

# 密码学

## 第二讲 密码学的基本概念

王后珍

武汉大学国家网络安全学院

空天信息安全与可信计算教育部重点实验室





# 目录

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SM4与分组密码的应用技术

第六讲 序列密码基础

第七讲 祖冲之密码

第八讲 中国商用密码HASH函数SM3

第九讲 复习





# 目录

- 第十讲 公钥密码基础
- 第十一讲 中国商用公钥密码SM2加密算法
- 第十二讲 数字签名基础
- 第十三讲 中国商用公钥密码SM2签名算法
- 第十四讲 密码协议
- 第十五讲 认证
- 第十六讲 密钥管理：对称密码密钥管理
- 第十七讲 密钥管理：公钥密码密钥管理
- 第十八讲 复习

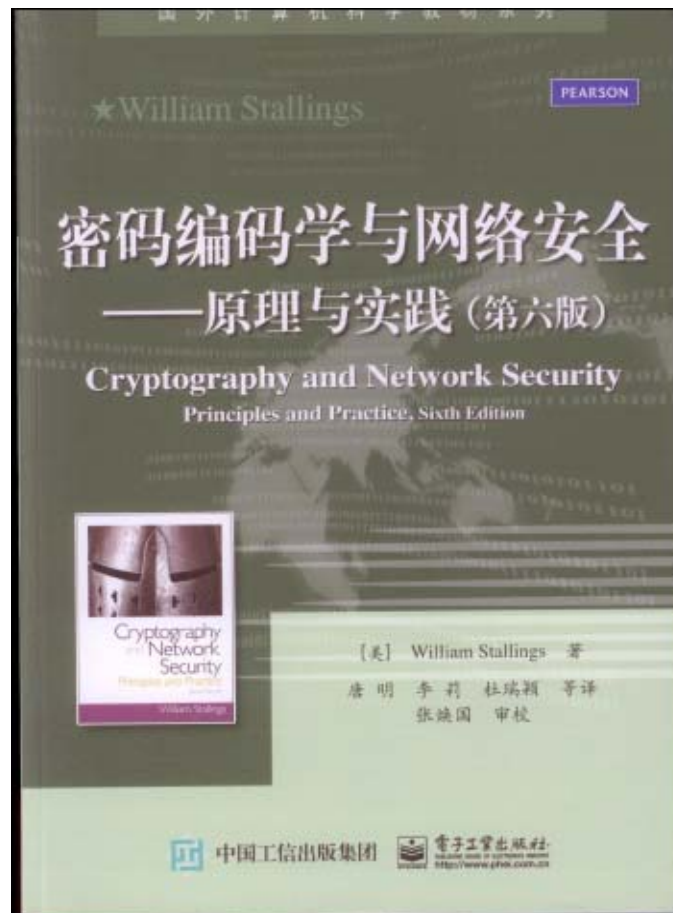


# 教材与主要参考书

## 教材



## 参考书



武汉大学





# 本讲内容

- 一、我国的密码政策
- 二、密码学的基本概念
- 三、古典密码





# 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！**





# 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

- 对数据进行伪装以隐蔽信息，使未授权者不能理解它的真实含义。
  - 所谓伪装就是对数据进行一组可逆的数学变换。
  - 伪装前的原始数据称为明文，伪装后的数据称为密文。
  - 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。
  - 用于加密的一族数学变换称为加密算法。用于解密的一族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，其中  $K = \langle K_e, K_d \rangle$   
 $K_e$  是加密钥， $K_d$  是解密密钥

④加密算法 $E$ ：一族由  $M \rightarrow C$  的加密变换

⑤解密算法 $D$ ：一族由  $C \rightarrow M$  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 $C$ :

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

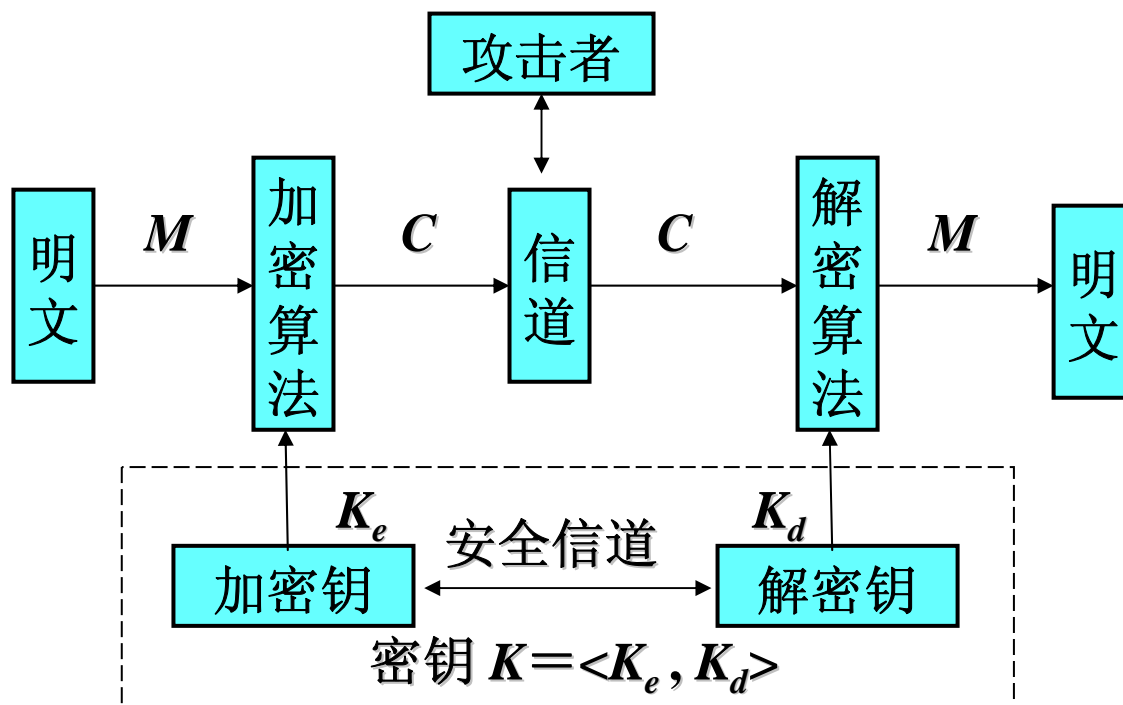
- 而解密算法 $D$ 在密钥 $K_d$ 的控制下将密文解出同一明文 $M$ 。

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



## 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/对称密码/单密钥密码：

■  $K_e = K_d$

■ 典型密码：DES，AES，SM4，ZUC，RC4

(2) 公开密钥密码/非对称密码/双密钥密码：

■  $K_e \neq K_d$

■ 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，ELGAMAL，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（ZUC）

##### (2) 分组密码：

- 明文、密文、密钥以块（分组）为单位加解密

- 商用密码的主流

- 典型密码：DES，AES，SM4





## 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, SM4, RC4, ZUC, RSA, ELGAMAL, ECC



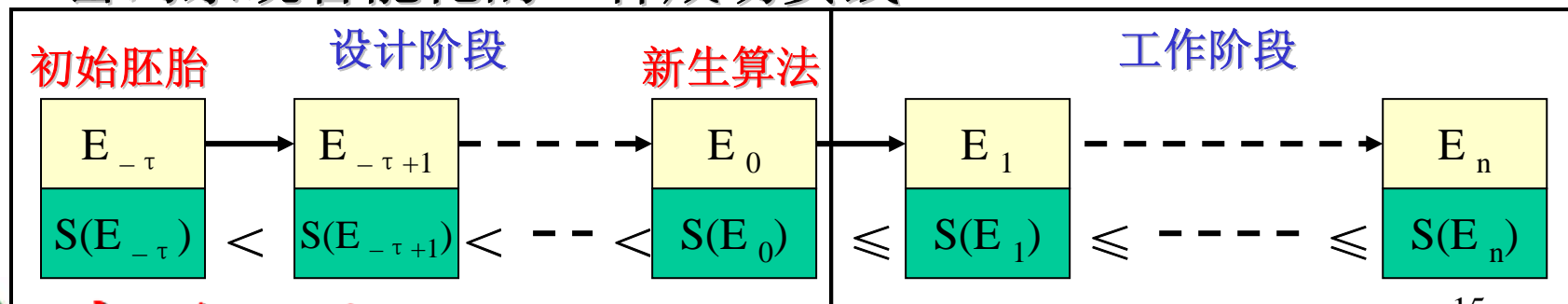
## 二、密码学的基本概念

### 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 基于物理学的密码：量子密码（量子密钥分发QKD）

- 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

- 在唯密文攻击下无条件安全的密码

- 安全基于量子的物理属性







## 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 基于生物学的密码：DNA密码

- 已有各种密码方案
- 安全性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密码分析方法都不能被攻破，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。它就是“**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

- 由 $C$ 求出 $M$ ：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；
- 由 $C$ 求出 $K$ ：密码分析者采用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 早期的基于数学的密码分析主要是统计分析。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数学分析。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

- 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。
- 获取密钥/获取密码算法为目的
  - ◆ 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**）

- 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**）

- 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。
- 计算机文件加密和数据库加密，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**）

- 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！

##### ④选择密文攻击（**Chosen-Ciphertext attack**）

- 选择密文攻击是指密码分析者能够选择密文并获得相应的明文。
- 主要攻击公钥密码的数字签名。
- 这也是对攻击者很有利的情况！





## 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。

#### (3) 数学

- ①设计一个密码就是设计一个数学函数；
- ②破译一个密码就是求解一个数学难题。





## 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。
- 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  $p$  ，  
解密密钥是置换矩阵  $p^{-1}$  。

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

- 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（简单代替密码）

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:  $f:A \rightarrow B$

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


$$j = i+k \bmod n, \quad 0 < k < n$$

■ 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。

■ 密文字母表是把明文字母表循环右移3位后得到的字母表。





## 三、古典密码

### (1)单表代替密码

#### ①、加法密码

■ 凯撒密码举例：

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


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

明文： MING CHEN WU DIAN FA DONG FAN GONG

密文： **PLQJ FKHQ ZX GLDQ ID GRQJ IDQ JRQJ**







## 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:  $f:A \rightarrow B$

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

$$j = ik \bmod n, \text{ 其中, } (n, k) = 1.$$

■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

#### ②、乘法密码

■采以英文字母表，取 $k=13$ 时， $(13,26)=13$ ，密文字母表为：

$B=\{A,N,A,N, A,N,A,N, A,N,A,N, A,N,A,N, A,N,A,N, A,N\}$

■密文字母表只包含A和N，密文将不能正确解密。

■若取 $k=5$ ， $(5,26)=1$ ，便得到如下合理的密文字母表：

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

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






## 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：

**$B = \{ \text{HAJRXOBKSZNCLTGDMUYFPVEIQW} \}$**



**武汉大学**





### 三、古典密码

#### ●举例：


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

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

明文： MING CHEN WU DIAN FA DONG FAN GONG

密文： **LSTBJ KXTEP RSHTO HRGTB OHTBG TB**





## 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，表示序号
- ◆ 12个汉字代表十二个月
- ◆ 30汉字代表一个月的三十天
- ◆ 9组符号代表数字一、二、...、九，表示银量
- ◆ 密文表要记住，不准写在纸上，且经常变化





