现代密码学

Modern Cryptography

张方国

中山大学计算机学院

Office: Room 305, IM School Building

E-mail: isszhfg@mail.sysu.edu.cn

HomePage: https://cse.sysu.edu.cn/content/2460

第一讲 引论

- 密码学简介Introduce to Cryptography
  什么是密码学？密码学的基本概念
- 为什么学习密码学？Why Cryptography
- 密码学的历史History of Cryptography
- 关于这门课About This Course

网络空间安全一级学科

- 2015年6月11日，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科

- 网络空间安全一级学科博士点（2016.02）
- 网络与信息安全发展，人才队伍建设是关键
- 网络空间安全学院（系）

密码法

促进密码事业发展，保障网络与信息安全

《中华人民共和国密码法》

中华人民共和国主席令

第三十五号

《中华人民共和国密码法》已由中华人民共和国第十三届全国人民代表大会常务委员会第十四次会议于2019年10月26日通过，现予公布，自2020年1月1日起施行。

中华人民共和国主席 习近平

2019年10月26日

密码科学与技术专业

2021年3月1日，教育部公布2020年度普通高等学校本科专业备案和审批结果，**新增37个本科专业**

15	工学	电子信息类	智能测控工程	工学	四年
16	工学	自动化类	智能工程与创意设计	工学	四年
17	工学	计算机类	密码科学与技术	工学	四年
18	工学	土木类	城市水系统工程	工学	四年
19	工学	矿业类	智能采矿工程	工学	四年

密码学系或密码学院

密码学是讲什么的?

密码学≠信息安全

密码学是保障信息安全的核心工具

什么是密码学？

- **密码学的英文是Cryptography**
  是由古希腊语κρυπτός（罗马化为kryptós）“隐藏的”和γράφειν（罗马化为gráphein）“书写”派生而来的；
  是研究如何隐密地传递信息的学科！
- **Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries)—from wiki.**
  密码学是第三方存在下的安全通信技术的研究与实践。

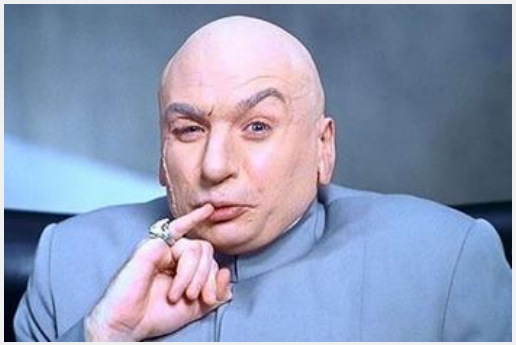
什么是密码学

著名的密码学者Ron Rivest解释道：

“密码学是研究如何在敌人存在的环境中通讯”

甲

乙



丙

影视中的密码

纳瓦霍密码

密码学的基本概念

密码学(Cryptography)，对信息进行编码实现隐蔽信息的一门学问

密码分析学(Cryptanalytics)，研究分析破译密码的学问。

两者相互对立，而又互相促进地向前发展。

密码术(Cryptology)：研究信息系统安全保密的科学。它包含以上两个分支

密码体制分类

- 单钥、私钥、对称密码体制：
- 双钥、公钥、非对称密码体制：

密码的主要研究内容

公钥加密
数字签名
私钥加密：分组密码，流密码
Hash函数
伪随机数
安全协议：承诺，零知识证明，多方计算等

为什么要研究密码学？

- 保密，自古以来就被非常重视：``事成于密，而败于泄"，``知己知彼，百战不殆"
- **密码在古代就被用于传递秘密消息。在近代和现代战争中，传递情报和指挥战争均离不开密码，外交斗争中也离不开密码**
- **信息化社会中，Internet一方面成为人们离不开的信息工具，同时它也成为公开的攻击对象目标和便利的工具**

信息社会环境下的安全威胁

- 信息泄露;
- 破坏信息的完整性:
- 拒绝服务:
- 非法使用(非授权访问):
- 窃听:
- 业务流分析:
- 假冒:
- 旁路控制:
- 木马;
- 抵赖;
- 重放;
- …

信息安全的基本要求

- 信息的保密性**Confidentiality**：
  保证信息不泄漏给未经授权的人
- 信息的完整性**Integrity**：
  防止信息被未经授权的篡改或破坏
- 认证性**Authentication**：
  对某一实体所声称的身份提供证实的行动
- (可用性**Availability**)

