

# 密码学

## 第二讲 密码学的基本概念

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室





# 内容简介

第一讲 信息安全概论

**第二讲 密码学的基本概念**

第三讲 数据加密标准 (DES)

第四讲 高级数据加密标准 (AES)

第五讲 中国商用密码 (SMS4)

第六讲 分组密码的应用技术

第七讲 序列密码

第八讲 复习

第九讲 公钥密码 (1)





# 内容简介

第十讲 公钥密码 (2)

第十一讲 数字签名 (1)

第十二讲 数字签名 (2)

第十三讲 **HASH**函数

第十四讲 认证

第十五讲 密码协议

第十六讲 密钥管理 (1)

第十七讲 密钥管理 (2)

第十八讲 复习

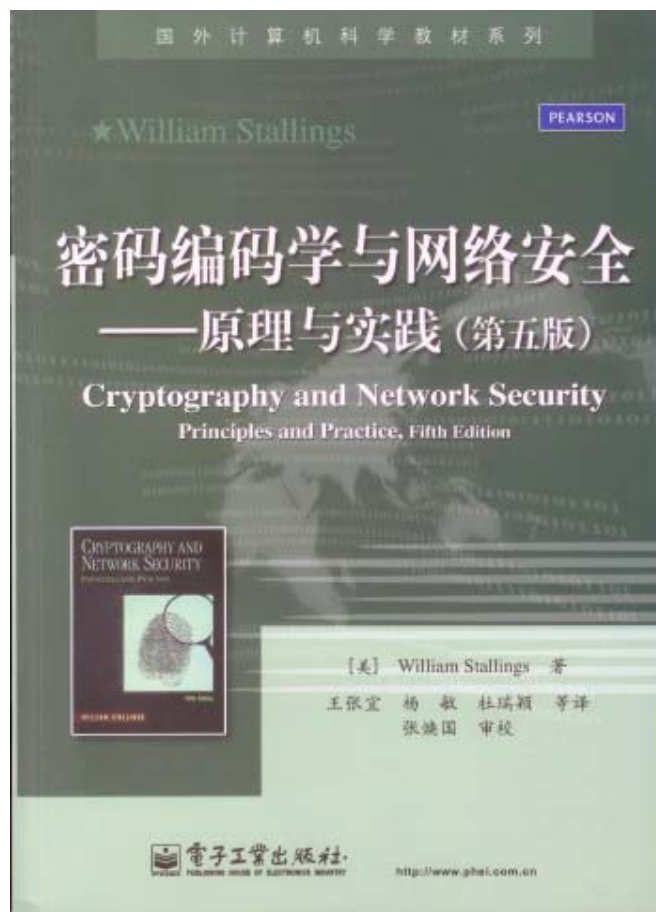


# 教材与主要参考书

## 教材



## 参考书



武汉大学





# 一、我国的密码政策

我国的密码分级：

①**核心密码：**

用于保护党、政、军的核心机密。

②**普通密码：**

用于保护国家和事企业单位的低于核心机密而高于商用的机密信息。

③**商用密码：**

用于保护国家和事企业单位的非机密的敏感信息。

④**个人密码：**

用于保护个人的隐私信息。

**前三种密码均由国家密码管理局统一管理！**



**武汉大学**



# 一、我国的密码政策

## 我国商用密码政策：

### ①统一领导：

国家密码管理局统一领导。

### ②集中管理：

国家密码管理局集中管理。

### ③定点研制：

只允许定点单位进行研制。

### ④专控经营：

经许可的单位才能经营。

### ⑤满足使用：

国内各单位都可申请使用。





## 二、密码学的基本概念

### 1、密码的基本思想

- 伪装以隐蔽信息，使未授权者不能理解它的真实含义。
  - 所谓伪装就是对信息进行一组可逆的数学变换。
  - 伪装前的原始信息称为明文，伪装后的信息称为密文。
  - 伪装的过程称为加密，去掉伪装还原明文的过程称为解密。
  - 加密在加密密钥的控制下进行，解密在解密密钥的控制下进行。
  - 用于加密的一簇数学变换称为加密算法。用于解密的一簇数学变换称为解密算法。





