装--------------------------------订--------------------------------线

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

密--------------------------------封--------------------------------线

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？

一、简答题

1. 给出密码学的基本安全属性（目标）？
   答：保密性、完整性、认证性、不可否认性、可用性。
2. 密钥长度是128比特的AES算法共包含10轮运算，请答出第五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？
   答：主要步骤：字节代换、行移位、列混合、轮密钥加。
   非线性部分：字节代换。
3. 应用在数字签名中的哈希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？
   答：安全性质：单向性、抗弱碰撞性、抗强碰撞性。
   分析复杂度：$O(2^n)$，$O(2^n)$，$O(2^{\frac{n}{2}})$.
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）？
   答：
   (1) p和q的长度相差不能太大。
   (2) p和q的差值不能太小
   (3) $gcd(p-1,q-1)$应该尽可能小
   (4) p和q应为强素数，即$p-1$和$q-1$都应有大的素因子。
5. 举例说明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。
   答：以Schnorr 签名算法为例，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160bits的整数，p是大于等于512bits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$Ver(y,(e,s),M)=true \iff H(r'|m)=e$。
6. 什么是柯克霍夫原则？简单解释为什么要做这样的假设。
   答：假设密码分析者已有密码算法及其实现的全部详细资料。作这种假设是为了确保密码的安全性完全依赖于密钥。
7. 给出密钥管理的三层结构，并叙述三层密钥管理的异同？
   答：三层结构：主密钥、密钥加密密钥、会话密钥。
   异同：相同点：目的都是为了保护数据的安全；每一层的密钥都保护下一层数据；各层密钥都用于加密操作，只是加密对象不同。
   不同点：安全级别不同，主密钥安全级别最高，密钥加密密钥次之，会话密钥最次；使用频率不同，主密钥使用频率最低，密钥加密密钥更高，会话密钥使用频率最高；存储方式不同。等等。

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）。
   答：优势：密钥分配简化；支持数字签名、身份认证；密钥管理简便。
   不足：计算开销大；密钥长度较长，传输成本高；存在中间人攻击。

二、计算分析题

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。
   解：

$$
\begin{aligned}
0x84 * 0x03 &= (10000100)_2 \times (00000011)_2 \\
&= (10000100)_2 \times (00000010)_2 \oplus (10000100)_2 \\
&= (00001000)_2 \oplus (00011011)_2 \oplus (10000100)_2 \\
&= (10010111)_2 \\
&= 0x97 \bmod m(x)
\end{aligned}
$$

2. 已知流密码的密文串1010110110和相应的明文串0100010001.
   1. 计算出此流密码的密钥流
      解：此流密码的密钥流为
      $1010110110 \oplus 0100010001 = 1110100111$
   2. 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。
      解：可以得到：

$$
\begin{cases}
k_1 = 1 \\
k_2 = 1 \\
k_3 = 1 \\
k_4 = 0 \\
k_5 = 1 \\
k_6 = 0
\end{cases}
$$

      则可以建立如下方程：

$$
\begin{pmatrix} k_4 \\ k_5 \\ k_6 \end{pmatrix} = \begin{pmatrix} k_1 & k_2 & k_3 \\ k_2 & k_3 & k_4 \\ k_3 & k_4 & k_5 \end{pmatrix} \begin{pmatrix} a_3 \\ a_2 \\ a_1 \end{pmatrix}
$$

      即

$$
\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_3 \\ a_2 \\ a_1 \end{pmatrix}
$$

      解得

$$
\begin{cases}
a_1 = 1 \\
a_2 = 0 \\
a_3 = 1
\end{cases}
$$

      由此可得密钥的递推关系为：

$$
k_{i+3} = a_3 k_i + a_2 k_{i+1} + a_1 k_{i+2} = k_i + k_{i+2}
$$

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

   1. 发送者选取明文m=5，计算密文c。

   解：

$$n=p\cdot q=33$$

$$c\equiv m^e \bmod n\equiv 5^7 \bmod 33=14$$

   即密文c为14.

