信息安全数学基础课程探究题目

必做题

需要探究的密码算法(协议)如下:

(1) AES算法

(2) RSA算法

(3) Rabin算法

(4) ElGamal算法(包括椭圆曲线版)

(5) Diffie-Hellman协议

(6) NTRU算法

(7) Merkle-Hellman背包密码

(8) DSA数字签名算法

探究内容包括但不限于(以下内容为必做):

(1) 密码算法(协议)的基本内容

(2) 密码算法(协议)安全性所依赖的数学难题

(3) 密码算法(协议)涉及到的数学原理

(4) 对密码算法(协议)的攻击方法及其涉及的数学原理

选做题

从下列密码学原语中选择一个进行探究:

(1) 基于身份的加密(Identity-Based Encryption, IBE)

(2) 基于属性的加密(Attribute-Based Encryption, ABE)
(3) 零知识证明(Zero-Knowledge Proof)
(4) 全同态加密(Fully Homomorphic Encryption, FHE)
(5) 不经意传输(Oblivious Transfer, OT)
(6) 函数加密(Functional Encryption, FE)
(7) 不可区分混淆(Indistinguishable Obfuscation, IO)
(8) 安全多方计算(Secure Multiparty Computation, SMPC)

注: 以上都是密码学原语, 并不是某个具体算法的名字.

探究内容包括但不限于(以下内容为必做):
(1) 描述该密码学原语的基本思想
(2) 列出该密码学原语的一个具体实例算法, 描述该实例算法的基本内容
(3) 给出该实例算法的安全性所依赖的数学难题
(4) 给出该实例算法中涉及到的数学原理