信息安全还包括

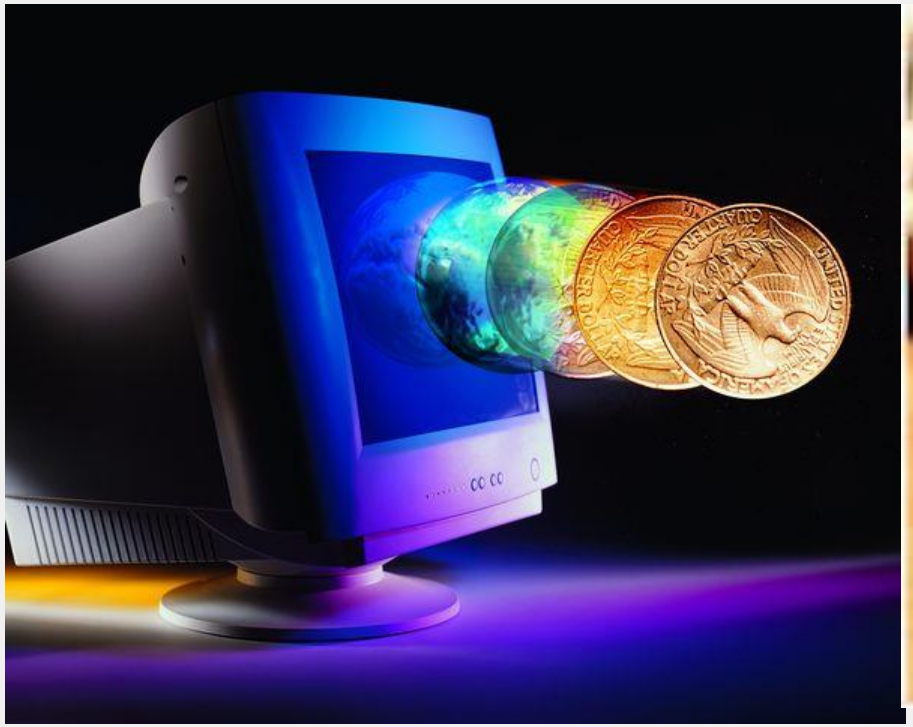
- 不可否认性
- 匿名性
- 接入控制
- 可用性

为什么要研究密码学？

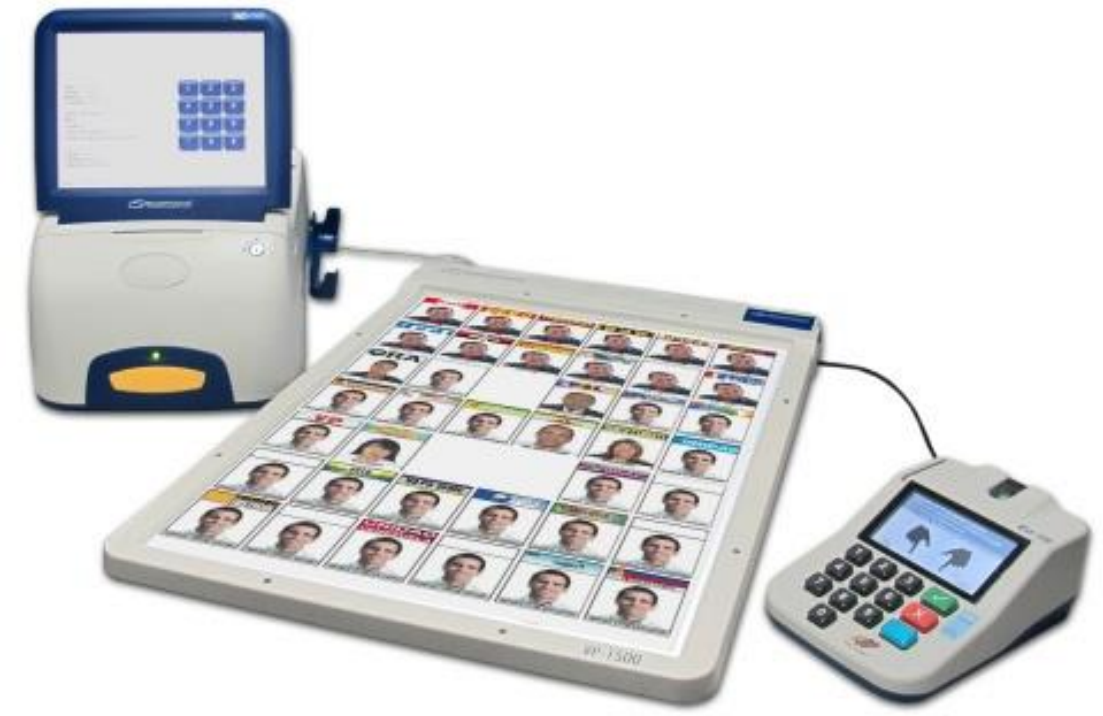
- **密码技术都可以实现这些信息安全要求：**
  C: 加密;
  I,A: 签名和MAC
  密码技术是保护信息安全的主要手段之一

