



# 密码学的概念及其发展史

主讲：任方

# 学科名：密码学

**Cryptology** [krip'tɒlədʒi]

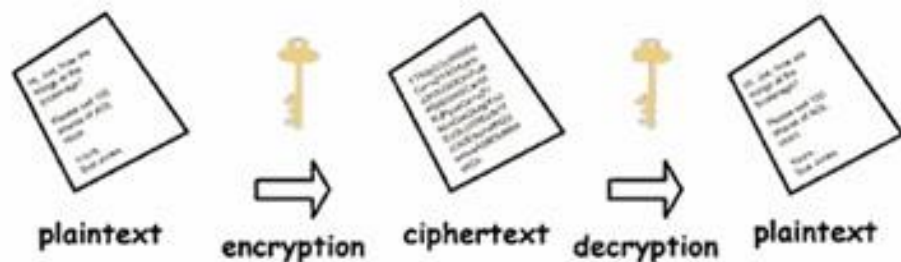
**cryptos** (“隐藏”之意)

**logos** (“词语、道理”之意)

# 概念辨析

此“密码”非彼“密码” → 用户登录密码

信息加密与  
解密的科学



密码/口令 (Password)

◆ 密码学 (Cryptology) 是结合数学、计算机科学、电子与通讯等诸多学科于一体的交叉学科，是研究信息系统安全保密的一门科学。

- 密码编码学 (Cryptography): 主要研究对信息进行编码, 实现对信息的隐蔽。
- 密码分析学 (Cryptanalytics): 主要研究加密消息的破译或消息的伪造。

# 密码学简史 (1) -- 古典密码

大约3000年以前，古埃及贵族

在书写墓碑上的铭文时，使用了变形的而不是普通的象形文字，揭开了有文字记载的密码史。

罗塞塔石碑  
现存大英博物馆



## 罗塞塔石碑上的文字（部分）

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14



# 斐斯托斯圆盘

## 斐斯托斯圆盘（Phaistos Disc）

- 1908年发现于希腊克里特岛南部的斐斯托斯，为黏土质地，大约制成于公元前2000年前。
- 圆盘上有至今未能释读的古文字，分别用45种不同符号表示241个印记，初步判定是以印章的方式绘上。
- 现保存于希腊伊拉克利翁考古学博物馆。



# 斯巴达密码棒

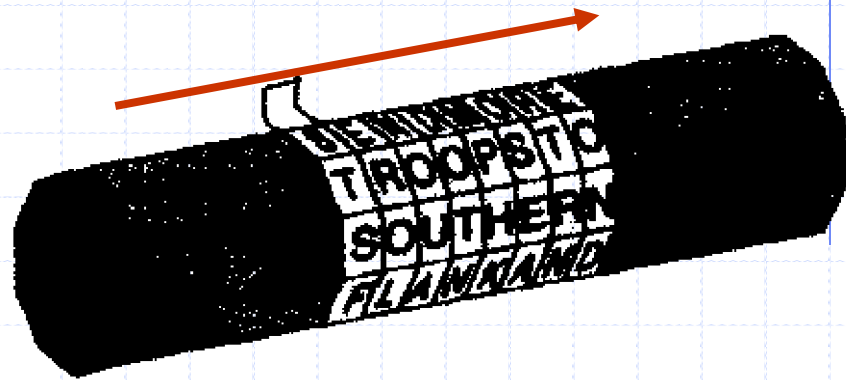
公元前 5 世纪，古斯巴达人  
用一条带子缠绕在一根木棍上，  
沿木棍纵轴方向写好明文，