### 三、古典密码

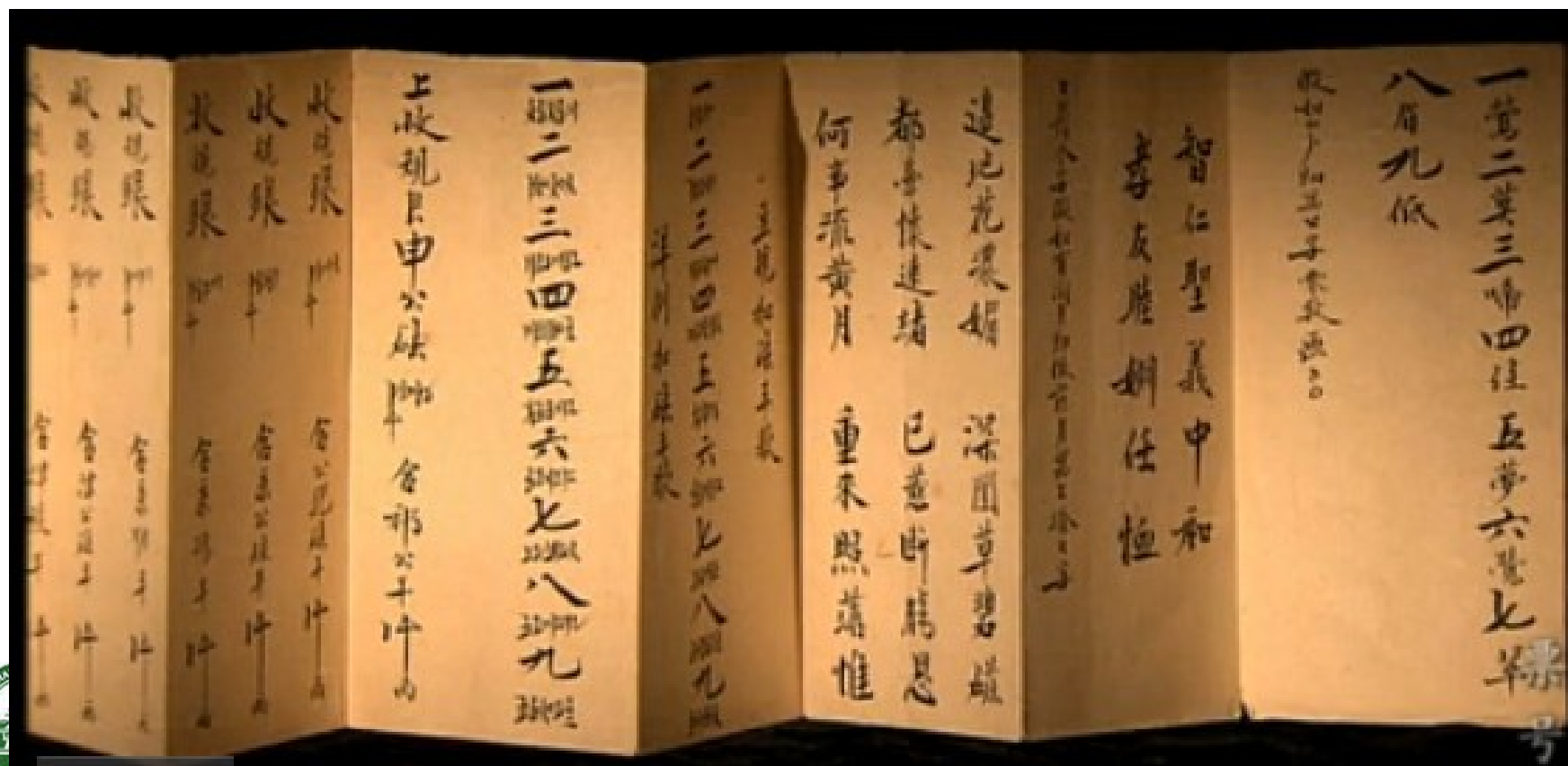
#### ● 举例：山西平遥市日升昌票号密码

银量

30天

12个月

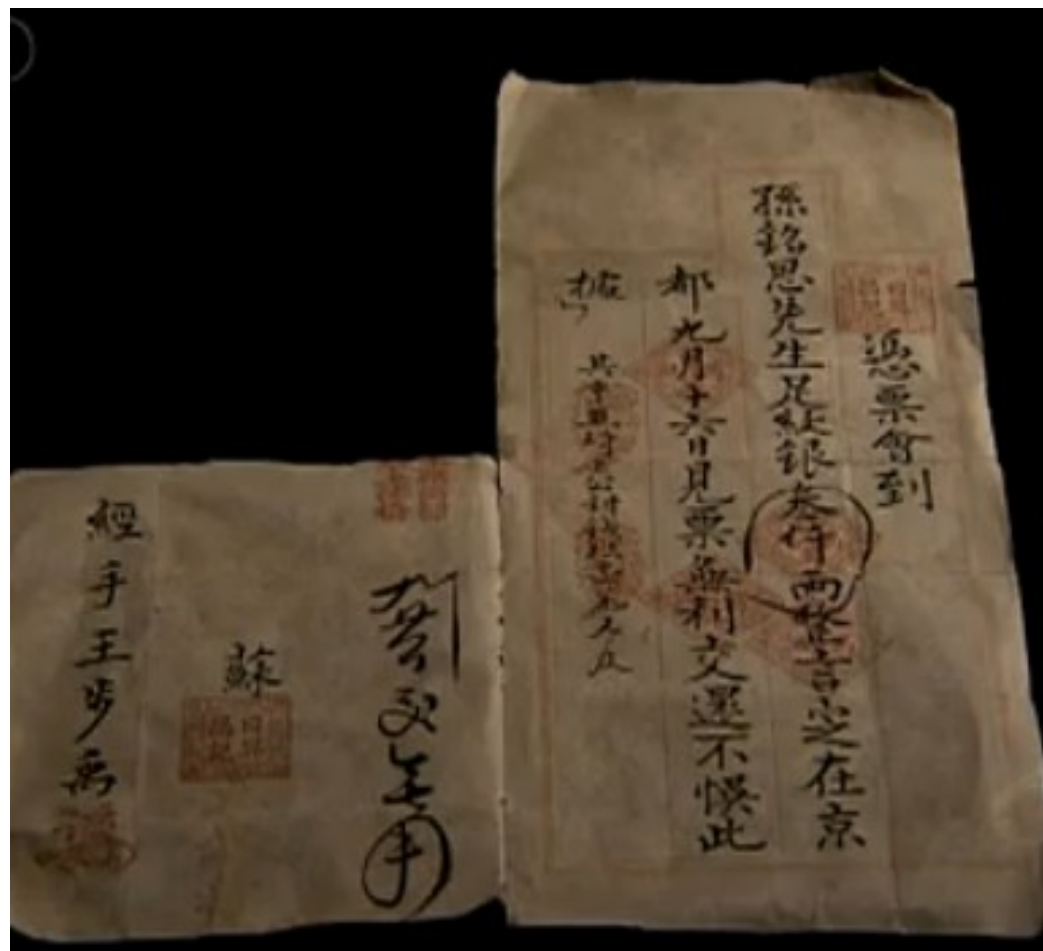
序号






### 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。








## 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。



武汉大学

# 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，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或重用，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  $f(a_i) = b_i = a_j$

$$j = i + k \bmod n, \quad 0 < k < n$$

■ 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。





## 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、说明密码体制的分类，它们各有什么特点？
- 2、什么是密码分析？密码分析的方法有哪些类型？它们各有什么特点？
- 3、已知置换如下：

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

- ①设明文=642135，求出密文。
- ②求出逆置换 $P^{-1}$ ，设密文=214365，求出明文。





谢 谢！



武汉大学



"BENEDICT CUMBERBATCH IS OUTSTANDING"

RADIO TIMES

"THE BEST BRITISH FILM OF THE YEAR"

★★★★★

THE INDEPENDENT

"AN INSTANT CLASSIC"

★★★★★

GLAMOUR

THE IMITATION GAME

BENEDICT CUMBERBATCH KEIRA KNIGHTLEY

BLACK PANTHER PICTURES PRESENTS A FILM BY JOHNNY JOHNSON "THE IMITATION GAME" A FILM BY JOHNNY JOHNSON CASTING BY JONATHAN HARRIS COSTUME DESIGNER JONATHAN HARRIS EDITOR JONATHAN HARRIS EXECUTIVE PRODUCERS JONATHAN HARRIS PRODUCED BY JONATHAN HARRIS WRITTEN BY JONATHAN HARRIS BASED ON THE BOOK BY SIMON SINGH

