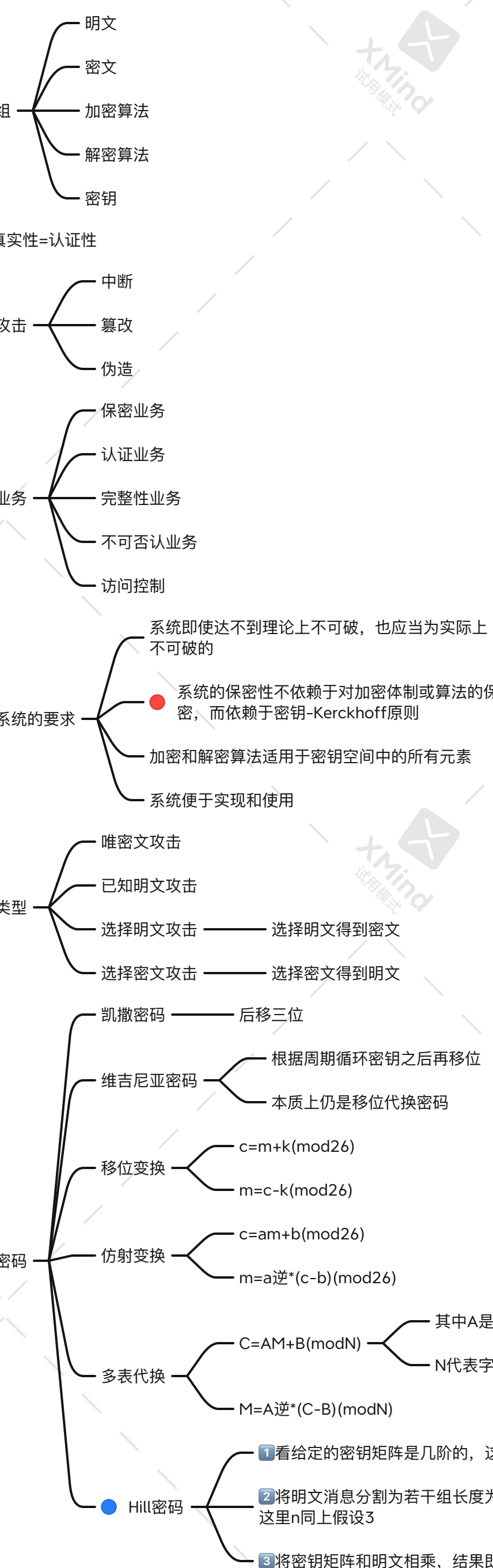


密码学

基础



香农

《保密系统的通信理论》为密码学奠定理论基础

建议密码设计的基本方法

- 混淆
- 扩散
- 迭代

Diffie-Hellman

《密码学的新方向》中提出公开密钥思想

数论

都是一个代数系统

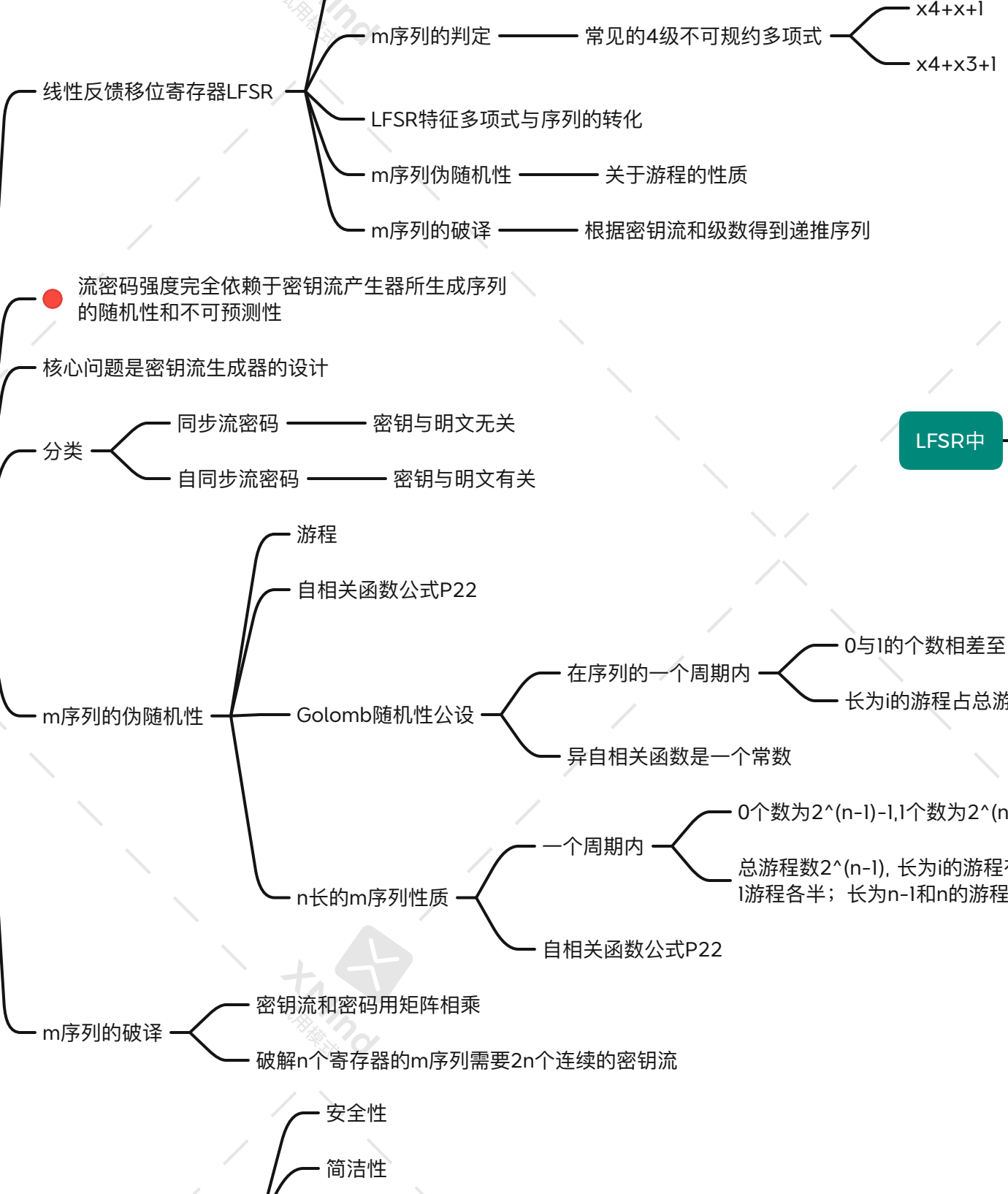
- 封闭性  $a, b \in G, a \cdot b \in G$
- 单位元结合律  $a \cdot b \cdot c = (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- 逆元 若有  $a \cdot l = l \cdot a = a$ , 存在  $a$  的逆元  $a^{-1}$
- 交换群  $a \cdot b = b \cdot a$

