密码学简介 2

远古时代

隐写书

小学那种荧光笔 — 藏头诗

★ 小结论
- 保护的信息本身
- 一旦发现隐藏的方法,信息就会暴露

加密术

置换permutation
- ★ 特点:明文中字符与密文中相同,只是出现的位置发生了变化
- ★ 密钥是什么?改变位置的规则,比如说置换表

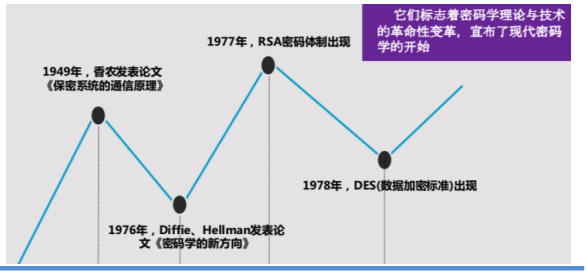
替换(代换)substitution
- ★ 特点:明文中出现过的字符不一定出现在密文中,但是位置保持不变
- ★ 密钥:代换规则

★ 加密与隐写术的区别

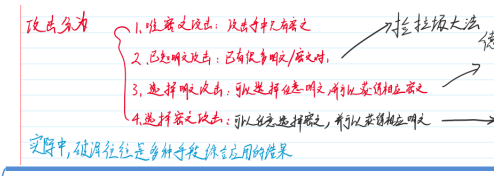
隐写术
保护的是信息本身，传递的仍是原来的信息，只是被藏了起来
一旦发现隐藏的方法，信息就会暴露

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

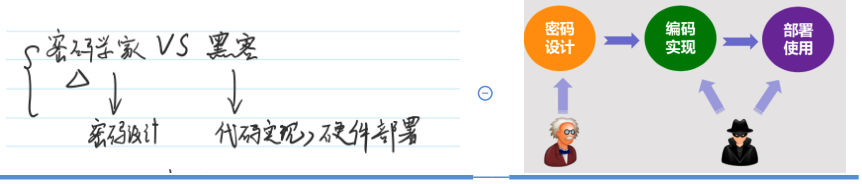
★ 密码学上的主要历史事件



关于密码分析



选择密文攻击最牛逼



破译的目的

恢复密钥
- ★ 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）

有时候，破译一部份也算是一种成功

几种攻击手段

★ 穷举攻击 — 暴力密钥空间所有密钥
- ★ 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

根据基佬霍夫斯原则 — 对密码分析的前提是不知道密钥,废话,知道了密钥还分析啥啊

保密算法的例子 — 纳瓦霍语密码 — 相当于温州话

安全性

★ 两个基本概念,相对性,概念性

课后习题

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