北京邮电大学 2022——2023 学年第一学期

《网络安全技术》期末考试试题

第 1 题（20 分）请使用对称密码基本方法完成如下加密过程

（1）在下表填写你的学号的最后三位数字

（2）每个数字用 6 比特进行编码，采用 DES 算法中的 S-box 方法，利用下表进行代换

	0000	0001	0010	0011	0100
00	0	8	2	6	1
01	7	4	9	5	3

得到的密文 C1（十进制数）为：

（3）对密文 C1 执行置换加密，置换函数是：{1，2，3 }->{3，1，2 }
得到的密文 C2（十进制数）为：

（4）将得到的密文 C2 中的每个数字用 4 比特二进制进行编码，将得到的 12 比特与密钥 K（**K=0101 0110 0110**）进行异或(XOR)运算，将得到的结果用 16 进制表示，则得到最后的密文 C（十六进制数）为：

（5）什么是暴力破解攻击？请分析上述密码算法，如果仅采用暴力破解攻击，则需要尝试的平均次数是多少（破解概率 50%）？

第 2 题（20 分） 请回答下面关于消息认证的问题。

（1）什么是消息认证？

（2）网络安全中要求的安全散列函数需要满足哪些性质？

（3）互联网 IP 和 TCP 协议均使用 checksum 算法生成数据的差错检测码，chechsum 算法属于一种纵向冗余校验散列函数（纵向带进位二进制加法运算），生成 16bit 固定长的散列值。请问 checksum 满足安全散列函数的哪些性质？不满足哪些性质？请分别说明你的理由（要求每个性质逐条说明并给出理由）。

checksum 计算过程举例如图 1 所示：

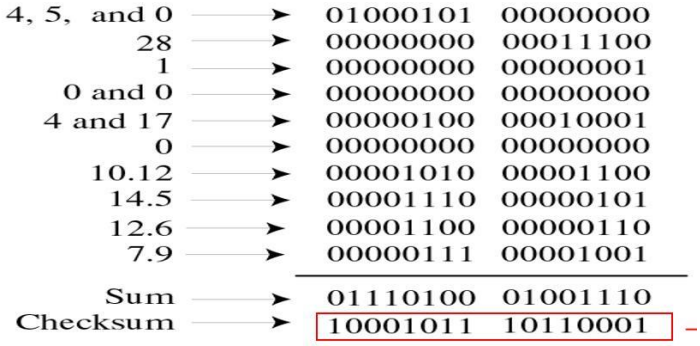

图 1：checksum 计算举例

第 3 题（15 分）请回答以下关于 KDC 的问题。

（1）互联网上密钥分配中心 KDC 的功能是什么？

（2）为什么要使用 KDC?

（2）请画图并说明利用密钥分配中心 KDC 在网络中给通信的双方 A、B 分发对称密钥 K_{AB} 的工作过程。（已知用户 A 与 KDC 之间共享的主密钥是 K_A，用户 B 与 KDC 共享的主密钥是 K_B）。

第 4 题（20 分）IPSec 是互联网的安全传输协议，请回答与 IPSec 相关的问题

（1）IPSec 是哪一层协议？提供的安全服务是什么？

（2）IPSec 由哪些协议组成?请说明各协议的功能。

（3）IPSec 利用滑动窗口实现抗重放攻击（如下图 2 所示），如果重传窗口 W=80，窗口右侧最大序号是 200，如果下一个收到的包序号是：

（i） 150 且认证正确;

（ii） 250 且认证正确;

（iii） 100 且认证正确。

窗口会如何滑动，窗口右侧序号 N 和左侧序号 N-W 分别是多少？

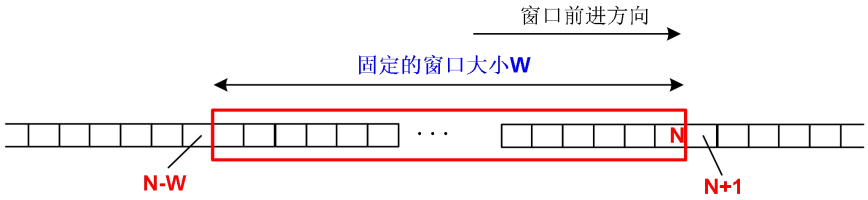

图 2：滑动窗口抗重放攻击

（4）IPSec 使用消息鉴别码 MAC 而不使用数字签名进行 IP 数据包的完整性保护，请尝试分析这样做的合理性。

第 5 题（15 分）安全电子交易协议 SET 协议是针对互联网上使用信用卡进行电子交易而设计的协议，其数据发送和验证的基本过程如图 3 所示。SET 采用双重签名技术（如图 4）。请分析并回答下述问题：