古典密码实现的两种基本方法

- 代换
- 置换

现仍是构造现代对称密码的核心方式

流密码



LFSR中

移位寄存器中存储器的个数=移位寄存器的阶数

移位寄存器中存储的数据=移位寄存器的状态

流密码和分组密码

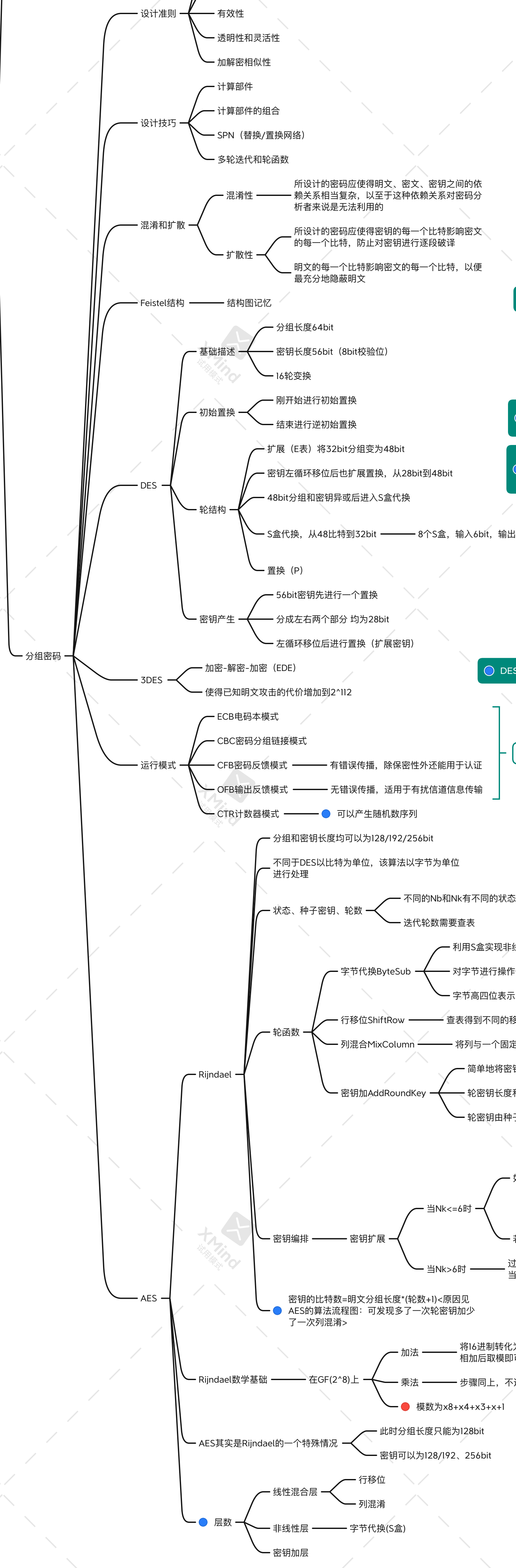
分组密码与流密码的区别就在于有无记忆性

流密码又叫单字母/单码代替

分组密码又叫多字母/多码代替