解下来的带子上就只有杂乱无章的密文字母。

解密者只需找到相同直径的木棍，

再把带子缠上去，沿木棍纵轴方向即可读出有意义的明文。

这种叫做“天书”的器械堪称人类历史上最早使用的密码器械。





# 凯撒密码



公元前1世纪，著名的恺撒密码（古罗马统帅恺撒：约公元前102~44）被用于高卢战争中（见《高卢战记》），这是一种简单易行的移位密码。

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

$$c = E_e(m) = \text{WKLVF LSKHU LVFHU WDLQO BQRWV HFXUH.}$$

$$m = \text{THISC IPHER ISCER TAINL YNOTS ECURE}$$

## 密码学简史 (2) --近代密码

1883年，荷兰密码学家A. Kerckhoffs在《军事密码学》中给出密码设计的一般规则：

- ❏ 密码系统应该是**计算安全的**；
- ❏ **密钥**由通信双方事先约定好，并根据一定协议进行更换；
- ❏ 密码系统应该易于使用；
- ❏ 密码系统应该精确而有效；
- ❏ 除了**密钥**，密码系统的所有细节都为对手所知。

Kerckhoffs原则在今天看来仍然具有十分重要的现实意义。

# 军事密码学

一战前，密码研究还只限于一个小领域，没有得到各国应有的重视。

第一次世界大战是世界密码史上的第一个转折点。随着战争的爆发，各国逐渐认识到密码在战争中发挥的巨大作用，积极给予大力扶持，使密码很快成为一个庞大的学科领域。

第一次世界大战进行到关键时刻，英国破译密码的专门机构“40号房间”利用缴获的德国密码本破译了著名的“齐默尔曼电报”，促使美国放弃中立参战，改变了战争进程。

# 军事密码学

第二次世界大战爆发后，世界各国非常重视对密码破译的研究工作，纷纷成立专门的研究和破译机构，在战争中发挥重要的作用。

欧洲战场：盟军破译了德国著名的“ENIGMA”密码机密码，德国的许多重大军事行动对盟军都不成为秘密。

ENIGMA 密码机被证明是有史以来最可靠的加密系统之一，二战期间它被德军大量用于铁路、企业当中，令德军保密通信技术长期处于领先地位。



插图I

转轮密码机ENIGMA，由Arthur Scherbius（阿图尔·舍尔比乌斯）于1919年发明，面板前有灯泡和插接板；4轮ENIGMA在1944年装备德国海军。它用3（最多为8）个正规轮和1（至多为2）个反射轮（Griechenualzen  $\beta$ ,  $\gamma$ ），这使得英国从1942年2月到12月都没能解读德国潜艇的信号。



# 军事密码学

1944年6月4日，德国U-505潜艇受到美海军特遣大队反潜深炸弹攻击，受伤浮起后，美军冲入无线电室，缴获了密码机和大量明、密报，并秘密将U-505潜艇拖回美国。德军误认为U-505潜艇沉没海底而未换密码。

在二战结束前的11个月里，依靠破译的密码，美军和同盟国军队共击沉德国潜艇300多艘，平均每天一艘，同时大大减少了自己船只的损失，对战争的胜利产生了重大影响。

相关电影：《U-571》





# 军事密码学

## ◆重要人物—阿兰图灵

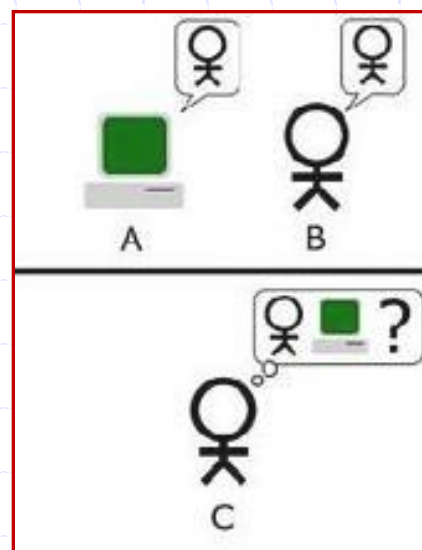
“计算机科学之父” “人工智能之父”