- **密码已经从军事走向日常生活：**
  电子邮件
  接入控制
  电子银行
  软件保护
  版权保护, …

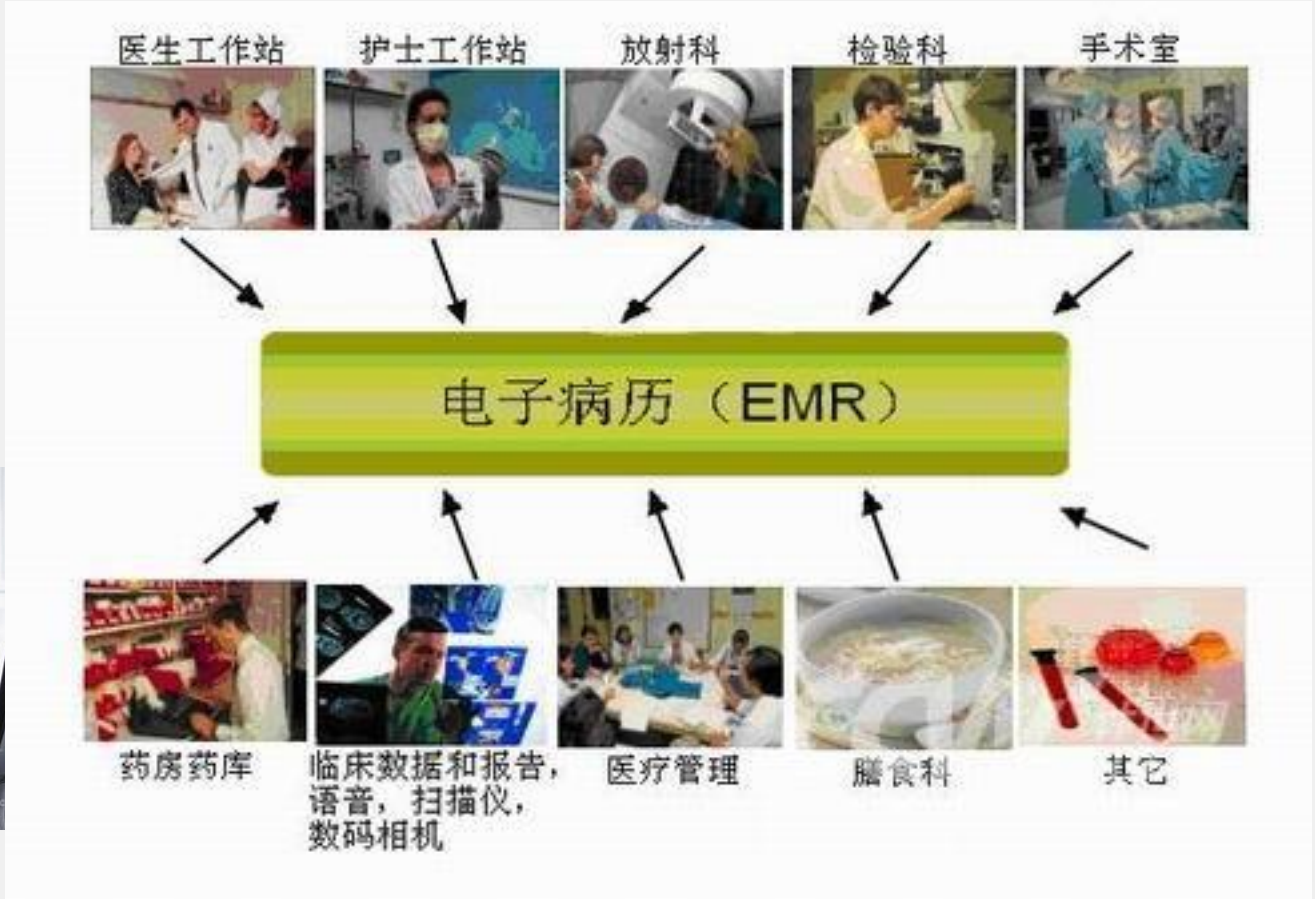
电子银行、电子拍卖等电子商务



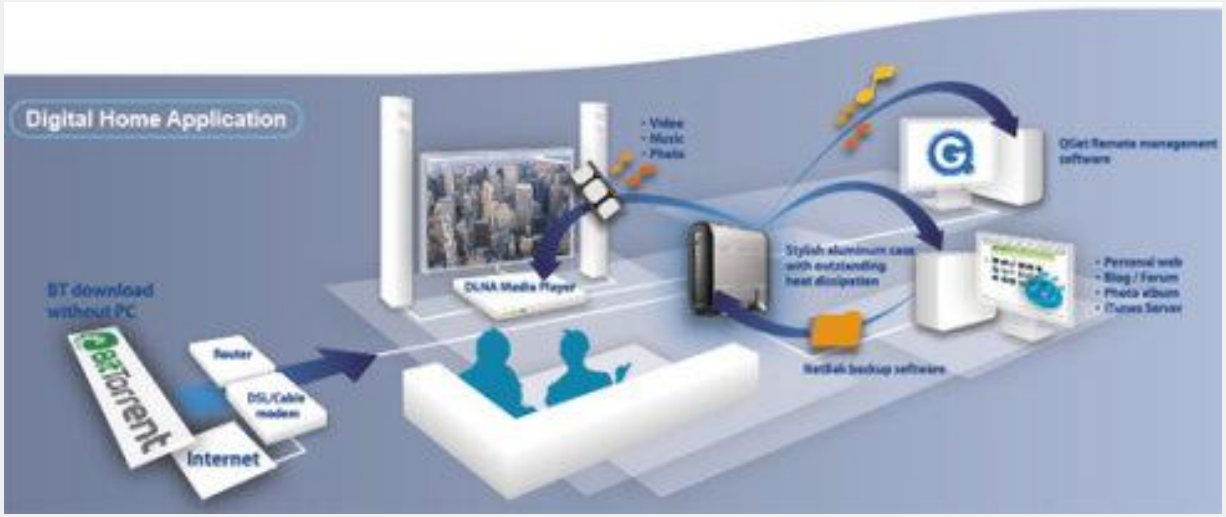
电子选举、电子税收等电子政务



电子医疗

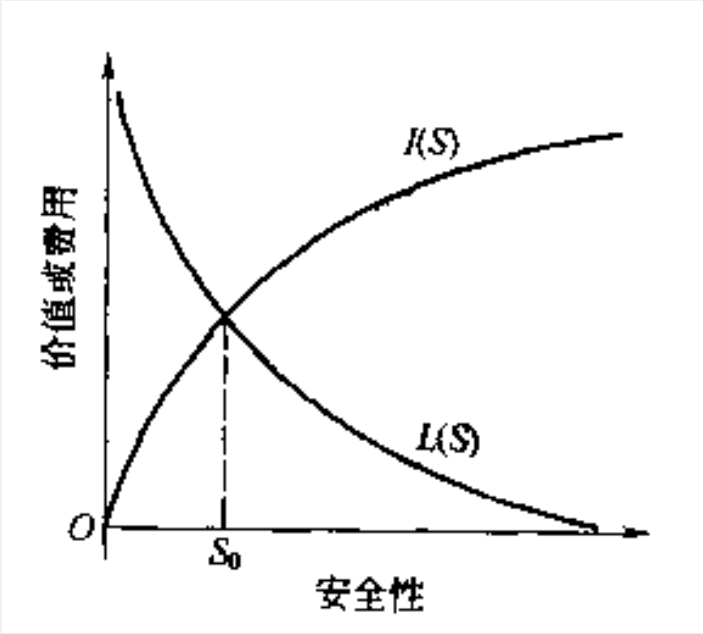

医生工作站
护士工作站
放射科
检验科
手术室
电子病历（EMR）
药房药库
临床数据和报告，
语音，扫描仪，
数码相机
医疗管理
膳食科
其它

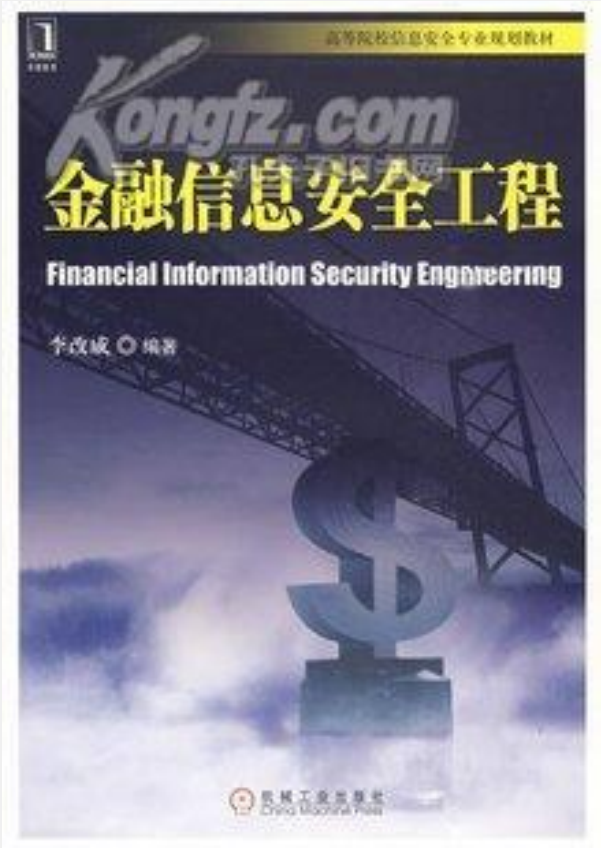
数字家庭


Digital Home Application
BT download
without PC
Router
DSL/Cable
modem
Internet
DLNA Media Player


325
APP DONE!

密码经济学


价值或费用
I(S)
L(S)
O
S_0
安全性


Kongfz.com
金融信息安全工程
Financial Information Security Engineering
李改成 ○ 编著


bitcoin

密码法律学

促进密码事业发展，保障网络与信息安全

《中华人民共和国密码法》

密码新应用

- 从密码应用这个角度来讲，有时候感觉到密码学不仅仅是一个数学，计算机，通信，物理等的交叉学科，它还是属于社会学的一部分。
- 任何一个新兴的网络，或一个新兴的社会需求，只要需要安全性或隐私性，密码工具就能用上去，从而成为密码学应用研究领域的一个研究热点

云计算

物联网

无线传感网络

智能电网


后台办公室
智能电网网络和设备
智能家居
Internet
MDMS
OMS
EMS
CIS
EA / 消息总线
CustomerIQ 套装
UtilityIQ 套装
GridScape
WAN
ACCESS POINT
接入点
RELAY
转发器
BRIDGE
GAS MRV
SILVERSPRING NETWORKS

人工智能

AI+安全

Safety and Security

密码学的研究历史

- 古典（传统）密码Classic Cryptography (1976年以前):

  远古密码, Ancient Ciphers,
  手工密码，MANUAL SYSTEMS，
  机械密码，Machine Ciphers，
  电子机械密码，ELECTRO-MECHANICAL SYSTEMS

