# 信息安全概论

## Introduction to Information Security


主讲教师：赵 彦 锋

院　　系：信息工程学院 软件工程系

邮　　箱：c_zhaoyf@163.com


2021 年 03 月


# 第二周

# 第五讲 密码学基础

- 代换密码
- 置换密码
- 转轮机
- 隐写术

# 2.1 密码学的发展历史

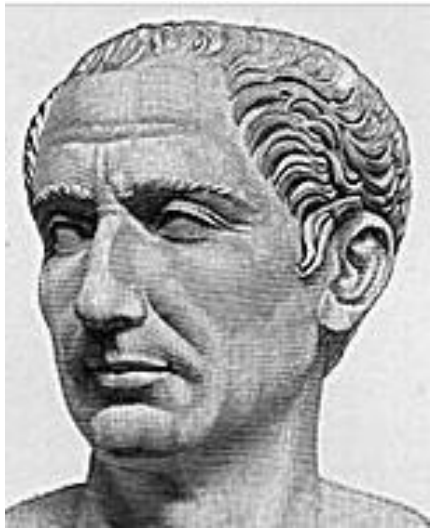
- 密码学作为信息安全理论与技术的基石，在信息安全领域发挥着中流砥柱的作用。密码学理论的应用，成为现代信息网络得以生存和不断发展的基本前提。
- Cryptography = crypto + graphy

  密码　　隐藏或秘密　　写

一般来讲，人们通常认为密码学是一种将信息表述为不可读内容的方式（加密），并且可以采用一种秘密方法将信息恢复出来（解密）。

# 2.1 密码学的发展历史

- 自人类社会出现战争便产生了密码
  - Julius Caesar发明了凯撒密码
  - 二战时德国使用Enigma机器加密
  - 美国军事部门使用纳瓦霍语(Navaho)通信员
- 密码由军事走向生活
  - 电子邮件
  - 自动提款机
  - 电话卡



# 2.1 密码学的发展历史

三个阶段：

- 1949年之前：　　密码学还称不上一门科学
- 1949～1975年：　《保密系统的通信理论》

  **密码学成为科学**
- 1976年以后：　密码学的新方向——**公钥密码学**

- 自人类社会出现战争便产生了密码

Phaistos圆盘，一种直径约为160mm的Cretan-Mnoan粘土圆盘，始于公元前17世纪。表面有明显字间空格的字母，至今还没有破解。

- Julius Caesar发明了凯撒密码

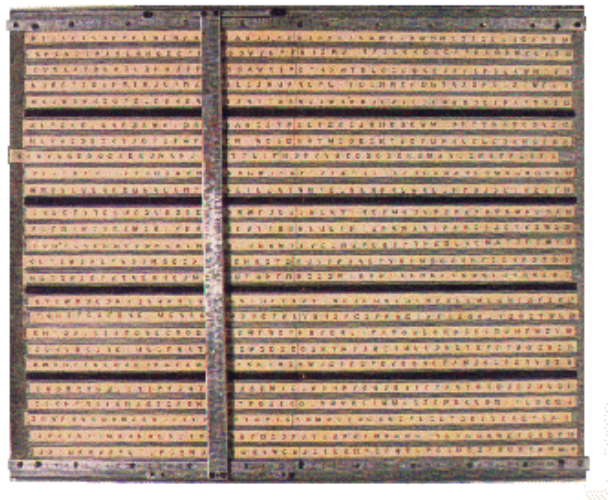
# 2.1 密码学的发展历史

- 1834年，伦敦大学的实验物理学教授惠斯顿发明了电机，这是通信向机械化、电气化跃进的开始，也为密码通信采用在线加密技术提供了前提条件。
- 1920年，美国电报电话公司的弗纳姆发明了弗纳姆密码。其原理是利用电传打字机的五单位码与密钥字母进行模2相加。

$$\begin{array}{r} 11010 \\ +\ 11101 \\ \hline 00111 \end{array} \qquad \begin{array}{r} 00111 \\ +\ 11101 \\ \hline 11010 \end{array}$$

# 2.1 密码学的发展历史

- 两次世界大战大大促进了密码学的发展。



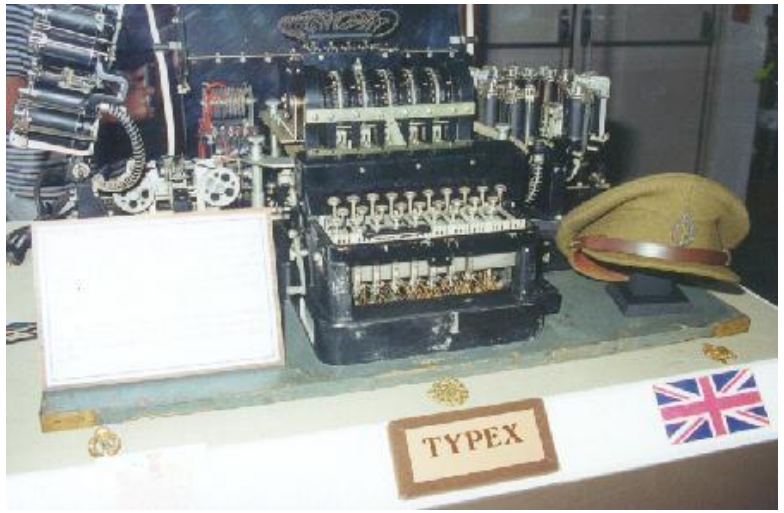
二战中美国陆军和海军使用的条形密码设备M-138-T4。根据1914年Parker Hitt的提议而设计。25个可选取的纸条按照预先编排的顺序编号和使用，主要用于低级的军事通信。


Kryha密码机大约在1926年由Alexander vo Kryha发明。这是一个多表加密设备，密钥长度为442，周期固定。一个由数量不等的齿的轮子引导密文轮不规则运动。

# 2.1 密码学的发展历史

- 两次世界大战大大促进了密码学的发展。


转轮密码机ENIGMA，由Arthur Scherbius于1919年发明，面板前有灯泡和插接板；4轮ENIGMA在1942年装备德国海军，英国从1942年2月到12月都没能解读德国潜艇的信号。




