# 密码学简介

主讲人：于红波
清华大学计算机系
2023-2-22

# 什么是密码学？密码用在哪些地方？

# 什么是密码学?

- 经典定义：密码学是研究保密通信的一门科学。研究在不安全的环境中，如何把所要传输的信息在发给接收者之前进行秘密转换以防止第三者对信息的窃取

  保证信息的机密性
- 现代定义：密码学主要研究如何构建能够经受住任何滥用的安全方案，即：在任何恶意企图使它们偏离规定的情况下，该方案仍能维护它所设计的功能（From Foundations of Cryptography – O. Goldreich）

  保证信息的机密性和可认证性

# 提纲

- 密码学发展史
- 主要密码技术及密码常识
- 《密码法》简单解读

# 密码学发展史

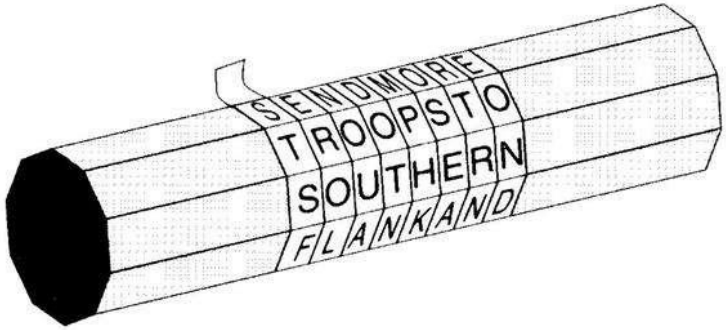
- 与计算设备有关
  - 笔、纸
    - Staganography（隐写术）：
      - Steganos（覆盖）
      - Graphein(写): 隐形墨水, 数字水印

芦花滩上有扁舟，
俊杰黄昏独自游。
义到尽头原是命，
反躬逃难必无忧。

武则天时代　宰相裴炎给徐敬业、
骆宾王传递信息“青鹅”

这是一棵树的照片，内含了隐蔽的图像。如果把每个色彩空间和数字3进行逻辑与运算，再把亮度增强85倍，得到下图。（来源于为维基百科）

# 密码学的发展




- 与计算设备有关
  - –笔、纸
    - Cryptography（密码术）：
    - 斯巴达密码：早在公元前5世纪，古希腊人发明了斯巴达密码，他们将一串信息附在在特定的木棍上，把木棍抽走，信息就会变成乱码。
    - 凯撒密码： 简单的代换密码