古典密码学

- 远古密码Ancient Ciphers

至少4000 多年前古埃及人在金字塔中加密象形文字

Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right

中国3000年前的密码

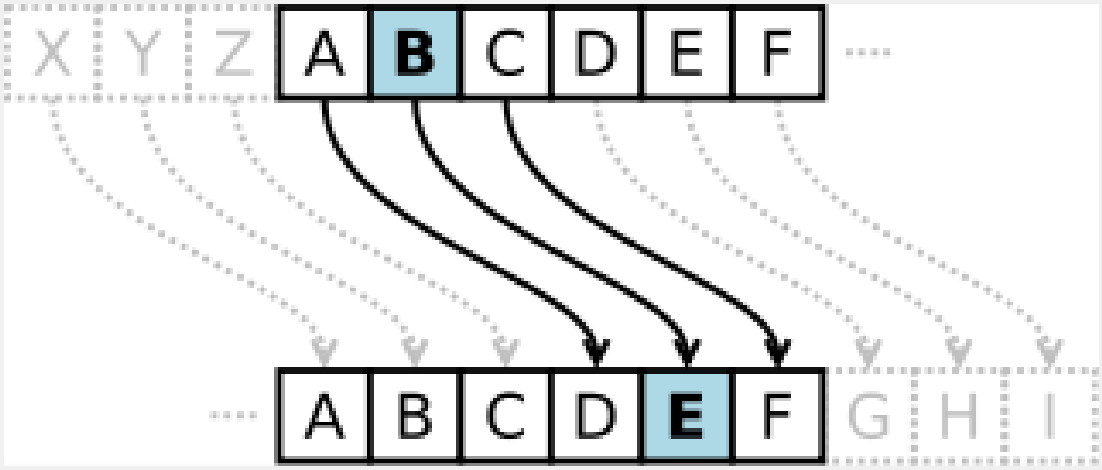
- 古中国周朝兵书《**六韬**．龙韬》也记载了密码学的运用，其中的《阴符》和《阴书》便记载了周武王问**姜子牙**关于征战时与主将通讯的方式

手工密码

公元前500年的古希腊人发明的Scytale密码

斯巴达密码棒

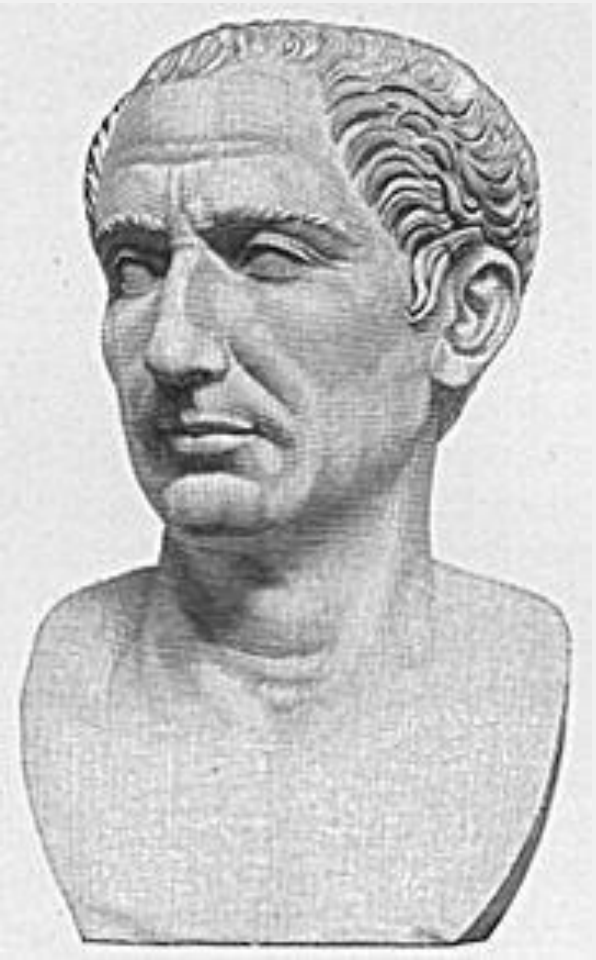
凯撒密码



明文： m = veni，vidi，vici

密文： c=E(m)= YHAL， YLGL，YLFL

（意思是“我来，我见，我征服”,曾经是恺撒征服本都王法那西斯后向罗马元老院宣告的名言）

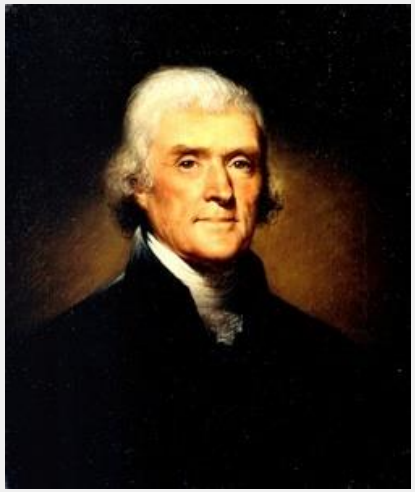


维吉尼亚密码

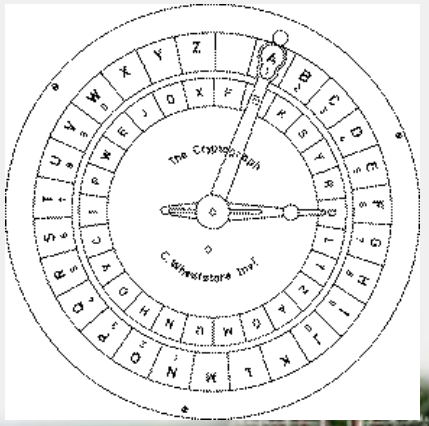
- 多表替换密码,抗击频率分析
- 意大利学者贝拉索1553年发明
- 维吉尼亚在1586年的改进
  （久而久之，贝拉索密码就被叫成了维吉尼亚密码）
- 查尔斯-巴比奇（Charles Babbage，1791-1871），英国数学家，于1854年成功破解了维吉尼亚密码，结束了维吉尼亚200多年的神话。

