装订线

（ 2019 —— 2020 学年第 1 学期）

课程名称：密码学基础
考试专业、年级：安全 17 级
考核方式：（闭卷）

可使用计算器（否）

题号	一	二	三	四	五	六	七	八	九	总分
得分										
评卷人										

得分：_____ 一、选择题（每题 1 分，共 10 分）

1. 如果A发送加密的信息给B，则B需要知道（ ）才能恢复出明文

A. A的私钥 B. A的公钥 C. B的私钥 D. B的公钥

2. 以下哪一个不属于单表代换密码？（ ）

A. 凯撒密码 B.维吉尼亚密码 C. 仿射密码 D. 移位密码

3. 在ElGamal密码中，如果选择p=11，生成元g＝2，私钥为x=5，则其公钥为（ ）

A、3 B、10 C、5 D、7

4. MD5算法中，若消息的长度为512位，则需要填充（ ）比特。

A、0 B、512 C、605 D、448

5. 在RSA签名算法中，若取两个素数p=7，q=11，则其欧拉函数ϕ(n)的值为( )。

A. 84 B. 72 C. 60 D. 112

6. RSA密码体制基于的数学困难问题是（ ）。

A、离散对数问题 B、背包问题 C、平方剩余问题 D、大整数因数分解问题

填空题、图解及特殊要求外，一般不留答题空间。 2、装订试卷、考生答卷时不得拆开或在框外留有任何标记，否则按零分计

（附卷纸 0 页）

7. 通信中仅仅使用数字签名技术，不能保证的服务是（ ）。

A、保密性服务 B、完整性服务 C、认证服务 D、防否认服务

8. 与公钥密码体制相比，对称密码体制的特点是（ ）

A、密钥分配复杂 B、可以实现数字签名

C、加密和解密速度慢 D、密钥的保存数量少

9. 在公钥数字证书是将用户的身份与其（ ）相联系。

A.私钥 B. CA C. 公钥 D. 序列号

10. AES算法支持三种密钥长度，分别是（ ）比特，（ ）比特和（ ）比特。

A. 64 128 256 B. 128 192 256 C. 128 256 512 D. 56 64 128

得分：____ 二、判断题（每题 1 分，共 10 分，对的写 T, 错的写 F）

1. DES的单轮加密变换由字节代替、行移位、列混合和密钥加4个变换组成。（ ）

2. 根据密钥流的生成是否与明文或密文有关，序列密码可以分为同步序列密码和异步序列密码两种。（ ）

3. 对称密码体制的加密和解密往往计算量比较小，所以，对称密码体制比公钥密码体制要更安全。（ ）

4. 1，3，5，10，18，37，85 不是超递增背包向量。（ ）

5. 公钥密码算法建立的理论基础是陷门单向函数。（ ）

6. 一般来说，主密钥的生命周期很长。（ ）

7.如果发送方用接收方的公钥加密消息，则可以实现消息的保密性。（ ）

8. IDEA 算法的分组长度为 64 位。( )

9. 与公钥密钥加密技术相比，对称加密技术的特点是加解密速度较快。（ ）

10. 如果找到两个消息x和x'，它们具有不同的 Hash 值，则是找到了一对碰撞消息。（ ）

得分：_____ 三、填空题（每空 1 分，共 10 分）

1. AES 的单轮加密变换由_____、_____、_____和密钥加 4 个变换组成。

2. 已知 DES 算法 S 盒如下：

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

如果该 S 盒的输入 101110，则其二进制输出为_____。

3. 背包密码体制所基于的数学困难问题为_____。

4. n 级线性反馈移位寄存器输出的最大周期为 _____。

5. 已知 AES 加密算法中的不可约多项式为 $m(x)=x^8+x^4+x^3+x+1$，请计算 81•08=_____，57 83 4A DB + 0A 0B 00 EF=_____。

6. SHA-1 算法输出的 Hash 值长度为_____比特，MD5 算法输出的 Hash 值长度为_____比特。

得分

得分

A

（附卷纸 0 页）

得分：____ 四、计算题（共 50 分）

得分：____ 1. （10 分）设多表代换密码 $C_i = AM_i (\mathrm{mod}\, 26)$ 中，已知密钥矩阵 $A = \begin{bmatrix} 1 & 3 \\ 3 & 4 \end{bmatrix} \mathrm{mod}\, 26$，密文 C=pbwz，求明文 M=?

得分：_____　2.（10 分）已知某线性反馈移位寄存器的反馈函数对应的联结多项式是 $C(D)=D^4+D^2+D+1$，求：

（1）写出该线性反馈移位寄存器的反馈函数并画出结构图；（4 分）

（2）设初始状态是$(a_4, a_3, a_2, a_1) = (1, 0, 0,)$，求此线性反馈移位寄存器产生的序列及其周期（写出具体过程）（6 分）。