英国的TYPEX打字密码机，是德国3轮ENIGMA的改进型密码机。它在英国通信中使用广泛，且在破译密钥后帮助破解德国信号。

# 2.1 密码学的发展历史

- 1949年香农发表了一篇题为《保密系统的通信理论》的著名论文，该文首先将信息论引入了密码，从而把已有数千年历史的密码学推向了科学的轨道，奠定了密码学的理论基础。
- 1976年，美国密码学家W.Diffie和M.Hellman在一篇题为《密码学的新方向》一文中提出了一个崭新的思想，不仅加密算法本身可以公开，甚至加密用的密钥也可以公开。
- 1977年美国国家标准局颁布了数据加密标准DES
- 2001年11月26日，正式颁布AES为美国国家标准。

## 1.密码学

密码学是一门研究信息系统保密的科学，包括两个分支，即密码编码学和密码分析学。密码编码学是对信息进行编码实现信息保密性的科学；而密码分析学是研究、分析、破译密码的科学。

- 密码学技术可以使消息的内容对(除发送者和接收者以外)的所有人保密。
- 可以使接收者验证消息的正确性。
- 是解决计算机与通信安全问题重要技术之一。

## 2.基本术语（Basic Terminology）

- 密码技术(Cryptography)---把可理解的消息变换成不可理解的消息，同时又可恢复原消息的方法和原理的科学或艺术。
- 明文(Plaintext)---变换前的原始消息。
- 密文(Ciphertext)---变换后的消息。
- 密码(Cipher)---用于改变消息的替换或变换算法。
- 密钥(Key)---用于密码变换的，只有发送者或接收者拥有的秘密消息。

## 2.基本术语（Basic Terminology）

- 编码(Encipher/Encode)---把明文变为密文的过程。
- 译码(Decipher/Decode)---把密文变为明文的过程。
- 密码分析（Cryptanalysis）---在没有密钥的情况下，破解密文的原理与方法。
- 密码学(Cryptology)---包括加密理论与解密理论的学科。

## 3. 一些密码学概念

- **Encryption**

  The mathematical function mapping plaintext to ciphertext using the specified key: $C=E_K(P)$

- **Decryption**

  The mathematical function mapping ciphertext to plaintext using the specified key: $P=E_K^{-1}(C)$

- **Cryptographic system**

  The family of transformations from which the cipher function $E_K$ is chosen.

## 3. 一些密码学概念

- **Key**

  **is the parameter which selects which individual transformation is used , and is selected from a keyspace *K***

- **$E_K$, K in *K* : P->C**

  **with unique inverse $P=E_K^{-1}$;K in *K*: C->P**

  **usually assume the cryptographic system is public , and only the key is secret information.**

## 4. 密码体制

通常一个完整密码体制要包括如下五个要素*M,C,K,E,D*：

明文空间 *M*

*M*是可能明文的有限集。

密文空间 *C*

*C*是可能密文的有限集。

密钥空间 *K*

*K*是一切可能密钥构成的有限集。

## 4. 密码体制

**通常一个完整密码体制要包括如下五个要素*M,C,K,E,D*：**

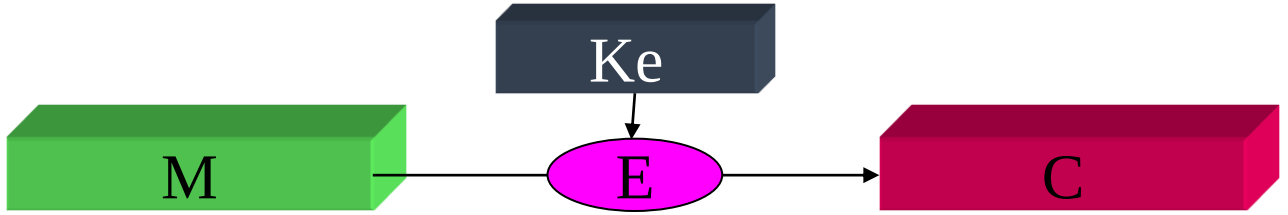
**加密算法 *E*** —— 一组由M到C的加密变换。

**解密算法 *D*** —— 一组由C到M的解密变换。

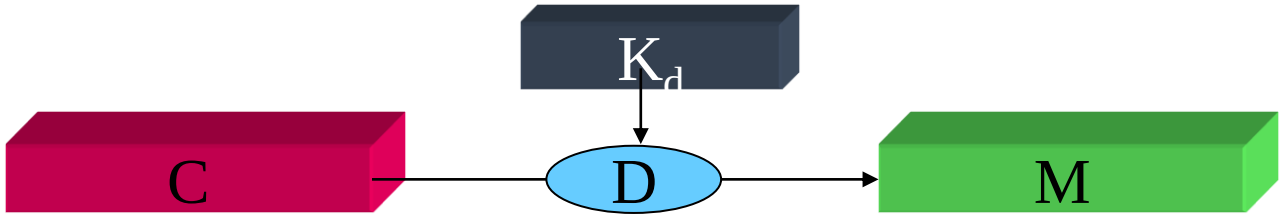
对于密钥空间的任一密钥，有一个加密算法和相应的解密算法，使得：$E_k$:M->C