机械密码

1790年代,杰弗逊圆盘（Jefferson cylinder）



1860年代, Wheatstone disc



电子机械密码

- 又称转轮密码

  用一组**转轮**或**接线编码轮**所组成的机器，用以实现长周期的多表代换密码

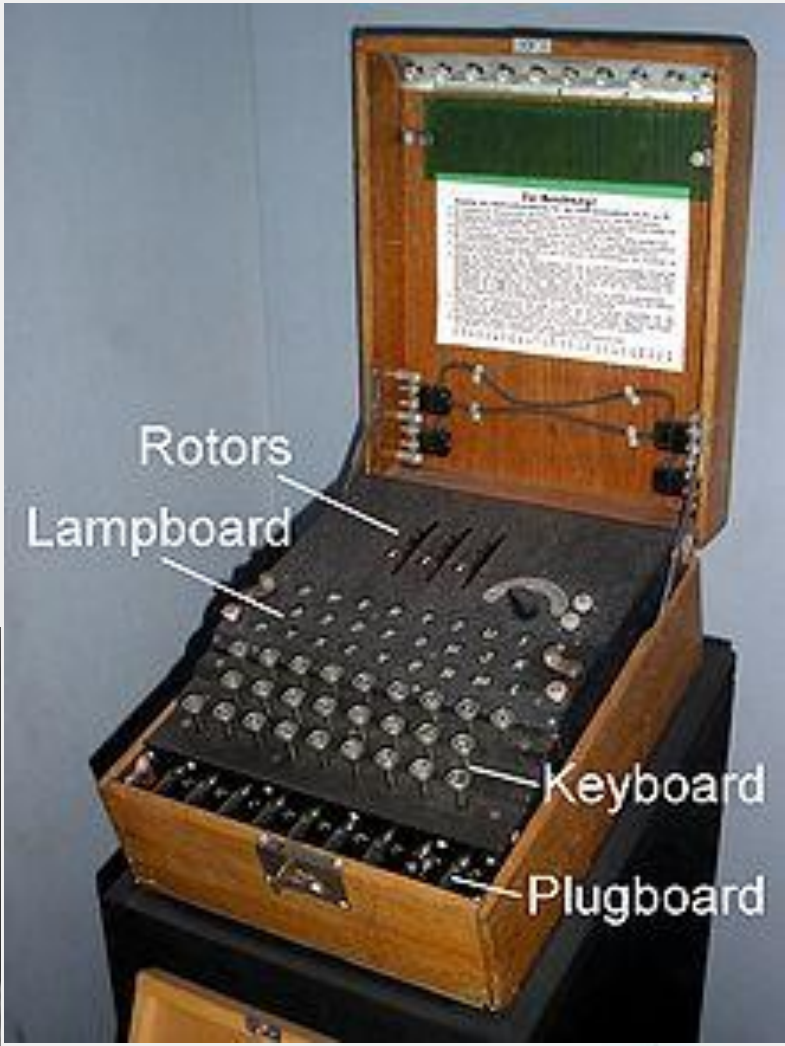
- 最有名的的代表

  Enigma,

  Purple（紫密）

恩尼格玛密码机的故事

- 1918年德国发明家亚瑟•谢尔比乌斯和理查德•里特创办了一家新技术应用公司，谢尔比乌斯利用电气技术发明一种能够自动编码的机器，并给自己所发明的电气编码机械取名“恩尼格玛”（ENIGMA，意为哑谜）。
- 恩尼格玛在1920年代早期开始被用于商业，后来也被一些国家的军队与政府采用过，在这些国家中，最著名的是第二次世界大战时的纳粹德国。

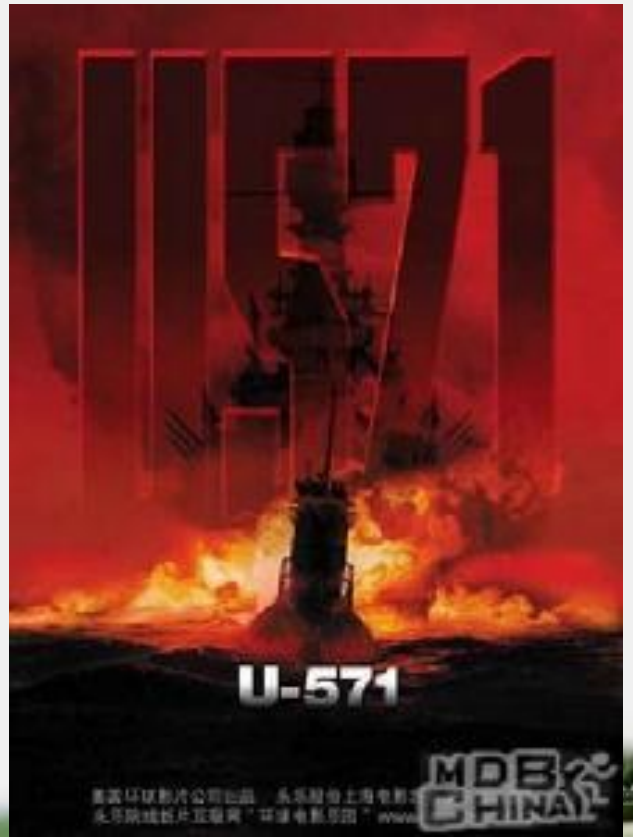


二战中，德国军队大约装备了三万台ENIGMA。

“闪电战”的提出者，德国装甲部队之父，纳粹德国的海因茨·古德里安(Heinz Guderian)将军在指挥车上。在照片的左下方我们可以看见一台ENIGMA。

德国潜艇指挥部密码的破译

- 1944.6.4德《U-505》潜艇受到美海军22.3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》拖回美国。德军误认为《U-505》沉没海底而未换密码，欧战结束前11个月，几乎每天击沉一艘潜艇，共计击沉300多艘。
- U-505是二战中美国海军俘虏的唯一一艘德国潜艇

