第七章

一、填空：

1. 两个用户通信时在建立密钥的过程中需要考虑的核心问题是_____和_____

2. 保证消息实时性常用_____和_____两种方法。

3. 单向认证中只关心保密性的认证方式是_____

4. 一次口令认证协议 S/KEY 中，如果当前系统存储的当前用户口令信息为(ID_u, $hash^c(Pwd)$，c)，其中 Pwd 是用户口令，则用户口令还能使用多少次_____

4. 交互式证明与数学证明的区别是什么_____

5. 交互式证明系统必须满足两个基本要求_____和_____

6. 完成以下协议：

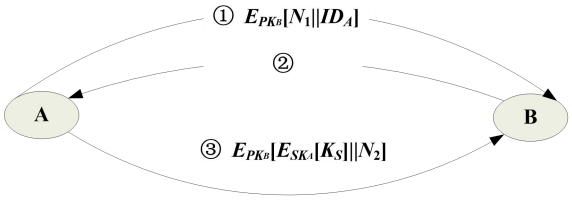
① P 随机选 r ($0<r<n$)，计算 $a \equiv r^2 \bmod n$，将 a 发送给 V。

② V 随机选 $e \in \{0,1\}$，将 e 发送给 P。

③ P 计算 $b \equiv ry^e \bmod n$，即 $e=0$ 时，$b=r$；$e=1$ 时，$b=ry \bmod n$。将 b 发送给 V。

④ 若 $b^2 =$ _____$\bmod n$，V 接受 P 的证明。

7. 具有保密性和认证性的密钥分配如图：试给出消息②的表示_____



具有保密性和认证性的密钥分配

二、选择：每一项有 1 个或多个选项是正确的

1. 在下面的认证类型中，发送方想要同接收方协商一个会话密钥，这属于_____

A. 身份认证　B. 密钥建立认证　C. 数据源认证　D. 消息完整性认证

2. 目前一些公司或机构中，员工上下班签到采用指纹系统进行认证，这属于_____

A. 身份证实　B. 身份识别　C. 零知识认证　D. 消息源认证

3. 下面可用于身份认证的选项是_____

A. 口令　B. 密钥　C. IC 卡　D. 指纹　E. 公钥

4. 下面哪一项技术针对抗等待重放攻击(　　)

A. 要求网络中各方以 KDC 的时钟为基准定期检查并调整自己的时钟

B. 使用一次性随机数的握手协议

C. 基于可信第三方认证

D. 获取旧会话密钥

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 数据源认证就是对发送方的身份进行认证。 ( )

2. 数据完整性认证也包括对数据新鲜性的认证。 ( )

3. 身份证实和身份识别的本质区别在于申请认证者是否首先出示自己的身份 ( )

面向链接的协议可以用时戳法实现新鲜性

4. 可采用询问-应答方式实现无连接应用过程的实时性认证？ （ ）

5. 询问-应答可用于防止重放攻击？ （ ）

6. 在身份的零知识证明协议中，其安全性与协议运行的轮数有关 ( )

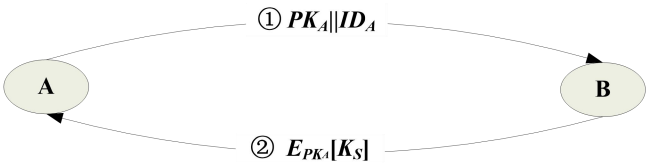
四、简答与计算：

1. Daolev-Yao 威胁模型的两点贡献是什么

2. 消息的新鲜性和主体的活现性的含义是相同的吗？为什么？

3．试给出无中心的单钥密钥分配的过程，并回答为什么不适合在大规模网络中应用

4. 试问对于如下的简单密钥分配协议的中间人攻击如何实现



简单使用公钥加密算法建立会话密钥

5．试述有限域 GF(p)上的 DH 密钥交换协议及其中间人攻击，为防止中间人攻击应采取什么办法，如果在椭圆曲线群上实现 DH 密钥交换中间人攻击又如何

6．实体认证中身份证实和身份识别的区别是什么？

7. NS 协议如下

① A→KDC：$ID_A \| ID_B \| N_1$

② KDC→A：$E_{KA}[K_S \| ID_B \| N_1 \| E_{KB}[K_S \| ID_A]]$

③ A→B：$E_{KB}[K_S \| ID_A]$

④ B→A：$E_{KS}[N_2]$

⑤ A→B：$E_{KS}[f(N_2)]$

请问基于旧会话密钥的重放可在第几步怎么进行?

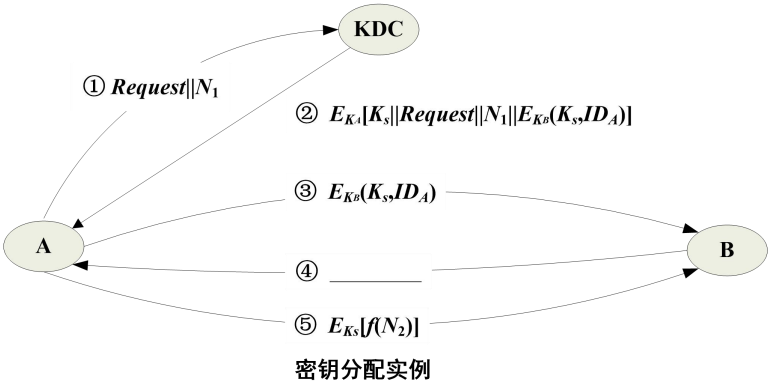
五、证明题：

六、综合题：

1. 如下图所示的密钥分发过程，

(1) 为什么消息②要插入消息①？　　(2) N_1 和 N_2 作用是什么？

(3) 试写出消息④的表达式。　　(4) 第③至⑤步的功能是什么？



密钥分配实例

2. NS 协议如下

① A→KDC：$ID_A \parallel ID_B \parallel N_1$

② KDC→A：$E_{KA}[K_S \parallel ID_B \parallel N_1 \parallel E_{KB}[K_S \parallel ID_A]]$

③ A→B：$E_{KB}[K_S \parallel ID_A]$

④ B→A：$E_{KS}[N_2]$

⑤ A→B：$E_{KS}[f(N_2)]$

请问基于旧会话密钥的重放可在第几步怎么进行?

3. 已知一改进的 NS 协议

① A→B：$ID_A \parallel N_A$

② B→KDC：$ID_B \parallel N_B \parallel E_{KB}[ID_A \parallel N_A \parallel T_B]$

③ KDC→A：$E_{KA}[ID_B \parallel N_A \parallel K_S \parallel T_B] \parallel E_{KB}[ID_A \parallel K_S \parallel T_B] \parallel N_B$

④ A→B：$E_{KB}[ID_A \parallel K_S \parallel T_B] \parallel E_{KS}[N_B]$

TB 是 B 建议的证书(会话密钥)截止时间，用于截止时间前再次发起会话时 K_S 是否可用的判别时间

N_A 和 N_B 的作用是什么？再次发起通信时如何认证？票据为_____