博士研究生资格考试试题

网络空间安全

2022 年 11 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、（20 分）简述国家密码管理局发布的几种国密算法。

二、（20 分）列举至少四种隐私保护技术。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，简述在隐私保护中的应用。

三、（20 分）什么是零知识证明协议？结合实际场景给出其中的一种应用。

四、（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。

五、(20分）用户A（身份是ID_A）和B（身份是ID_B）按照以下协议建立共享的会话密钥K_s，其中KDC是密钥分配中心，K_A和K_B分别是A、B与KDC共享的主密钥。

(1) A→KDC：$ID_A \| ID_B \| N_1$

(2) KDC→A：$E_{K_A}\left(K_S \| ID_A \| ID_B \| N_1\right) \| E_{K_B}\left(K_S \| ID_A\right)$

(3) A → B：$E_{K_B}\left(K_S \| ID_A\right)$

(4) B → A：$E_{K_S}\left(N_2\right)$

(5) A → B：$E_{K_S}\left(f\left(N_2\right)\right)$

问：

1. N_1在此的作用？
2. 最后两步的作用是什么？
3. 协议中去掉函数 f 行不行？为什么？