# 一、密码学的基本概念

## 2、密码体制(Cryptosystem)的构成

由五个部分组成： $\langle M, C, K, E, D \rangle$

①明文空间 $M$ ：全体明文的集合

②密文空间 $C$ ：全体密文的集合

③密钥空间 $K$ ：全体密钥的集合， $K = \langle K_e, K_d \rangle$   
 $K_e$ 是加密钥， $K_d$ 是解密密钥

④加密算法 $E$ ：一簇由 $M \rightarrow C$ 的加密变换

⑤解密算法 $D$ ：一簇由 $C \rightarrow M$ 的解密变换。

而且解密变换是加密变换的逆。







## 二、密码学的基本概念

### 2、密码体制(Cryptosystem)的构成

- 对于一个确定的密钥，加密算法将确定出一个具体的加密变换，解密算法将确定出一个具体的解密变换，而且解密变换就是加密变换的逆变换。
- 对于明文空间中的每一个明文 $M$ ，加密算法 $E$ 在密钥 $K_e$ 的控制下将明文 $M$ 加密成密文 $C$ :

$$C = E(M, K_e)$$

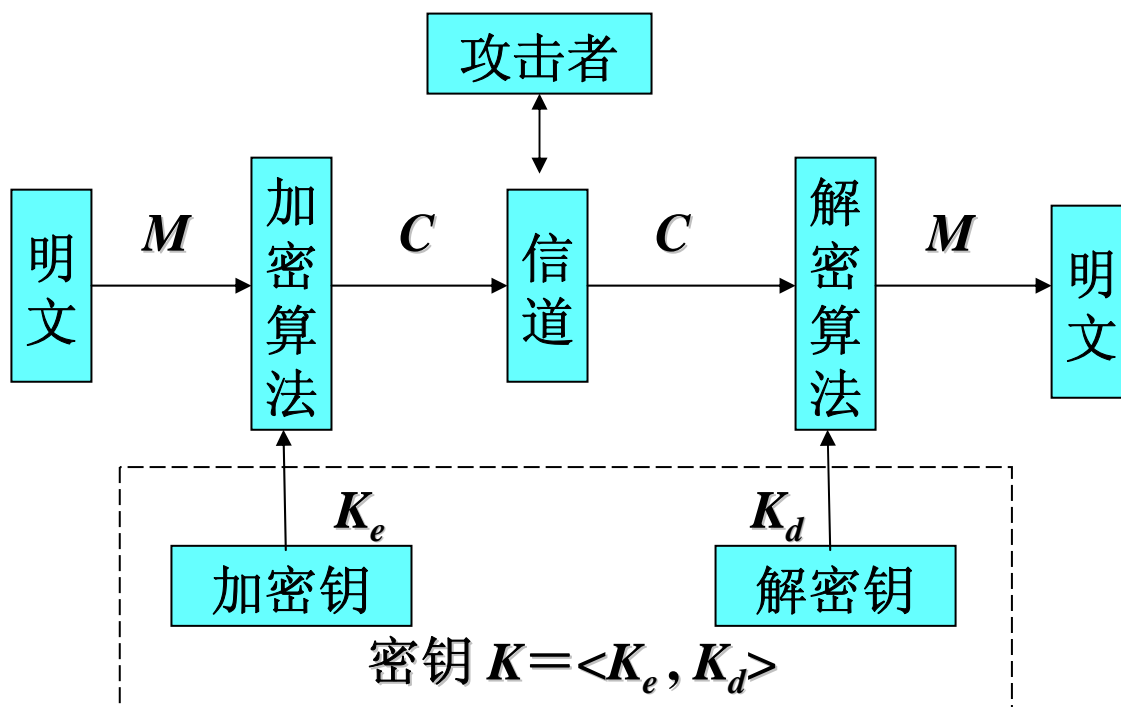
- 而解密算法 $D$ 在密钥 $K_d$ 的控制下将密文解出同一明文 $M$ 。

