



现代密码学

中国海洋大学 信息安全实验室

教学目标

1

掌握基本知识、基本原理

2

掌握密码技术的应用

3

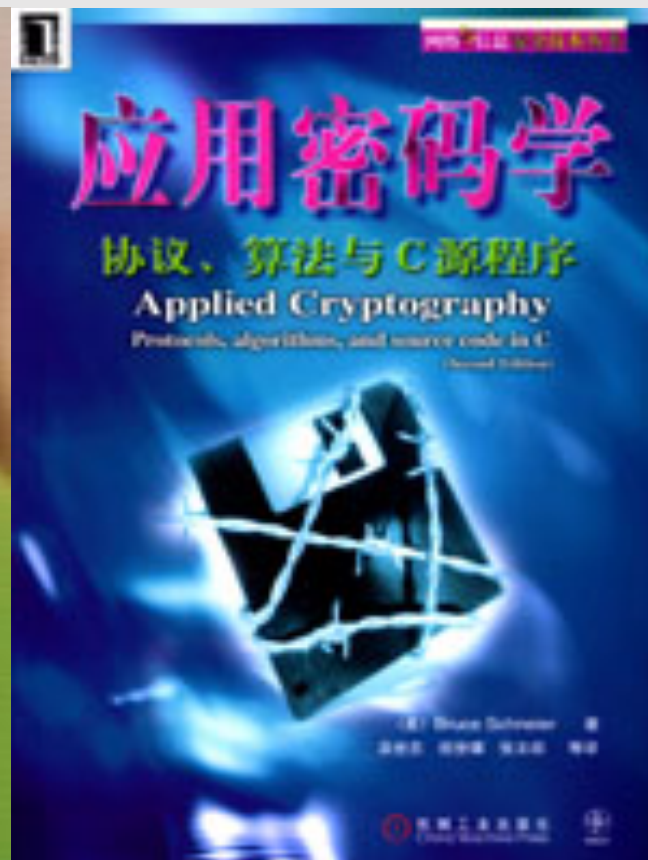
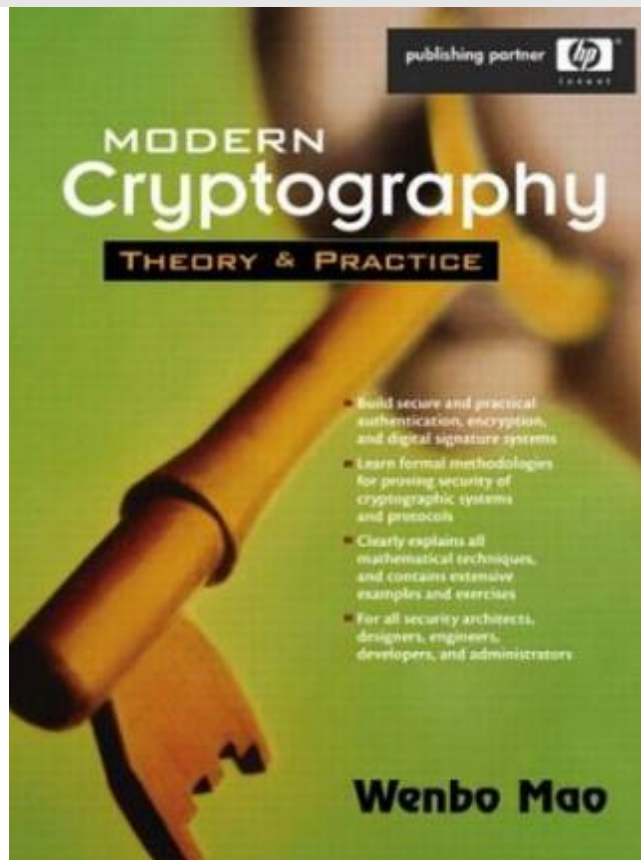
了解密码学的发展动态