单码密码体制不仅可用来加密，还可用来认证

对称密码体制



扩散性的理解

粘连性 明文、密文、密钥的每一位都相互依赖

不连续性/雪崩性 当改变明文的任何一个比特时，对应密文改变的比特个数是一个随机变量

不可部分被译性 分组密码不能分解成若干子密码，对分组密码的攻击要彻底破解，要么一无所获

DES加密第一轮的k1, 1616后解密第一轮的k16

如果某一组明文/密文对 (m, c) 使得方程  $m = D(c, z)$  特别容易解出z, m就称为一个弱明文, z就称为一个弱密钥

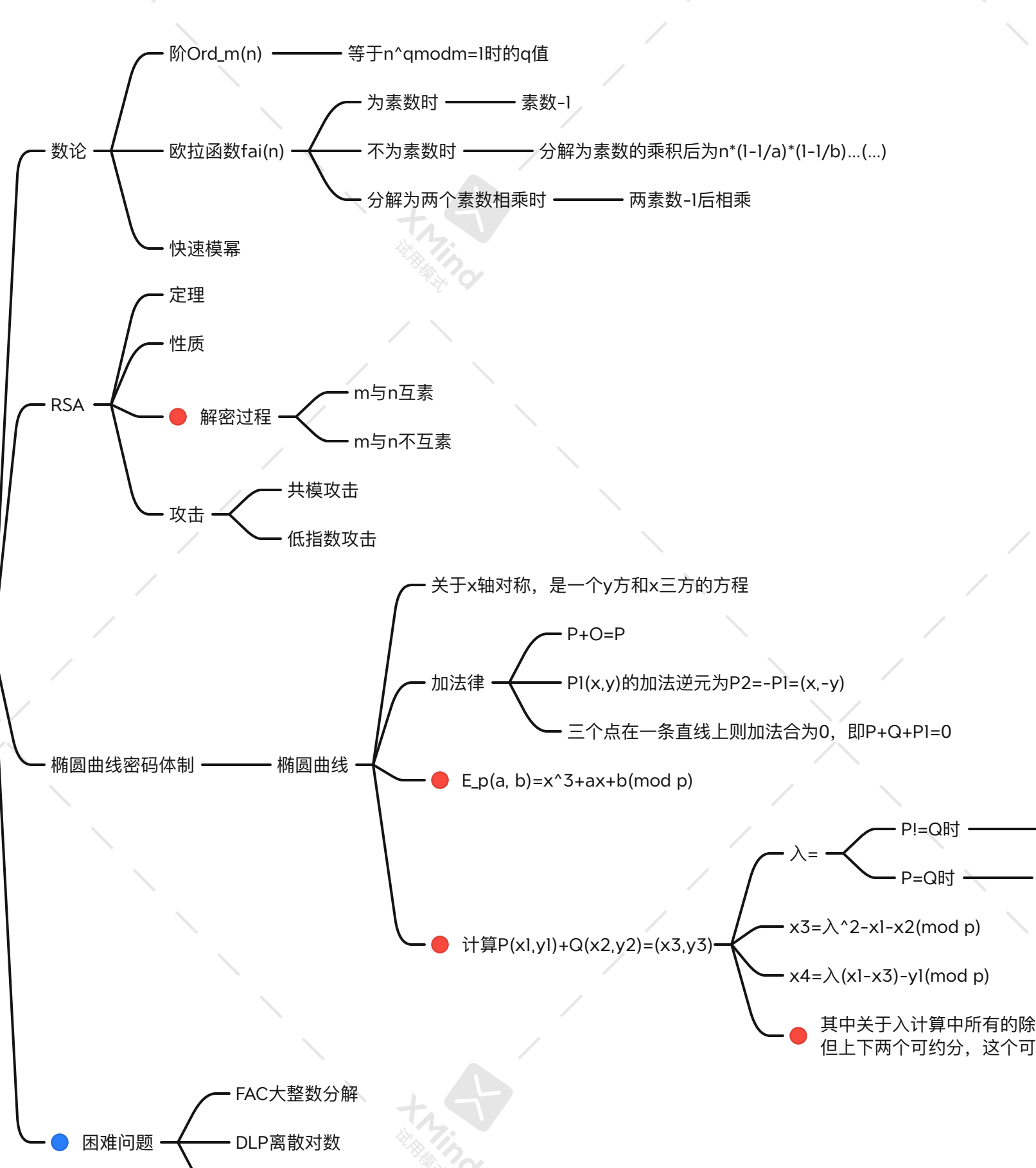
DES普通的CBC模式和CBC-MAC的区别

普通的CBC模式中要对第一个明文使用初始向量IV并后再加密处理

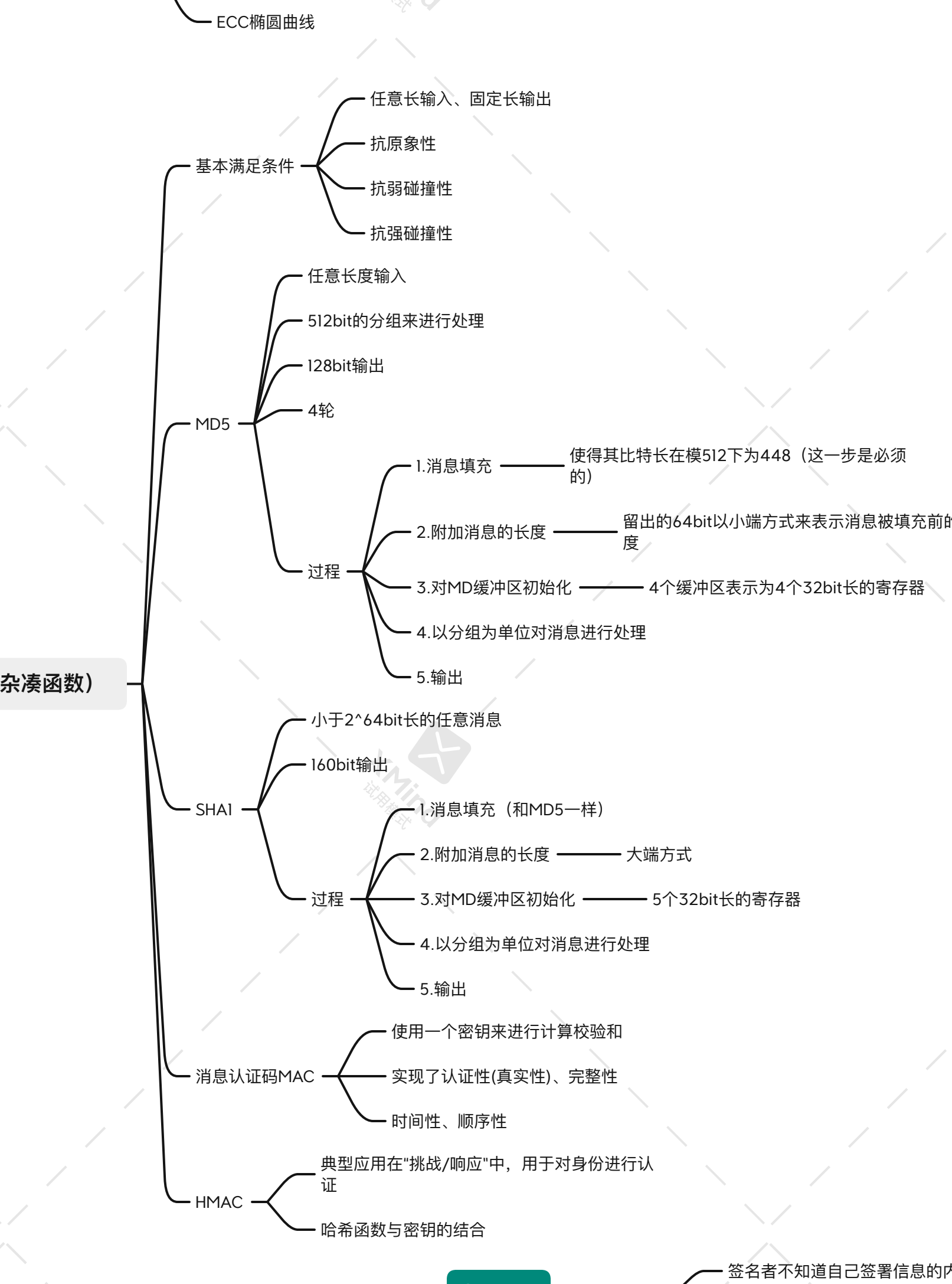
具体结构图和伪代码见P47

CBC和CFB的区别见第三章讲义(word)

