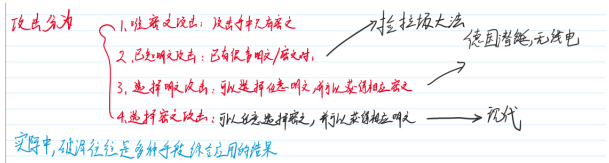
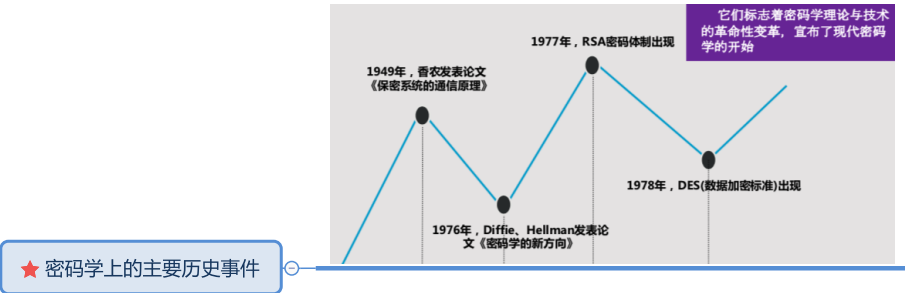
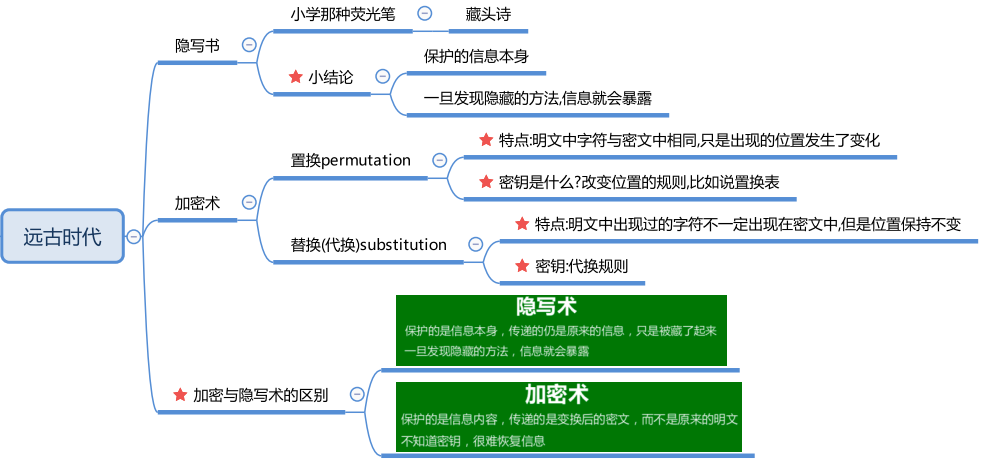
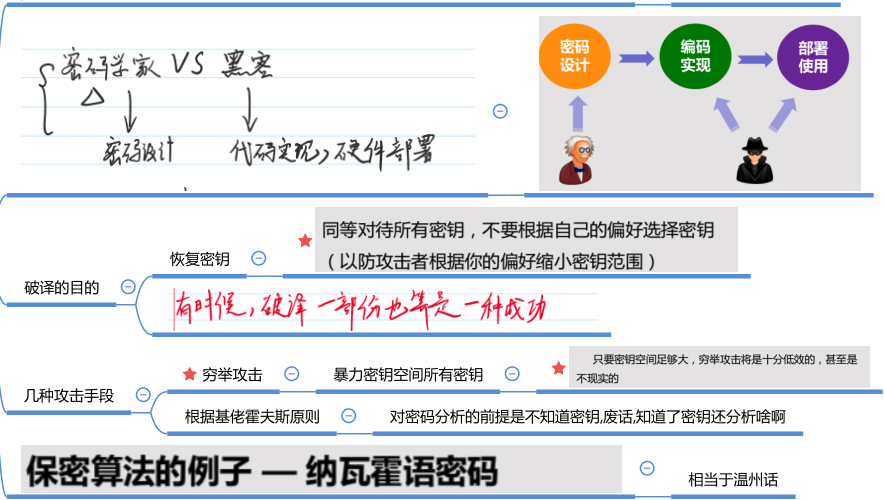


密码学简介 2



关于密码分析



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