英国在1939年对德宣战之后，图灵作为主要参与者和贡献者，领导着一个200来位密码专家的队伍，为成功破译“**ENIGMA**”立下大功。

以他名字命名的“图灵奖”有“计算机界的诺贝尔奖”之称。



阿兰·图灵  
1912-1954



图灵试验

# 军事密码学

**亚洲战场：**1940年，密码学家**威廉·F·弗里德曼**（被美国人称为是“世界上最伟大的密码专家”）领导的小组破译“紫密”，得知日本可能偷袭美国，但没有引起重视。此后一年，日军成功偷袭珍珠港。

1942年，**约瑟夫·约翰·罗彻福特**破译日军的“JN25”密码，从而导致日本在中途岛海战中失利，既报了珍珠港的一箭之仇，又使太平洋战场的局面得到彻底扭转。中途岛作战的胜利本质上是情报的胜利。

二战期间，美军破译日本海军密码多达75种，由于密码被破译，日本总吨数约三之二的商船被美国潜艇击沉，给日本军队带来了严重的战争后果。

中途岛密码战——“AF”之谜

# 军事密码学

## 山本五十六之死

日本联合舰队总司令山本五十六是日本太平洋战争的重要策划者和组织者之一，谋划了对珍珠港的袭击。

1943年4月18日山本到日军掌控的所罗门群岛视察，这一日程用“JN25”密码机加密，播给日本第一基地部队等众多的军事单位。美军截获该密文，通过破译JN25密码的专用IBM设备破译出。尼米兹上将经研究决定出击：4月18日出动战斗机将山本座机击落。密码分析术使得美国获得了一次相当于大战役的胜利。



# 军事密码学

二战中密码分析术至少立下四件大功：

中途岛海战

山本之死

切断日军海上生命线

打败德国潜艇

二战结束后，一位深知战时密码破译价值的美国官员说，**密码破译使第二次世界大战缩短了几年**。这种说法虽有些夸张，但重要情报的破译确实影响了战争的进程，挽救了成千上万的生命。

# 军事密码学

第二次世界大战促进了密码的飞速发展。由于密码对于战争的胜负具有越来越重要的影响，各国不惜花大量的人力物力进行密码的研究和破译。

以美国为为例：一战时期美国陆海军的密码工作人员大约为四百人，二战时激增到一万六千余人。

密码的编制结构更加科学，编制方法愈加复杂，各种密码的保密性出现了飞跃性的提高。许多国家开始使用密码机进行加密，密码告别人工加密，走向机械加密的开始。



(a) Enigma 机



(b) TYPEX 密码机



(c) C-36 型密码机



(d) M-209

图 1-1 几个典型的密码机



## 密码学简史 (3) -- 密码科学的建立

1948年以前的密码技术可以说是一种艺术，而不是一种科学，那时的密码专家是凭直觉和信念来进行密码设计和分析的，而不是靠推理证明。

1948年，C. E. Shannon(1916~2001)在贝尔系统技术杂志上发表论文《通信的数学理论》，创立了著名的新理论——信息论，1949年发表的另一篇划时代的文章：《保密系统的通信理论》标志着密码术到密码学的转变。

# 伟大的Shannon

- 为了表彰Shannon的伟大功绩，2000年10月6日**IEEE Information Society** 的**25**名成员在Shannon的儿童时代的老家**Michigan**的**Gaylord**举行了**Shannon**塑像的落成典礼。塑像底座正面刻文如下：

*Claude Elwood Shannon*

*Father of Information Theory*

*Electrical engineer, Mathematician, and native son of Gaylord. His creation of **information theory**, the **mathematical theory of communication**, in the 1940s and 1950s inspired the revolutionary advances in **digital communications** and **information storage** that have shaped the modern world.*

# 伟大的Shannon

- “在我看来，两三百年之后，当人们回过头来看我们的时候，他们可能不会记得谁曾是美国的总统。他们也不会记得谁曾是影星或摇滚歌星。但是仍然会知晓Shannon的名字。学校里仍然会教授信息论。”（*Dr. Richard Blahut, Oct. 6, 2000, Gaylord, Michigan*）



# 密码科学的建立

20世纪70年代中期，密码学界发生了两件跨时代的大事：

第一、Diffie和Hellman发表的题为“密码学新方向”文章，提出了“**公钥密码**”新体制，冲破了传统“**单钥密码**”体制的束缚。

传统密码体制主要功能是**信息的保密**，双钥(公钥)密码体制不但赋予了通信的保密性，而且还提供了**消息的认证性**。新的双钥密码体制无需事先交换密钥就可通过不安全信道安全地传递信息，大大简化了密钥分配的工作量。

