第二讲　常规加密

--- 经典密码

上海交通大学安全学院
郑燕飞

第二讲的主要内容

- 经典密码
  - 替代技术
  - 置换技术
- 分组密码的原理
  - Feistel密码
- DES
  - DES加密
  - DES分析
- 分组密码的设计准则

替代和置换

* 替代技术

  明文字母由其他字母或数字或符号所代替

* 置换技术

  对明文字母的某种置换取得一种类型完全不同的映射

恺撒密码

- 恺撒密码——把字母表中的每个字母用该字母后面第三个字母进行代替
  - 明文：
  - 密文：
- 一个例子：
  - 明文：we are students
  - 密文：zhduhvwxghqwv
- 恺撒密码的数学表示

$$c = E(m,k) = (m + k) \bmod q$$

$$m = D(c,k) = (c - k) \bmod q$$

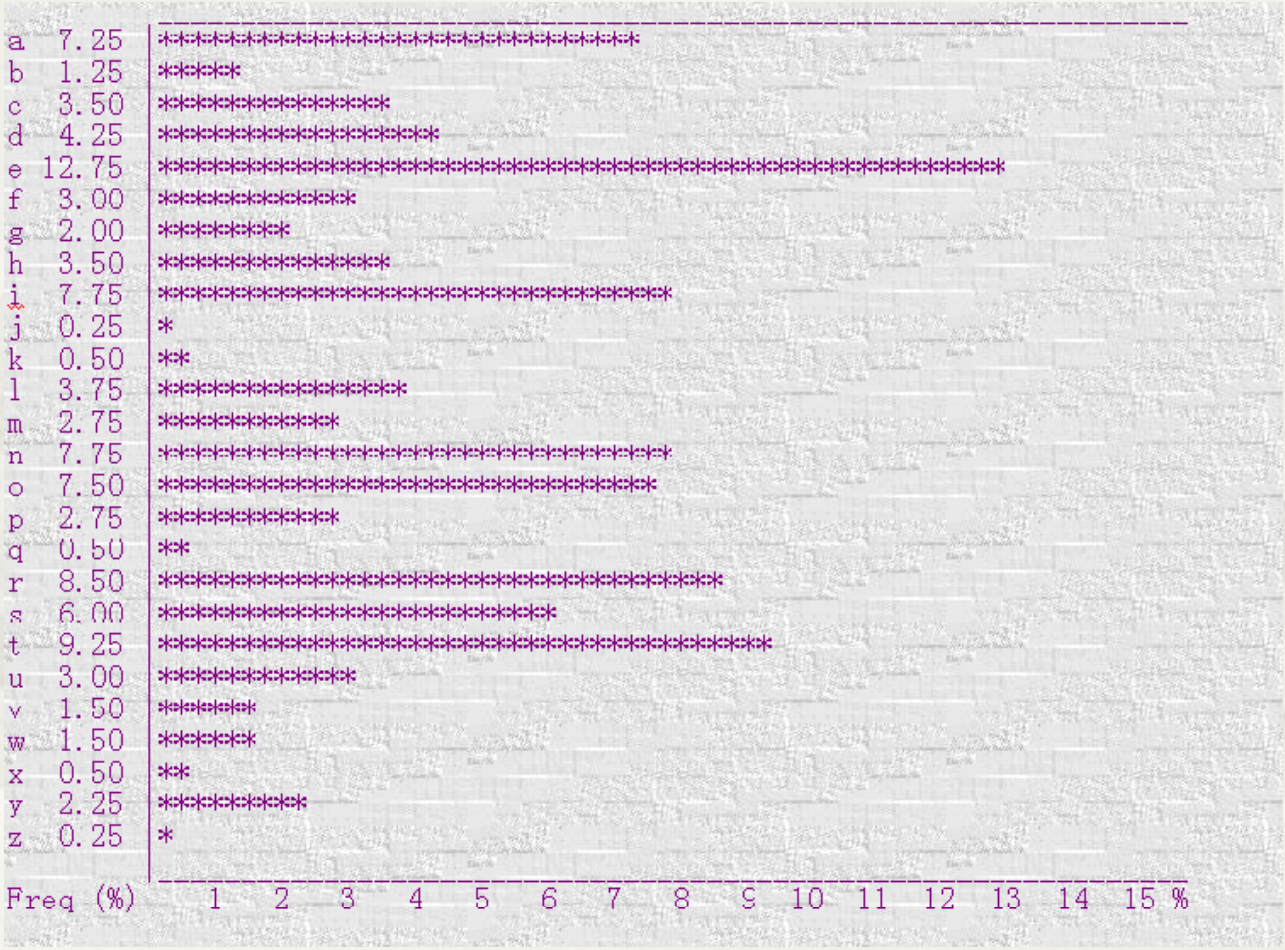
恺撒密码

- 对恺撒密码进行强行攻击密码分析
  - 加密和解密算法已知
  - 密钥空间大小为25
  - 明文容易识别攻击
- 增大恺撒密码的密钥空间
  - 简单方法给出密钥
  - 写出密钥（删除重复字母）
  - 在其下面以次写出剩余字母（行列）
  - 按列读取字母得到密文
- 利用语言的规律性

密码分析

- 人类语言有冗余度
- 字母使用频率不相同
- 在英文中，e的使用率最高
- 其次，T,R,N,I,O,A,S
- 其他字母使用频率较低
- 密文反应了明文字母出现的规律性

英文字母使用频率


a 7.25
b 1.25
c 3.50
d 4.25
e 12.75
f 3.00
g 2.00
h 3.50
i 7.75
j 0.25
k 0.50
l 3.75
m 2.75
n 7.75
o 7.50
p 2.75
q 0.50
r 8.50
s 6.00
t 9.25
u 3.00
v 1.50
w 1.50
x 0.50
y 2.25
z 0.25
Freq (%)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 %

英文字母中常见的组合

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

Playfair密码

- 构造关键字矩阵如下：

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

Playfair密码

- 加密规则
  - 处理明文,填充字母
    - Balloon —》ba lx lo on
  - 同行字母替代
  - 同列字母替代
  - 非同行同列字母替代
- 分析
  - 26×26种字母组合
  - 频率分析变得困难

Hill密码

- m个连续明文字母被m个密文字母代替
- 由m个线性方程决定替代方法
- m=3时的系统描述：
  - 编码（a=0,b=1,…z=25)

$$C_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$

$$C_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$

$$C_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

- C＝KP

Hill密码

- 一个例子：
  - 明文为pay more money
  - 加密密钥为 $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$
  - p=15,a=0,y=24
  - K(15,0,24) mod 26 = (11,13,18)

Vigenere密码

* Vige

	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

Vigenere密码

- Vigenere加密
  - 密钥

    deceptivedeceptivedecepitve
  - 明文

    wearedicoveredsaveyourself
  - 密文

    zicvtwqngrzgvtwavzhcqyglmgj

Vigenere密码

- 密码分析
  - 猜测关键字长度
    - 两个相同明文字母序列出现在一定距离里，该距离失关键字长度的整数倍，那么它们将产生相同的密文序列
  - 分割vigenere密码为单字母密码
    - 密钥以关键字长度为周期
- 改进
  - 消除关键字的周期性
    - AT&T的工程师设计一个使用非常长的密钥工作的系统
    - 只要有足够的密文，或已知明文仍能够破译
- 一次一密方案
  - 使用与消息一样长的随机密钥
  - 实际使用困难：发送者和接收者必须拥有该随机密钥

置换技术——栅栏技术

- are—》rea
- 明文： wait me at the gate

  加密： wimateae

  atethgt

  密文： wimateaeatethgt