# 密码学的发展史

- 与计算设备有关
  - 笔、纸

# 密码学的发展史

- 与计算设备有关
  - 笔、纸
    - Cryptography（密码术）
      - Transposition（易位）

      COW: COW, OCW, CWO ,OWC ,WCO,WOC

      For example, consider this short sentence. $5*10^{31}$
      - Substitution（替换）

      明码表 A D H I K M O R S U W Y Z

      密码表V X B G J C Q L N E F P T

      Meet at midnight: CUUZ VZ CGXSGIBZ

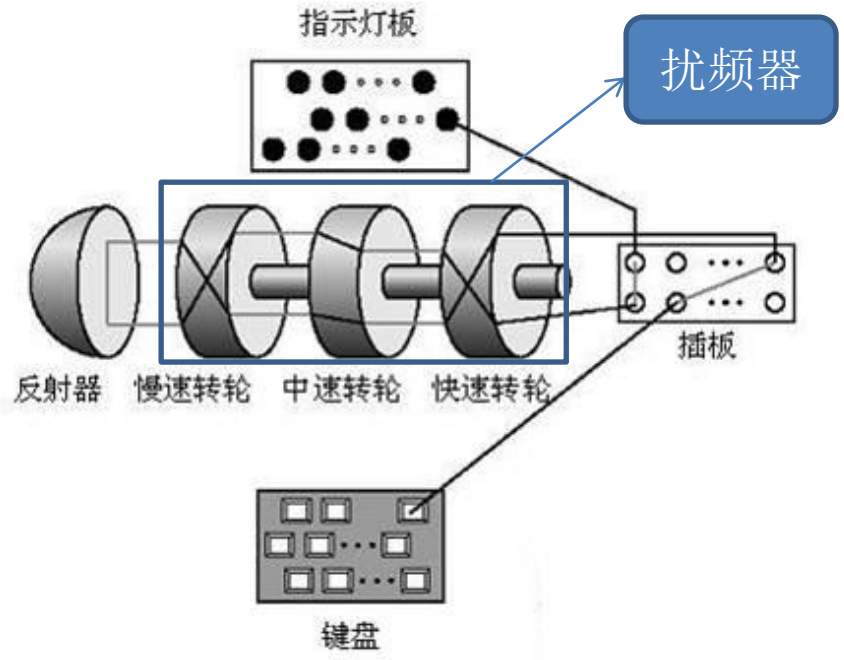
**密码隐藏的是内容，隐写术隐藏的是消息本身。**

# 密码学发展史

- 与计算设备有关
  - 密码盘：15世纪-20世纪
    - 简化了加密过程
    - 单表代换、多表代换
  - 电子计算装置
    - 轮转机（Roter Machines: 1920s-1960)
      - Enigma密码机(德国)
      - Sigaba（美国）
      - Typex（英国）
      - Lorenz SZ 40/42（德国，盟军代号“金枪鱼”）
      - Siemens and Halske T52（德国，盟军代号“鲟鱼”）
      - 紫密码机（日本）

# 密码学的发展史

- Enigma密码机由德国Scherbius发明，1920年代被用于商业，在二战中被军事广泛使用
  - 键盘、扰频器、接线板（插板）、指示板、反射器




密码：

1.线路接线板设置： A/L, P/R, T/D, B/W, K/F, O/Y

2. 扰频器排列：2-3-1

3. 扰频器定位：Q-C-W

# 密码学的发展史

- Enigma密码机
  - 3个扰频器：
    - 26*26*26=17576
  - 插件板：26个字母中任意交换6对
    - 100391791500
  - 密钥总的数目
    - 17576*6* 100391791500=$10^{16}$

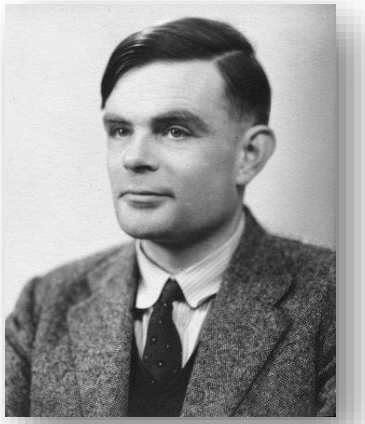
# 密码学的发展史-ENIGMA密码机的破解

- 1932年，波兰密码学家Rejewski，Zygalski, 和Rozycki设计Bomba破译德军使用的ENIGMA (3个扰频器)
  - Schmidt出卖军用密码机扰频器文件给法国
  - 密钥设定： 每一条信息传递新密钥
  - 每条信息重发送两次，违背一次一密原则
    - 原始密钥（扰频器定位）QCW, 信息密钥PGH
    - PGHPGH加密成KIVBJE
- 1938年12月德国增加了ENIGMA的安全性(5个扰频器)，Rejewski的技术破解受限
- 1939年6月波兰将Bomba技术提供给法国和英国