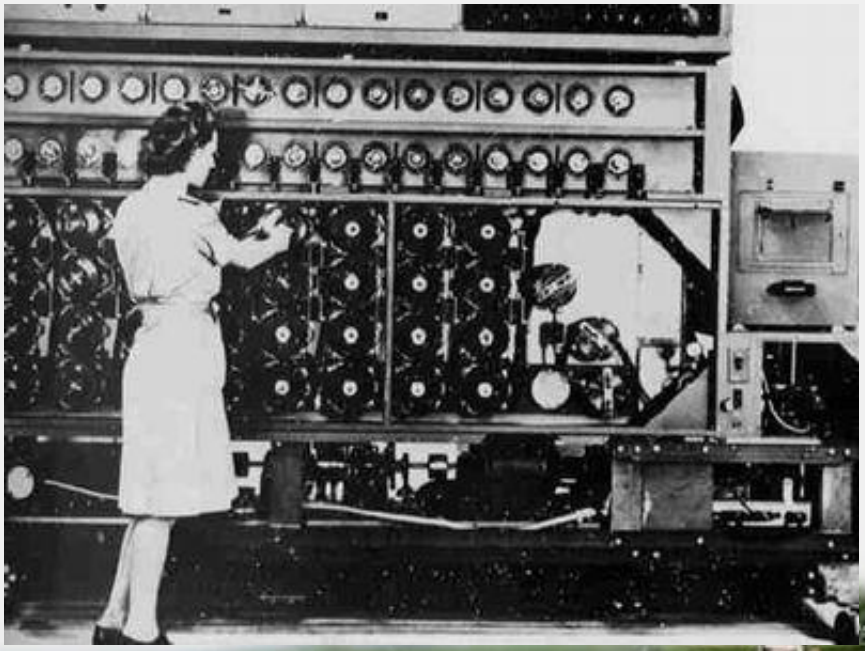


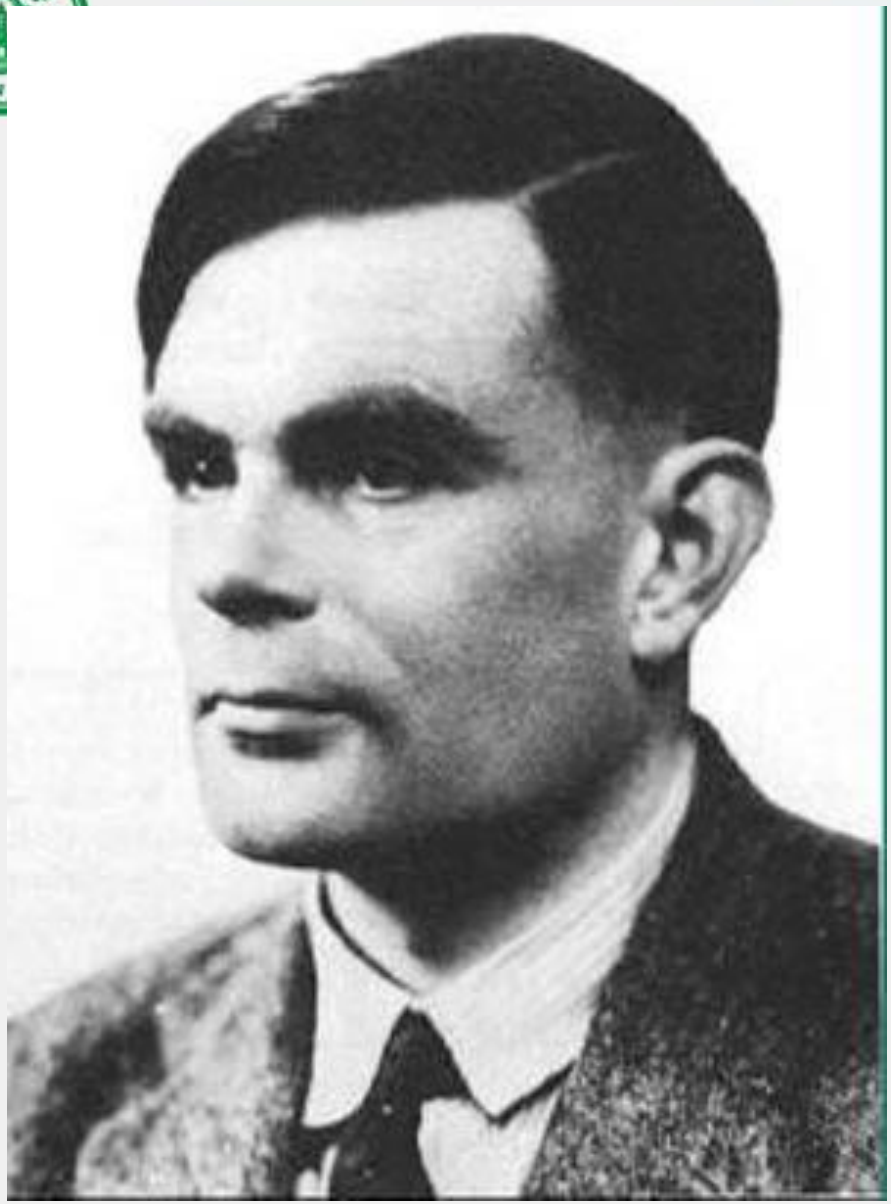
艾伦.图灵(Alan Turing)

(1912.6.23-1954.6.7)

- 二战中帮助英国破译恩尼格玛密码机的密码的最大功臣
- 计算机之父
- 人工智能之父
- “图灵机”(Turing Machine)

图灵和他制造的“炸弹”






ACM
A.M. TURING AWARD

紫密的破解

日本的紫密(**97-shiki** ōbun inji-ki (九七式欧文印字機)): 1937, Kazuo Tanabe

珍珠港事件(1941.12.7, 7:30AM)

破译紫密：“AF方位”