推荐三本书

入门

进阶

杂货铺







期末考试

- **题型**：单选、判断、填空、简答、综合
- **内容**：
 - 基本知识、基本概念题
 - 计算题
 - 算法题（与实验相关的内容）
 - 惊喜题

期末考试重点

- PPT里带★页面

期末成绩构成

- 平日成绩占30%（点名、实验报告等）
- 期末考试卷面成绩占70%



第1章

密码学概述

1.1 密码学简介

1.2 密码学发展史

1.3 关于密码分析

为什么要学密码学？

密码学到底都能干些什么？



保证你发出的信息，除指定人以外，其他人难以知道内容

机密性



检查信息是否被篡改过

完整性



- 确认对方的身份；证明你的身份
- 确认信息是谁发出的

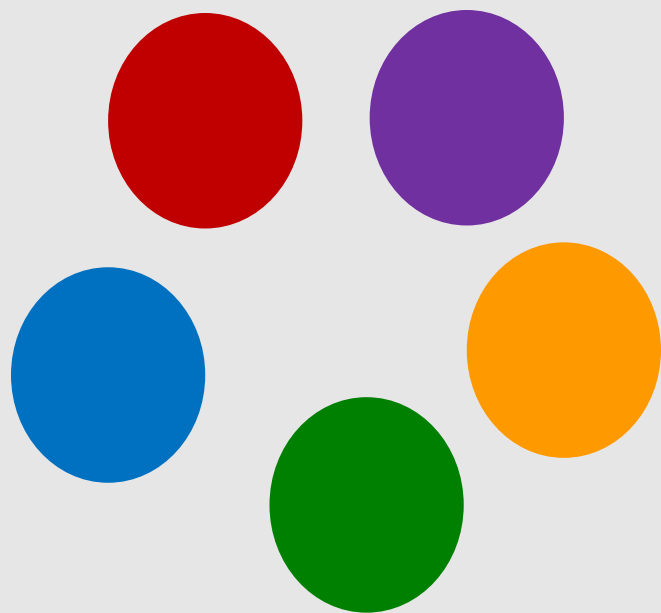
认证



证明自己身份的同时，不泄露
自己的身份

匿名性

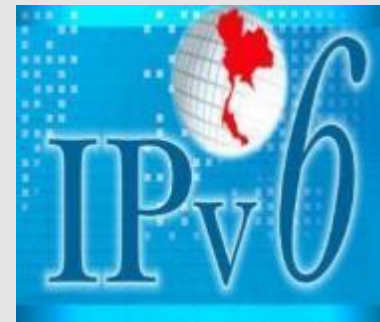
密码学能干些啥



能干的事还有很多很多，品种繁多，五花八门

离开密码学，很多安全需求很难或无法实现

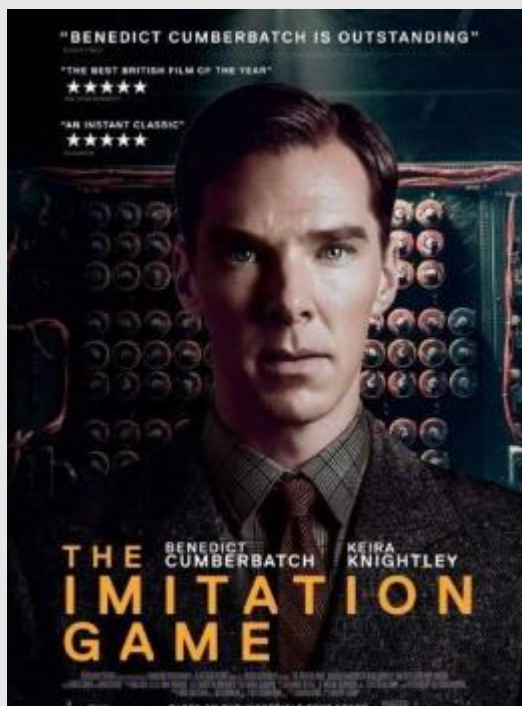
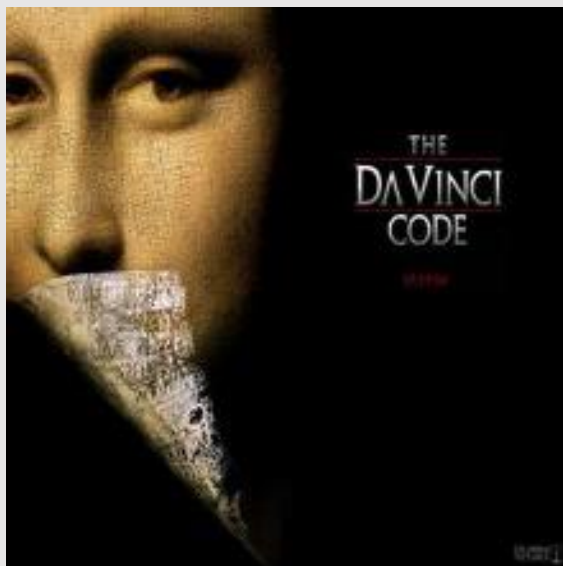
生活中哪些地方用到密码技术



高大上的应用



影视作品中的密码学



为什么要学密码学？

- ① 密码学与现实生活息息相关
- ② 学习网络安全应该具备一定的密码学知识
- ③ 仅使用计算机学科的方法无法满足某些安全需求
- ④ 密码学提供了丰富多彩的安全保护手段，可以满足不同的安全需求

图灵奖历史上的密码学家



获得时间	获奖者	获奖原因
1995	Blum	计算复杂度理论，及其在密码学和程序校验上的应用
2000	Andrew.C.C.Yao	计算理论，包括伪随机数生成，密码学与通信复杂度
2002	Rivest、Shamir、Adleman	RSA加密算法
2012	Goldwasser、Micali	可证明安全性理论
2015	Diffie、Hellman	公钥密码学



1.1 密码学简介



密码学是信息安全的基础

提供理论/技术支持

密码学不是万能的，离开它却是万万不能的



机密性

确保信息不被非法获取

常见威胁：

- 窃听
- 盗窃文件
- 社会工程学

.....



