密 码 学

（第二讲）

古典密码

张焕国

武汉大学计算机学院

目　录

目　录

一、古典密码

虽然用近代密码学的观点来看，许多古典密码是很不安全的，或者说是极易破译的。但是我们不能忘记古典密码在历史上发挥的巨大作用。

另外，编制古典密码的基本方法对于编制近代密码仍然有效。

一、古典密码

C. D. Shannon:

- 采用混淆、扩散和乘积的方法来设计密码
- 混淆：使密文和明文、密钥之间的关系复杂化
- 扩散：将每一位明文和密钥的影响扩大到尽可能多的密文位中。
- 乘积和迭代：多种加密方法混合使用
  对一个加密函数多次迭代

古典密码编码方法：

- *置换，代替，加法*

一、古典密码

1、置换密码

- *把明文中的字母重新排列，字母本身不变，但其位置改变了，这样编成的密码称为置换密码。*
  - 最简单的置换密码是把明文中的字母顺序倒过来，然后截成固定长度的字母组作为密文。

明文：明晨5点发动反攻。

MING CHEN WU DIAN FA DONG FAN GONG

密文：**GNOGN AFGNO DAFNA IDUWN EHCGN IM**

一、古典密码

- *把明文按某一顺序排成一个矩阵，然后按另一顺序选出矩阵中的字母以形成密文，最后截成固定长度的字母组作为密文。*

例如：

明文：**MING CHEN WU DIAN FA DONG FAN GONG**

矩阵：**MINGCH**
ENWUDI
ANFADO
NGFANG
ONG

选出顺序：*按列*

改变矩阵大小和取出序列可得到不同的密码

密文：**MEANO INNGN NWFFG GUAA CDDN HIOG**

一、古典密码

- 理论上：

①、*置换密码的加密钥是置换矩阵* $\mathbf{p}$ *，*

解密钥是置换矩阵 $\mathbf{p^{-1}}$ *。*

$$P = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{bmatrix}$$

②、*置换密码经不起已知明文攻击。*

一、古典密码

2、代替密码

首先构造一个或多个密文字母表，然后用密文字母表中的字母或字母组来代替明文字母或字母组，各字母或字母组的相对位置不变，但其本身改变了。这样编成的密码称为代替密码。

①*单表代替密码*
②*多表代替密码*
③*多名代替密码*

一、古典密码

(1). *单表代替密码*

只使用一个密文字母表，并且用密文字母表中的一个字母来代替明文字母表中的一个字母。

明文字母表： $A=\{a_0, a_1, \ldots, a_{n-1}\}$

密文字母表： $B=\{b_0, b_1, \ldots, b_{n-1}\}$

定义一个由A到 B的映射： $f:A\rightarrow B$

$$f(a_i)=b_i$$

设明文： $M=(m_0, m_1, \ldots, m_{n-1})$，

则密文： $C=(f(m_0), f(m_1), \ldots, f(m_{n-1}))$。

简单代替密码的密钥就是映射函数f或密文字母表B。

一、古典密码

(1)*单表代替密码*

①、*加法密码*

- *A和B是有 n个字母的字母表。*
- *定义一个由A到B的映射：* $f:A \rightarrow B$

$$f(a_i) = b_i = a_j$$

$$j = i + k \bmod n$$

- *加法密码是用明文字母在字母表中后面第 k个字母来代替。*
- *K=3 时是著名的凯撒密码。*

一、古典密码

(1)*单表代替密码*

②、*乘法密码*

- *A和B是有n个字母的字母表。*
- *定义一个由A到B的映射：* $f:A \rightarrow B$

$$f(a_i) = b_i = a_j$$

$$j = ik \bmod n$$

其中， $(n, k)=1$。

- 注意：*只有* $(n, k)=1$，*才能正确解密。*

一、古典密码

(1) 单表代替密码

③ 密钥词组代替密码：

随机选一个词语，去掉其中的重复字母，写到矩阵的第一行，从明文字母表中去掉这第一行的字母，其余字母顺序写入矩阵。然后按列取出字母构成密文字母表。

一、古典密码

举例：

密钥： ***HONG YE***

矩阵： ***HONGYE*** *选出顺序：按列*

ABCDFI

JKLMPQ *改变密钥、矩阵大小*

RSTUVW *和取出序列，得到不同的*

XZ *密文字母表。*

密文字母表：

B={ HAJRXOBKSZNCLTGDMUYFPVEIQW }

一、古典密码

(2)、多表代替密码

- 单表代替密码的安全性不高，一个原因是一个明文字母只由一个密文字母代替。
- 构造多个密文字母表，
- 在密钥的控制下用相应密文字母表中的一个字母来代替明文字母表中的一个字母。一个明文字母有多种代替。

Vigenere密码：著名的多表代替密码

一、古典密码

Vigenre方阵

密文字母 \ 明文字母	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
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
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

一、古典密码

Vigenre密码的代替规则是用明文字母在Vigenre方阵中的列和密钥字母在Vigenre方阵中的行的交点处的字母来代替该明文字母。例如，设明文字母为P，密钥字母为Y，则用字母N来代替明文字母P。