$$M = D(C, K_d) = D(E(M, K_e), K_d)$$



## 二、密码学的基本概念

### 2、密码体制(Cryptosystem)的构成





## 二、密码学的基本概念

### 3、密码体制的分类

● 从加密钥与解密密钥是否相等划分：

(1) 传统密码：

■  $K_e = K_d$

■ 典型密码：DES, AES, SMS4, RC4

(2) 公开密钥密码：

■  $K_e \neq K_d$

■ 且由 $K_e$ 不能计算出 $K_d$

■ 于是可将 $K_e$ 公开，这样也不会危害 $K_d$ 的安全

■ 典型密码：RSA, EIGAMAL, ECC





## 二、密码学的基本概念

### 3、密码体制的分类

#### ●从密钥的使用方式划分：

##### (1) 序列密码：

- 明文、密文、密钥以位（字符）为单位加解密
- 核心密码的主流
- 典型密码：RC4，祖冲之密码

##### (2) 分组密码：

- 明文、密文、密钥以分组为单位加解密
- 商用密码的主流
- 典型密码：DES，AES，SMS4







## 二、密码学的基本概念

### 3、密码体制的分类

● 从密码算法是否变化划分：

#### (1) 固定算法密码

- 密码在工作过程中算法固定不变，密钥可变
- 迄今为止的绝大多数密码都是固定算法密码
- 典型密码：AES，DES，SMS4，RC4，RSA，EIGAMAL，ECC



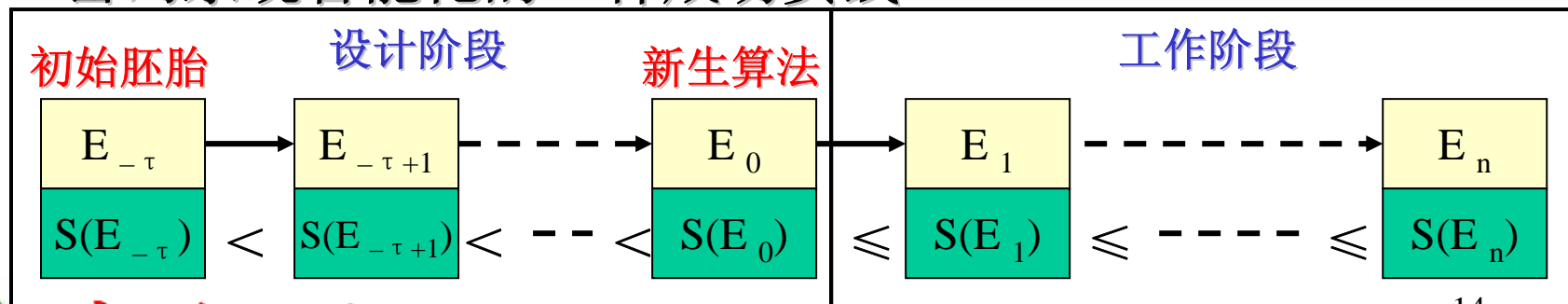
## 二、密码学的基本概念

### 3、密码体制的分类

- 从密码算法是否变化划分：

#### (2)演化密码

- 借鉴生物进化，将密码学与演化计算结合
- 密码算法不断演化变化，而且越变越好
- 实现密码设计与密码分析自动化的一种方法
- 密码系统智能化的一种成功实践





## 二、密码学的基本概念

### 3、密码体制的分类

- 从是否基于数学划分

- (1) 基于数学的密码

- 前面所有的密码

- (2) 基于非数学的密码

- ① 量子密码

- 在唯密文攻击下无条件安全的密码
  - 基于量子的保密物理属性
  - 利用量子力学产生真随机数作密钥，利用量子通信的保密性传输密钥，利用模2加进行加密，而且按一次一密方式工作





## 二、密码学的基本概念

### 3、密码体制的分类

- 从是否基于数学划分

- (2) 基于非数学的密码

- ② DNA密码

- 基于生物学中的困难问题
- 由于不基于计算，所以无论计算机的计算能力多么强大，与DNA密码都是无关的
- 尚不成熟：缺少理论，技术实现复杂







## 二、密码学的基本概念

### 4、密码学的组成

- 研究密码编制的科学称为**密码编制学**(Cryptography)
- 研究密码破译的科学称为**密码分析学**(Cryptanalysis)
  - 密码分析学俗称密码破译
- 密码编制学和密码分析学共同组成**密码学**(Cryptography)