BASED ON THE INCREDIBLE TRUE STORY

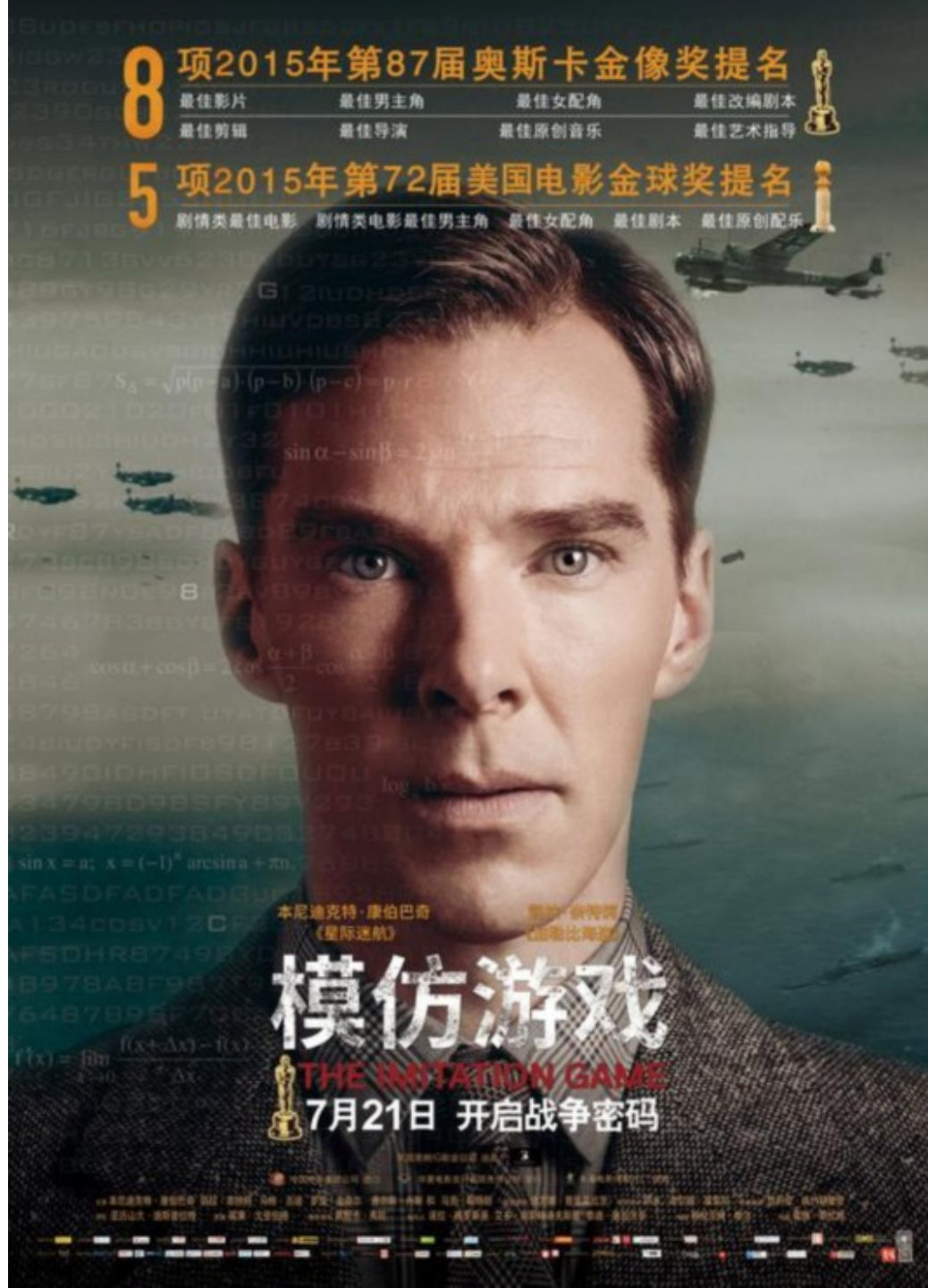
IN CINEMAS JANUARY 2015

《模仿游戏》获  
第87届奥斯卡金像  
奖最佳改编剧本奖。

《模仿游戏》讲  
述了“计算机科学之  
父”艾伦·图灵的传  
奇人生，故事主要聚  
焦于图灵协助盟军破  
译德国密码系统“英  
格玛”，从而扭转二  
战战局的经历。



这部由“卷福”主演的《模仿游戏》曾拿下8项奥斯卡提名、5项金球奖提名，但引进国内的路途却曲曲折折，在经历了全球同步上映无望之后，时隔七个月正式公映又不幸遇上“国产保护月”，上映空间被缩减无几（每日不足5%的排片，上映六天，仅报收1840万……）