公钥密码体制

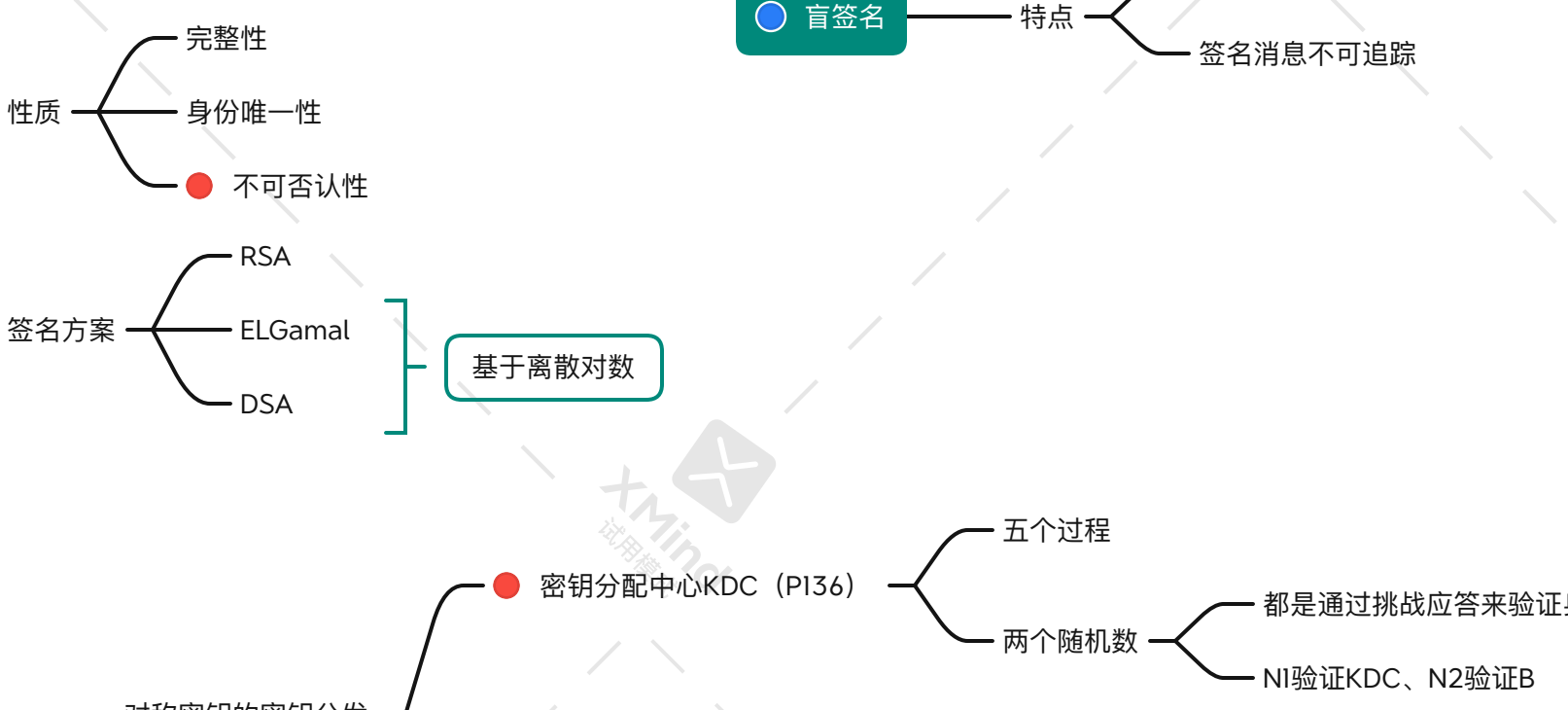


哈希函数 (散列、杂凑函数)