## 二、密码学的基本概念

### 5、密码分析

- 如果能够根据密文**系统地**确定出明文或密钥，或者能够根据明文-密文对**系统地**确定出密钥，则我们说这个密码是**可破译的**。
- 一个密码，如果无论密码分析者截获了多少密文和用什么方法进行攻击都不能被攻破，则称为是**绝对不可破译的**。
- 理论上，绝对不可破译的密码是存在的。
  - “一次一密”
- 理论上，任何可实用的密码都是可破译的。





## 二、密码学的基本概念

### 5、密码分析

#### ● 穷举攻击

- 密码分析者采用依次试遍所有可能的密钥对所获密文进行解密，直至得到正确的明文；或者依次用一个确定的密钥对所有可能的明文进行加密，直至得到所获得的密文。
- 显然，理论上，对于任何可实用密码只要有足够的资源，都可以用穷举攻击将其攻破。





## 二、密码学的基本概念

### 5、密码分析

#### ● 穷举攻击 实例

- 1997年美国一个密码分析小组宣布：1万多人参加，通过INTERNET网络，利用数万台微机，历时4个多月，通过穷举攻破了DES的一个密文。
- 美国现在已有DES穷举机，多CPU并行处理，24小时穷举出一个密钥。







## 二、密码学的基本概念

### ● 基于数学的分析

■ 所谓数学分析是指密码分析者针对加解密算法的数学依据通过数学分析的方法来破译密码。

◆ 统计分析攻击 早期的基于数学的密码分析主要是统计分析，它是指密码分析者通过分析密文和明文的统计规律来破译密码。

◆ 统计分析攻击在历史上为破译密码作出过极大的贡献。许多古典密码都可以通过统计分析而破译。

■ 公钥密码特别容易受到这种攻击。因为公钥密码是一种基于数学困难问题的密码。

■ 为了对抗这种数学分析攻击，应当选用具有坚实数学基础和足够复杂的加解密算法。





## 二、密码学的基本概念

### 5、密码分析

#### ● 基于非数学的分析

- 所谓基于非数学的密码分析是指，密码分析者获取并分析密码芯片的物理参数（如，功率、电流、声音、执行时间，等）来破译密码。
- 这种攻击又称为侧信道攻击
- 侧信道攻击的原理在于：
  - ◆ 密码芯片在执行不同的指令时所消耗的功率、电流、时间、发的声音是不同的。
  - ◆ 密码芯片在处理不同的数据时所消耗的功率、电流、时间、发的声音也是不同的。
- 以获取密钥为目的的侧信道攻击
- 以获取密码算法为目的的侧信道攻击
  - ◆ 芯片物理解刨
  - ◆ 侧信道分析与数学分析结合





## 二、密码学的基本概念

### 5、密码分析

- 根据占有的数据资源分类：

- 密码学的基本假设：

- ◆ 攻击者总能获得密文
- ◆ 攻击者总能知道密码算法，但不知道密钥
- ◆ 攻击者有足够的计算资源

#### ① 仅知密文攻击（**Ciphertext-only attack**）

- 所谓仅知密文攻击是指密码分析者仅根据截获的密文来破译密码。
- 因为密码分析者所能利用的数据资源仅为密文，因此这是对密码分析者最不利的情况。





## 二、密码学的基本概念

### 5、密码分析

- 根据占有的数据资源分类：

#### ② 已知明文攻击（**Known-plaintext attack**）

- 所谓已知明文攻击是指密码分析者根据已经知道的某些明文-密文对来破译密码。
- 攻击者总是能获得密文，并猜出部分明文。
- 计算机程序文件加密特别容易受到这种攻击。







## 二、密码学的基本概念

### 5、密码分析

- 根据占有的数据资源分类：

#### ③选择明文攻击（**Chosen-plaintext attack**）

- 所谓选择明文攻击是指密码分析者能够选择明文并获得相应的密文。
- 计算机文件加密和数据库加密特别容易受到这种攻击。
- 这是对攻击者最有利的情况！





## 二、密码学的基本概念

### 6、密码学的理论基础

#### (1) 信息论

- ①从信息在信道传输中可能受到攻击，引入密码理论；
- ②提出以**扩散、混淆**和**乘积**等基本方法设计密码；
- ③阐明了密码体制，完善保密，理论保密和实际保密等概念。