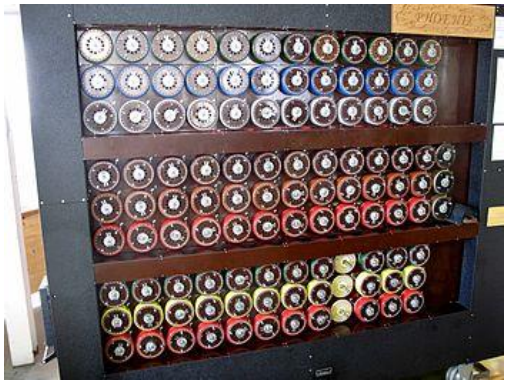
# 密码学的发展史-ENIGMA密码机的破解

- 自1939年英国的科学家和数学家在Bletchley（布莱切里）庄园开始了新的ENIGMA的破译工作
- 图灵设计了**the British bombe**，利用已知的明密文对破译ENIGMA
- 得到德军法国边境集结的详细计划：盟军法国诺曼底登陆，德军损失四十万
- 美国弗里德曼小组经过
  两年的努力破解了日本紫密，
  从而击落了日本舰队总司令
  山本五十六座机

Enigma的破解使得二战至少提前一年结束



阿兰. 图灵



**the British bombe:**图灵机模型

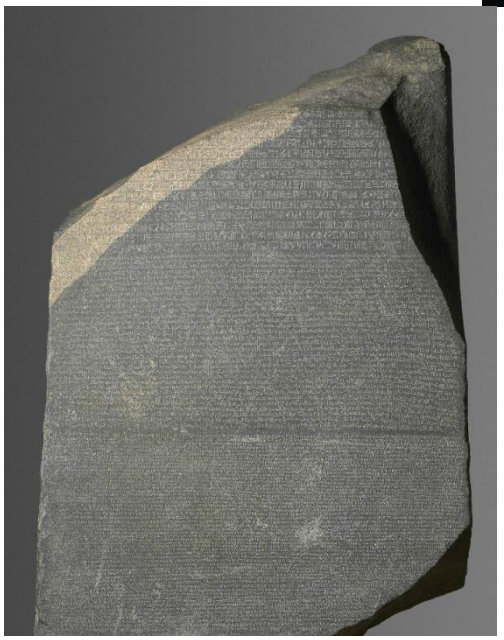
# 失落的语言和古代文字

- 纳瓦霍密码(Navajo code)-二战中的无敌密码
  - 没有文字，语法、声调、音节复杂
  - 非纳瓦霍族人全球不超过30个，没有德国人和日本人
  - 不可破解的密码
- 罗塞塔石碑
  - 三种文字

  古埃及象形文

  埃及草书

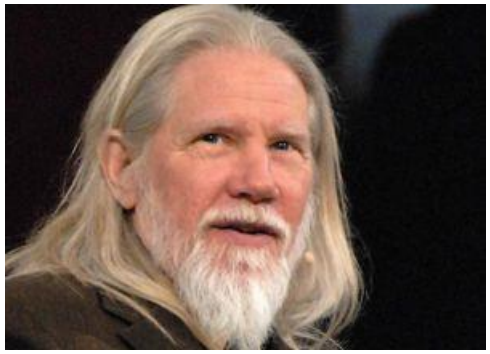
  古希腊文

1799年于埃及罗塞塔发现，现存于大英博物馆

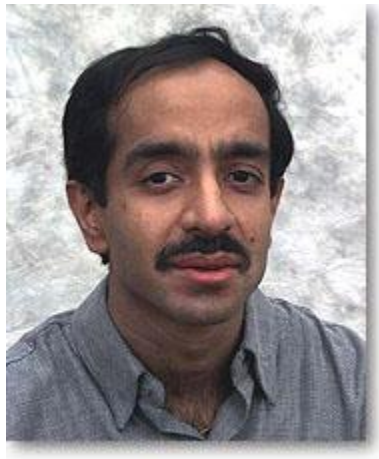
# 密码学发展史

- 与计算设备有关
  - 电子计算机
    - 现代密码算法
      - 对称密码体制：DES（1976年）， AES，
        - » 1949年，Shannon发表《保密系统的信息理论》，提出熵的概念，建立了完善安全性为对称密码学建立了理论基础，密码学从艺术成为科学
        - » 密钥分发问题
      - 公钥密码体制： RSA, ECC
        - » Whitfield Diffie
        - » Martin Hellman
        - » Ron. Rivest, Adi Shamir, Leonard Adleman.