和$D_k$:C->M分别为加密、解密函数，满足 $D_k(E_k(m))=m$, 这里$m \in M$

- 加密： $C = E(M,K_e)$




- 解密： $M = D(C, K_d)$

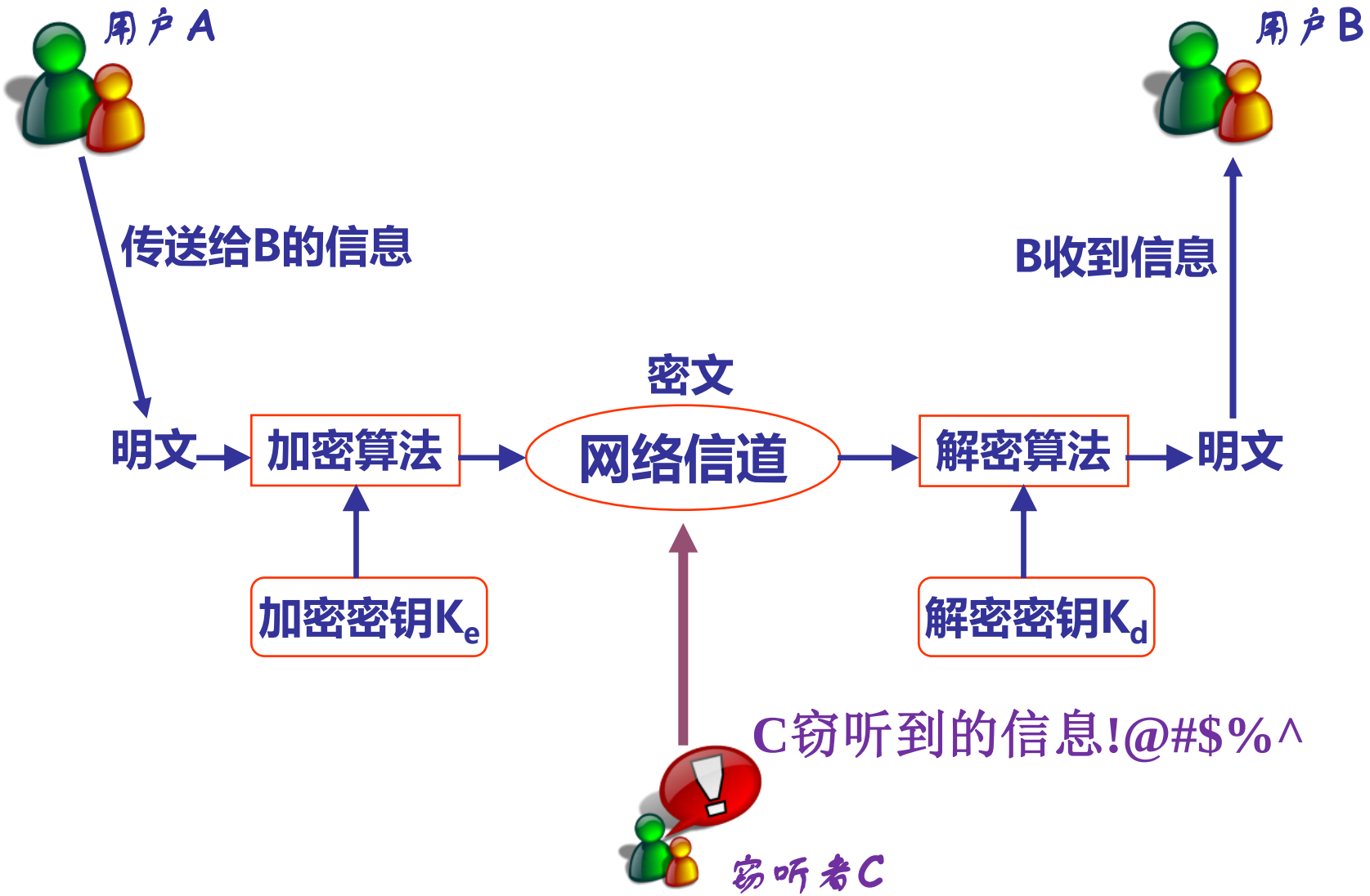



M------明文　　C------密文

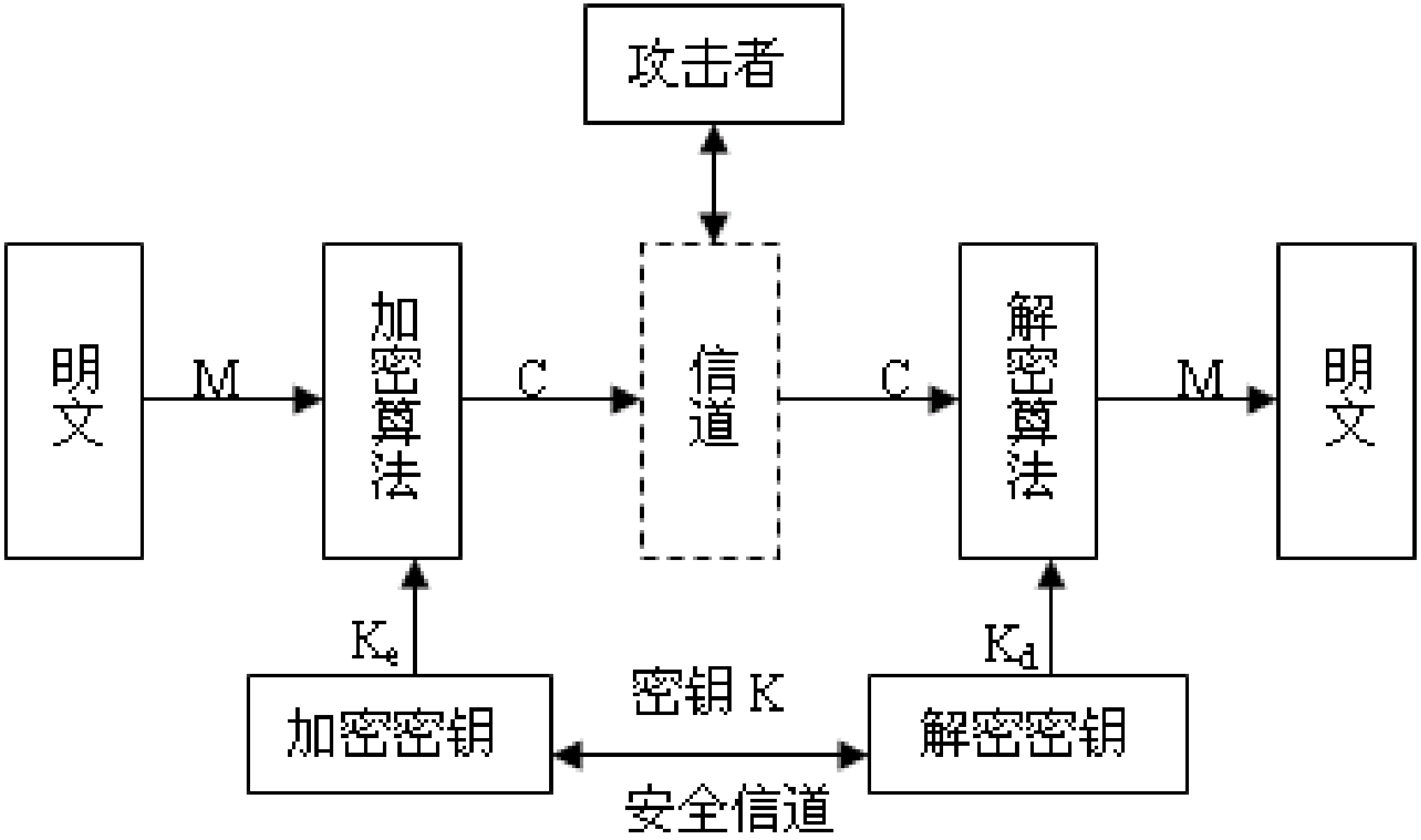
$K_e$-----加密密钥　　$K_d$-----解密密钥

E-------加密算法　　D------解密算法

# 2.2 密码学的基本概念


用户A
用户B
传送给B的信息
B收到信息
密文
明文
加密算法
网络信道
解密算法
明文
加密密钥$K_e$
解密密钥$K_d$
C窃听到的信息!@#$%^
窃听者C

# 信息加密传输的过程



## 5. 密码算法分类

**按发展进程分：古典密码、对称密钥密码、公开密钥密码。**

- 古典密码是基于字符替换的密码，现在很少用，但它代表密码的起源。
- 现在使用的是对位进行变换的密码算法，这些算法按密钥管理方式可分为两类，即对称加密算法和公钥加密算法；对称加密算法的加密密钥和解密密钥相同，这类算法也称为秘密密钥算法或单密钥算法。

## 5. 密码算法分类

### 根据密钥的使用方式分类

- **对称密码体制（秘密钥密码体制）**

  用于加密数据的密钥和用于解密数据的密钥相同，或者二者之间存在着某种明确的数学关系。

  加密：$E_K(M)=C$

  解密：$D_K(C)=M$

- **非对称密码体制（公钥密码体制）**

  用于加密的密钥与用于解密的密钥是不同的，而且从加密的密钥无法推导出解密的密钥。

  用公钥KP对明文加密可表示为：$E_{KP}(M)=C$

  用相应的私钥KS对密文解密可表示为：$D_{KS}(C)=M$

## 5. 密码算法分类

### 根据密钥的使用方式分类

- **对称密码体制（秘密钥密码体制）**

  用于加密数据的密钥和用于解密数据的密钥相同，或者二者之间存在着某种明确的数学关系。

  加密：$E_K(M)=C$

  解密：$D_K(C)=M$

- **非对称密码体制（公钥密码体制）**

  用于加密的密钥与用于解密的密钥是不同的，而且从加密的密钥无法推导出解密的密钥。

  用公钥KP对明文加密可表示为：$E_{KP}(M)=C$

  用相应的私钥KS对密文解密可表示为：$D_{KS}(C)=M$

## 5. 密码算法分类

**按加密模式分对称加密算法又可分为：序列密码和分组密码**

- 序列密码每次加密一位或一个字节的明文，又称为流密码，序列密码是手工和机械密码时代的主流。