   2. 阐述接收者接收到c以后的解密过程。

   解：接收者接收到密文c后，用私钥d（其中$d\equiv e^{-1} \bmod n$，是事先保管好的）进行运算：

$$m\equiv c^d \bmod n$$

   m即为解密后得到的明文。

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。

   解：过程如下：

   设p和g公开

   A随机选取一个大数a，计算$g_a\equiv g^a \bmod p$，并将结果g_a传给B；

   B随机选取一个大数b，计算$g_b\equiv g^b \bmod p$，并将结果g_b传给A；

   A计算$k\equiv g_b^a \bmod p$；

   B计算$k\equiv g_a^b \bmod p$；

   因为$k\equiv g_a^b\equiv (g^a)^b\equiv g^{ab}\equiv g_b^a\equiv k \bmod p$，最终通信双方A和B各自计算出共同的会话密钥$k$。

   可能存在的攻击：中间人攻击。攻击者可以截获并替换A和B之间交互的信息，最终可以监听到他们实际通信的数据。

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$(p=43,g=3,y_B=22)$.

   1. 设发送方选择的随机整数k=5，求明文M=5所对应的密文。

      解：

$$c_1\equiv g^k \bmod p\equiv 3^5 \bmod 43=28$$
$$c_2\equiv My_B^k \bmod p\equiv 5\cdot 22^5 \bmod 43=23$$

      因此对应的密文为C(28, 23).

   2. 若接截获到A发送的密文是C=(28, 19)，求M.

      解：由上题可知，当$c_1=28$时，对应的随机整数k=5.

      由$c_2\equiv My_B^k \bmod p$，可以得到：

$$19\equiv M\cdot 22^5 \bmod 43$$

      解得$M=6$.

   3. 若接截获到A发送的密文是C=(27, 17)，求M.

      解：由$c_1=27$得：

$$c_1\equiv g^k \bmod p\equiv 3^k \bmod 43=27$$

可以求得$k=3$.
由$c_2 \equiv My_B^k \bmod p$，可以得到：

$$17 \equiv M \cdot 22^3 \bmod 43$$

解得$M=50$.

6. 在RSA算法中，若系统中的两个用户公用一个模数N，但是拥有不同的e和d，试分析这种系统配置的危害性。
解：设两个用户的公钥分别为e_1和e_2，且二者互素，明文消息是m，密文分别是
$c_1 \equiv m^{e_1} \bmod n$，$c_2 \equiv m^{e_2} \bmod n$.
攻击者截获c_1和c_2后，可如下恢复m：
用扩展欧几里得算法计算出满足$re_1+se_2=1 \bmod n$的两个整数r和s，由此可得：

$$c_1^r c_2^s \equiv (m^{e_1})^r (m^{e_2})^s \equiv m^{re_1+se_2} \equiv m \bmod n$$

从而得到明文m.

三、综合题

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160bits的整数，p是大于等于512bits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$Ver(y,(e,s),M)=true \iff H(r'|m)=e$。

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。
答：如果直接使用$e=(r|m)$，攻击者截取到的签名(e,s)中，e是可以被直接查看和使用的。因为e包含了r和消息m的信息，没有经过任何加密或混淆，攻击者可以利用这些信息尝试构造有效的签名。例如，攻击者可以通过截取到的r和消息m构造出相同的e，然后试图推导出签名者的私钥x。使用安全的哈希函数H计算$H(r|m)$能确保e是难以反向推导的，增加了签名的安全性，防止攻击者进行相关攻击。
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。
答：由于

$$y=g^x \bmod p$$
$$r=g^k \bmod p$$
$$s=k+xe \bmod q$$

可以得到：

$$r' = g^s y^{-e} = g^s g^{-xe} = g^{s-xe} = g^{xe+k-xe} = g^k = r \bmod p$$

从而

$$H(r|m) = H(r'|m) = e$$

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？
答：若使用相同的参数k，则：

$$s_1 = k + xe_1 \bmod p$$
$$s_2 = k + xe_2 \bmod p$$

从而可得

$$s_1 - s_2 = x(e_1 - e_2) \bmod p$$

又由于$(s_1 - s_2)$、$(e1 - e2)$大概率不为零，故可以求得x：

$$x = (s_1 - s_2)(e_1 - e_2)^-1 \bmod p$$

从而导致私钥被泄露，