艾伦·图灵，计算机科学之父，战时密码的破译者，偏见的牺牲品。

——英国官方给图灵的纪念铜牌

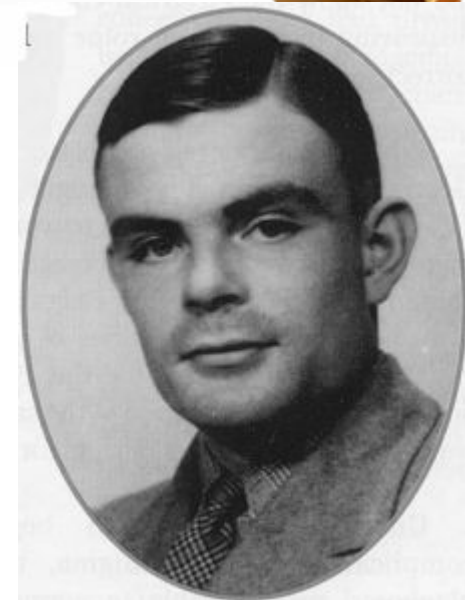
# Enigma: 密码学界划时代的丰碑



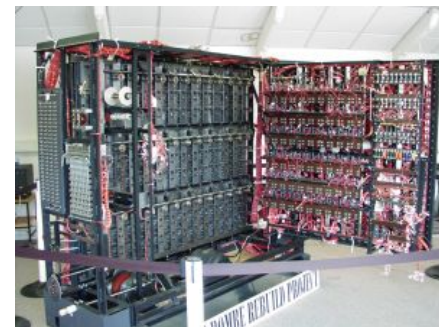
德国人  
亚瑟·谢尔比乌斯



波兰数学家和密码学家  
马里安·雷耶夫斯基



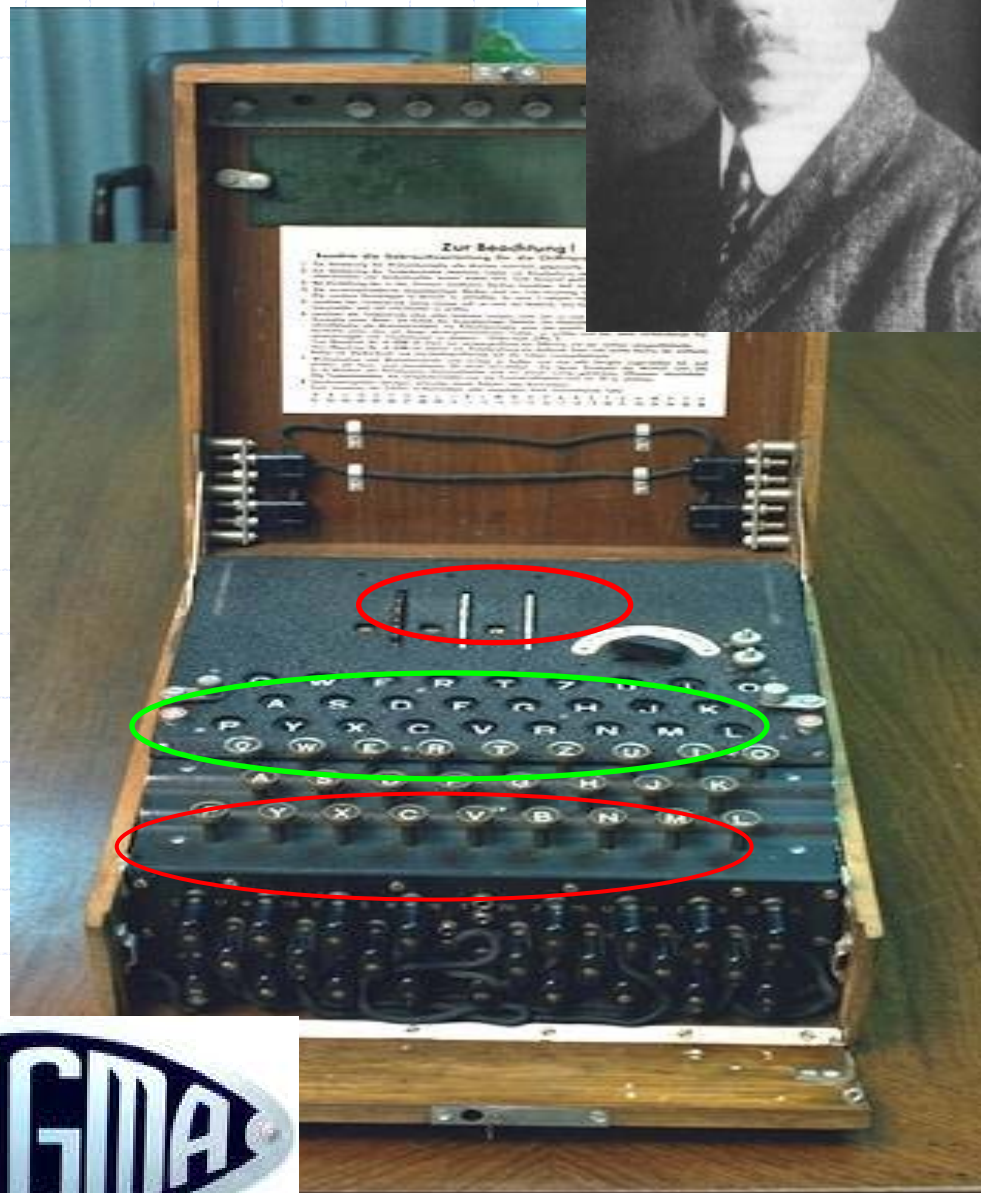
英国天才的数学家和  
计算机理论专家  
阿兰·图灵





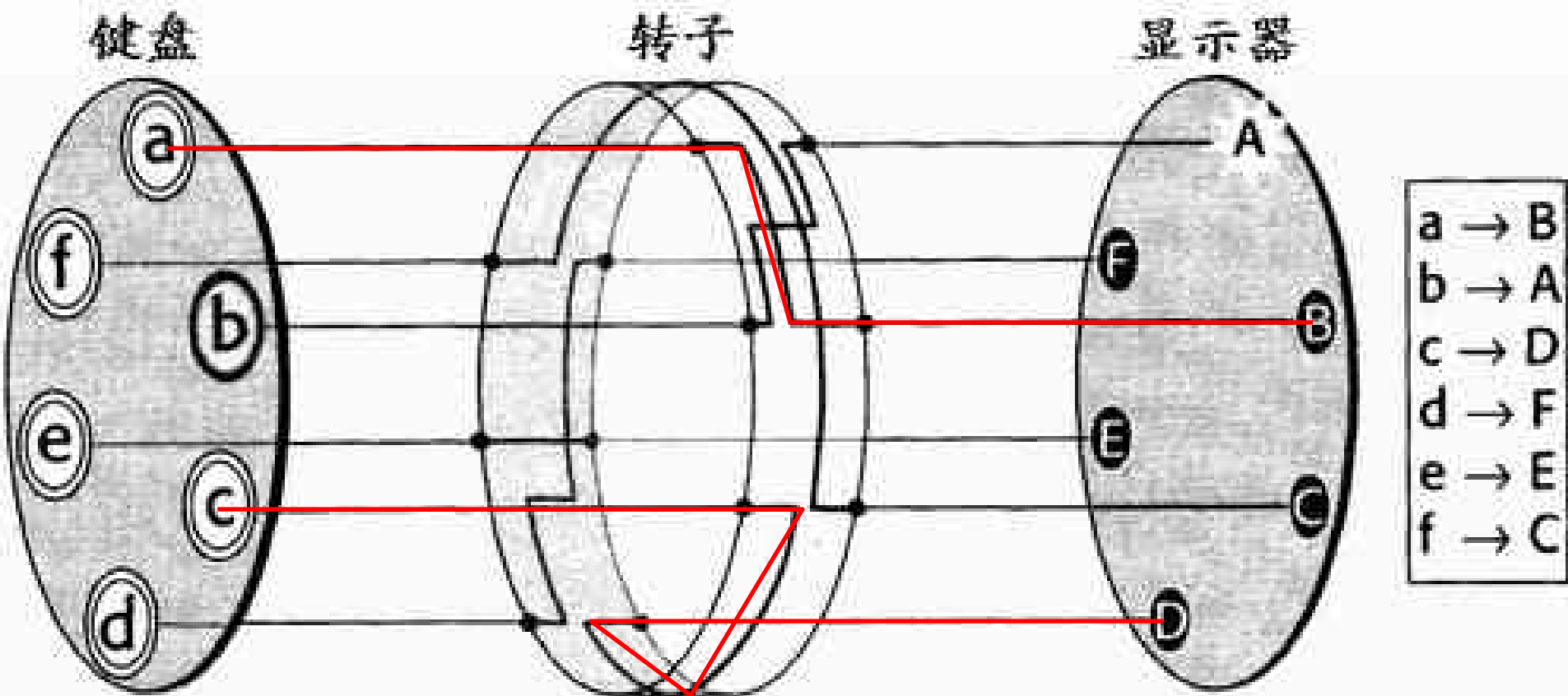
# Enigma密码机

- ❖ 创世纪的机械密码机
- ❖ 发明者：  
**Arthur Scherbius**  
亚瑟·谢尔比乌斯
- ❖ 时间：1918
- ❖ 意义：彻底改变了手工加密的历史，实现了加密的机械化
- ❖ Enigma：德语：谜
- ❖ 因此又称“谜密”