- 分组密码将明文分成固定长度的组，用同一密钥和算法对每一个组进行加密，输出也是固定长度的密文。

## 5. 密码算法分类

### 根据明文和密文的处理方式分类

- **分组密码体制（Block Cipher）**

  设M为明文，分组密码将M划分为一系列明文块$M_i$，通常每块包含若干字符，并且对每一块$M_i$都用同一个密钥$K_e$进行加密。

  $M=(M_1, M_2,\ldots ,M_n)$，$C=(C_1, C_2 , \ldots ,C_n,)$，其中$C_i=E(M_i,K_e)$，$i=1,2\ldots,n$。

- **序列密码体制（Stream Cipher）**

  将明文和密钥都划分为位(bit)或字符的序列，并且对明文序列中的每一位或字符都用密钥序列中对应的分量来加密。

  $M=(M_1, M_2,\ldots ,M_n)$，$K_e=(k_{e1}, k_{e2},\ldots,k_{en})$，$C=(C_1, C_2,\ldots,C_n)$，其中$C_i=E(m_i,k_{ei})$，$i=1,2,\ldots,n$。

## 5. 密码算法分类

- 经典密码算法---代替

  简单代替、多表代替、多字母代替等

- 经典密码算法---换位
- 对称加密算法---DES、AES
- 公钥加密算法---RSA、背包密码、Rabin、椭圆曲线等

## 1. 单表代换密码

简单代替密码就是将明文字母表M中的每个字母用密文字母表C中的相应字母来代替，这一类密码包括：移位密码、替换密码、仿射密码、乘数密码、多项式代替密码、密钥短语密码等。

- 移位密码是最简单的一类代替密码，将字母表的字母右移k个位置，并对字母表长度作模运算。形式为

$$E_k(m)=(k+m) = c \bmod q$$

解密变换为：

$$D_k(c)=(c-k)=m \bmod q$$

## 1. 单表代换密码

其中q为字母表M的长度，“m”既代表字母表M中的位置，也代表其在M中的位置。“c”既代表字母表C中的位置，也代表其在C中的位置，凯撒（Caesar） 密码是对英文26个字母进行移位代替的密码，其q=26 。这种密码称为凯撒密码，是因为凯撒使用过k=3的这种密码。

M= Peking University 加密为：C=Ujpnsl Zsnajwxnyd

## 1. 单表代换密码

其中q为字母表M的长度，“m”既代表字母表M中的位置，也代表其在M中的位置。“c”既代表字母表C中的位置，也代表其在C中的位置，凯撒（Caesar） 密码是对英文26个字母进行移位代替的密码，其q=26 。这种密码称为凯撒密码，是因为凯撒使用过k=3的这种密码。

