数为m的倍数时，这两个明文字母组对应的密文字母组必相同。
  - 但反过来，若密文中出现两个相同的字母组，它们所对应的明文字母组未必相同，但相同的可能性很大。
  - 将密文中相同的字母组找出来，并对其相同字母数综合研究，找出它们的相同字母数的最大公因子，就有可能提取出有关密钥字的长度m的信息。

惟密文攻击

例：

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBJJCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE

CHR出现5个位置：1,166,236,276,286

距离差：165,235,275,285，gcd(165,235,275,285)=5

猜测 m=5

惟密文攻击

重合指数法（Coincidence Index）

设一门语言由n个字母构成，每个字母发生的概率为p_i，其中$1 \le i \le n$,则重合指数指其中两个随机元素相同的概率的和，记为$CI = \sum_{i=1}^{n} {p_i}^2$

- 例如：完全随机文本CI =0.0385

$$26\left(\frac{1}{26}\right)^2 = 0.0385$$

- 有信息冗余的英文文本CI =0.065

惟密文攻击

- 实际使用CI的估计值CI’：
  - L：密文长。
  - fi：密文符号i发生的数目。

$$CI' = \sum_{i=1}^{n} \frac{f_i}{L} \frac{f_i - 1}{L - 1}$$

惟密文攻击

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

1. 对于不同的m, 重新对密文m分组

$$\vec{y} = \vec{y}_1\vec{y}_2\cdots\vec{y}_m = \begin{cases} y_1 y_{m+1}\cdots y_{km+1} \\ y_2 y_{m+2}\cdots y_{km+2} \\ \cdots\cdots \\ y_m y_{2m}\cdots y_{(k+1)m} \end{cases}$$

2. 对不同的分组，分别求取重合指数

0.046196	0	0	0	0	0	0	0	0	0
0.048129	0.043472	0	0	0	0	0	0	0	0
0.044211	0.047018	0.041053	0	0	0	0	0	0	0
0.042607	0.0401	0.051378	0.043233	0	0	0	0	0	0

当m为5时，重合指数平均接近于0.065

0.033333	0.036667	0.03	0.04	0.053333	0.033333	0.026667	0.036667	0.026667	0
0.064935	0.069264	0.08658	0.04329	0.090909	0.064935	0.056277	0.073593	0.069264	0.103896

惟密文攻击

- 其它作用：
  - 区分单表代换密码和多表代换密码

单表代换密码的统计规律和自然语言的概率相似；多表代换则会发生很大变化，与随机文本的分布概率近似

  - 确定两段文本是否是同一种方法进行加密

同一加密方法，则CI应该近似

惟密文攻击

例：

CI’ (C1)=0.0412

k o o m m a c o m o q e g l x x m q c c k u e y f c u r
y l y l i g z s x c z v b c k m y o p n p o g d g i a z t x d
d i a k n v o m x h i e m r d e z v x b m z r n l z a y q
i q x g k k k p n e v h o v v b k k t c s s e p k g d h x y
v j m r d k b c j u e f m a k n t d r x b i e m r d p r r j
b x f q n e m x d r l b c j h p z t v v i x y e t n i i a w d
r g n o m r z r r e i k i o x r u s x c r e t v

CI’ (C2)=0.0445

z a o z y g y u k n d w p i o u o r i y r h h b z x r c e a
y v x u v r x k c m a x s t x s e p b r x c s l r u k v b
x t g z u g g d w h x m x c s x b i k t n s l r j z h b x m
s p u n g z r g k u d x n a u f c m r z x j r y w y m i