完整性

确保能够发现信息是否被改动过

常见威胁：

- 合法用户的失误
- 非法用户的篡改



可用性

确保系统正常提供服务

常见威胁：

- 设备故障
- 软件错误
- 环境因素
- 人为攻击

攻击者能干些什么 —— 两种攻击形式



被动攻击

对机密性的破坏

窃听

主动攻击

对完整性、可用性等的破坏

篡改
冒充
.....



保证机密性

防范“信息泄露”

保证完整性

防范“信息篡改”

提供非否认

防范“否认干过的事”



研究内容：保护系统安全

组成部分：

密码编码学
(设计密码)

密码分析学
(破译密码)

一把双刃剑：

- ① 帮助分析密码算法的安全性
- ② 帮助破坏受保护信息的安全性

明文

需要加密的信息

加密

隐藏信息的过程

密文

加密后的明文

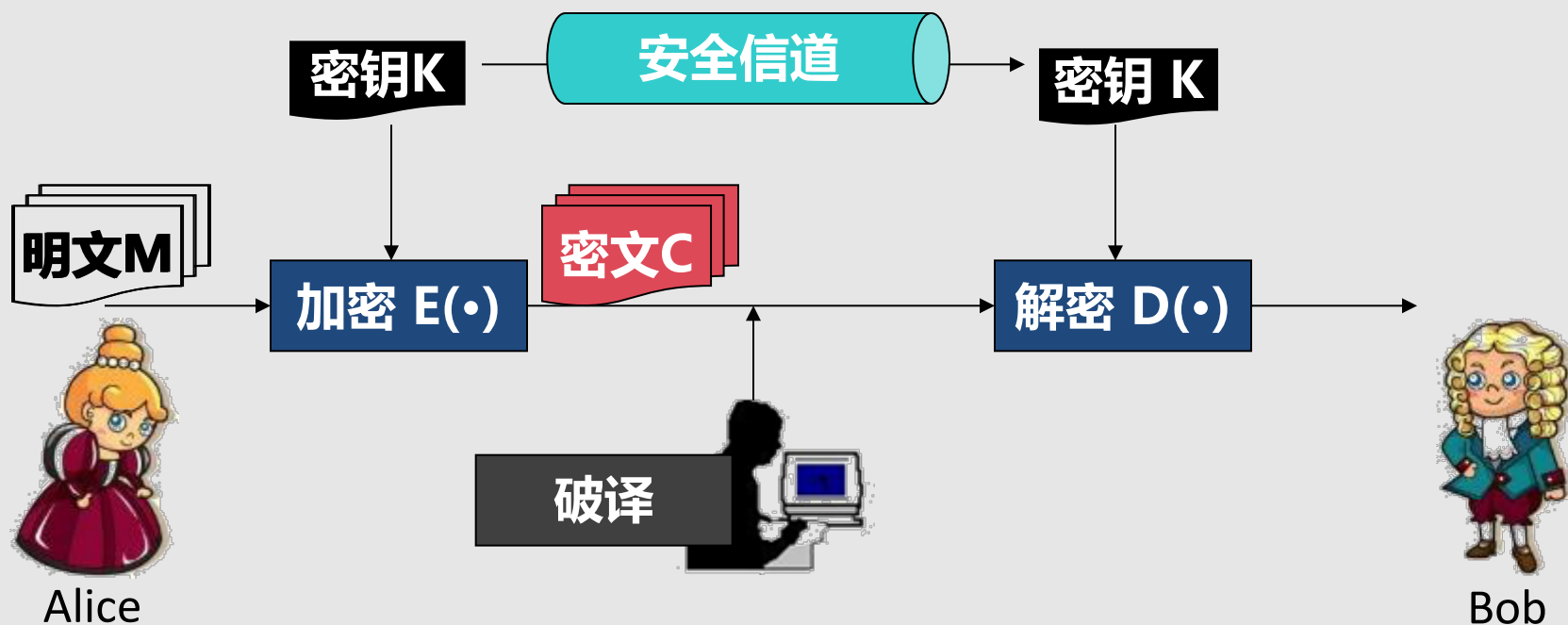
解密

从密文恢复
明文的过程

密码分析

破译密码的过程

秘密通信模型



加密	$E_K(M) = C$
解密	$D_K(C) = M$
$D_K(E_K(M)) = M$	

区别两个术语



密钥 (key)

用于“变换”：密码算法的辅助输入
是一些随机串

口令 (password)

用于“身份认证”：确认对方或
是一些容易记忆，
常被翻译成“密码”

二维码登录 邮箱帐号登录

邮箱帐号或手机号码 @163.com

输入密码

☐ 十天内免登录 [忘记密码?](#)

登录 注册

被删邮件能恢复啦 [升级邮箱>](#)

Q:为什么不构造一个不需要密钥的算法?

