博士研究生资格考试试题

网络空间安全
2020 年 7 月

注：1、答卷方式：开卷，笔试；2、答题时间：3 小时；3、满分 100 分。

一、 解释下列术语：(25 分，每题 5 分)

a) Provable security

b) Man in the middle attack

c) Bilinear Map

d) Quadratic residue

e) PKI

二、（15 分）Elgamal 加密算法是不是语义安全的？请简单论述你的理由。

三、（15 分）什么是安全多方计算？给出一个典型的安全多方计算的算法，简述在数据隐私保护中应用。

四、（15 分）Peggy 想向 Victor 证明自己知道一个秘密的 x 满足 $A^x=B \bmod p$ 成立，其中 p 是一个大素数，x 与 p-1 互素，在不泄漏 x 的前提下，请替 Peggy 构造一个零知识证明协议完成该任务。

五、（15 分）简述属性加密（Attribute-based Encryption）方案，说明 CP 与 KP 的区别，并陈述其在云计算安全中的应用。

六、(15 分）在 Shamir 门限方案中，设 $t=3, p=17, n=5$，5 个用户 $x_i = i\left(1 \le i \le 5\right)$ 所对应的的子密钥分别是 8、17、10、0、11，从中任选 3 个，构造插值多项式并求共享密钥 K。