# 量子密码

- 与计算设备相关
- 量子计算机
  - Peter Shor 算法：提出了量子质因数分解算法（1994）
  - 量子计算机能够破译
    - RSA
    - 离散对数问题：Diffie Hellman 密钥交换协议
    - 椭圆曲线密码系统
  - Grover 搜索算法: $\mathrm{O}(n) \rightarrow \mathrm{O}(\sqrt{n})$
  - 建立抗量子的公钥密码体系

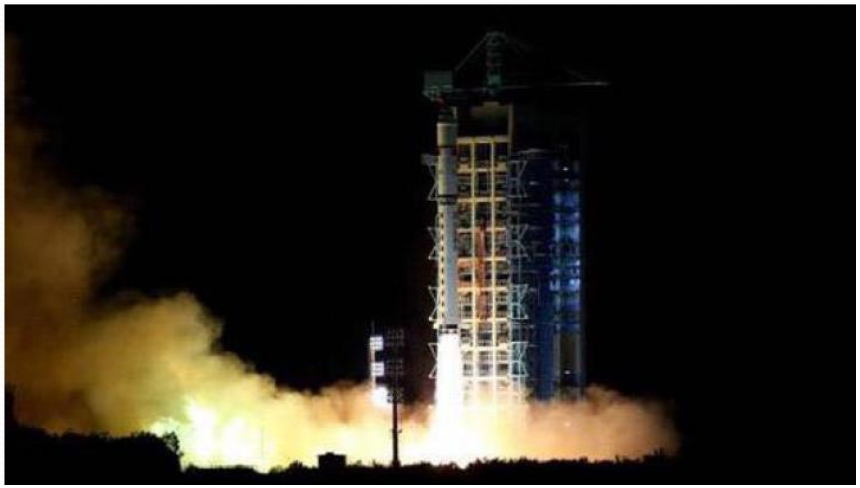