如果攻击者知道了算法，他们只需执行该算法就可以恢复你的明文

貌似保密密码算法就可以解决这个问题

事实证明，攻击者总能通过各种手段发现你用的是哪个算法



柯克霍夫斯原则 密码学的基本原则

“即使密码系统的任何
细节已为人所知
只要密钥没有泄漏
它也应该是
安全的”



Auguste Kerckhoffs
1835 –1903
荷兰语言学家、密码学家



1. 知道算法的人可能叛变 历史上这种事屡见不鲜

2. 设计者有个人喜好 喜欢使用一些固定结构，易被猜测

3. 频繁更换算法不现实 设计安全的密码算法很困难

意义在于，
密码算法很难保密



加解密是在密钥的控制下进行的

加密体制的形式化描述

它是一个五元组 (P, C, K, E, D)

P

明文空间：所有可能的明文组成的有限集

C

密文空间：所有可能的密文组成的有限集

K

密钥空间：所有可能的密钥组成的有限集

E

所有加密算法组成的有限集

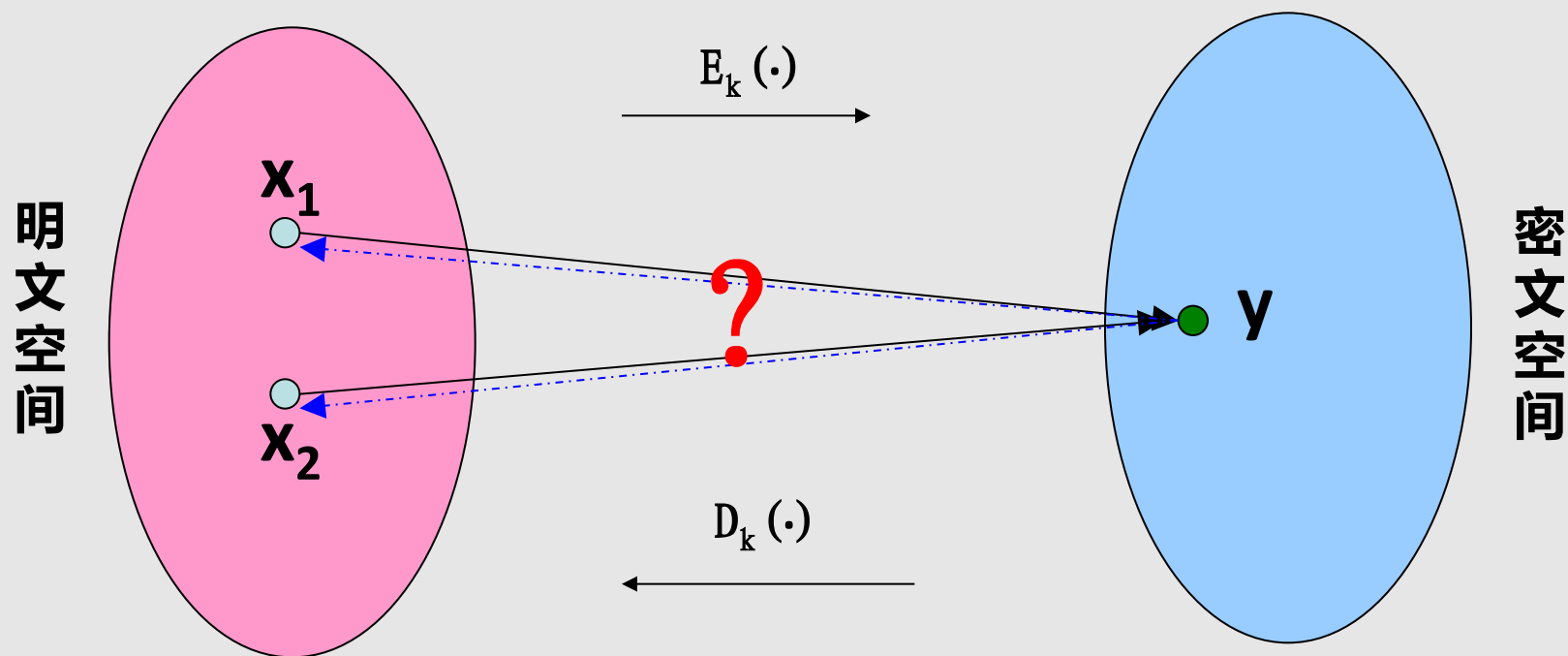
D

所有解密算法组成的有限集



加密算法(函数)必须是一个单射函数

Q: 加密函数不是单射会怎么样？



加密： $y = E_k(x_1) = E_k(x_2)$

$\neq x_2$



实用的加密体制必须满足以下两条



容易性：加密算法、解密算法都应该易于计算



安全性：对于任何攻击者，难以恢复明文/密钥

区别两种技术



隐写术



加密术

隐写术

洋葱法



隐写术

剃光头



我康宣，今年一十八岁，姑苏人氏，身家清白，素无过犯。只
为家况清贫，鬻身华相府中，充当书僮。身价银五十两，自
秋节起，暂存帐房，俟三年后支取，从此承值书房，每日焚
香扫地，洗砚、磨墨等事，听凭使唤。从头做起。立此契为凭。



芦花从中一扁舟，
俊杰俄从此地游，
义士若能知此理，
反躬难逃可无忧。





特点

保护的是信息本身（把信息隐藏起来）

缺点：一旦发现隐藏的方法，信息就会暴露（安全性差）

洋葱法 —— 用火烤

古希腊剃头法 —— 把可疑的人剃成秃瓢

藏头诗 —— 检查诗词的开头和结尾

.....