同一加密方法

惟密文攻击

- 拟重合指数法

  Chi测试

$$\chi = \sum_{i=1}^{n} p_j q_j$$

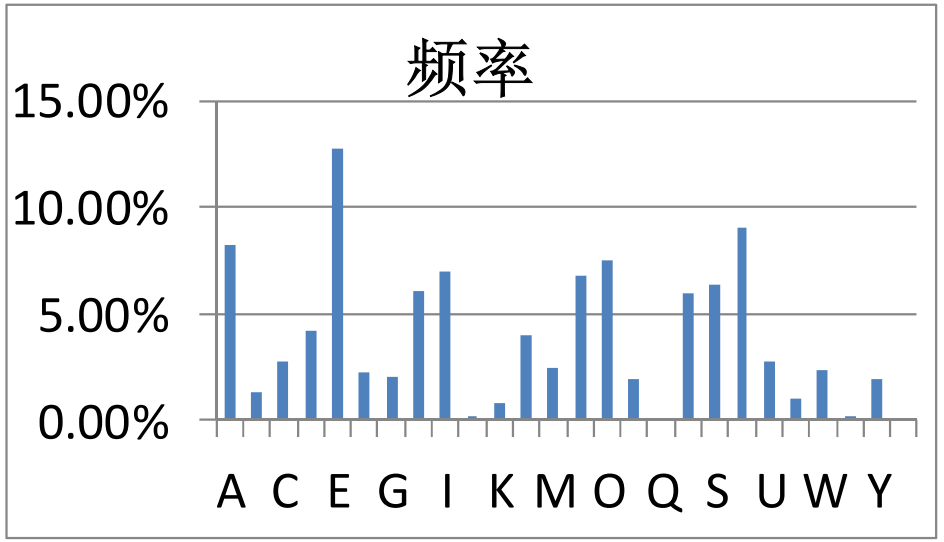
p_j: 第j个符号在第一个分布中发生的概率

q_j: 第j个符号在第二个分布中发生的概率

当两个频率分布类似时，χ值相对较高

惟密文攻击

- 对于一个移位密码



1. 统计每个字母的频数：

$A{:}f_0, B{:}f_1, C{:}f_2, \ldots, Z{:}f_{25}$

2. 令密文长度为n′ = n/m， 26个字母的概率分布：

$$A: p_0 = \frac{f_0}{n'}, B: p_1 = \frac{f_1}{n'}, C: p_2 = \frac{f_2}{n'}, \cdots, Z: p_{25} = \frac{f_{25}}{n'}$$

