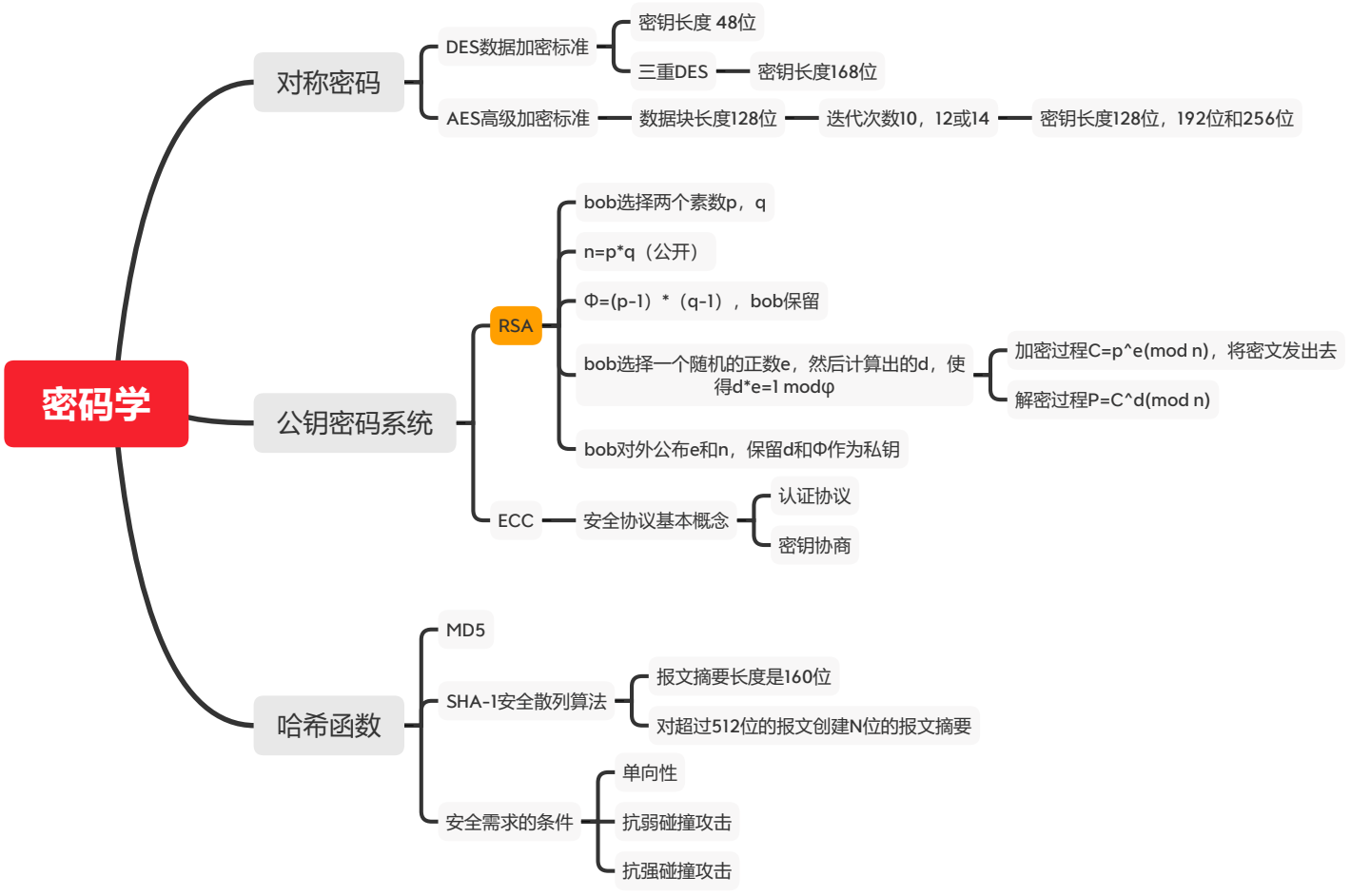
密码学
对称密码
DES数据加密标准
密钥长度 48位
三重DES
密钥长度168位
AES高级加密标准
数据块长度128位
迭代次数10，12或14
密钥长度128位，192位和256位
公钥密码系统
RSA
bob选择两个素数p，q
n=p*q（公开）
Φ=(p-1）*（q-1），bob保留
bob选择一个随机的正数e，然后计算出的d，使得d*e=1 modφ
加密过程C=p^e(mod n)，将密文发出去
解密过程P=C^d(mod n)
bob对外公布e和n，保留d和Φ作为私钥
ECC
安全协议基本概念
认证协议
密钥协商
哈希函数
MD5
SHA-1安全散列算法
报文摘要长度是160位
对超过512位的报文创建N位的报文摘要
安全需求的条件
单向性
抗弱碰撞攻击
抗强碰撞攻击