加密术

两种常用基本技术



置换

又叫 易位
(permutation)



代换

又叫 替换、代替
(substitution)

公元前400年，斯巴达人使用的加密工具

Scytale





特点

明文中字符与密文中相同，只是出现的位置发生变化

Q: 密钥是什么？

改变位置的规则

兽栏密码

明密文字母对照表：

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:	:.

明文：system

密文：: | : | : | : | □ | □



特点

明文出现的字符不一定出现在密文中，但位置保持不变

Q: 密钥是什么？

代换规则



隐写术

保护的是信息本身，传递的仍是原来的信息，只是被藏了起来
一旦发现隐藏的方法，信息就会暴露



加密术

保护的是信息内容，传递的是变换后的密文，而不是原来的明文
不知道密钥，很难恢复信息



1.2 密码学发展史

密码学发展历程



密码学的发展历程大致经历三个阶段

古代加密阶段



密码最早应用于军事和政治领域



存于石刻或史书中的记载表明，许多古代文明，包括埃及人、希伯来人、亚述人都在实践中逐步发明了密码系统

从某种意义上说，战争是科学技术进步的催化剂

自从有了战争，人类就面临着通信安全的需求，使得密码技术源远流长

古典密码阶段



密码开始应用于商业领域



虽然名字叫“古典密码”，但在近代得到广泛发展和应用

古典密码系统已经初步体现出现代密码系统的雏形，它比古代加密方法更复杂



古典密码的典型代表：

单表代换密码

多表代换密码

转轮机密码

加密手段：

一般是对字符的变换

使用手工或机械变换的方式实现



现代密码阶段



密码开始应用于民用领域（特别是互联网）



密码是非常古老的技术，但**真正形成学科还是20世纪40-70年代的事**，这是受计算机科学蓬勃发展的刺激和推动的结果



计算机和电子时代的到来，使密码设计者轻易摆脱手工设计时易犯的错误，也不必承受电子机械方式的高额费用

快速计算机和现代数学为密码技术提供了新的概念和工具，也给攻击者提供了有力武器



在这一阶段，密码理论蓬勃发展，密码算法的设计与分析互相促进，出现了大量的密码算法和各种攻击方法

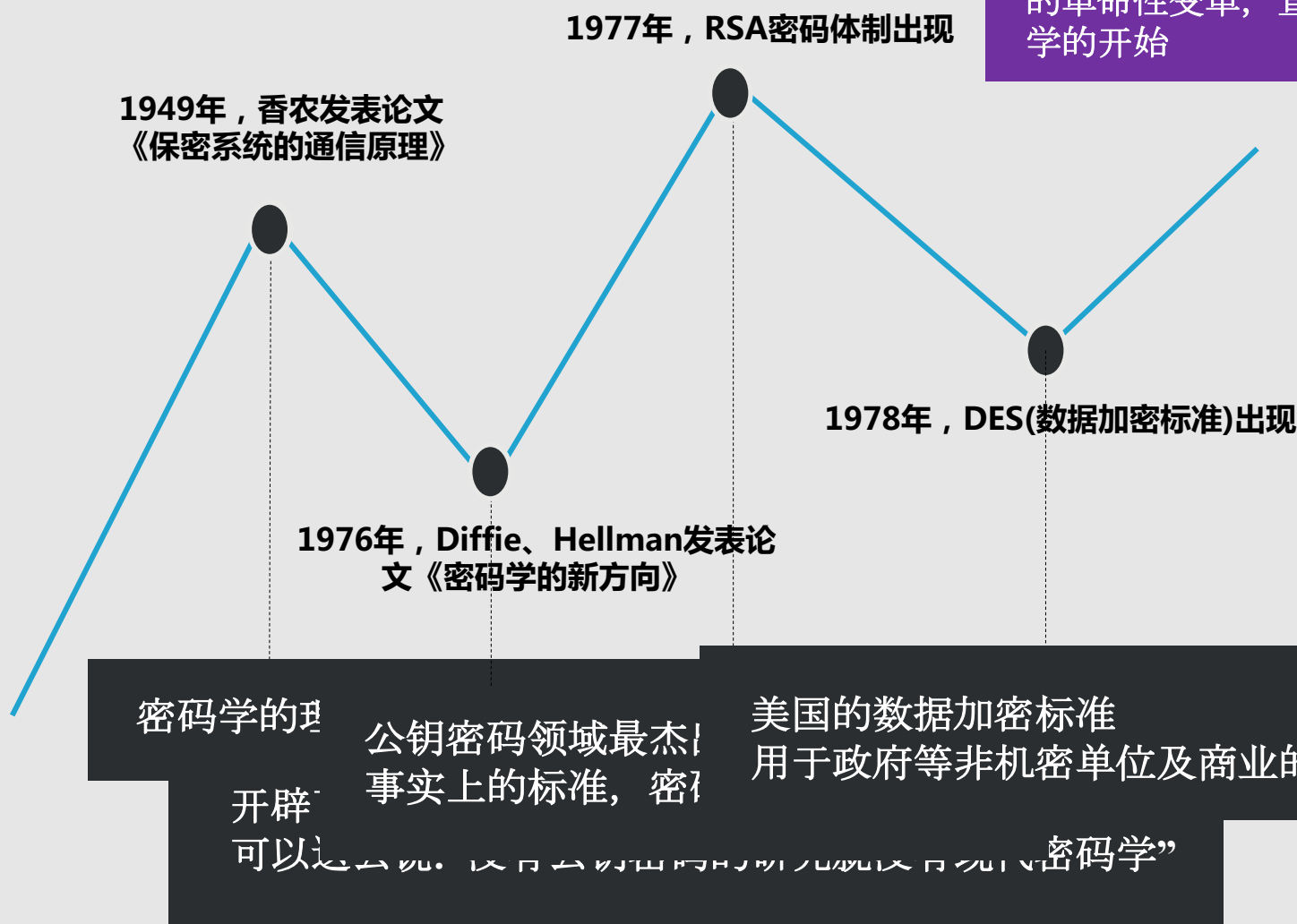


密码技术的应用范围也在不断扩展，出现了许多通用的密码标准 (DES、AES等)，促进了网络和技术的不不断发展

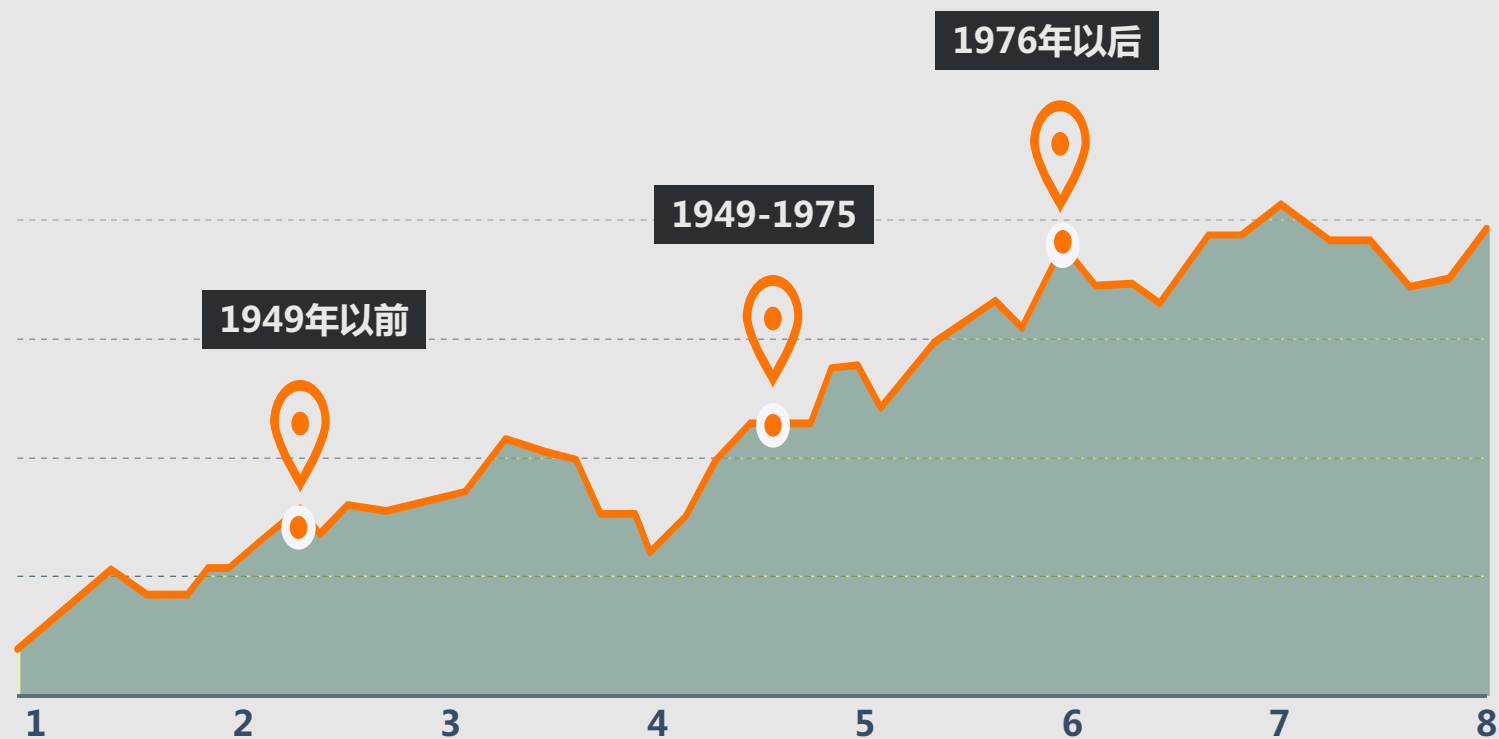