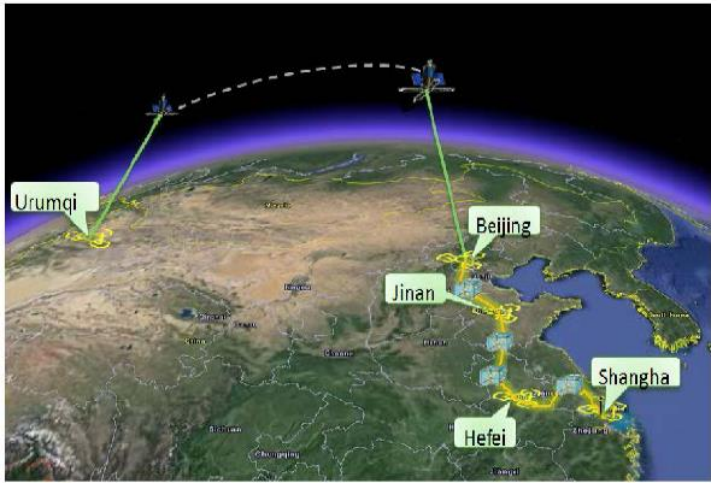
# 量子密码

## 量子密钥分发

京沪干线


墨子号量子卫星

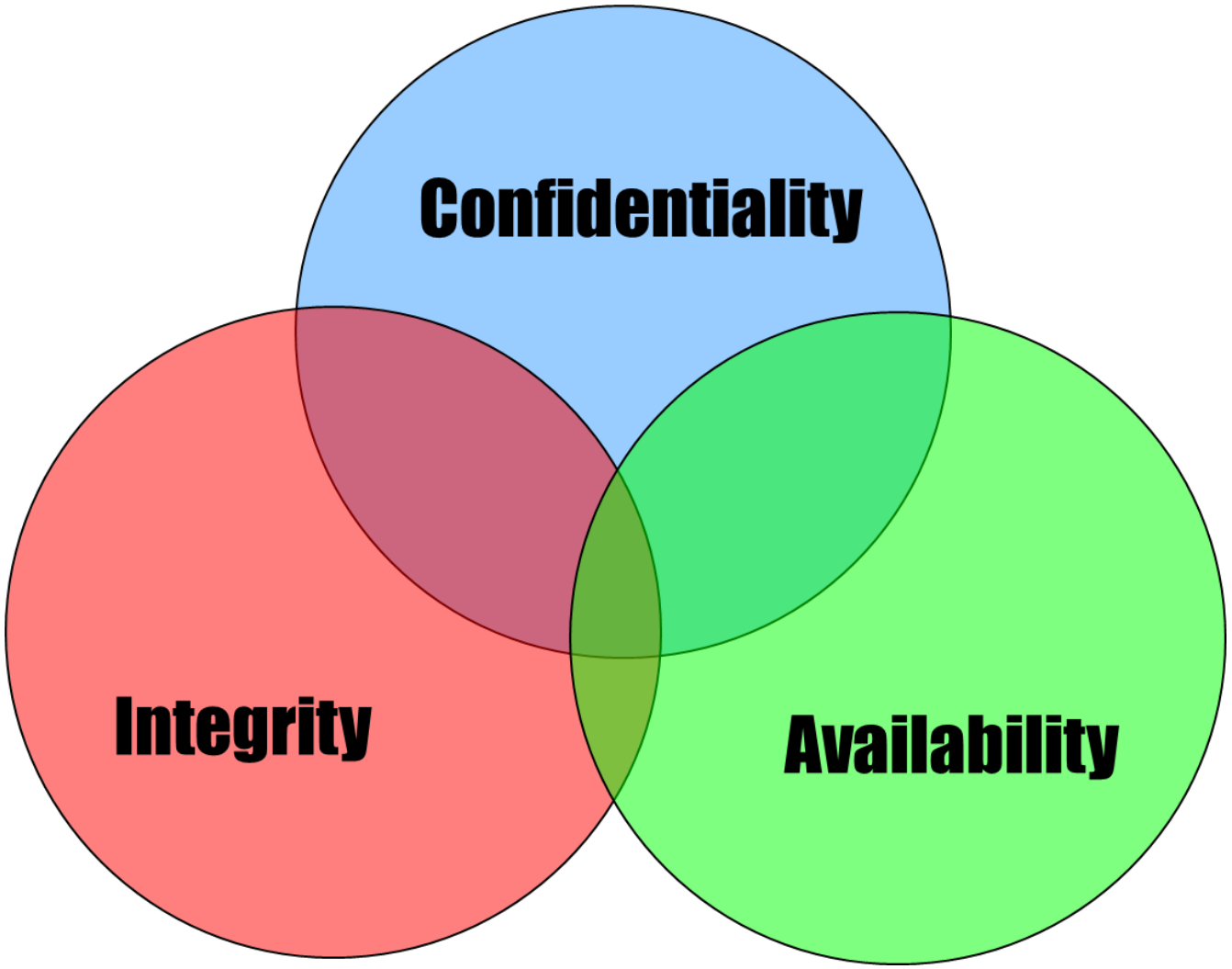




# 现代密码学研究内容

- 加密
  - 加密算法，用来保证信息的机密性
- 认证
  - Hash函数（数字指纹，杂凑函数，单向散列函数）：完整性
  - 消息认证码：消息是否来自所期望的通信对象？
  - 数字签名：防伪装，篡改，否认等威胁技术
  - 证书： 为公钥加上数学数字签名
- 密钥-秘密的精华
- 随机数和密码应用技术