#### (2) 计算复杂性理论

- ①**密码的安全性以计算复杂度来度量；**
- ②现代密码往往建立在一个数学难题之上，而“难”是计算复杂度的概念；
- ③计算复杂度只能为密码提供一个必要条件。





## 二、密码学的基本概念

### 7、密码设计的基本方法

#### (1) 公开设计原则

密码的安全应仅依赖于对密钥的保密，不依赖于对算法的保密。


#### (2) 扩散和混淆

- 扩散(diffusion): 将明文和密钥的每一位的影响散布到尽量多的密文位中，理想情况下达到完备性。
- 混淆(confusion): 使明文、密钥和密文之间的关系复杂化。

#### (3) 迭代与乘积

- 迭代: 设计一个轮函数，然后迭代。
- 乘积: 将几种密码联合应用。





### 三、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。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。

- 古典密码编码方法：

置换，代替，模2加法







## 三、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 EHC GN IM**





### 三、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            选出顺序：按列

ENWUDI

ANFADO

NGFANG

ONG###

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#





## 三、古典密码


●理论上：

①、置换密码的加密钥是置换矩阵  $\mathbf{p}$  ，  
解密密钥是置换矩阵  $\mathbf{p}^{-1}$  。

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

②、置换密码经不起已知明文攻击。





## 三、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







## 三、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:  $A = \{ a_0, a_1, \dots, a_{n-1} \}$

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

定义一个由A到B的映射:  $f: A \rightarrow B$


$$f(a_i) = b_i$$

设明文:  $M = (m_0, m_1, \dots, m_{n-1})$ ,

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

简单代替密码的密钥就是函数  $f$  或密文字母表  $B$ 。





## 三、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。





## 三、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。





## 三、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。







### 三、古典密码

●举例：

密钥： **HONG YE**

矩阵： **HONGYE**      选出顺序： **按列**

**ABCD FI**

**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 }**





### 三、古典密码

#### ● 举例：山西平遥市日升昌票号密码

密文代替表：9个汉字代表数字一、二、...、九

12汉字代表十二个月

30汉字代表一个月的三十天





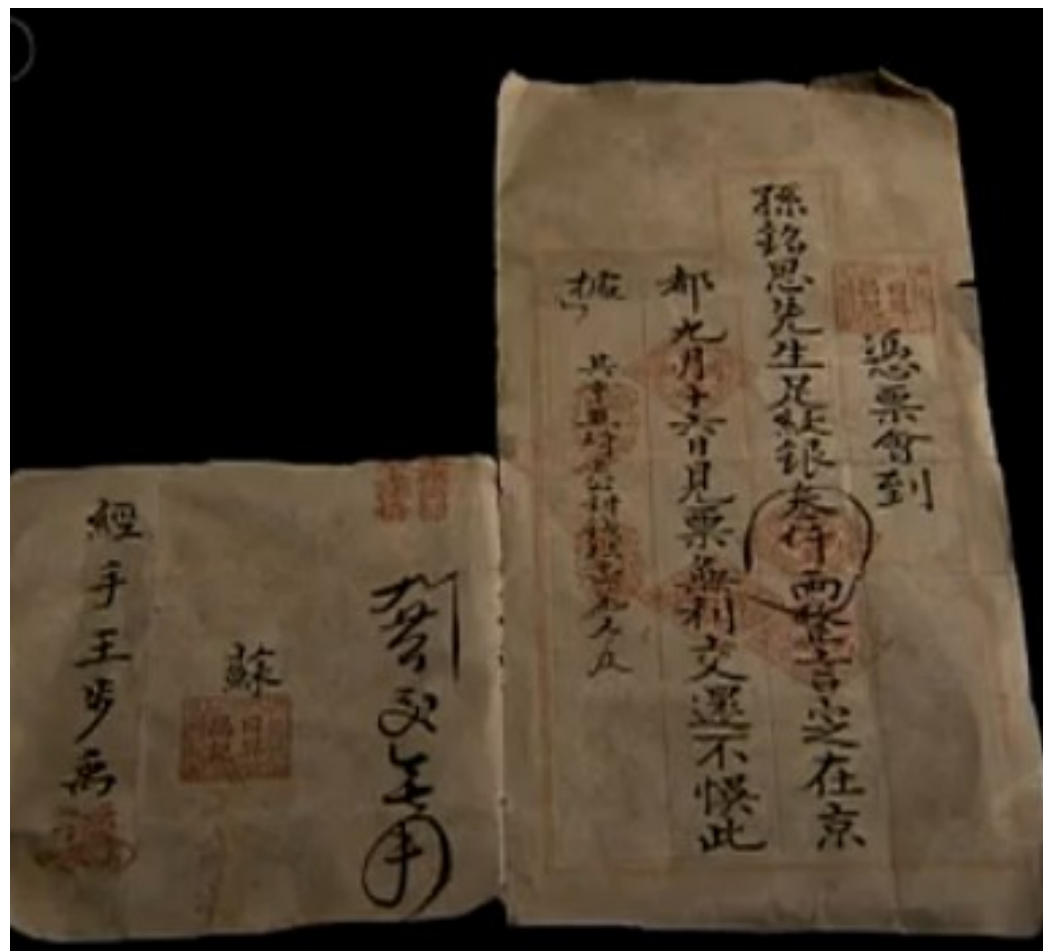
### 三、古典密码

- 举例：日升昌票号密码


应用：在银票上加写密押

密押：

- 把银子重量及日期等内容加密成密文，并写在银票上。
- 兑换银子时重新形成密押并与银票上的比较，以确定真伪。



武汉大学




## 三、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。
- 这样，一个明文字母就有多种代替。







