信息安全数学基础课程探究题目

1 探究内容

1.1 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) ElGamal算[illegible]曲线版);

(4) Diffie-Hellman协议;

(5) NTRU算法.

探究内容包括但不限于(以下三点为必须体现在报告中的内容):

(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)涉及到本课程所学的数学原理.

注: 关于RSA算法, 除了上述三点外, 还需探究对RSA的攻击方法及其涉及的数学知识.

1.2 选做题

从下列密码学原语中选择一个进行探究:

(1) 数字签名(Digital Signature);

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

(1) 基于属性的加密(Attribute-Based Encryption, ABE);

(1) 零知识证明(Zero-Knowledge Proof);
(1) 全同态加密(Fully Homomorphic Encryption, FHE);
(1) 不经意传输(Oblivious Tranfer).

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(以下四点为必须体现在报告中的内容):
(1) 描述该密码学原语的基本思想;
(1) 列出该密码学原语的一个具体实
(1) 给出该实例的安全性所依赖的数
(1) 给出该实例中涉及到的数学原理.

2 报告要求

1. 语言通顺, 结构清晰
2. 字数不限
3. 必须列出所有参考的资料和文献, 且完成选做题时必须参考至少一篇经典英文文献
4. 最好采用规范的论文写作格式(不强制)