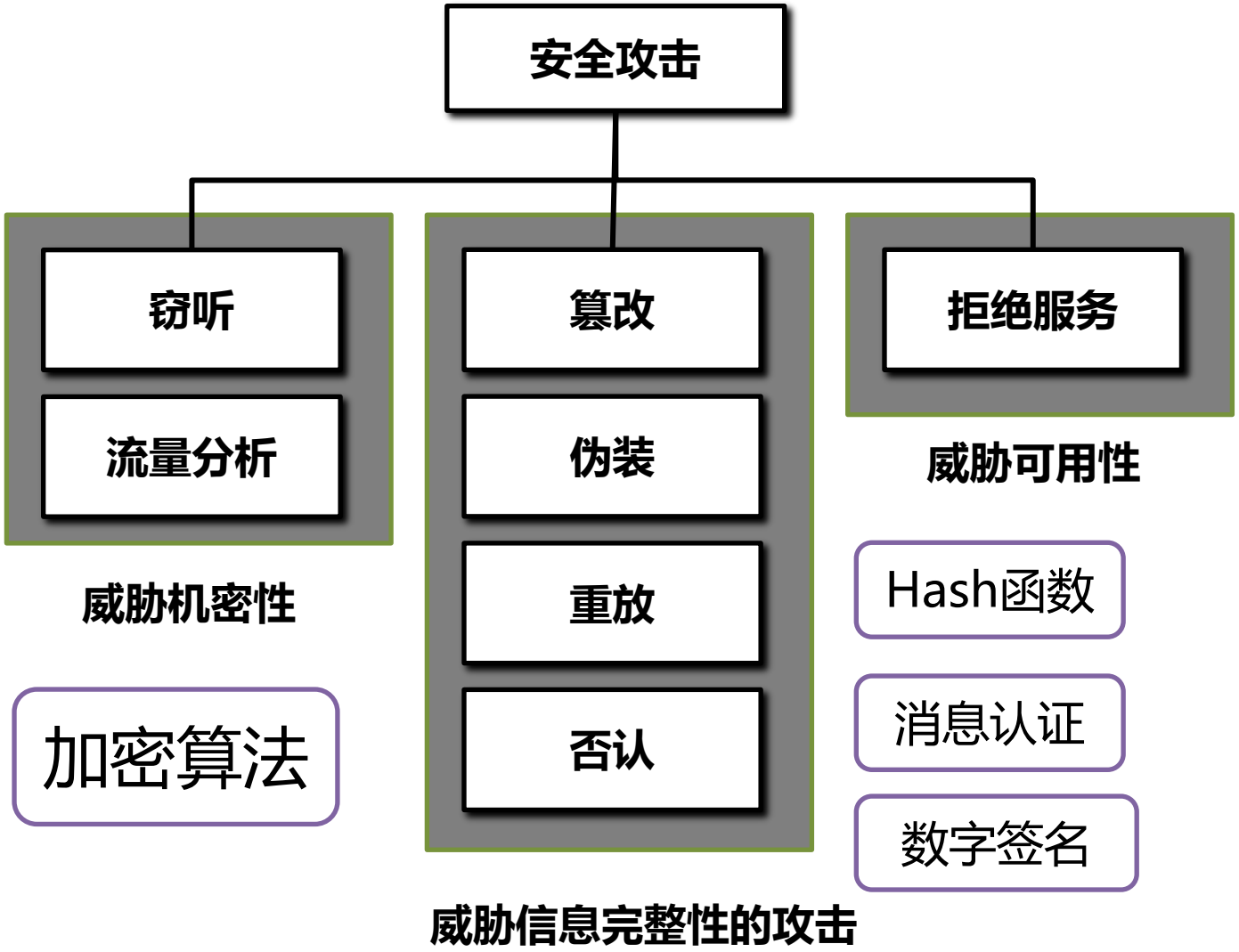
# 安全目标： CIA



# 安全目标： CIA

- Confidentiality：保密性、机密性
  - 保护信息内容不会被泄露给未授权的实体
  - 保密场景：业务数据、网络拓扑、流量
- Integrity：完整性
  - 保证信息不被未授权地修改，或者可以检测出非授权修改
  - 攻击示例：篡改、插入、重放
- Availability：可用性
  - 保证资源的授权用户能够访问到应得资源或服务
  - 攻击示例：拒绝服务（网络、系统、硬件、人）