（1） 电子商务交易中哪几方与 SET 协议相关

（2） 图 1 中的数字信封的产生方法和作用是什么？

（3） 图 1 中的数字签名的产生方法和作用是什么？

（4） 为什么要采用双重签名？结合图 2，请说明商家验证签名的过程。

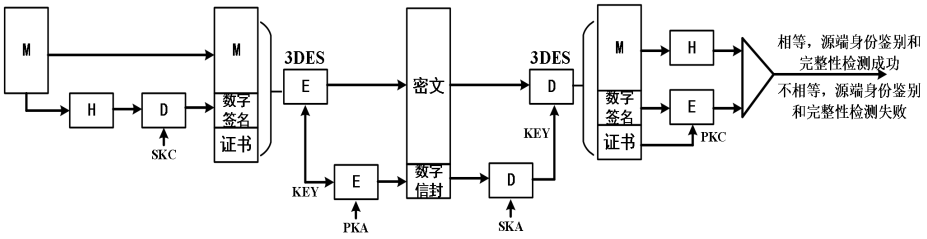

图 3：SET 数据发送与验证

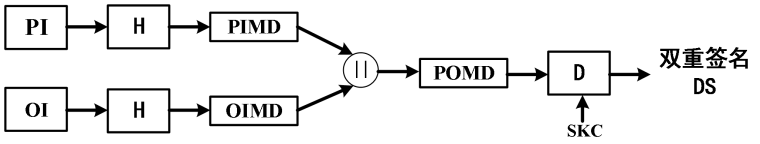

图 4：SET 的双重签名

符号定义：

M=消息，PKC/SKC=持卡人账户 C 的公/私钥, PKA/SKA=商家 A 的公/私钥

KEY=随机生成的对称密钥

PI=支付信息；OI=订货信息

PIMD=支付信息报文摘要;OIMD=订货信息报文摘要

POMD=两组信息摘要的摘要;E/D=RSA 加密/解密算法

第 6 题（10 分）Kerberos 协议是在 Needham-Schroeder 协议基础之上开发的，Needham-Schroeder 协议是一个基于对称密码体制的密钥交换协议，协议的工作原理如图 5 所示，其中，Alice 与 Bob 是需要获得共享密钥的双方，Trent 为可信的第三方。Alice 与 Bob 分别与 Trent 具有共享的秘密密钥 K_{TA} 和 K_{TB}，这两个密钥仅用于密钥分配。协议相关符号定义如表 1 所示：

表 1：对称密钥交换协议中使用的符号

符号	*含义*
A	Alice 的名字
B	Bob 的名字
K_{TA}	Trent 与 Alice 之间的共享密钥
K_{TB}	Trent 与 Bob 之间的共享密钥
K_{AB}	Alice 与 Bob 之间共享的随机会话密钥
R_A, R_B	随机数，分别由 Alice 和 Bob 选择

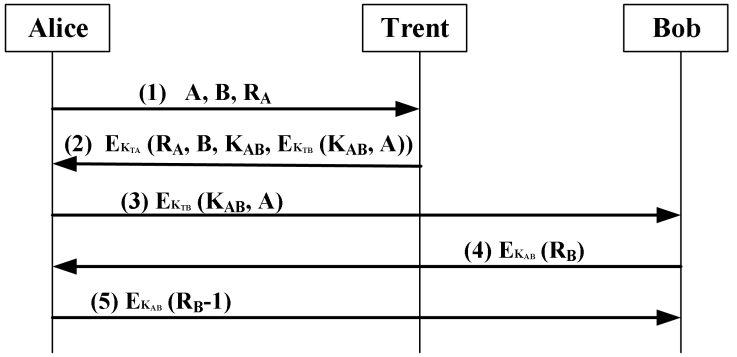

图 5：Needham-Schroeder 协议

请回答如下问题

1. 该协议中谁负责产生 Alice 与 Bob 之间的随机会话密钥 K_{AB}？
2. 该协议是否能够抗中间人攻击？为什么？
3. 该协议是否能够抗重放攻击？为什么？
4. 该协议支持 Alice 与 Bob 之间的双向身份认证吗？请说明你的理由。