M= Peking University 加密为：C=Ujpnsl Zsnajwxnyd

## 1. 单表代换密码

- 在替换密码中，可对明文字母表进行q个字符的所有可能置换得到密文字母表。移位密码是替换密码算法一个特例。
- 希腊密码（二维字母编码查表）:公元前2世纪

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

## 1. 单表代换密码

- 希腊密码（二维字母编码查表）:公元前2世纪

例:　　Peking University

35 15 25 24 33 22 45 33 24 51 15 42 43 24 44 54

## 1. 单表代换密码

- Caesar（凯撒）密码-----加密

方式一：公式计算

明文编码：如a = 0，b = 1，…，z = 25，明文P = $p_1 p_2 \cdots p_n$

（加密）运算：$c_i = p_i + k \mod 26$，$i = 1, 2, \ldots, n$

解码得密文：C = $c_1 c_2 \cdots c_n$

## 1. 单表代换密码

- Caesar（凯撒）密码-----加密

**方式二：查表（例k=3）**

| 明文 | a | b | c | d | e | f | g | h | i | j | k | l | m | n |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 密文 | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |

| 明文 | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 密文 | R | S | T | U | V | W | X | Y | Z | A | B | C |

## 1. 单表代换密码

- Caesar（凯撒）密码-----解密

方式一：公式计算

密文编码：如a = 0，b = 1，…，z = 25，密文C = $c_1 c_2 \cdots c_n$

（解密）运算：$p_i = c_i - k \bmod m$，$i = 1, 2, \ldots, n$

解码得明文：P = $p_1 p_2 \cdots p_n$

## 1. 单表代换密码

- Caesar（凯撒）密码-----解密

方式二：查表（例k=3）

| 密文 | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 明文 | x | y | z | a | b | c | d | e | f | g | h | i | j | k |

| 密文 | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 明文 | l | m | n | o | p | q | r | s | t | u | v | w |

## 1. 单表代换密码

- Caesar（凯撒）密码-----特点

  密钥空间：$|K| = 25$，容易破译

- Caesar（凯撒）密码-----穷举攻击

  三个特征：

  已知加密和解密算法、密钥空间、明文语言。

## 1. 单表代换密码

- Caesar（凯撒）密码-----穷举攻击

密文：PHHW PH DIWHU WKH WRJD SDUWB

穷举 密钥 $K=1$， 明文 $P$ = oggv og chvgt vjg vqic rctva

$K=2$， 明文 $P$ = nffu nf bgufs uif uphb qbsuz

$K=3$， 明文 $P$ = meet me after the toga party

……

$K=24$， 明文 $P$ = rjjy rj fkyjw ymj ytlf ufwyd

$K=25$， 明文 $P$ = qiix qi ejxiv xli xske tevxc

前提：明文语言是已知

## 2. 多表代换密码

- 周期替代密码（维吉尼亚（Vigenere）密码）

这种替代法是循环的使用有限个字母来实现替代的一种方法

。若明文信息$m_1m_2m_3…m_n$，采用n个字母（n个字母为$B_1$，$B_2$，…$B_n$）替代法，那么，$m_n$将根据字母$B_n$的特征来替代

，$m_{n+1}$又将根据$B_1$的特征来替代，$m_{n+2}$又将根据$B_2$的特征来替代……，如此循环。可见$B_1$，$B_2$，…$B_n$就是加密的密钥。

## 2. 多表代换密码

- 周期替代密码（维吉尼亚（Vigenere）密码）

这种加密的加密表是以字母表移位为基础把26个英文字母进行循环移位，排列在一起，形成26×26的方阵。该方阵被称为维吉尼亚表。

## 2. 多表代换密码

➢ 周期替代密码（维吉尼亚（Vigenere）密码）----加密

方式一：数学公式

设明文P = $p_1 p_2 \Lambda\ p_n$，密钥k = $k_1 k_2 \Lambda\ k_n$，密文C = $c_1 c_2 \Lambda\ c_n$

① 明文编码；

② 计算 $c_i = p_i + k_i \mod 26$，$i = 1, 2, \ldots, n$；

③ 密文解码。

说明：若明文长度大于n，则K重复使用。

## 2. 多表代换密码

- 周期替代密码（维吉尼亚（Vigenere）密码）----加密

**方式二：查表---构造替换表：**

| | a | b | c | d | e | f | g | h | i | j | k | l | m | …… | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | A | B | C | D | E | F | G | H | I | J | K | L | M | …… | U | V | W | X | Y | Z |
| b | B | C | D | E | F | G | H | I | J | K | L | M | N | …… | V | W | X | Y | Z | A |
| c | C | D | E | F | G | H | I | J | K | L | M | N | O | …… | W | X | Y | Z | A | B |
| d | D | E | F | G | H | I | J | K | L | M | N | O | P | …… | X | Y | Z | A | B | C |
| e | E | F | G | | | | | | | | | | | …… | | | | | | |
| f | F | G | H | | | | | | | | | | | …… | | | | | | |
| g | G | H | I | | | | | | | | | | | …… | | | | | | |
| … | … | … | … | … | … | … | … | … | … | … | … | … | … | … | … | … | … | … | … | … |
| u | U | V | W | | | | | | | | | | | | | | | | | |

| | a | b | c | d | e | f | g | h | i | j | k | l | m | ..... | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | A | B | C | D | E | F | G | H | I | J | K | L | M | ..... | U | V | W | X | Y | Z |
| b | B | C | D | E | F | G | H | I | J | K | L | M | N | ..... | V | W | X | Y | Z | A |
| c | C | D | E | F | G | H | I | J | K | L | M | N | O | ..... | W | X | Y | Z | A | B |
| d | D | E | F | G | H | I | J | K | L | M | N | O | P | ..... | X | Y | Z | A | B | C |
| e | E | F | G | | | | | | | | | | | ..... | | | | | | |
| f | F | G | H | | | | | | | | | | | ..... | | | | | | |
| g | G | H | I | | | | | | | | | | | ..... | | | | | | |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| u | U | V | W | | | | | | | | | | | | | | | | | |
| v | V | W | X | | | | | | | | | | | | | | | | | |
| w | W | X | Y | | | | | | | | | | | | | | | | | |
| x | X | Y | Z | | | | | | | | | | | | | | | | | |
| y | Y | Z | A | | | | | | | | | | | | | | | | | |
| z | Z | A | B | C | D | E | F | G | H | I | J | K | L | S | T | U | V | W | X | Y |

