复习大纲

一. 流密码

- 伪随机发生器（PRG）
- 一次性密码本
- PRG的安全定义
- 语义安全
- 怎么攻击流密码和一次性密码本

二. 分组密码

- 性质，原理
- 怎么攻击
- AES块密码
- 如何使用分组密码：一次/多次密钥

三. MAC和哈希函数

- 什么是MAC
- PRF
- CBC-MAC和NMAC
- 什么是抗碰撞（生日悖论）
- Merkle-Damgard
- HMAC

四. 身份验证加密

- 为什么要加密
- 怎么构成认证加密
- 攻击方式
- 导出密钥
- 多种形式的加密（确定性，可调整...）

五. 密钥交换系统（复习数论）

- 什么是受信任的第三方
- Diffie-Hellman协议
- 公钥加密
- 同余，费马/欧拉定理，二次剩余等数论知识

六. 怎么使用公钥加密

- 怎么构造
- RSA例子
- 攻击RSA
- Diffie-Hellman的公共密钥加密：ElGamal
- 公钥加密的摘要