密码学历史上的重要事件

它们标志着密码学理论与技术的革命性变革，宣布了现代密码学的开始



密码学发展历程 (另一种说法)



1949年以前

密码学只是一门技术/艺术

1949-1975

密码学形成一门科学

1976年以后

密码学新方向：公钥密码学



1.3 关于密码分析



对加密体制进行攻击的分类

依据攻击者知道信息的多少，可如下分类：

攻击强度依次增强

唯密文攻击	只有一些密文，好的现代密码系统对此通常是免疫的
已知明文攻击	已有很多明文/密文对
选择明文攻击	可以任意选择明文，并可获得相应密文
选择密文攻击	可以任意选择密文，并可获得相应明文

在实际中，破译通常是多种手段综合应用的结果

池步洲，福建省闽清县人。自幼家境贫寒，直到10岁才上学，却用3年时间完成小学课程，考入福州英华书院（今福建师范大学附属中学）。

后留学日本早稻田大学。

抗战爆发后，回国抗日。经同学介绍加入中统，是当时中统内唯一的留日学生。

尽管没学过密码破译，却用**统计**、**大胆猜测**，以及自己对日本的了解，破译大量日军密电。

珍珠港事件：东风，有雨

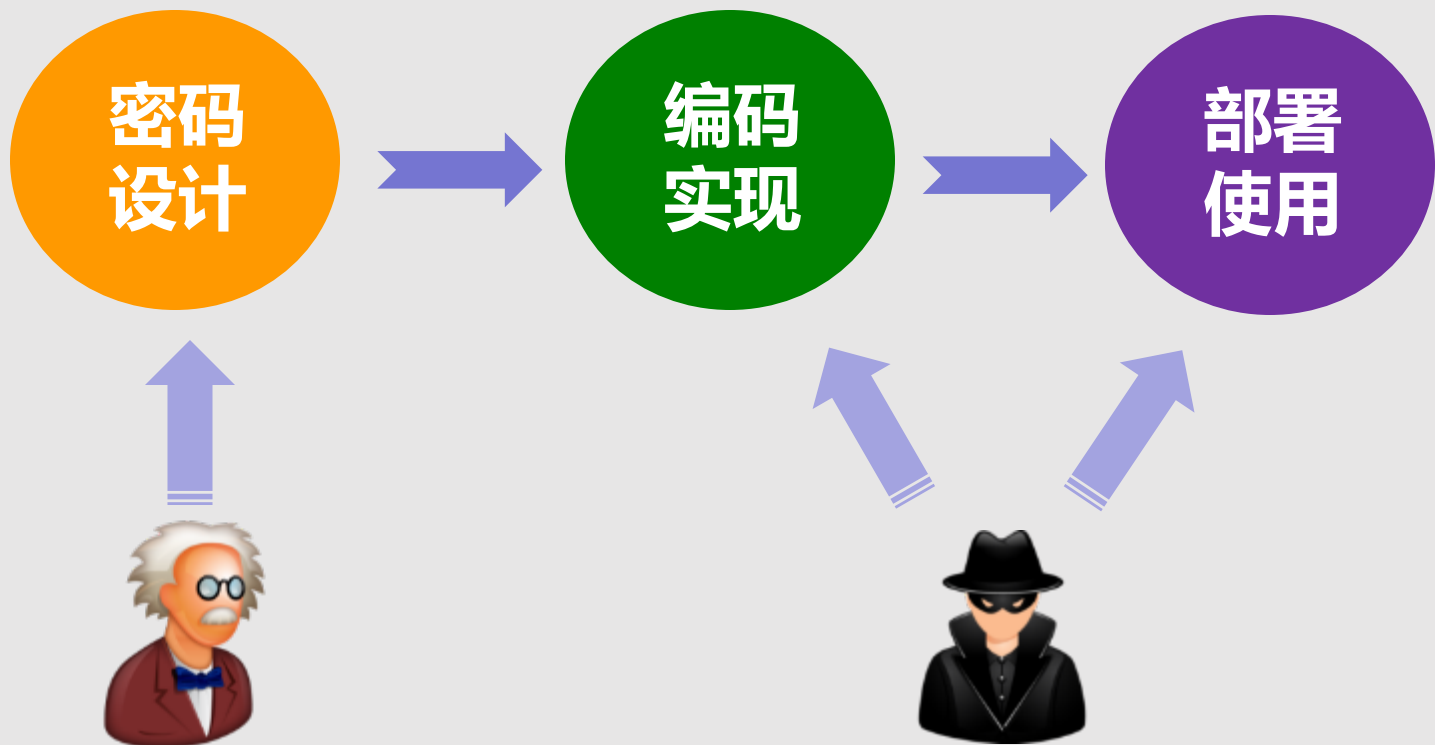
击毙山本五十六

...