# 信息安全面临的威胁


安全攻击
窃听
流量分析
威胁机密性
加密算法
篡改
伪装
重放
否认
威胁信息完整性的攻击
拒绝服务
威胁可用性
Hash函数
消息认证
数字签名

# 几条密码常识

- **不要使用保密的密码算法**
  - “由公司开发一种密码算法， 并将这种算法保密，这样就能保证安全”？
  - 使用公开的，被公认为强度较高的密码算法
    - 密码算法早晚会被公诸于世， 如RC4
    - 开发高强度的密码算法是非常困难的
- **使用低强度的密码比不进行任何加密更危险**
  - 获得一种错误的安全感， 如16世纪苏格兰玛丽女王

# 几条密码常识

- 任何密码总有一天都会被破解

  一次一密 完美密码

  量子密码 可能完美的密码

- 密码只是信息安全的一部分

  –安全是“系统安全”，系统的强度取决于其中最脆弱的环节的强度

# 密码法

2019年10月26日，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通过了《中华人民共和国密码法》，进一步规范了密码应用和管理，提升了密码法制度化保障水平。密码法自2020年1月1日起实施。

# 密码法解读

1. 什么是密码?

根据密码法（第二条）的法律定义：密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

2. 密码分为几类?

密码法根据应用场景和加密强度的要求，把密码范围三类（第六条、第七条）：核心密码、普通密码和商用密码。国家对密码进行分类管理。

# 密码法解读

## 3.哪些行为属于与密码相关的违法犯罪行为?

密码法主要规定了三种情形（第十二条）属于与密码相关的犯罪:

一、窃取他人加密保护的信息。

二、非法侵入他人的密码保障系统。

三、利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

例如，制作勒索病毒、加密传播木马病毒及各类不法信息，都属于第三种情形。

# 密码法解读

## 4 .做密码工作是否需要持证上岗?

一般不用。但如果要做核心密码和普通密码，就需要“持证上岗”了。

密码法（第十八条）规定：国家建立适应核心密码、普通密码工作需要的人员录用、选调、保密、考核、培训、待遇、奖惩、交流、退出等管理制度。

# 密码法解读

## 5．生产和销售密码产品，是否需要检测?

简单的说就是：生产者自愿，但使用领域受限。

根据密码法（第二十五条）要求：国家鼓励商用密码从业单位自愿接受商用密码检测认证，提升市场竞争力。但法律对此并不强求。

密码法（第二十六条）也要求：涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。

# 密码法解读

## 6. 企业、行业可以自定密码标准吗?

可以。

根据密码法《第二十二条》规定，密码既有国家标准，也可以有行业标准，同时，在商用密码领域，国家还支持社会团体、企业制定高于国标准、行业标准的团体标准、企业标准。

# 密码法解读

## 7. 外商必须使用中国密码吗？国产密码在外国能用吗？

在除关键信息基础设施之外的一般商用领域，使用什么密码是企业的自由，外商和国内企业一视同仁。同时，国产密码也在走向国际化。例如，SM2、SM3、SM4、SM9、祖冲之序列密码算法等国产密码算法，已经成为国际标准，或者获得国际标准提案立项。

参见《密码法》二十一、二十三条。

# 密码法解读

## 8.密码也能进出口吗?

能，但有限制。

根据密码法（第二十八条）要求：对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。但是，大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

# 谢谢！