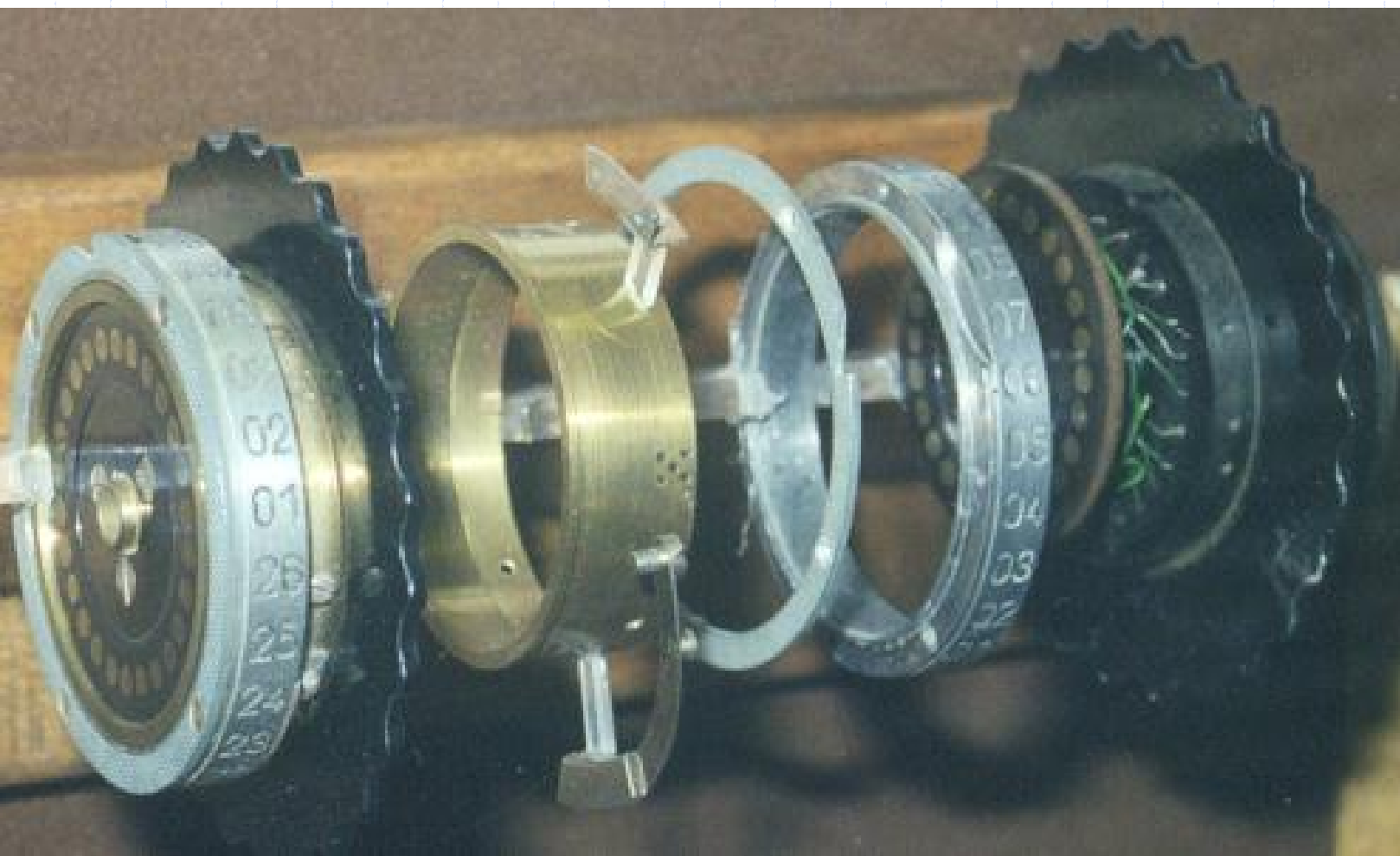




# 构成

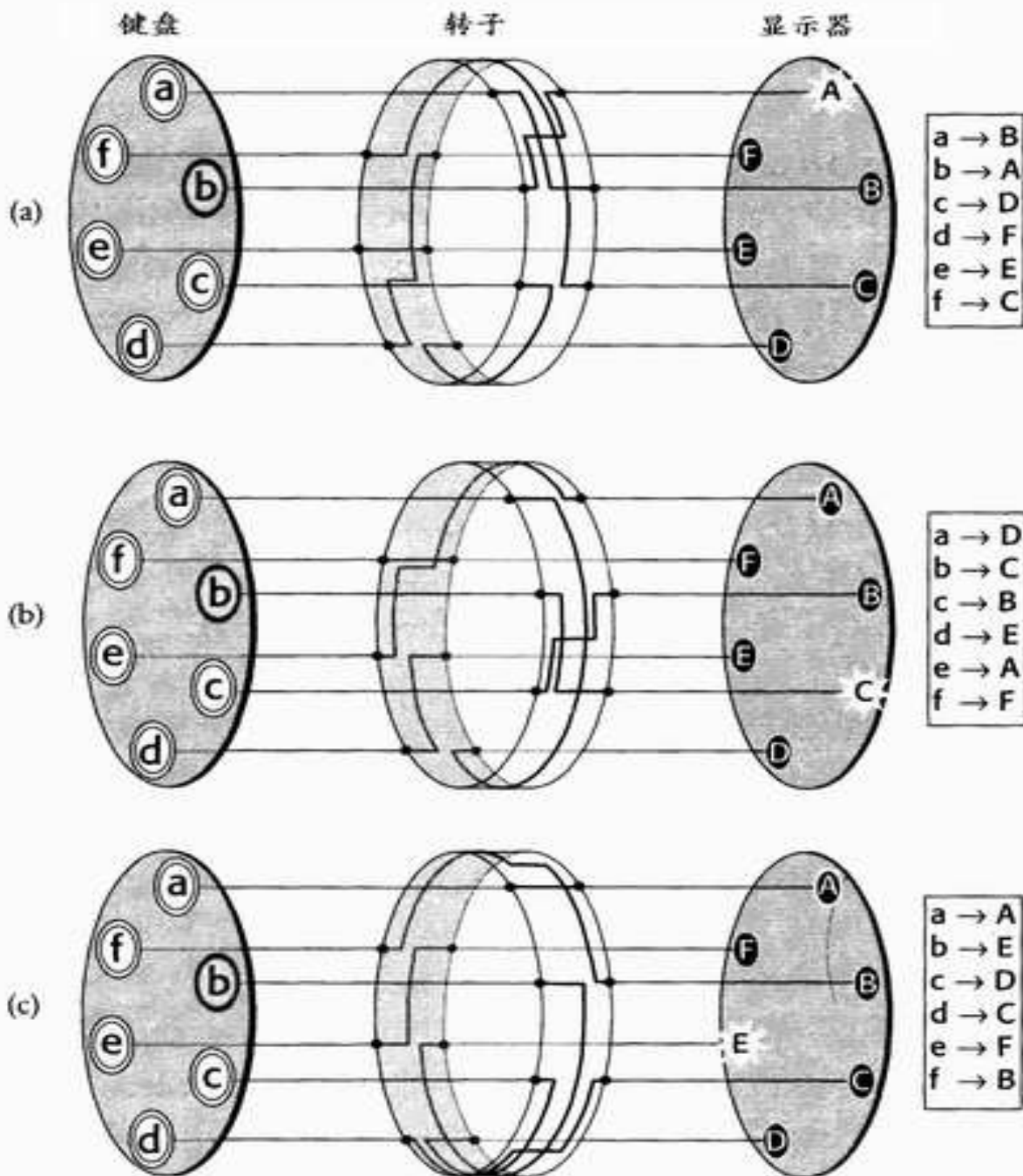


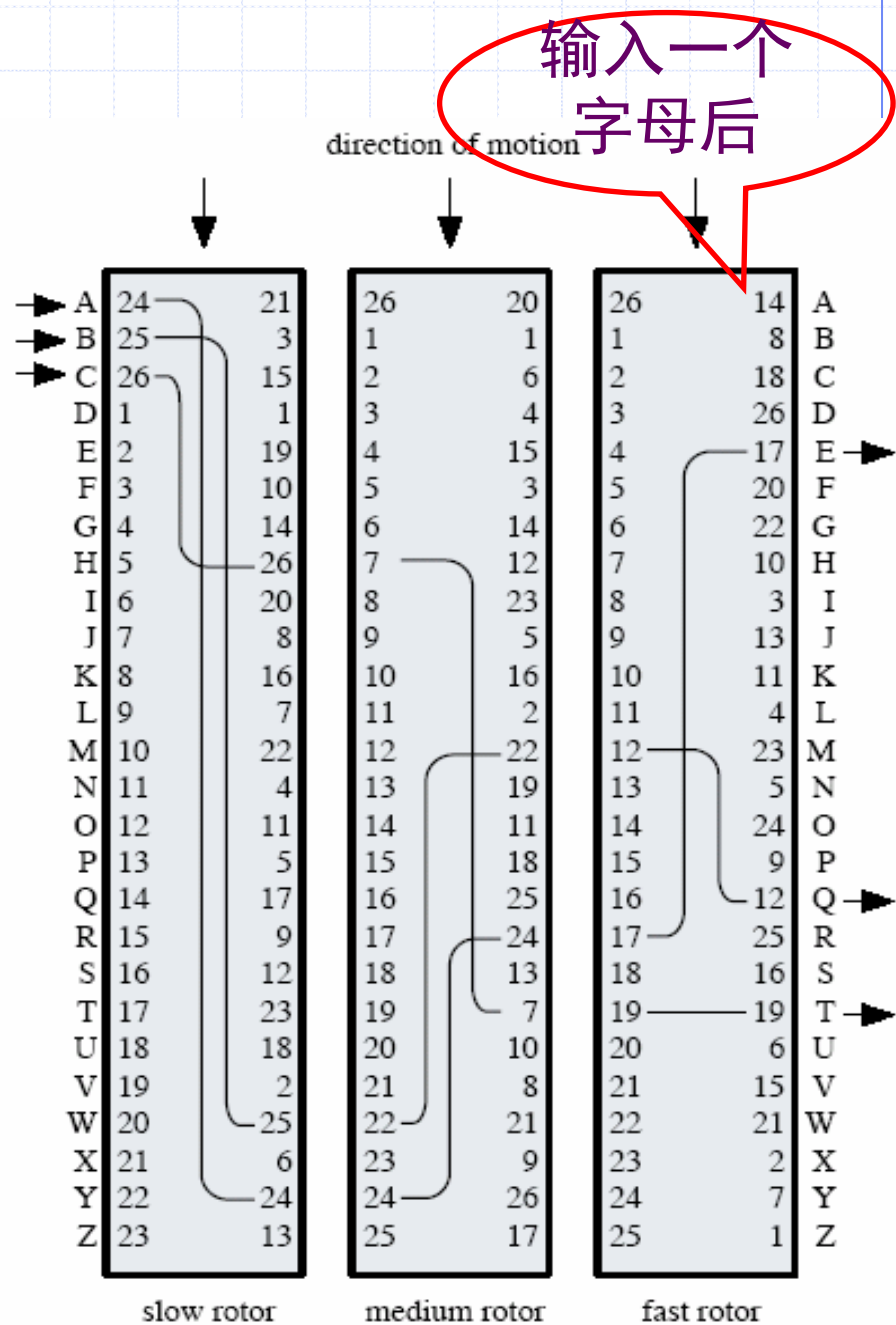
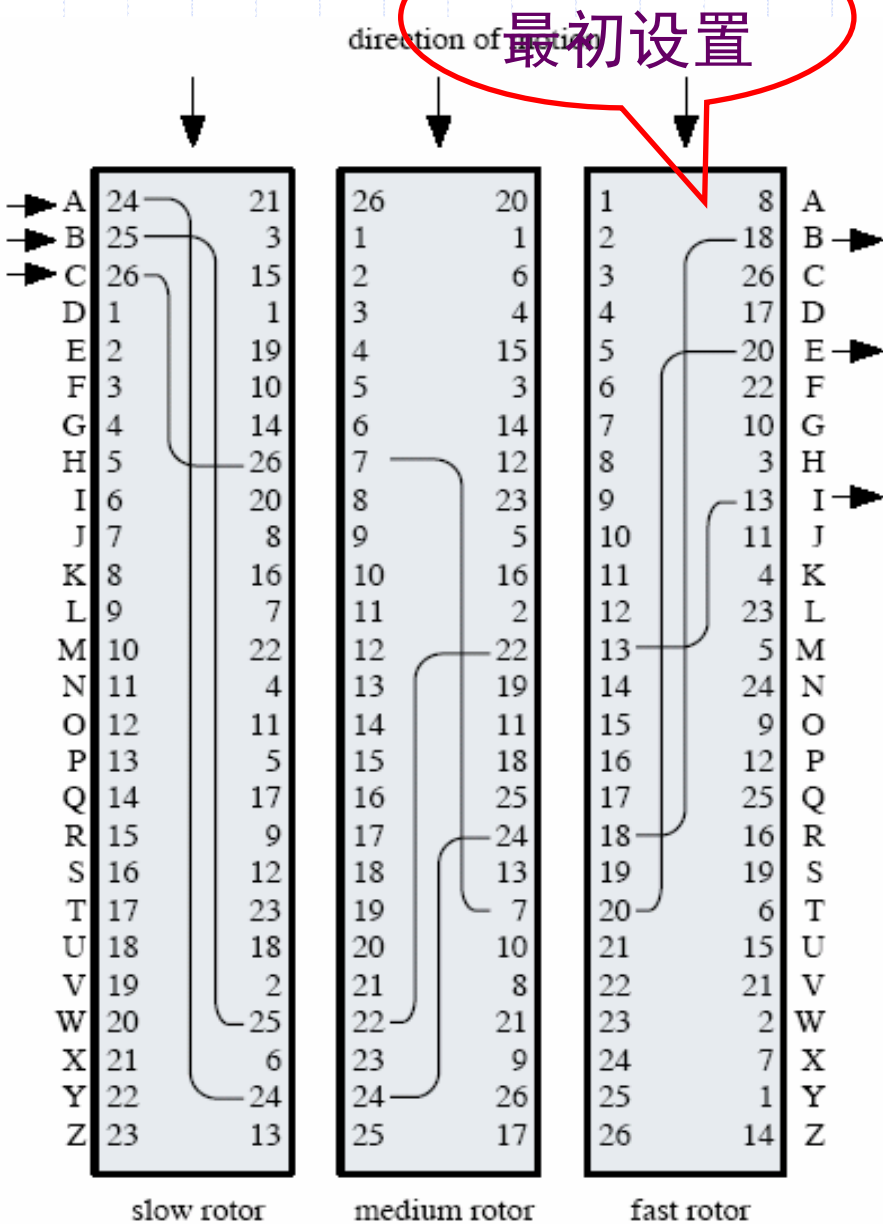
# 主要部件：转子