3. 获得通常文本的字母概率分布**Q**：

$$A{:}q_0, B{:}q_1, C{:}q_2, \ldots, Z{:}q_{25}$$

惟密文攻击

4. 对概率分布$p_0,p_1,\ldots,p_{25}$进行移位i (0≤i≤25)，得到序列

$$P_i = p_{0-i \pmod{26}}, p_{1-i \pmod{26}}, \cdots, p_{25-i \pmod{26}}$$

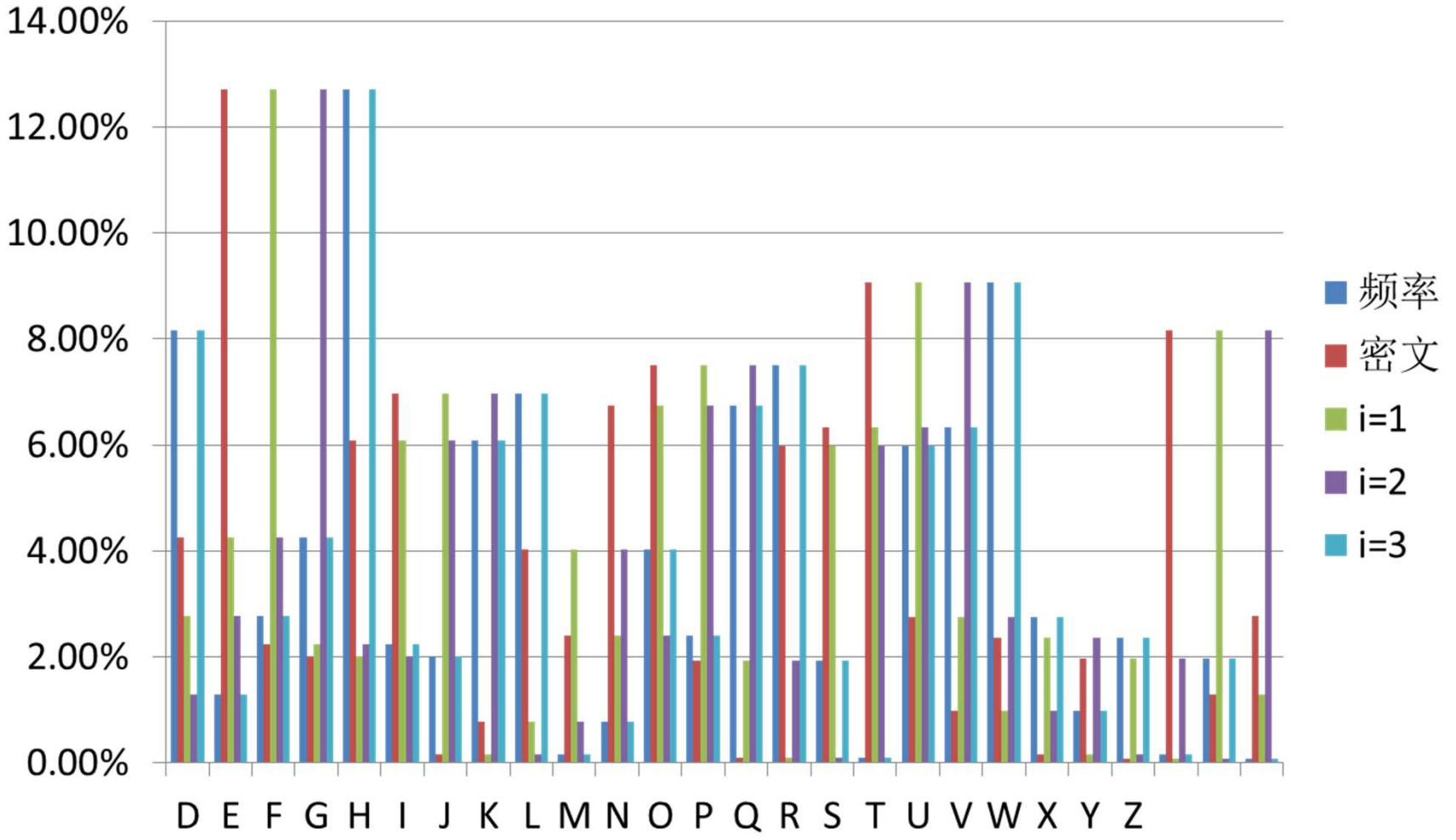
5. 对分布P_i和Q计算相关卷积

$$Correlation(P_i, Q) = \sum_{j=0}^{25} p_{(j-i) \bmod 26} q_j$$

6. 最大相关值$Correlation(P_i, Q)$

- 对应的位移量i，即为密钥估计值

惟密文攻击


14.00%
12.00%
10.00%
8.00%
6.00%
4.00%
2.00%
0.00%
D E F G H I J K L M N O P Q R S T U V W X Y Z
频率
密文
i=1
i=2
i=3

惟密文攻击

CHREE
VOAHM
AERAT
BIAXX
WTNXB
EEOPH
BSBQM
QEQER
BWRVX
UOAKX
AOSXX
WEAHB
WGJMM
QMNKG
RFVGX

WTRZX
WIAKL
XFPSK
AUTEM
NDCMG
TSXMX
BTUIA
DNGMG
PSREL
XNJEL
XVRVP
RTULH
DNQWT
WDTYG
BPHXT

FALJH
ASVBF
XNGLL
CHRZB
WELEK
MSJIK
NBHWR
JGNMG
JSGLX
FEYPH
AGNRB
IEQJT
AMRVL
CRREM
NDGLX

RRIMG
NSNRW
CHRQH
AEYEV
TAQEB
BIPEE
WEVKA
KOEWA
DREMX
MTBHH
CHRTK
DNVRZ
CHRCL
QOHPW
QAIIW

XNRMG
WOIIF
KEE

惟密文攻击

提取第一列：

C	W	F	R	X
V	W	A	N	W
A	X	X	C	K
B	A	C	A	
W	N	W	T	
E	T	M	B	
B	B	N	W	
Q	D	J	K	
B	P	J	D	
U	X	F	M	
A	X	A	C	
W	R	I	D	
W	D	A	C	
Q	W	C	Q	
R	B	N	Q	

计算

p0=7/63
p1=6/63
p2=6/63
p3=4/63
p4=1/63
p5=2/63
p6=0
p7=0
p8=1/63
p9=2/63
p10=2/63
p11=0
p12=2/63
p13=4/63
p14=0
p15=1/63
p16=4/63
p17=3/63
p18=0
p19=2/63
p20=1/63
p21=1/63
p22=9/63
p23=5/63
p24=0
p25=0