- 中途岛海战中的胜利称之为“情报的胜利”。

柯克霍夫原则

A.Kerckhoffs, 1883

即使密码系统的任何细节已为人悉知，
只要密钥（key）未泄漏，它也应是安全的。

Shannon密码理论

完善保密Perfect Secrecy
“Confusion”混淆，
“Diffusion”扩散

密码学的研究历史

- 现代密码学**Modern Cryptography (1976/77 Today)**
  代表事件：
  公钥密码学的提出和美国数据加密标准DES的颁布

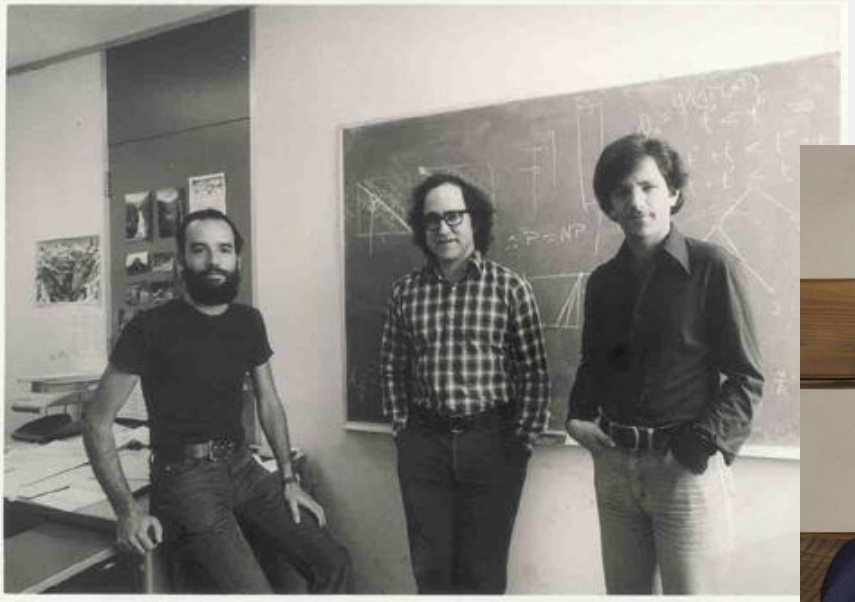
  意义：密码学成为了一门科学，研究从军事和外交走向了公开

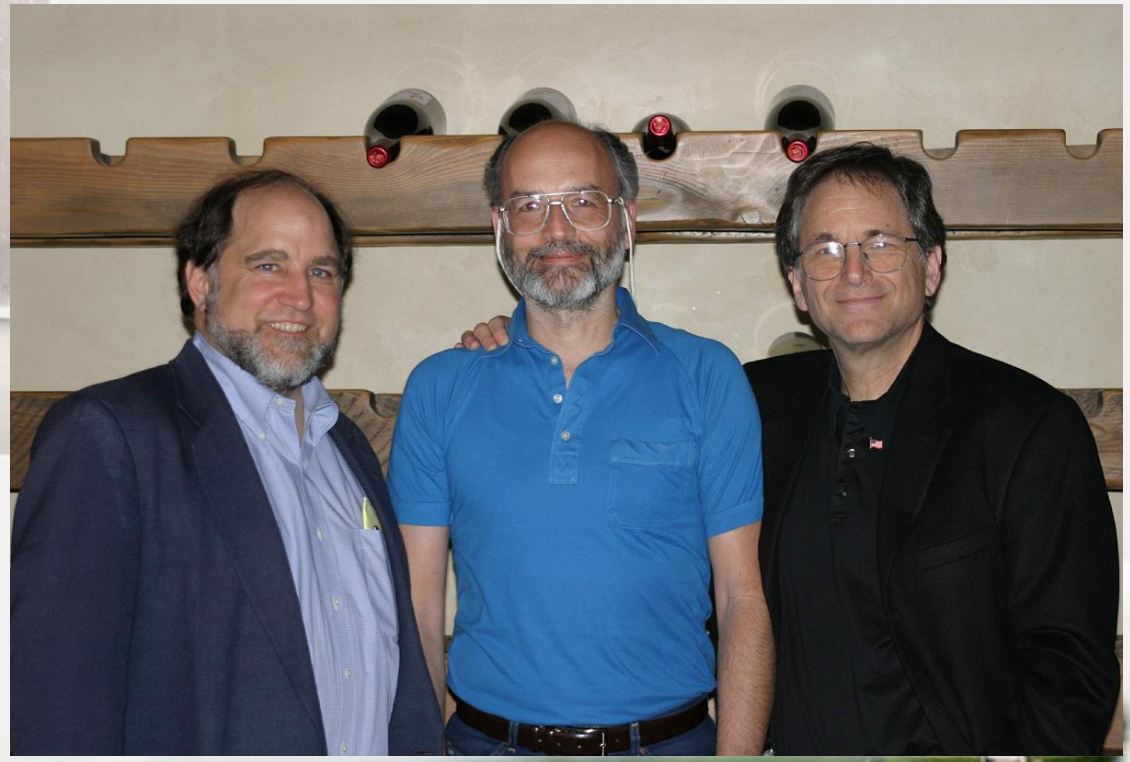
– 1976 : Public-Key Cryptography (Whit Diffie and Marty Hellman)
New Directions in Cryptography. IEEE.IT,1976

Whitfield Diffie and Martin Hellman win ACM 2015 A.M. Turing Award

现代密码学

- 1977 : Data Encryption Standard, DES (NIST)
- 1978 : RSA (Rivest, Shamir, Adleman)





现代密码学

- McEliece scheme ('78)
- Rabin scheme ('79)
- 背包方案('79-):
  Merkle-Hellman, Chor-Rivest
- ElGamal PKC（'85）
- **ECC：** 椭圆曲线密码体制（'85）

Goldwasser/Micali于1982年提出语义安全，1984年又证明了语义安全与密文不可区分性的等价性

Silvio Micali Shafi Goldwasser





1984:

- semantic security
- indistinguishability

2012图灵奖于2013年3月13日揭晓，Shafi Goldwasser和Silvio Micali因为在理论密码学领域做出的杰出贡献而获得2012 ACM图灵奖。

Award Citation

For transformative work that laid the complexity-theoretic foundations for the science of cryptography, and in the process pioneered new methods for efficient verification of mathematical proofs in complexity theory.

现代密码学

- 1994年 Shor的量子算法
- Lattice Cryptography('97-)
- 1998年，DES被破译
- Paillier scheme(99)
- 2000: AES（ 2000年10月2日确定了以Rijdeal作为AES的标准算法）
- IBE, pairing based cryptosystem(2001)

Sahai- Waters

Attribute-based encryption (ABE)

Boneh-Franklin

现代密码学

- Xiaoyun Wang, MD5(2004)
- Ideal Lattice scheme(07,08)，全同态密码

- Sha-3(2012)
- 多线性对(2013)

- 不可区分的混淆IO及其应用2013-14
- 中小特征有限域DLP计算(2013-14)
- 区块链(1.0, 2.0, 3.0…)及其应用
- NIST后量子密码标准2020.07

- …..

现代密码学研究涉及到多个学科

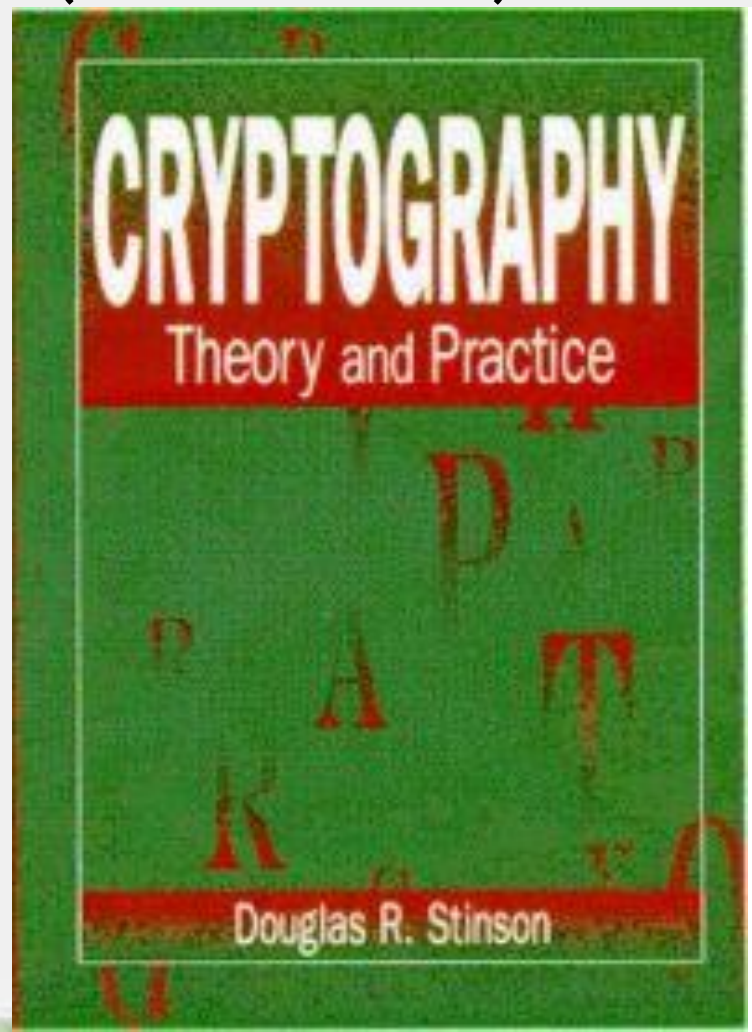
- 数学：数论，代数，概率论
- 计算复杂性理论
- 信息论
- 物理学：量子
- 通信
- 软硬件的实现
- 经济学、政治学、。。。
- 等等