# 转子

- ❖ 加密一次，转子就旋转一次，这样对应关系就变了
- ❖ 这就是谢尔比乌斯关于ENIGMA的最重要的设计：每次使用不同的替换密钥



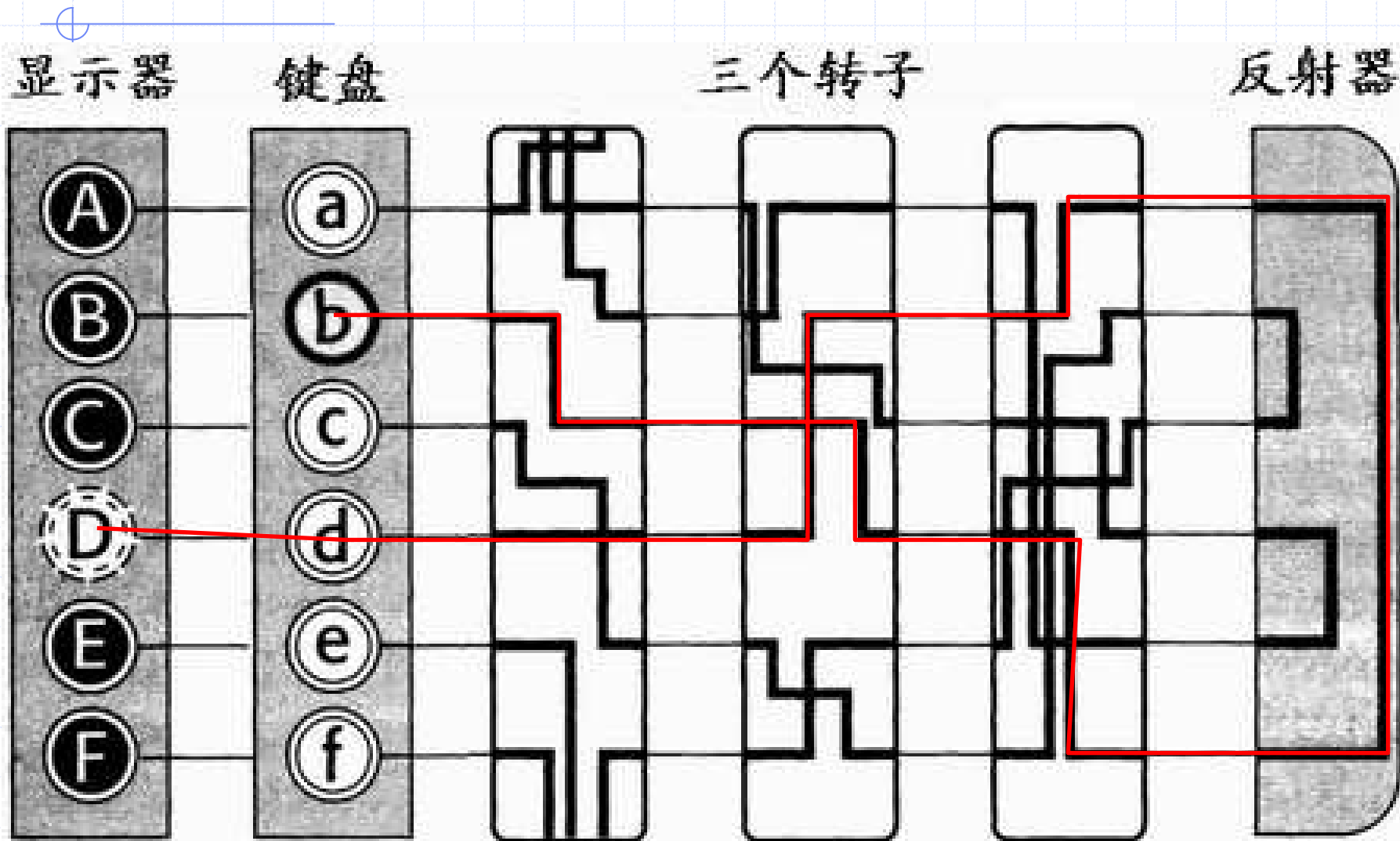




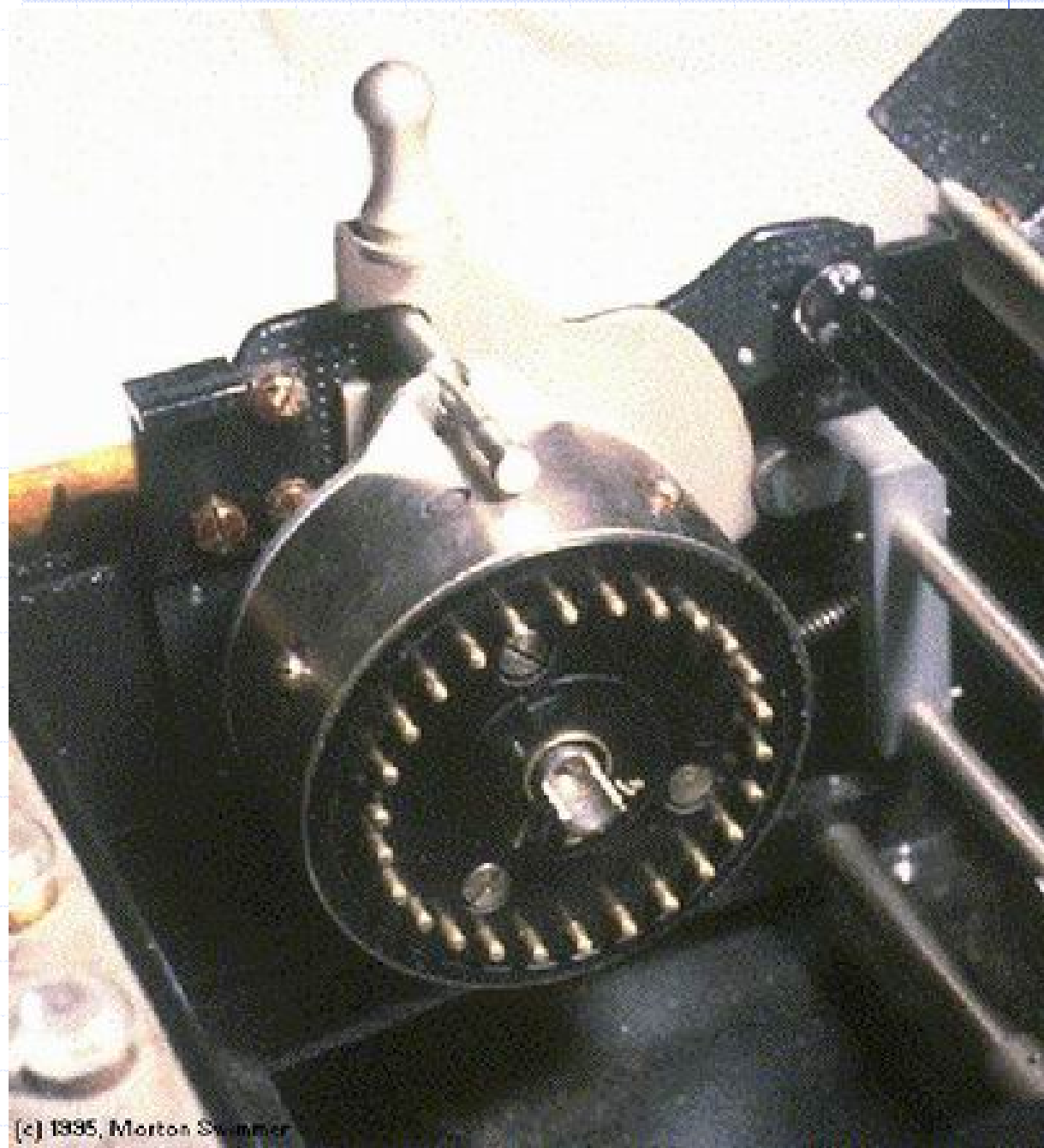
# 多转子

- ❖ 第一个转子旋转一周，就带动第二个转子旋转；
- ❖ 第二个转子旋转一周，就带动第三个转子旋转
- ❖ 三个轮子，可以变化出 $26 \times 26 \times 26 = 17576$ 种字母代换关系
- ❖ 如果增加轮子，字母间的代换关系将增加26种
- ❖ 相当于使用17576张字母代换表进行加密，完全打乱了字母频率，因而频率分析完全失效
- ❖ 使用简单的强力破解：
  - 对第一个明文字母：有17576变换,对第二个明文字母：有17576变换，对10个字母的密文： $17576^{10} = 10^{42}$ 种变换，其中一种是对的
- ❖ 但由于密码机的转轮之间的关系，实际的变换没有这么多。密钥为三个字母，共17576种，此时强力破解有效。

# 反射器



# 反射器实物



# 加密解密过程

## ❖ 发送消息过程

- 发信人首先要调节三个转子的方向，使它们处于17576个方向中的一个（事实上转子的初始方向就是密匙）
- 然后依次键入明文，并把闪亮的字母依次记下来，然后就可以把加密后的消息用比如电报的方式发送出去。

## ❖ 解密过程

- 当收信方收到电文后，使用一台相同的ENIGMA，按照原来的约定，把转子的方向调整到和发信方相同的初始方向上，
- 然后依次键入收到的密文，并把闪亮的字母依次记下来，就得到了明文。

## ❖ 结果：

- 于是加密和解密的过程就是完全一样的
- 这都是反射器起的作用，也是此系统非常出彩的地方之一。（当然副作用也很厉害）



# 连接板

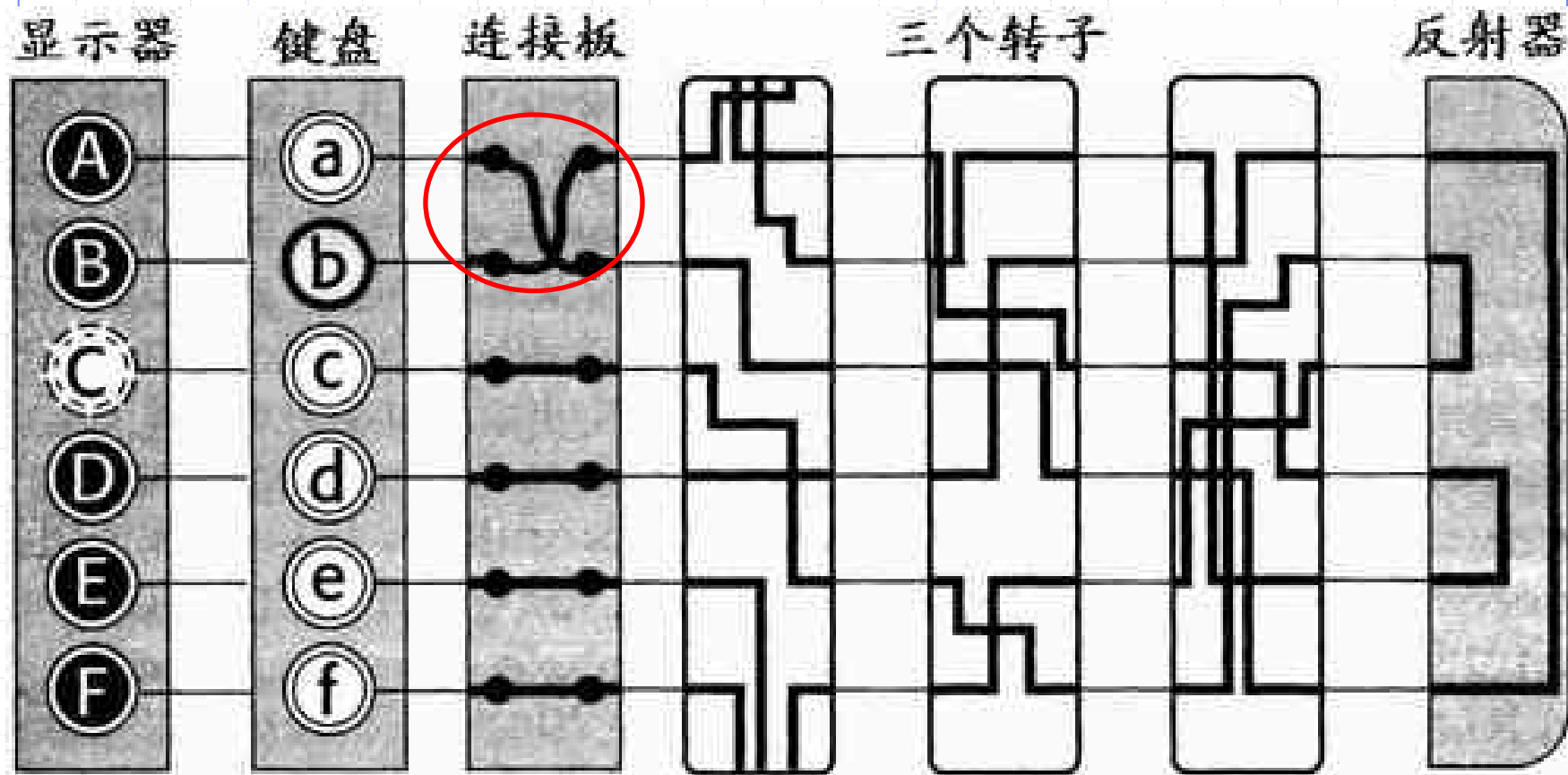
## ❖ 方案4：增加单表替换

- 加连接板：  
输入字母的  
两两交换



连接板和线

# 连接板用途示意图



# 密码分析

- ❖ 连接板上两两交换6对字母的可能性数目非常巨大，有100391791500种
- ❖ 看看这时的密钥数量：
  - 转子自身的初始方向： $26 \times 26 \times 26 = 17576$
  - 转子之间的相互位置：6
  - 连接板连线的状况：100391791500
  - 所有可能的密钥数量： $10^{16}$
- ❖ 结果：
  - 密钥数量暴增，暴力破解无效
  - 频率分析无效
  - Kasiski试验无效



一代巨星  
横空出世！

# 商业上的成功

## ❖ 历史:

- 1918年发明
- 1923年，A型出现，带反射板
- 1926年，获得德国海军订单，接着政府，企业，铁路部门开始使用
- 1928年，德国陆军，空军采购
- ...
- 仅德国军队就采购了3万台



# 成功的关键？

## ❖ 技术领先：

### ➤ Enigma是复合加密体制：

#### ◆ 多表代换+单表代换

### ➤ 密钥空间巨大，所有人都认为是不可破的

## ❖ 时代需要

### ➤ 一战英国破译德国密码的解密，对德国刺激很大

### ➤ 战争？



# Enigma的破解

- ❖ 随着德国军队装备Enigma，最着急的是
  - 波兰人
  - 1926年2月，波兰人发现德军海军密码没法破译了
  - 1928年7月，发现德国国防军的密码无法破译了
  - 无法了解德军动态！
  - 必须破译
- ❖ 方法：
  - 语言学家不行了，寻找数学家
  - 从接近德国的Poznam大学，招募数学专业学生
  - 著名的波兰三杰，就出自这个专业，包括破译Enigma的关键人物：Marian Rejewski（马里安·雷耶夫斯基）

