**博士研究生资格考试试题**

网络空间安全

2019年6月

注：1、答卷方式：开卷，笔试；2、答题时间：3小时；3、满分100分；4、试题分必答和选答题。

一、解释下列术语（20分，每题5分）

a) Provable security

可证明安全性：通过有效的变换，将对密码体制的任何有效攻击归约为一类已知NP问题的一个实例。

b) Man in the middle attack

中间人攻击：通信双方都诚实的执行协议，而敌手拦截并修改从一方发送到另一方的消息。

c) Bilinear map

设*G*1，*G*2和*Gt*都是*q*阶循环群，其中*q*为素数。如果映射*e*: *G*1 × *G*2 → *Gt*满足以下性质：

（1）双线性性：对于任意*a*, *b*∈*Z*，*u*∈*G*1，*v*∈*G*2，有*e* (*ua*, *vb*) = *e* (*u*, *v*)*ab*。

（2）非退化性：存在*u*∈*G*1，*v*∈*G*2，使得*e* (*u*, *v*) ≠ 1。

（3）可计算性：对于任意*u*∈*G*1，*v*∈*G*2，存在有效算法可以计算*e* (*u*, *v*)。

则称*e*是一个双线性映射。

d) Quadratic residue

设*n*是正整数且*a*和*n*互素。如果存在*x*使得*x*2 ≡ *a* (mod *n*)，则称*a*是对模*n*的二次剩余。

二、（20分）ElGamal加密算法是不是语义安全的？请简单论述你的理由。

由ElGamal加密算法所依赖的假设决定。

三、（20分）叙述拉格朗日插值算法，并给出一个例子说明如何在秘密分享中使用。

（1）拉格朗日插值法可以给出一个恰好穿过二维平面上若干个不重复点的最低阶多项式。已知有*n* + 1个定点 (*x*0, *y*0), …, (*xn*, *yn*)。若对于任意*i* ≠ *j*，都有*xj* ≠ *xj*都不相等，则拉格朗日插值多项式为

。

其中每个*lj* (*x*)为拉格朗日基本多项式，其表达式为

。

（2）可以通过以下方式构造秘密分享协议。如果打算形成一个（*m*, *n*）门限方案，即重构秘密*M*需要*n*份分享中的*m*份，则首先生成一个*m* - 1次多项式

。

其中，*p*是一个公开的大素数，系数*a*1, …, *am*-1是秘密的随机数。而后，通过计算该多项式在不同点的取值得到*n*份分享。其中，第*i*份分享*ki*为*F*(*xi*)。由于*m* - 1次多项式只有*m*个未知数，故只需任意*m*份分享即可建立方程组并解出秘密*M*。

四、（20分）Peggy想向Victor证明自己知道一个秘密的*x*满足*Ax*= *B* mod *p*成立，其中*p*是一个大素数，*x*与*p* - 1互素。在不泄露*x*的前提下，请替Peggy构造一个零知识证明协议完成该任务。

**见2020第4题**

（1）Peggy生成随机数*s*并计算*t* = *As* (mod *p*)。Peggy将*t*作为承诺发送给Victor。

（2）Victor生成随机数*c*。Victor将*c*作为挑战发送给Peggy。

（3）Peggy计算*r* = *s* + *cx*。Peggy将*r*作为响应发送给Victor。

（4）Victor验证*Ar*是否与*tBc*相等。若相等，则Victor接受证明。

五、（20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。