明文：**MING CHEN WU DIAN FA DONG FAN GONG**

密钥：**XING CHUI PING YE KUO YUE YONG DA JIANG LIU**

密文：**JQAME OYVLC QOYRP URMHK DOAMR NP**

解密就是利用Vigenre方阵进行反代替。

一、古典密码

3、代数密码：

① **Vernam密码**

明文、密文、密钥都表示为二进制位：

$M=m_1,m_2,\ldots,m_n$ $K=k_1,k_2,\ldots,k_n$ $C=c_1,c_2,\ldots,c_n$

② *加密*： $c_1=m_i \oplus k_i$,i=1,2,… ,n

解密： $m_1=c_i \oplus k_i$,i=1,2,… ,n

③因为加解密算法是模2加，所以称为代数密码。

④对合运算：$f=f^{-1}$，*模2加运算是对合运算。*

密码算法是对和运算，则加密算法＝解密算法，工程实现工作量减半。

⑤ **Vernam密码经不起已知明文攻击。**

一、古典密码

⑥ 如果密钥序列有重复，则**Vernam**密码是不安全的。

⑦ *一种极端情况：一次一密*

- 密钥是随机序列。
- 密钥至少和明文一样长。
- 一个密钥只用一次。

⑧ *一次一密是绝对不可破译的，但它是不实用的。*

⑨ 一次一密给密码设计指出一个方向，人们用序列密码逼近一次一密。

二、古典密码的穷举分析

1、单表代替密码分析

①*加法密码*

- *因为*$f(a_i)= b_i=a_j$

$$j=i+k \bmod n$$

- 所以k=1,2，...，n-1,共n-1种可能，*密钥空间太小。以英文为例，只有25种密钥。*
- *经不起穷举攻击。*

二、古典密码的穷举分析

1、单表代替密码分析

②乘法密码

- *因为*$f(a_i)= b_i=a_j$

  $j=ik \bmod n$，且（k,n）=1。

- 所以k共有ϕ（n）种可能，*密钥空间更小。*
- *对于英文字母表，n=26，*

  k=1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

  取掉1，共11种，比加法密码更弱。
- *经不起穷举攻击。*

二、古典密码的穷举分析

1、单表代替密码分析

③*密钥词语代替密码*

- *因为密钥词语的选取是随机的，所以密文字母表完全可能穷尽明文字母表的全排列。*
- 以英文字母表为例，n=26，所以共有26！种可能的密文字母表。

$$26! \approx 4\times10^{26}$$

- *用计算机也不可能穷举攻击。*
- *注意：穷举不是攻击密钥词语代替密码的唯一方法。*

三、古典密码的统计分析

2、密钥词组单表代替密码的统计分析

- 任何自然语言都有自己的统计规律。
- 如果密文中保留了明文的统计特征，就可用统计方法攻击密码。
- 由于单表代替密码只使用一个密文字母表，一个明文字母固定的用一个密文字母来代替，所以密文的统计规律与明文相同。
- 因此，单表代替密码可用统计分析攻破。

三、古典密码的统计分析

- *英语的统计规律*
  - *每个单字母出现的频率稳定。*

最高频率字母	*E*
次高频率字母	*T A O I N S H R*
中高频率字母	*D L*
低频率字母	*C U M W F G Y P B*
最低频率字母	*V K J X Q Z*

三、古典密码的统计分析

- *英语的统计规律*
  - *频率最高的双字母组：*

    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

三、古典密码的统计分析

- *英语的统计规律*
  - *频率最高的三字母组：*

    THE ING AND HER ERE ENT THA WAS ETH FOR DHT HAT SHE ION HIS ERS VER

    其中THE的频率是ING的3倍！

三、古典密码的统计分析

- *英语的统计规律*
  - *英文单词以E，S，D，T为结尾的超过一半。*
  - *英文单词以T，A，S，W为起始字母的约占一半。*
  - *还有其它统计规律！*
  - *教科书上有一个完整的统计分析例子。*

三、古典密码的统计分析

经得起统计分析是对近代密码的基本要求！

复习题

①已知置换如下：

$$P=\begin{pmatrix}1&2&3&4&5&6\\3&5&1&6&4&2\end{pmatrix}$$

明文＝**642135**,密文＝？

密文＝**214365**，明文＝？

②使加法密码算法称为对合运算的密钥**k**称为对合密钥，以英文为例求出其对合密钥。

复习题

③ 已知一个加法密码的密文如下：
BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKF UHCQD
用穷举法求出明文。

④以英文为例，用加法密码，取密钥常数 k= 7，对明文 **INFORMATION SECURITY**，进行加密，求出密文。

⑤证明，在置换密码中，置换**p**是对合的，当且仅当对任意的**i**和**j(i, j=1,2,3,…,n)**，若**p(i)=j**，则必有**p(j)=i** 。

⑥编程实现**Vigenre**密码。

⑦ 分析仿射密码的安全性。


谢 谢！