# 波兰数学家的功绩

马里安·亚当·雷耶夫斯基（**Marian Adam Rejewski**，1905年—1980年），波兰数学家和密码学家。



20世纪30年代领导波兰密码学家率先对德国使用的**Enigma**密码进行了系统性的研究和破译。

在破译过程中，雷耶夫斯基首次将严格的数学化方法应用到密码破译领域，这在密码学的历史上是一个重要成就。

雷耶夫斯基等人在二战期间破译了大量来自德国的信息，他们的工作成为整个二战期间盟国破译德军**Enigma**密码的基础。

雷耶夫斯基与波兰数学家杰尔兹·罗佐基和亨里克·佐加爾斯基并称为密码研究领域的“波兰三杰”。



波兰三杰

# 布莱奇利庄园



《拦截密码战》

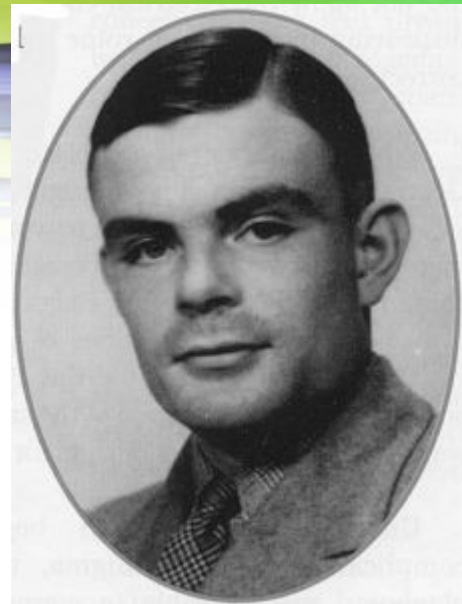
布莱奇利园当局曾以《每日电讯报》的填字游戏作为面试测试，限令面试者要在**12**分钟内完成填字游戏。此外，该报社亦曾被要求举办填字游戏比赛，然后再招揽胜出者参与“一项特别的工作，为战事作出贡献”。



## 阿兰·图灵（Alan Turing）

这个名字无论是在计算机领域、数学领域、人工智能领域还是哲学、逻辑学等领域，都可谓“掷地有声”。图灵是计算机逻辑的奠基者，许多人工智能的重要方法也源自这位伟大的科学家。

他在**24**岁时提出了图灵机理论，**31**岁参与了**Colossus**（二战时，英国破解德国通讯密码的计算机）的研制，**33**岁时构思了仿真系统，**35**岁提出自动程序设计概念，**38**岁设计了“图灵测试”，在后来还创造了一门新学科——非线性力学。虽然图灵去世时只有**42**岁，但在其短暂而离奇的生涯中的那些科技成就，已让后人享用不尽。人们仰望着这位伟大的英国科学家，把“计算机之父”、“人工智能之父”、“破译之父”等等头衔都加冕在了他身上，甚至认为，他在技术上的贡献及对未来世界的影响几乎可与牛顿、爱因斯坦等巨人比肩。



# 英国的破译

- ❖ Bletchley Park（布莱奇利庄园）
- ❖ 阿兰.图灵（Alan Turing）
- ❖ 方法:
  - 针对Enigma密码机的特性：自反的
  - 所以，某一位如果从来没有某字母，则可能就是该字母
  - 同时，针对德军报文发送的特点（如每日6:05分发送天气预报），猜测与天气有关的单词





## ❖ 如天气预报密文

- 第7个字母：从来不出现W
- 第8个字母：从来不出现E
- 第9个字母：从来不出现T
- 第10个字母：从来不出现T
- 第11个字母：从来不出现E
- 第12个字母：从来不出现R

