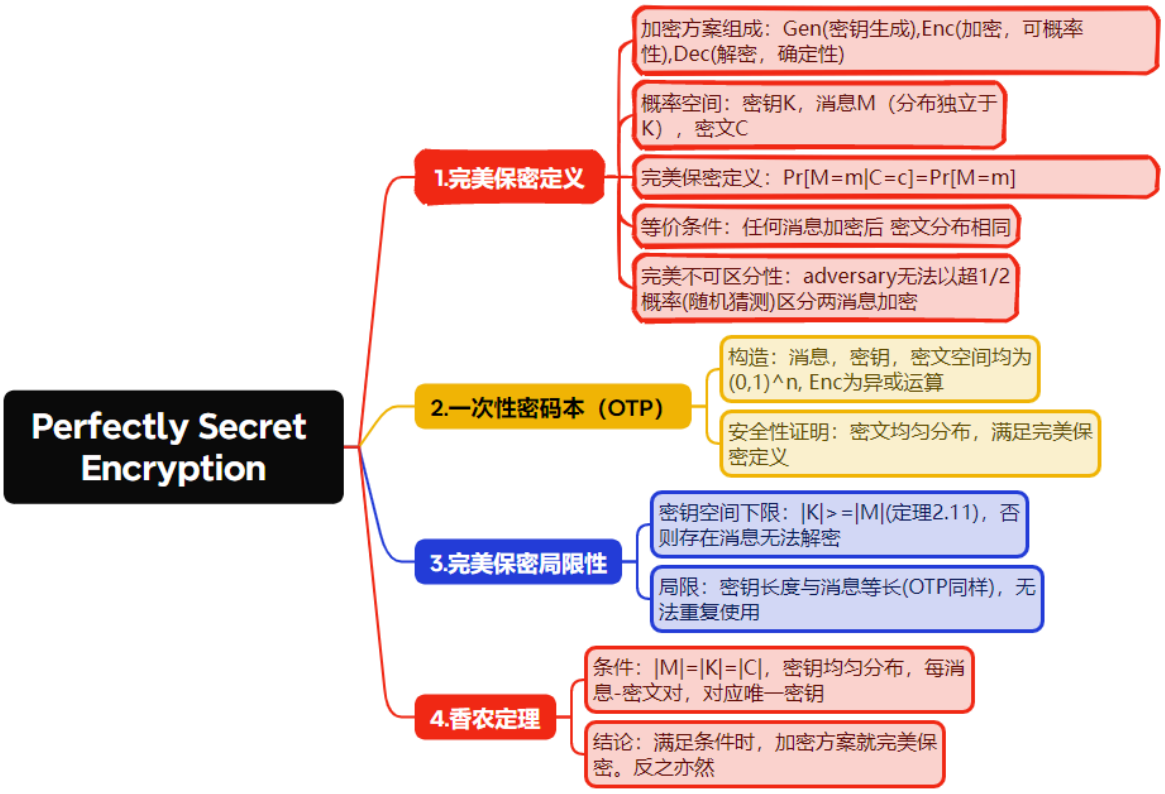
Chapter 2: Perfectly Secret Encryption (完美保密加密)

即便对手具备无限计算能力也可证明安全的加密方案。

思维导图：



关键问题

问题1：完美保密加密的核心定义是什么？

答案：完美保密要求对于任意消息分布、消息m和密文c（$Pr[C=c]>0$），有$Pr[M=m|C=c]=Pr[M=m]$，即观察密文后对消息的概率认知与观察前相同，密文不泄露任何消息信息。其等价于任意两消息加密后的密文分布相同，且无法通过密文区分两消息的加密（完美不可区分性概率为1/2）。

问题2：一次性密码本（OTP）的安全性如何保证？它有哪些实际局限？

答案：OTP通过等长随机密钥与消息异或实现完美保密，因密文均匀分布，满足$Pr[M=m|C=c]=Pr[M=m]$。其局限在于：①密钥长度必须与消息相等，存储和传输长密钥困难；②密钥只能使用一次，重复使用时异或密文会泄露消息差异，甚至可通过频率分析恢复明文（如VENONA项目案例）。

问题3：香农定理如何刻画完美保密的条件？

答案：当消息空间、密钥空间、密文空间大小相等（$|M|=|K|=|C|$）时，方案完美保密的充要条件是：①密钥均匀分布（每个密钥被选中概率为$1/|K|$）；②对任意消息m和密文c，存在唯一密钥k使k加密m得到c。该定理为判断完美保密提供了简洁条件，如OTP满足这些条件故完美保密。