## 2. 多表代换密码

- 周期替代密码（维吉尼亚（Vigenere）密码）----加密

方式二：查表---规则：表上边对应明文，左边对应密钥，交叉处为密文字母。

## 2. 多表代换密码

- 周期替代密码（维吉尼亚（Vigenere）密码）----解密

**方式一：数学公式**

$$p_i = c_i - k_i \bmod 26, i = 1, 2, \ldots, n$$

**方式二：查表---逆向查表**

## 2. 多表代换密码

- 周期替代密码（维吉尼亚（Vigenere）密码）----解密

方式二：查表---逆向查表

加密过程：P = “encode and decode”，k = “mykey”

## 加密过程：P = “encode and decode” ，k = “mykey”

| 字母序号 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 明文编码 | P = | 4 | 13 | 2 | 14 | 3 | 4 | 0 | 13 | 3 | 3 | 4 | 2 | 14 | 3 | 4 |
| 密钥编码 | k = | 12 | 24 | 10 | 4 | 24 | 12 | 24 | 10 | 4 | 24 | 12 | 24 | 10 | 4 | 24 |
| 加密 | C= | 16 | 37 | 12 | 18 | 27 | 16 | 24 | 23 | 7 | 27 | 16 | 26 | 24 | 7 | 28 |
| 模运算 | | | 11 | | | 1 | | | | | 1 | | 0 | | | 2 |
| 密文解码 | C = | Q | L | M | S | B | Q | Y | X | H | B | Q | A | Y | H | B |

# 解密过程：C = “QLMSBQYXHBQAYHB”，k = “mykey”

| 字母序号 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 密文编码 | C = | 16 | 11 | 12 | 18 | 1 | 16 | 24 | 23 | 7 | 1 | 16 | 0 | 24 | 7 | 2 |
| 密钥编码 | k = | 12 | 24 | 10 | 4 | 24 | 12 | 24 | 10 | 4 | 24 | 12 | 24 | 10 | 4 | 24 |
| 加密 | C = | 4 | -13 | 2 | 14 | -23 | 4 | 0 | 13 | 3 | -23 | 4 | -24 | 14 | 3 | -22 |
| 模运算 | | | 13 | | | 3 | | | | | 3 | | 2 | | | 4 |
| 密文解码 | C = | e | n | c | o | d | e | a | n | d | d | e | c | o | d | e |

## 2. 多表代换密码

- 周期替代密码（维吉尼亚（Vigenere）密码）----特点

  密钥空间：$|K| = 26^n$

  字母的统计规律进一步降低

  明、密文字母不是一一对应关系

  特例：$k_1 = k_2 = \cdots = k_n = k$ 时，是Caesar密码

- 密码分析

  寻找密钥长度T（即周期）：用卡西斯基试验

  将明文分为T组，按照Caesar密码的破译方法处理

## 2. 多表代换密码

- Vernam（弗纳姆）密码（1918）---加密

  设明文P= $(p_1 p_2 \cdots p_n)_{(2)}$ ， 密钥K= $(k_1 k_2 \cdots k_n)_{(2)}$，

  密文C= $(c_1 c_2 \cdots c_n)_{(2)}$

  加密计算： $c_i = p_i \oplus k_i$ ， （$i$=1,2,3,…,n）

  说明：若明文长度大于n，则k重复使用。

## 2. 多表代换密码

- Vernam（弗纳姆）密码（1918）---解密

$p_i = c_i \oplus k_i$，　（$i$=1,2,3,…,n）

- Vernam（弗纳姆）密码（1918）---安全性

当n很大时使用循环密钥不太安全，使用不循环密钥不太现实；

对大的n，选两个较短密钥，用本方法循环加密，生成长密钥。

## 3. 多字母代换密码

不同于前面介绍的代替密码都是每次加密一个明文字母，多字母代替密码将明文字符划分为长度相同的消息单元，称为明文组，对字符块成组进行代替，这样一来使密码分析更加困难，多字母代替的优点是容易将字母的自然频度隐蔽或均匀化。从而有利于抗击统计分析。Playfair密码、Hill密码都是这一类型的密码。

## 3. 多字母代换密码

- Playfair（普莱费厄）密码---应用

构造Playfair板，选密钥K：例K=“monarchy”

| | | | | |
|---|---|---|---|---|
| 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 |

## 3. 多字母代换密码

- Playfair（普莱费厄）密码---**加密**

明文分组（填充）：2个字母 / 组

同行字母对加密：循环向右，ei→FK

同列字母对加密：循环向下，cu→EM，xi→AS

其它字母对加密：矩形对角线字母，且按行排序，ya→BN，es→IL（或JL）

## 3. 多字母代换密码

- Playfair（普莱费厄）密码---解密

  加密的逆向操作

- Playfair（普莱费厄）密码---特点

  密钥空间： $|K|=25!\approx 1.6\times 10^{25}$

  字母的统计规律降低

  明、密文字母不是一一对应关系

  属于字母组的代换技术

## 3. 多字母代换密码

- Hill（希尔）密码（1929）---加密

  明文分组并编码

  $C \equiv KP \bmod 26$,其中，K为密钥矩阵，P、C分别为明、密文分组

- Hill（希尔）密码（1929）---解密

  密文分组并编码：$P \equiv K^{-1}C \bmod 26$

  对密钥矩阵K 的要求：在mod 26下可逆

## 3. 多字母代换密码

- Hill（希尔）密码（1929）---举例

加密密钥矩阵K= $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{pmatrix}$

明文分组P=“pay more money” = “pay mor emo ney” = $P_1P_2P_3P_4$

明文编码 $P_2 = \begin{pmatrix} m \\ o \\ r \end{pmatrix} = \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix}$