1908—2003
卒于日本神户

几点说明(1): 密码设计 vs. 密码实现



设计上安全的密码算法，由于实现或使用不当，可能引入安全漏洞



几点说明(2): 恢复明文 vs. 恢复密钥

破译的主要目的：恢复密钥

因为知道了密钥，便可恢复出该密钥加密的所有明文
(当然有些时候，破译的目的也在于恢复特定的明文)

通过密文推导密钥，至少要和推导明文一样困难



同等对待所有密钥，不要根据自己的偏好选择密钥
(以防攻击者根据你的偏好缩小密钥范围)

密钥应随机选择



几点说明(3): 全部破译 vs. 部分破译

并不一定恢复出整个明文才算成功破译

有时候，恢复出明文的部分信息，甚至几个关键词，也算成功破译。

部分破译又往往成为全部破译的突破口



几点说明(4): 穷举攻击 vs. 其他攻击

穷举攻击(暴力攻击、蛮力攻击)

目的：

穷举搜索密钥

方法：

依次测试密钥空间中的所有密钥

密钥空间要足够大，以抵抗密钥穷举攻击



只要密钥空间足够大，穷举攻击将是十分低效的，甚至是不现实的

但这并不是充分条件，因为穷举不是破译密码的唯一方法，还有效率高于穷举攻击的其他分析方法

各种分析方法的效率谁高谁低呢？常以穷举攻击的效率作为比较的标准



几点说明(5): 保密密钥 vs. 保密算法

根据柯克霍夫斯原则，对密码进行分析的前提是，在不知道密钥的条件下，对公开的密码算法进行分析。

但在政府或军事应用中，也存在保密算法的情况。

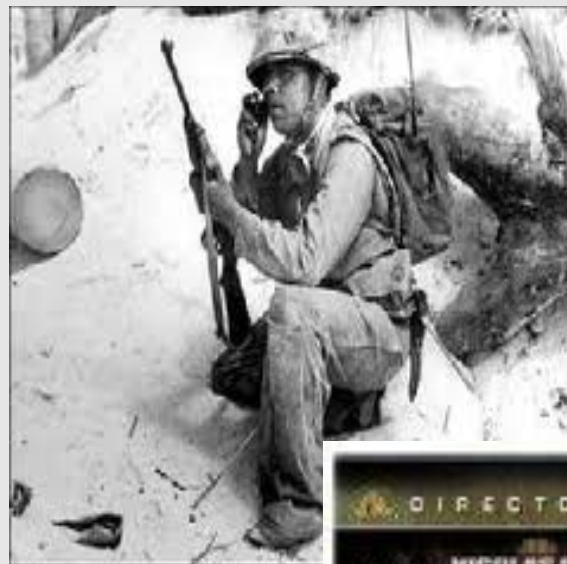
不过前提是，算法必须是安全的。通过保密算法进一步加强安全性。

保密算法的例子 — 纳瓦霍语密码

纳瓦霍语密码的特点：

粗略的讲，安全性在于算法的保密性，密钥固化在算法中

安全原理：日本人对纳瓦霍语一无所知





对密码安全性的一些直观认识

- 密钥空间要足够大
- 密钥应该随机选择
- 通过密文推导密钥，至少要和推导明文一样困难
 - 明文与密文之间的统计关系要尽量小
 - 密钥与密文之间的统计关系要尽量小

.....



相对

抛弃“绝对”的想法，安全都是相对的

概率

抛弃“百分之百”的想法

本章小结

1. 掌握信息安全三要素、密码学主要功能、两种攻击形式的含义
2. 掌握密码学研究的内容、组成部分及各种术语
3. 掌握柯克霍夫斯原则的内容和意义，隐写术、加密术的区别，置换、代换的内容和区别
4. 掌握密码分析的四种方法
5. 了解密码学史上的几个重大事件

练习题

1. 信息安全三要素是 (**机密性、完整性、可用性**)
2. 密码学由(**密码编码学、密码分析学**)两部分组成？
3. 加密的两种基本技术是 (**置换、代换**)
4. 按照攻击者知道信息的多少，密码分析
(**唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击**)
四种类型

5. 加密和解密都是在 (**B**) 控制下进行的

A.口令 B.密钥 C.字符串 D.算法

6. 以下哪种攻击破坏数据的机密性 (**B**)

A. 篡改 B.窃听 C.冒充 D.匿名

7. 以下哪种属于被动攻击 (**B**)

A. 篡改 B.窃听 C.冒充 D.以上答案都不对