## 三、古典密码

### ●Vigenere密码：著名的多表代替密码

**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。





# 三、古典密码

## Vigenre方阵

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

密文字母

密  
钥  
字  
母

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

武汉大学





## 三、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：

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

② **加密**：  $c_i = m_i \oplus k_i, i=1, 2, \dots, n$


**解密**：  $m_i = c_i \oplus k_i, i=1, 2, \dots, n$

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。






### 三、古典密码

- ⑤ Vernam密码经不起已知明文攻击。
- 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。







## 三、古典密码

### 4、古典密码分析

#### (1)单表代替密码分析

##### ①加法密码分析


■ 因为 $f(a_i) = b_i = a_j$

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

■ 所以 $k=1,2, \dots, n-1$  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。





## 三、古典密码

### 4、古典密码分析

#### (1)单表代替密码分析

#### ②乘法密码分析

■ 因为  $f(a_i) = b_i = a_j$

$j = ik \bmod n$ , 且  $(k, n) = 1$ 。

■ 所以  $k$  共有  $\phi(n)$  种可能, 密钥空间更小。

■ 对于英文字母表,  $n = 26$ ,


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

去掉1, 共11种, 比加法密码更弱。

■ 经不起穷举攻击。

武汉大学





## 三、古典密码

### 4、古典密码分析

#### (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。

$$26! \approx 4 \times 10^{26}$$

- 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

### 4、古典密码分析

#### (1)单表代替密码分析

#### ③密钥词语代替密码

- 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，一个明文字母固定地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，密钥词语代替密码可用统计分析攻破。







## 三、古典密码

### 4、古典密码分析

(1)单表代替密码分析

③密钥词语代替密码

#### ● 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

### 4、古典密码分析

#### (1)单表代替密码分析

#### ③密钥词语代替密码

#### ● 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

### 4、古典密码分析

#### (1)单表代替密码分析

#### ③密钥词语代替密码

#### ● 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

### 4、古典密码分析

#### (1)单表代替密码分析

#### ③密钥词语代替密码

#### ● 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！

#### ● 经得起统计分析是对近代密码的基本要求！







# 作业题

- 1、p28第3题。
- 2、p28第5题。
- 3、p28第9题。





谢 谢！



武汉大学