加密 $C_2 \equiv KP_2 \equiv \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 527 \\ 651 \\ 375 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 3 \\ 11 \end{pmatrix} \bmod 26$

## 3. 多字母代换密码

- Hill（希尔）密码（1929）---举例

解码 $C_2 = \begin{pmatrix} H \\ D \\ L \end{pmatrix}$，即 $C_2$=“HDL”

## 3. 多字母代换密码

- Hill（希尔）密码（1929）---举例

解密

$$C_2 = \text{“HDL”} = \begin{pmatrix} H \\ D \\ L \end{pmatrix} = \begin{pmatrix} 7 \\ 3 \\ 11 \end{pmatrix}$$

$$P_2 \equiv K^{-1} C_2 \equiv \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 7 \\ 3 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 220 \\ 222 \\ 355 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix} \bmod 26$$

所以

$$P_2 = \begin{pmatrix} m \\ o \\ r \end{pmatrix} = \text{“mor”}$$

## 3. 多字母代换密码

- Hill（希尔）密码（1929）---特点

  密钥空间：$|K|=25! \approx 1.6\times10^{25}$

  字母的统计规律降低

  明、密文字母不是一一对应关系

## 3. 多字母代换密码

- Hill（希尔）密码（1929）---模运算下矩阵求逆

  可逆的条件：

  K模m可逆<=>$K^{-1}$ ,(|$K$|,m)=1,且 $K^{-1}$ =|$K$|$^{-1}\tilde{K}$

  其中，$\tilde{K}$ 是矩阵K 的伴随矩阵， |$K$|$^{-1}$是数|$K$|模m的逆。

## 3. 多字母代换密码

- **Hill（希尔）密码（1929）---举例**

$$m=26,\ K=\begin{pmatrix}4 & 3\\ 7 & 6\end{pmatrix},\ |K|=3,\ (3,26)=1,\ 故|K|^{-1}=3^{-1}存在,\ 3^{-1}$$

$$\equiv 9\ (\mathrm{mod}\ 26),\ 所以$$

$$K^{-1}\equiv 3^{-1}\tilde{K}\equiv 9\begin{pmatrix}6 & -3\\ -7 & 4\end{pmatrix}\equiv\begin{pmatrix}54 & -27\\ -63 & 36\end{pmatrix}\equiv\begin{pmatrix}2 & 25\\ 15 & 10\end{pmatrix}\ (\mathrm{mod}\ 26)$$

## 3. 多字母代换密码

- Hill（希尔）密码（1929）---举例

$$m=26,\ \mathrm{K}=\begin{pmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{pmatrix},\ |K|=-939\equiv 23\ (\mathrm{mod}\ 26),\ (23,26)=1,$$

故$|K|^{-1}=23^{-1}$存在，$23^{-1}\equiv 17\ (\mathrm{mod}\ 26)$，所以

$$\tilde{K}=\begin{pmatrix}300 & -313 & 267\\ -357 & 313 & 252\\ 6 & 0 & -51\end{pmatrix}\equiv\begin{pmatrix}14 & -1 & 7\\ -19 & 1 & 8\\ 6 & 0 & 1\end{pmatrix}\ (\mathrm{mod}\ 26)$$

$$|K|^{-1}\equiv 17\begin{pmatrix}14 & -1 & 7\\ -19 & 1 & 8\\ 6 & 0 & 1\end{pmatrix}\equiv\begin{pmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{pmatrix}\ (\mathrm{mod}\ 26)$$

## 4. 换位密码

在换位密码中，明文的字母保持相同，但顺序被打乱了，由于密文字符与明文字符相同，密文中字母的出现频率与明文中字母的出现频率相同，密码分析者可以很容易地由此进行判别。虽然许多现代密码也使用换位，但由于它对存储要求很大，有时还要求消息为某个特定的长度，因而比较少用。

## 5. 一次一密

- 随机密钥：给出任何长度与密文一样的明文，都存在着一个密钥产生这个明文。因此，如果用穷举法搜索所有可能的密钥，就会得到大量可读、清晰的明文，但没有办法确定哪一个是真正所需的。
- 理论上不可破：一次一密的安全性完全取决于密钥的随机性，如果构成密钥的字符流是真正随机的，那么构成密文的字符流也是真正随机的。
- 实际上不可行

  产生大量的随机密钥难；

  密钥分配与保护更难。

# 2.3 经典密码体制---置换技术（通过置换而形成新的排列）

## 1. 栅栏技术

- 思想：以列（行）优先写出明文，以行（列）优先读出各字母作为密文。
- 例子：先行后列

明文=“meet me after the toga party” $\Rightarrow$ $\begin{cases} mematrhtgpra \\ etefeteoaat \end{cases}$

$\Rightarrow$MEMATRHTGPRYETEFETEOAAT=密文

## 1. 栅栏技术

- 思想：以列（行）优先写出明文，以行（列）优先读出各字母作为密文。
- 例子：先列后行

明文=“attackpostponeduntiltwoamxyz”

$$\Rightarrow \begin{cases} a & t & t & a & c & k & p \\ o & s & t & p & o & n & e \\ d & u & n & t & i & l & t \\ w & o & a & m & x & y & z \end{cases}$$

$\Rightarrow$ AODWTSUOTTNAAPTMCOIXKNLYPETZ＝密文

- 破译：找周期

## 2. 改进

- 带有密钥：密钥K=4312567（密文中先取第3列，依次再取第4、2，1，5，6，7列）
- 例子：先列后行

明文＝ATTA CKPO STOP NEDU NTIL TWOA MXYZ

密文＝TTNA APTM TSUO AODW COIX KNLY PETZ

本质：置换=$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \cdots & 24 & 25 & 26 & 27 & 28 \\ 3 & 10 & 17 & 24 & 4 & 11 & \cdots & 27 & 7 & 14 & 21 & 28 \end{pmatrix}$