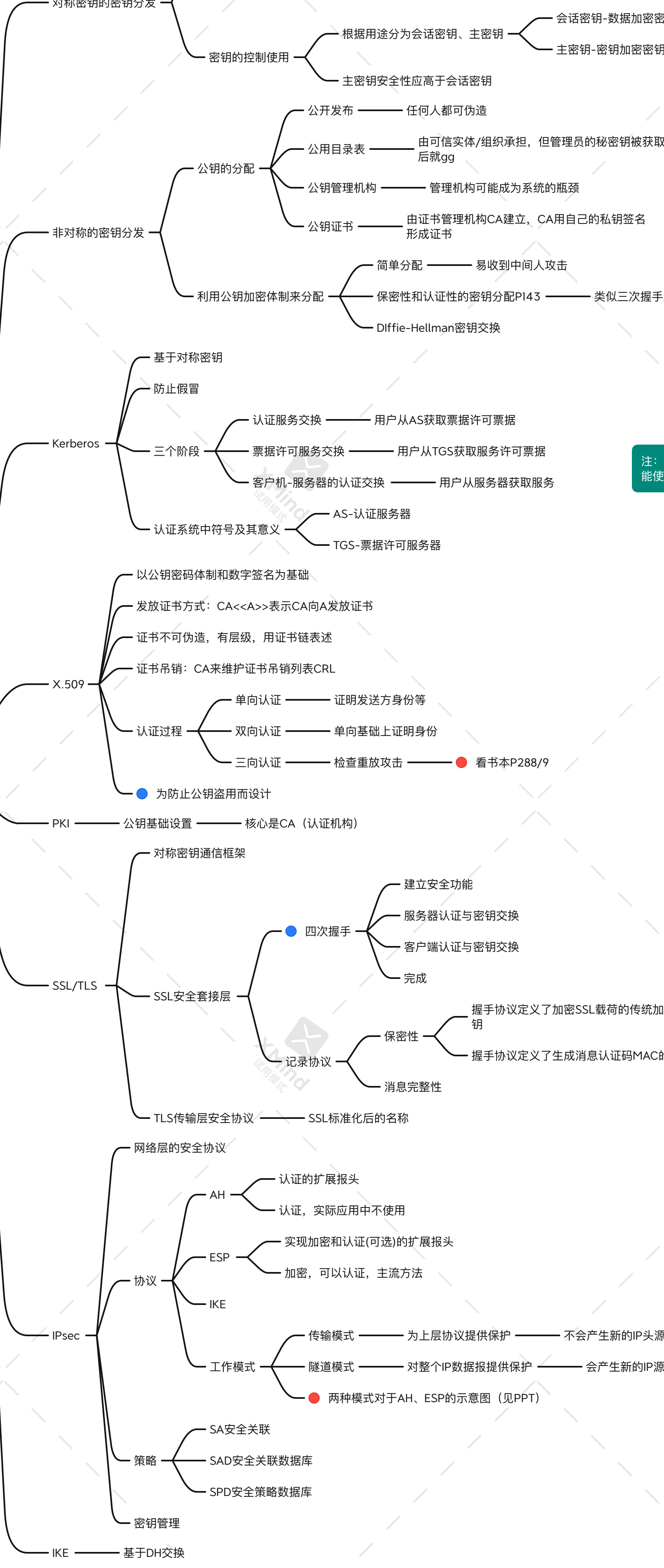


两者安全性的比较P79

数字签名



安全协议



注: 票据许可票据使用且有效期较长; 而认证符只能使用一次且有效期很短