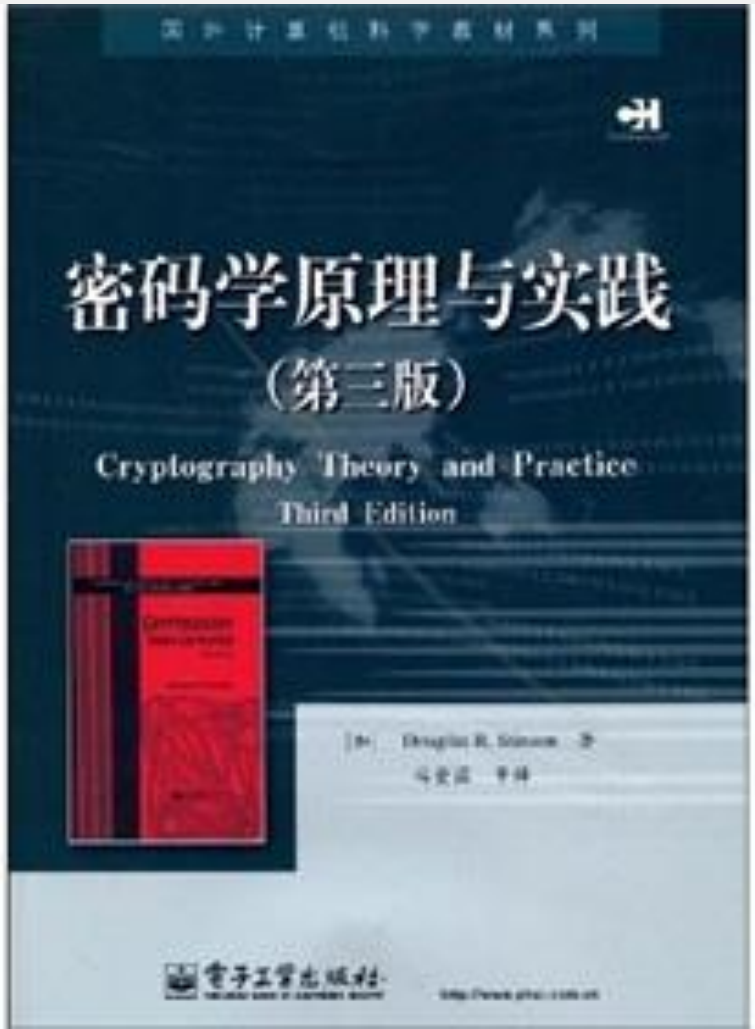
讲授内容

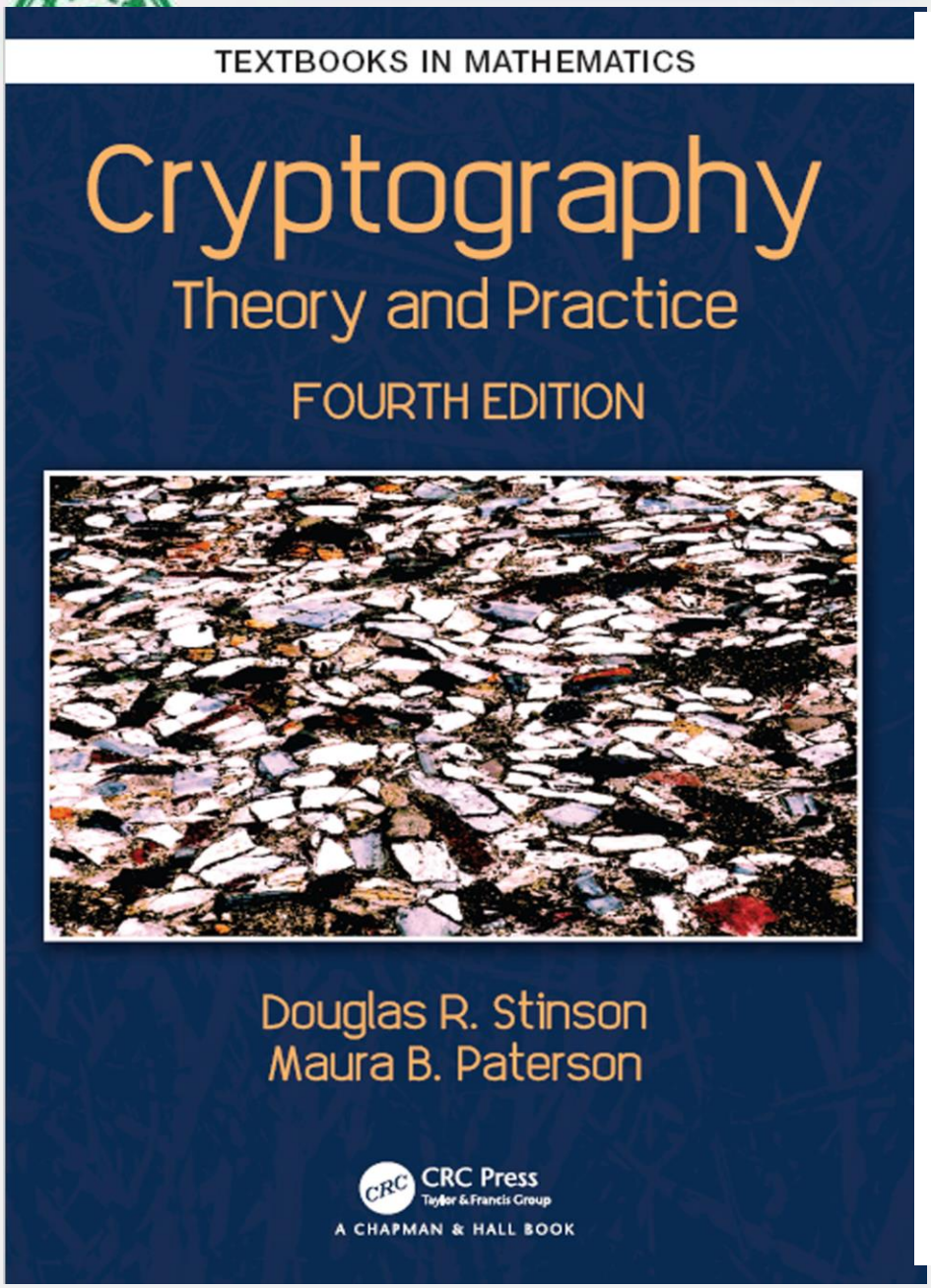
- 密码学引论
- 古典密码学及其分析
- 完善保密理论：概率论与Shannon理论
- 私钥密码体制：原理与构造--DES, AES
- Hash函数与MAC
- 整数分解与RSA密码体制
- DLP密码体制
- 数字签名
- 伪随机数产生器

主要学习用书

- **Douglas R. Stinson, *Cryptography-Theory and Practice*, (Second Edition) CRC Press, 2002.**







其他参考书目

- J. Katz and Y. Lindell, Introduction to Modern Cryptography, Chapman - Hall/CRC Press, 2007.
- Wenbo Mao, Modern Cryptography: --Theory and Practice, Prentice-Hall, PTR，2003 .中译本“现代密码学:理论与实践”
- Stallings, W., Cryptography and Network Security. Principles and Practice, 3rd edition, Prentice Hall, 2002
- 王育民，刘建伟，《通信网的安全》——理论与技术，西安电子科技大学出版社，2000
- Dan Boneh, Stanford University：Online Cryptography Course http://crypto.stanford.edu/~dabo/courses/OnlineCrypto/

课程成绩

- 平时40%
  考勤5+次课堂测试
  （助教：廖梓文）

- 期末60%
  闭卷考试

Questions ?