惟密文攻击

计算：

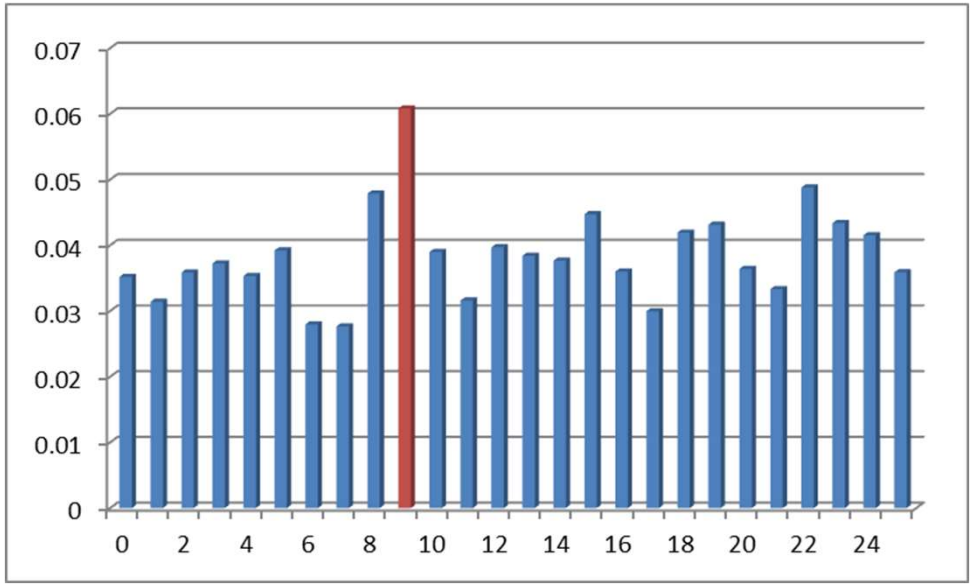
$Correlation(P_0, Q)$

$Correlation(P_1, Q)$

…

$Correlation(P_{25}, Q)$

从而得到



得到最高标记为9，取出值9，赋值给k1，即k1=J(9)