- 再改进：重复加密

## 2. 改进

**关于置换一例：** 将编号为 1～52 的卡片分为 1～26 ，27～52 两组，交错互相插入。则这样的交错插入重复 8 次后就会恢复到原来的牌序。

（证）

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 洗牌前 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | … | 26 | 27 | 28 | … | 49 | 50 | 51 | 52 |
| 洗牌后 | 1 | 27 | 2 | 28 | 3 | 29 | 4 | 30 | 5 | … | 39 | 14 | 40 | … | 25 | 51 | 26 | 52 |

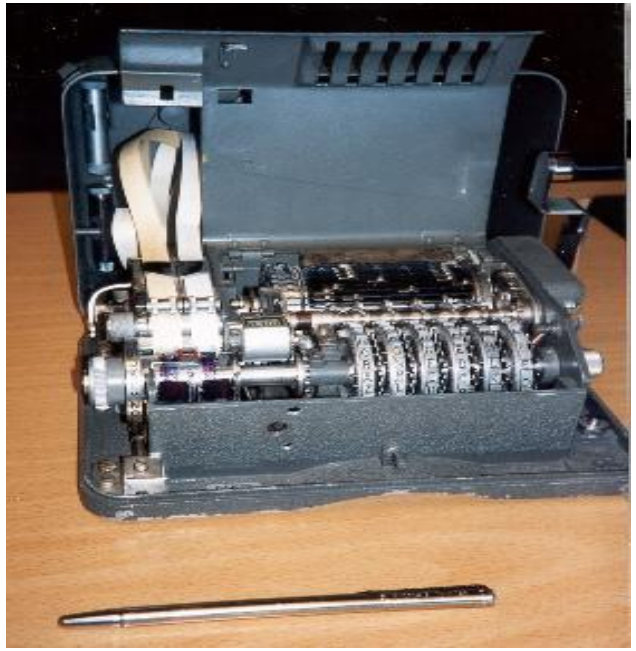
第一次插入相当对 1～52 作一次置换 p＝(1)(2，27，14，33，17，9，5，3)(4，28，40，46，49，25，13，7)(6，29，15，8，30，41，21，11)(10，31，16，34，43，22，37，19)(12，32，42，47，24，38，45，23)(18，35)(20，36，44，48，50，51，26，39)(52).

其中最长的轮换为 8 阶，而 k 阶轮换重复 k 次后恢复原状，故结论成立。

所以，美国的研究人员认为，扑克牌洗 7 次最合适。

# 2.3 经典密码体制---转轮机

- 应用：德国（Enigma密码机）和日本（Purple密码机）
- 机械式
- 原理：一个圆筒定义一个单表替换
- 多层迭代26*26*26=17576个替换字母表



# 2.3 经典密码体制---隐写术

- 隐藏明文信息的方法

  隐写术：隐藏信息的存在

  密码学：通过对信息的转换实现信息的对外不可读

- 方法

  嵌入技术

  字符标记

  不可见墨水

  针刺

# 2.3 经典密码体制---隐写术

- 特点

  优点：即使秘密通信被发现，但重要内容不会丢失

  缺点：

  需要额外的付出以隐藏相对较少的信息

  一旦被破解，整个方案无用

  解决办法：利用密钥，先加密再隐写

- 其他隐写方法

  头皮上的秘密，蛋壳上的秘密

- 现代隐写术：数字水印---版权保护、防伪

# 2.4 密码分析

**密码分析学是在不知道密钥的情况下，恢复出明文的科学。**

成功的密码分析能恢复出消息的明文或密钥。密码分析也可以发现密码体制的弱点，最终得到上述结果。密钥通过非密码分析方式的丢失叫做泄露。常用的密码分析攻击有四类。

- **唯密文攻击（Cipher Text-Only Attack）**

密码分析者有一些消息的密文，这些消息都用同一加密算法加密。密码分析者的任务是恢复尽可能多的明文，或者最好是能推算出加密消息的密钥来，以便可采用相同的密钥解出其他被加密的消息。

- **已知明文攻击（Known-Plaintext Attack）**

密码分析者不仅可得到一些消息的密文，而且也知道这些消息的明文。分析者的任务就是用加密信息推出用来加密的密钥或推导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。

- **选择明文攻击（Chosen-Plaintext Attack）**

分析者不仅可得到一些消息的密文和相应的明文，而且他们也可选择被加密的明文。这比已知明文攻击更有效。因为密码分析者能选择特定的明文块去加密，那些块可能产生更多关于密钥的信息，分析者的任务是推出用来加密消息的密钥或导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。

- **适应选择明文攻击（Adaptive-Chosen-Plaintext Attack）**

这是选择明文攻击的特殊情况。密码分析者不仅能选择被加密的明文，而且也能基于以前加密的结果修正这个选择。在选择明文攻击中，密码分析者还可以选择一大块被加密的明文，而在自适应选择密文攻击中，可选取较小的明文块，然后再基于第一块的结果选择另一明文块，依此类推。

- **选择密文攻击（Chosen-Cipher Text Attack）**

密码分析者能选择不同的被加密的密文，并可得到对应的解密的明文，例如密码分析者存取一个防篡改的自动解密盒，密码分析者的任务是推出密钥。

- **选择密钥攻击（Chosen-Key Attack）**

这种攻击并不表示密码分析者能够选择密钥，它只表示密码分析者具有不同密钥之间的关系的有关知识。

- **软磨硬泡攻击（Rubber-Hose Cryptanalysis）**

这种攻击是对密码分析者威胁、勒索，或者折磨某人，直到他给出密钥为止。行贿有时称为购买密钥攻击（purchase-key attack）。这些是非常有效的攻击，并且经常是破译算法的最好途径

- **语言冗余度与密码分析**

人类语言是有冗余度的；

字母使用的频率是不相同的；

在英语中，E的使用率是最高的，其次是T,R,N,I,O,A,S。其他字母使用的较低，

- **英语字母及组合使用频率**

| 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 |


# Thank you!

网络攻击是实现“不战而屈人之兵”最有效的武器之一

没有网络信息安全就没有国家安全