双钥密码体制适应了通信网的需要，为密码学技术应用于商业领域开辟了广阔的天地。

# 密码科学的建立

第二、美国国家标准局**NBS**于**1977**年公布实施美国数据加密标准**DES**（**Data Encryption Standard**），密码学史上第一次公开加密算法，并广泛应用于商用数据加密。

这两件引人注目的大事揭开了密码学的神秘面纱，标志着密码学的理论与技术的划时代的革命性变革，为密码学的研究真正走向社会化作出了巨大贡献，同时也为密码学开辟了广泛的应用前景。从此，掀起了现代密码学研究的高潮。

# 密码学的作用和意义

历史上的战争，特别是两次世界大战，对于保密学的理论与技术的发展起了巨大的推动作用。

在通信安全、保密、密码分析上的优势，被认为是赢得历史上许多主要军事冲突(包括二次世界大战)胜利的关键因素之一。

我们正在步入一个崭新的信息社会，信息在社会中的地位和作用越来越重要，每个人的生活都与信息的产生、存储、处理和传递密切相关。“谁掌握了信息，控制了网络，谁就将拥有整个世界！”

信息的安全与保密问题成了人人都关心的事情，使密码学脱去神秘的面纱，成为大家感兴趣并为更多人服务的科学。



# 密码学发展的回顾

密码学发展大致分为三个阶段：

- ◆ 古典密码时期

- ◆ 近代密码时期

- ◆ 现代密码时期

## 古典密码时期

- ◆ 起始时间：从古代到**19**世纪末，长达几千年。
- ◆ 密码体制：纸、笔或者简单器械实现的替代及换位。
- ◆ 通信手段：信使

## 近代密码时期

- ◆ 起始时间：从**20**世纪初到**20**世纪**50**年代，即一战及二战时期。
- ◆ 密码体制：手工或电动机械实现的复杂的替代及换位。
- ◆ 通信手段：电报通信。

## 现代密码时期

- ◆ 起始时间：从**20世纪50年代**至今。
- ◆ 密码体制：分组密码、序列密码以及公开密钥密码，有坚实的数学理论基础。
- ◆ 通信手段：无线通信、有线通信、计算网络等。

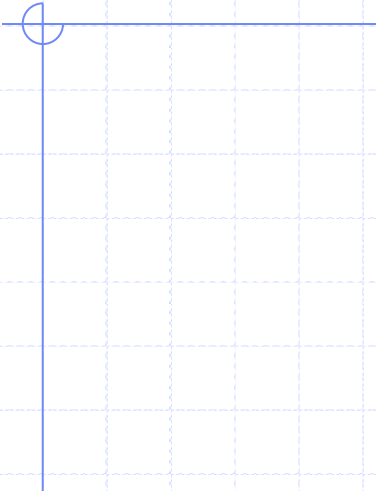
# 现代密码学的三大重要事件

- ◆ **1949年Shannon**发表题为《保密系统的通信理论》，为密码系统建立了理论基础，从此密码学成了一门科学。（第一次飞跃）
- ◆ **1976年后**，美国数据加密标准（**DES**）的公布使密码学的研究公开，密码学得到了迅速发展。
- ◆ **1976年**，**Diffe**和**Hellman**提出公开密钥的加密体制，**1978年**由**Rivest**、**Shamir**和**Adleman** 提出第一个比较完善的公钥密码体制算法（第二次飞跃）

# 对于密码学的理解

- 揭开密码学的神秘面纱，密码学不仅仅应用于军事、外交、情报等领域。
- 密码作为一门技术源远流长,但密码成为一门”实用”的学科只不过30余年的事。
- 密码学已经成为平常人正常生活、学习不可缺少的部分。这与计算机科学的蓬勃发展息息相关。
- 密码学不仅具有信息通信加密功能，而且具有数字签名、身份认证、安全访问等功能。
- 密码学提供的只是技术保障作用。





**THE END !**