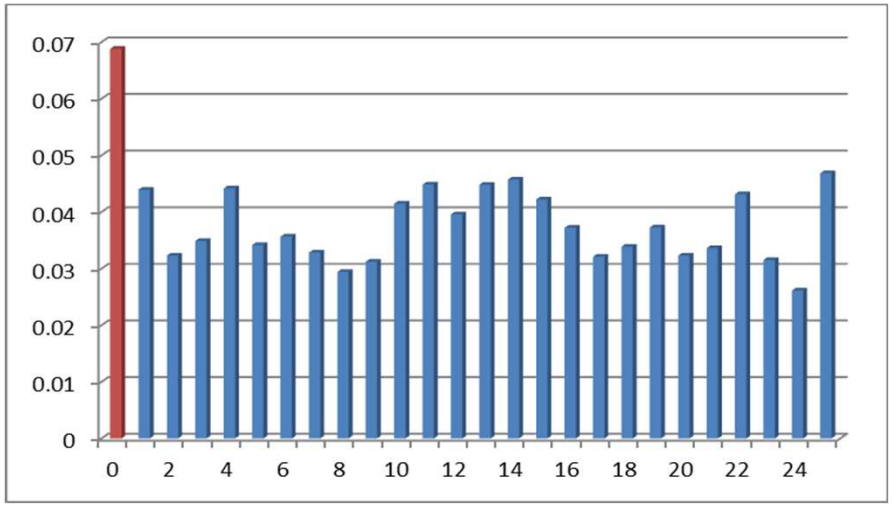
然后，解密pi=ci-k1，进行字母替换，得到第一列字母，解密得到如下明文：

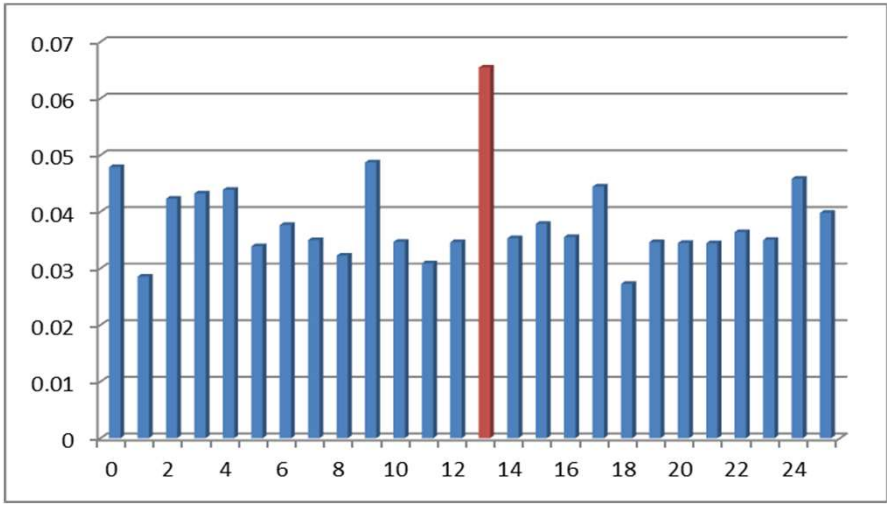
惟密文攻击

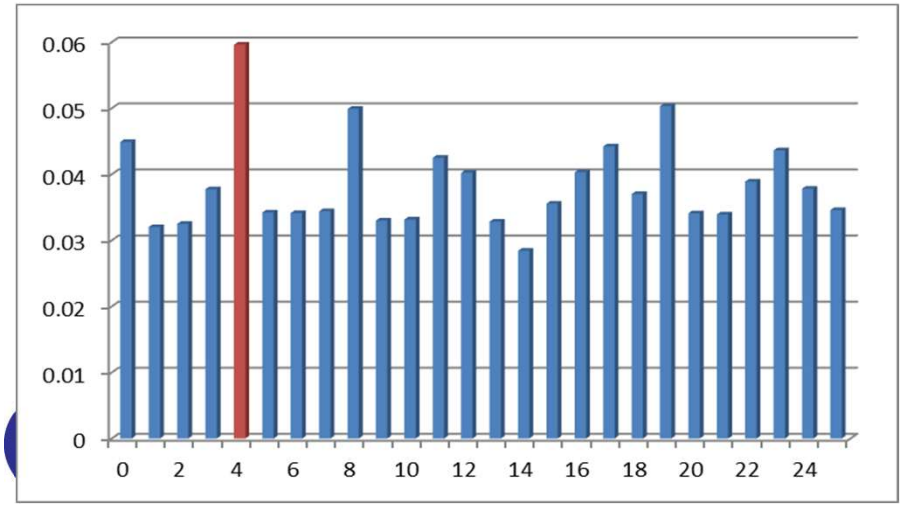
T	hi	u	E	e	h
M	i	g	A	I	h
R	n	o	a	E	o
S	n	o	w	T	N
N	o	i	r	R	b
V	r	u	z	K	
s	e	n	r	s	
h	k	s	t	n	
s	s	w		b	
l		r		u	
r		o		d	
n		T		t	
n		N		u	
		D		t	

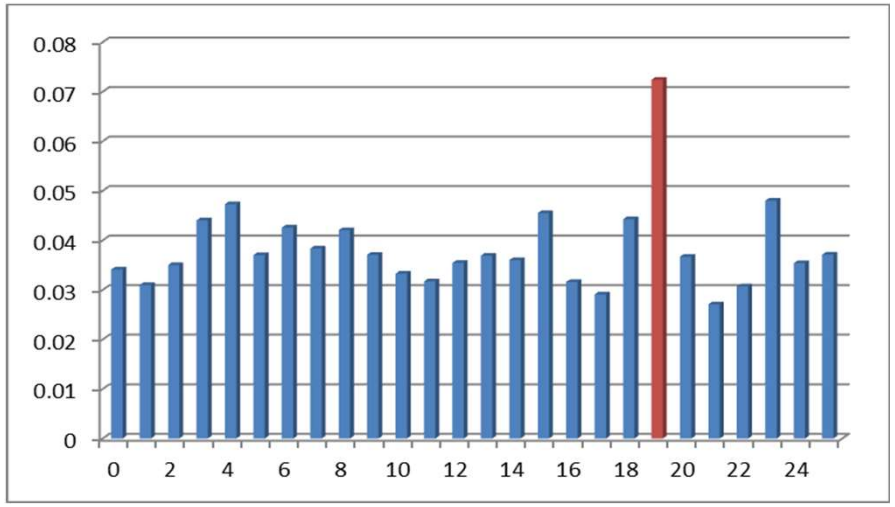
密文子串的拟重合指数

同理，可得到其他四列的值，取出相应的值









明文

K2=A(0)，　K3=N(13)，　K4=E(4)，　K5=T(19)最终得到如下明文：

The almond tree was in tentative blossom. The days were longer, often ending with magnificent evenings of corrugated pink skies. The hunting season was over, with hounds and guns put away for six months. The vineyards were busy again as the well-organized farmers treated their vines and the more lackadaisical neighbors hurried to do the pruning they should have done in November.

惟密文攻击

- 移位密码、仿射密码和单表代换密码都没有破坏明文的频率统计规律，可以直接用统计分析法

- 维吉尼亚密码
  - Kasiski测试或者重合指数确定密钥长度m
  - 密文按m分组后，利用拟重合指数分析得到每个单表的密钥
  - 利用单表密钥恢复明文

主要知识点小结

- 代换密码
- 置换密码
- Hill密码
- 转轮密码
- 代换密码的惟密文攻击

THE END !