信息安全导论 期末考试试卷 B 卷

软件工程专业 大学三年级学生 2012-2013 学年第一学期

重庆大学软件学院 考试日期：2013-2-21 周四

开卷考试 考试时间：120 分钟

试题	1	2	3	4		总分
分数						

考试说明：本试卷由 4 个部分组成，共计 100 分。考生需在 120 分钟之内回答完所有考题内容。可以采用英文或中文作答，所有答案必须填写在答题纸上。

第 1 部分：单选题 (10 分，每题 1 分).

1. (__) 是加密算法或散列函数的一个重要特性：当输入发生轻微的变化时（比如仅变换 1 个数位），输入将发生非常显著的变化.
   A. 混淆 B. 扩散 C. 雪崩效应 D. 数字水印
2. (__) 是一种信息安全目标(服务)，它要求消息不能被未经授权的一方修改.
   A. 保密性 B. 完整性 C. 可用性 D. 访问控制
3. 将明文转换为密文的过程称为(__).
   A. 隐写术 B. 置换 C. 替换 D. 加密
4. 下面哪一种是被动攻击? (__).
   A. 流量分析 B. 冒充 C. 拒绝服务 D. 篡改
5. 数据加密标准中 DES 轮密钥的长度是(__).
   A. 56 bit B. 64 bit C. 48 bit D. 128 bit
6. 在高级加密标准 AES 的最后一轮加密过程中没有执行下面的哪一个变换? (__).
   A. Add Round Key B. Mix Columns C. Shift Rows D. S-Box
7. 2-DES 的安全性并没有远远超越 DES 是因为 (__) 攻击对它的可行性.
   A. Replay B. Birthday C. Meet-in-the-Middle D. Man-in-the-Middle
8. 下面哪种对称分组密码的操作模式不能用作流加密? (__)
   A. CBC B. CFB C. OFB D. CTR
9. 下面的哪种应用在保密通信中迫切地需要采用诸如 RC4 算法的流加密技术来满足更快速的加密和解密? (__)
   A. Key Distribution B. E-mail C. Internet Telephony D. Secret File Transmission
10. 假设 Annie (A) 想使用公钥加密算法给 Blanco (B) 发送一份加密的信息，在 Blanco 这一端应该使用哪一个密钥来解密? (__)
    A. A 的公钥 B. A 的私钥 C. B 的私钥 D. B 的公钥

第 2 部分：填空 (30 分，每空 2 分)

1. 数据加密标准 DES 的轮函数中四个变换依次是 (1), (2), (3) and (4). 在 DES 加密标准中加密过程使用了几个 S-box? (5).
2. 在高级数据加密标准 AES 中，每轮的行移位变换中，第二行向左移了多少位置(字节) (6)? 在列混淆的变换中，下面两个变换的结果是多少：{01}⊙{AF} (7), {02}⊙{6E}(8)?下面关于 XOR 的运算结果是多少：[1⊕0⊕1⊕1]=(9)? AES 加密算法中有几个 S-box (10)?
3. 设 $E_K(M)$ 和 $D_K(M)$ 分别表示一个对称加密的加密和解密函数, M 和 C 分别表示明文和密文. 若 $C=K_2 \oplus E_K(M \oplus K_1)$, 则 M = (11).
3. φ(n)表示欧拉函数, gcd(m,n)表示 m 和 n 的最大公约数. 求下面的结果：φ(35) = (12); 423 mod 7 = (13); gcd(325, 42) = (14).
4. Armstrong 和 Bella 采用 Diffie-Hellman 密钥交换算法来协商一个会话密钥，他/她们选择了素数 19 和素数根 3, 并各自选择 6 和 2 作为自己的私钥，那么最终计算出的会话密钥是 (15).

第 3 部分：算法题- RC4 3 bit 算法 (20 分)

RC4 3-bit 是简化的 RC4 算法，密钥长度在 3-24 比特之间选择. 24 bit 的状态向量 S[] 具有 8 个元素 S[0], S[1], … S[7]. 每个长度 3 bits. 向量 T[]与向量 S[]的长度相等. 算法有三个环节: **initialization**, **permutation**, 和 **key stream generation**.

For **initialization**, use the following algorithm to initialize the state vector S and the vector T.

```
/* Initialization */
for i = 0 to 7 do
    S[i] = i;
    T[i] = K[ i mod keylen];
** NOTICE: this algorithm is the same as the RC4 except the loop is from 0 to 7 and not 0 to 255)
```

Use the following algorithm to produce the initial **permutation**:

```
/* Initial Permutation of S */
j = 0;
for i = 0 to 7 do
    j = (j + S[i] + T[i]) mod 8;
    Swap(S[i], S[j]);
```

The following algorithm can be used to produce the **key stream**.

```
/* Stream Generation */
i, j = 0;
while (true)
    i = (i + 1) mod 8;
    j = (j + S[i]) mod 8;
    Swap (S[i], S[j]);
    t = (S[i] + S[j]) mod 8;
    k = S[t];
```

请在答题纸的工作表上面完成 RC4 3bit 算法的一个实例。

第 4 部分 4: 问答题(40 分，每题 10 分)

1. 信息安全的三个要素（也称金三角 CIA）是什么？请简要地解释一下.
2. 主动攻击和被动攻击的区别有哪些?
3. 请写出 RSA 算法的加密和解密的公式，并列出 RSA 算法生成公钥和私钥的步骤?
4. Adams 发送了一个编码（密码） **C=** $AES(Ks, (M \,||\, RSA(KR_A, SHA\text{-}1(\mathbf{M})))) \,||\, RSA(KU_B, Ks)$ 给 Beckham. 这套安全机制里面提供了哪些安全服务? 请绘制一个流程图，告诉 Beckham 怎么样阅读和验证来自 Adams 的消息 **M**.
   备注: KR_A 是 A 的私钥，KU_B 是 B 的公钥; Ks 是 A 和 B 的共享会话密钥. AES、RSA、SHA-1 是密码学的算法(函数).

—The END of Question Paper—