## ❖ 这些字母很可能就是WETTER

- 由此构造明文-密文关系，以及字母循环圈

❖ 如

W	E	T	T	E	R
E	T	Q	W	K	Y

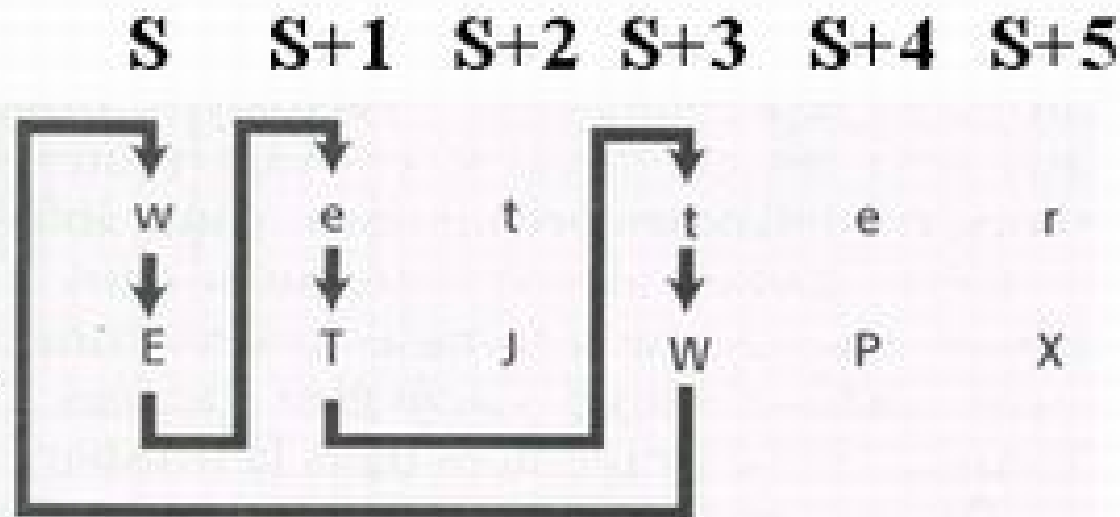
❖ 字母循环

➢ W-E-T-W

ENIGMA的  
转子位置

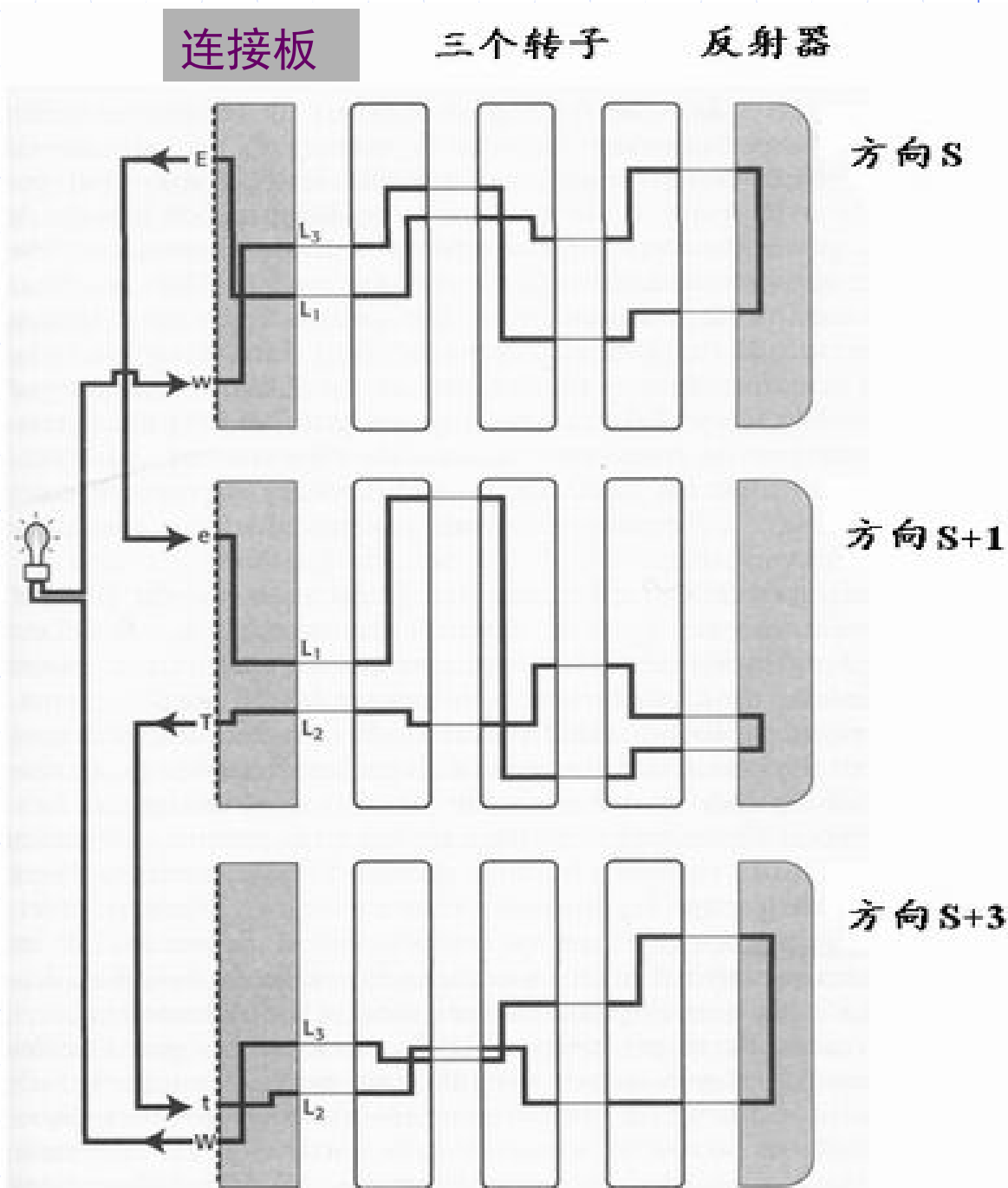
猜出的明文

加密后的密文

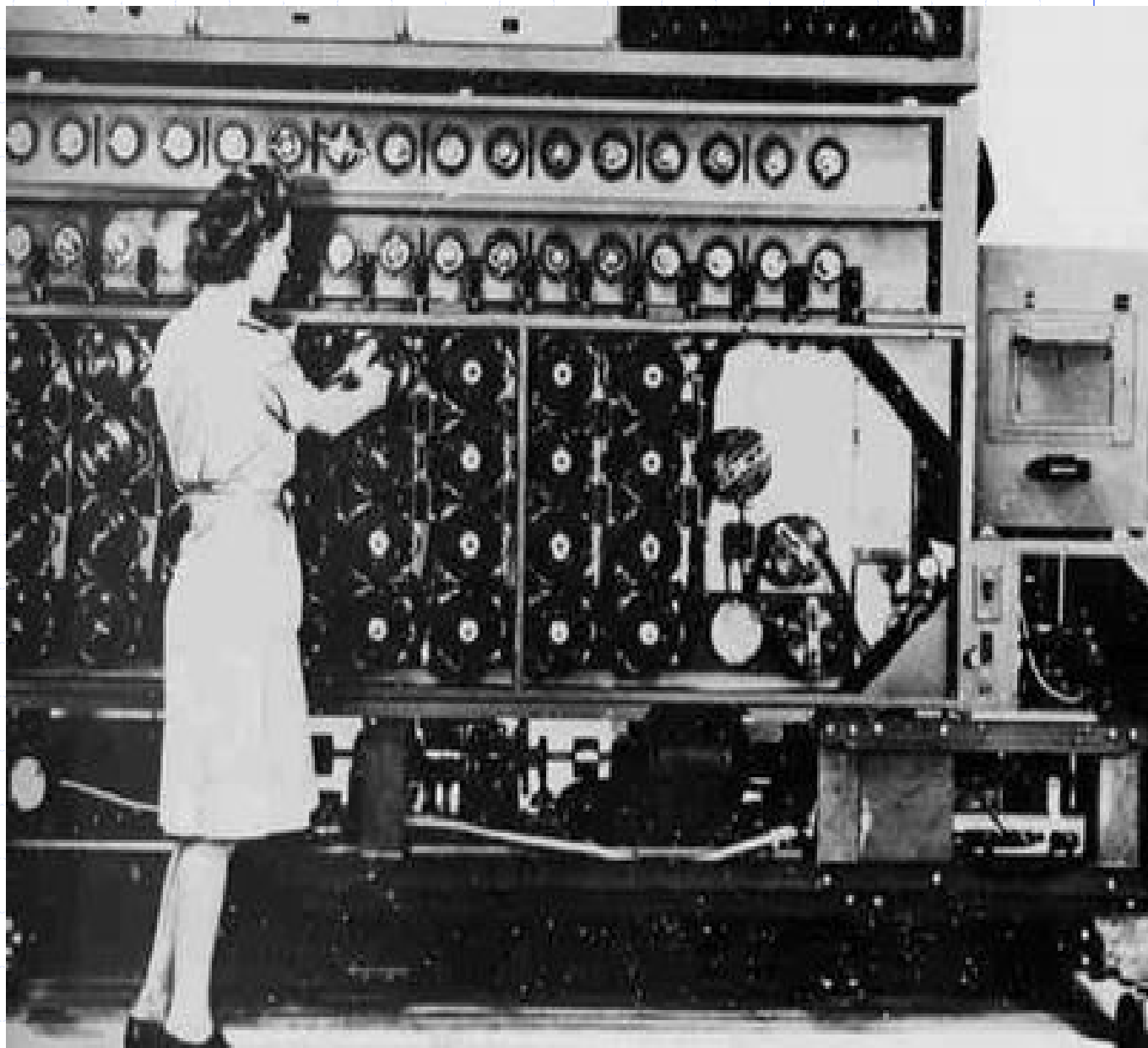


# 方法

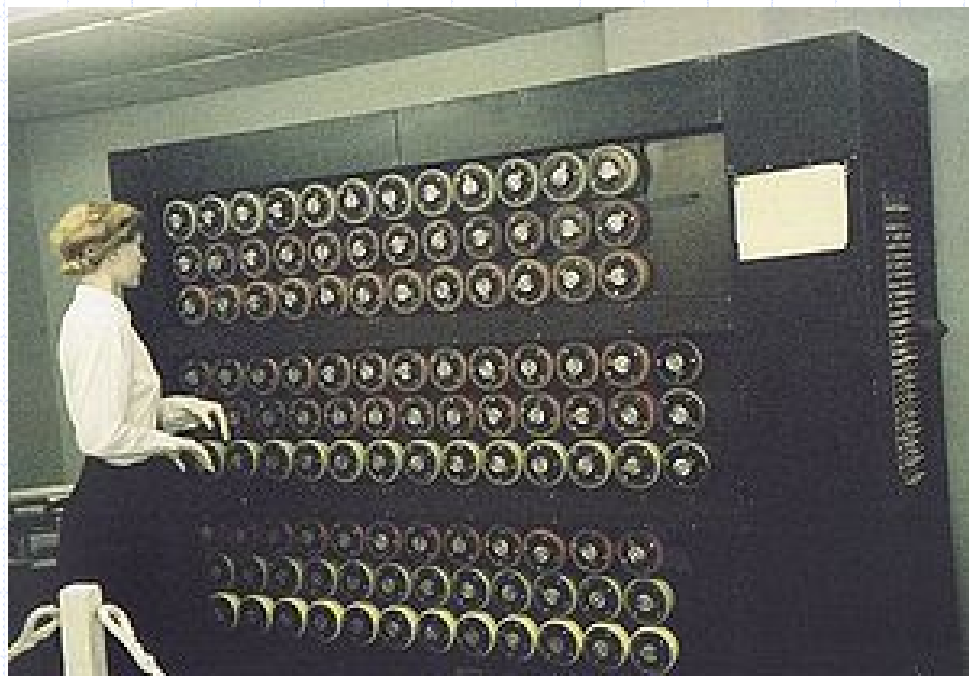
- ❖ 根据猜测的结果，将三台密码机如图连接
- ❖ 无论连接板如何，只要转子位置对了，这个电路将是通的。
- ❖ 因而连好电路后，可以通过自动旋转轮子，直到电路通了就停下来，此时的转轮位置，就是初始转轮位置
- ❖ 消除了连接板的效应



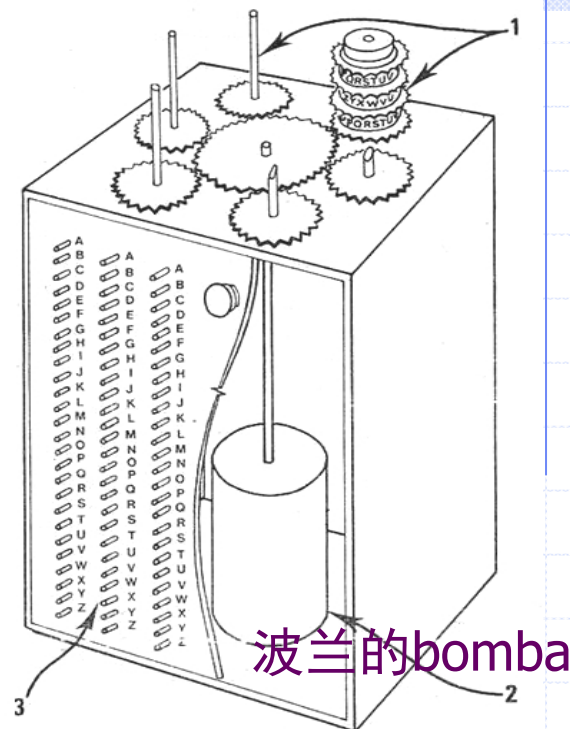
❖ 因此，英国人也制造了自动破解的机器，称为 bombe







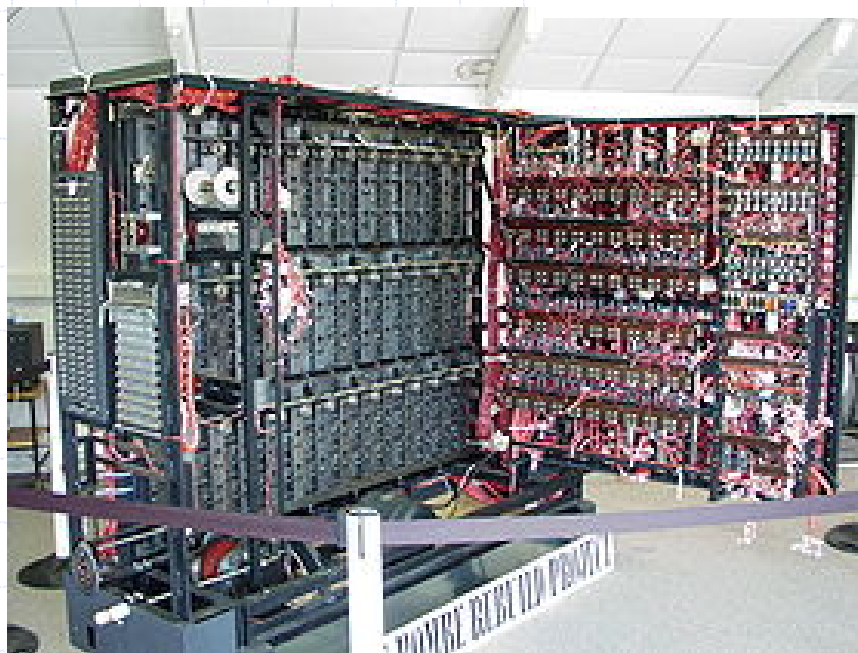
英国  
bombe



波兰的bomba



美国版本bombe



## ❖ 对付Enigma的Bombe

- 1941年，英国制造了16台bombe
- 1943年底，英国共有99台Bombe
- 1945年3月，英国共有211台Bombe

## ❖ 结果：

- 德军的报文，3个小时就能破译

## ❖ 破译队伍：12000人

## ❖ 费用：耗资惊人，倾全国之力

- Enigma: 3万USD
- Bombe: ? ?

## ❖ 代价！

# 战果

- ❖ 1940年，破译纳粹空军“RED”通用密钥网
- ❖ 1941年，纳粹北非空军作战密钥网被攻破
- ❖ 1942年，纳粹空军多个密钥网被攻破
- ❖ 1941年，纳粹海军多个密钥网被攻破
- ❖ ...
- ❖ 1943年8月29日，本月1-18日所有截获电文全部被破译
- ❖ ...

# 后话：Enigma输在哪里

- ❖ 对Enigma安全性估计过高
  - 导致德国在使用掉以轻心
    - ◆ 即使在遭受损失时，也不敢将其与Enigma的失密联系起来
  - 导致盟国一开始不敢轻言破解
- ❖ 德国在使用时的所犯的错误的被破解的原因
  - 军民混用
  - 使用规则制定错误
    - ◆ 初始转轮设置变动周期过长
    - ◆ 加密的密文与密钥一起发送
    - ◆ 新旧机型混用
    - ◆ 不同密级文件，都用Enigma处理
    - ◆ 格式错误：死板的格式



# 启示

- ❖ 科学技术的发展，是密码学前进的基石
- ❖ 实践的需要，是推动密码科学前进的最大动力
- ❖ 密码编码和分析，是相互对抗和相互促进的，相辅相成
- ❖ 密码对抗中，人的因素是第一位的