装 线 订 线 封 密

专业：_____ 班级：_____ 学号：_____ 班内序号：_____ 姓名：_____

北京邮电大学 2021——2022 学年第 2 学期

《现代密码学》期末考试试题 （A 卷）

一、简答题（每题 5 分，共 40 分）

1) 给出密码学的基本安全属性（目标）？

2) 密钥长度是 128 比特的 AES 算法共包含 10 轮运算，请答出第 5 轮的轮函数包含的主要步骤有哪些？并说明其中的非线性部分是哪一个？

3) 应用在数字签名中的 Hash 函数应满足的安全性质是什么？假设散列函数输出的消息摘要长度为 n 比特，对应这几条性质的分析复杂度分别是多少？

4) 给出 RSA 单向陷门函数安全参数应该满足的条件（至少三条）？

5) 举例说明基于离散对数数字签名的基本流程，包括密钥生成、签名和签名验证。

6) 什么是柯克霍夫原则？简单解释为什么要做这样的假设。

7) 给出密钥管理的三层结构，并叙述三层密钥管理的异同？

8) 与对称密码体制相比，请指出公钥密码体制有哪些优势和不足（总数合计三条）。

二、计算分析题（每题 8 分，共 48 分）

1） 用快速计算方法求 0x84 乘以 0x03 模 $m(x)=x^8+x^4+x^3+x+1$ 的值。

2） 已知流密码的密文串 1010110110 和相应的明文串 0100010001。

（a）计算出此流密码的密钥流。

（b）如果已知密钥流是使用 3 级线性反馈移位寄存器产生的，试破译该密码系统。

3） 已知 RSA 算法中，两个大素数分别为 p=3，q=11，公钥 e=7。

（a）发送者选取明文 m=5，计算密文 c。

（b）阐述接收者接收到 c 以后的解密过程。

4） 简述无密钥的 Diffie-Hellman 密钥交换协议，并分析其可能存在的攻击。

5） 若使用 ElGamal 单向陷门函数加解密信息，已知接收方 B 的公钥(p=43, g=3, y_B=22).

（a）设发送方 A 选择的随机整数 k=5，求明文 M=5 所对应的密文.

（b）若截获到 A 发送的密文是 C=(28,19)，求 M.

（c）若截获到 A 发送的密文是 C=(27,17)，求 M.

6） 在 RSA 算法中，若系统中的两个用户共用一个模数 N，但是拥有不同的 e 和 d，试分析这种系统配置的危害性。

三、 综合题（每题 12 分，共 12 分）

1) Schnorr 签名算法签名过程及验签过程如下：

初始化：选取大素数 p, q，q 是大于等于 160 bits 的整数，p 是大于等于 512 bits 的整数，满足 q|p-1。选取 Z_p^* 中阶是 q 的元素 g。用户随机选取 $1 < x < q$，计算 $y = g^x \bmod p$。则公钥为（y,g,p,q），私钥为 x。

签名算法：待签消息为 m，签名者对 m 做如下运算：

(a) 选择随机数：$1 < k < q$；

(b) 计算 $r = g^k \bmod p$，$s = k + xe \bmod q$，其中 $e = H(r|m)$，H 为安全 Hash 函数；

(c) 签名 $S = Sig_k(m) = (e, s)$。

验签算法：验证者收到消息 m 及签字 S=(*e,s*)后

(a) 计算 $r' = g^s y^{-e} \bmod p$，而后计算 $H(r'|m)$。

(b) 验证 Ver(y,(e,s),M)=true $\Leftrightarrow H(r'|m) = e$。

回答以下问题：

（1）阐述在签名过程中，使用安全 Hash 函数计算 H(r|m)，而不直接使用(r|m)的原因。

（2）证明上述算法的正确性，即为什么按照签名算法、验签算法，接收者能够正确验证签名？写出具体推证过程。

（3）若签名者使用相同的参数 k 签了两份不同的消息 m_1和 m_2，会产生什么后果？