模 拟 考 试 卷

课程名称 密码学 考试学期 得分

适用专业 网络空间安全 考试形式 闭卷 考试时间长度 120 分钟

试题	一	二	三	四	五	六	七	八	九	十	十一	十二	总分
得分													

姓名

学号

一、填空（说明：请把答案填在题目中的横线上。共 30 个空，每空 1 分，共计 30 分）。

1、ISO 7498-2 确定了五大类安全服务，即_____、_____、_____、_____、和_____。

2、古典密码体制对现代密码学的研究和学习具有十分重要的意义，实现古典密码体制的两种基本方法代，即_____和_____仍是构造现代分组密码的核心方式。

3、信息安全中所面临的威胁攻击是多种多样的，一般将这些攻击分为两大类，即_____和_____。

4、EDE（三重 DES）的密钥长度是_____比特；分组长度是_____比特；输出密文长度是_____比特。

5、1976 年，美国两位密码学者_____和_____提出了_____的新思想，它为解决传统密码中的诸多难题提出了一种新思路。

6、用户 Alice 给用户 Bob 发送消息时选择使用公钥加密算法进行加密，则加密时使用的密钥是公开钥还是秘密钥？_____该密钥由谁产生？_____。

7、用户 Alice 的密钥对为（PK_A,SK_A），用户 Bob 的密钥对为（PK_B,SK_B），公钥加解密算法均记为 f，若 Alice 给 Bob 发送一个既加密又认证的消息 m，则相应的密文可表示为_____。

8、椭圆曲线密码算法 ECC 的安全性是基于_____困难问题构建的。

9、SHA-1 算法的分组长度为_____比特；输出长度为____比特；轮数为_____轮；

所以，用穷搜索攻击寻找具有给定消息摘要的消息的复杂度为_____；以大于0.5 的概率用穷搜索攻击找出具有相同消息摘要的两个不同消息的复杂度为_____。

10、n-LFSR（n 级线性反馈移位寄存器）最大周期是_____。

11、在一次性口令认证协议 S/KEY 中，如果系统存储的当前用户 U 的口令信息为 $(ID_u, hash^c(Pwd), c)$，其中，*Pwd* 是 U 的口令，则该用户口令可使用_____次。

12、 AES 的状态在明文输入时第 n 个字节放在状态阵列的位置(i, j)上，则第 13 个字节所对应的状态阵列的位置(i, j)＝_____。

13、DES 的初始置换和扩展置换如下表所示，则长为 64 比特的明文分组中第 6 个比特在置换后的位置是_____; DES 加密过程中某轮的右 32 比特中第 27 个比特在经过扩展置换后的位置是_____。

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

（a）初始置换

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

（b）扩展置换 E

14、已知一超递增背包向量 A=(1, 3, 5, 11, 21, 44, 87, 175, 349, 701)，现在背包容积为 s＝721，该背包的解是_____。

二 判断（说明：正确的在后面的括号内打“√”，错误的在后面的括号内打“×”。共 5 题，每题 1 分，共计 5 分）

1、安全永远是相对的，永远没有一劳永逸的安全防护措施。 (　　)

2、公钥证书是不能在网络上公开的，否则其他人可能假冒我的身份或伪造我的数字签名。 （　　）

3、流密码可以分为同步流密码和异步（自同步）流密码，其中密钥流的产生并不是独立于明文流和密文流的流密码称为同步流密码。（　　）

4、DES 算法是一种多轮迭代密码。 (　　)

5、ELGamal 算法的安全性是基于离散对数问题，它的最大特点就是在加密过程中引入了一个随机数，使得加密结果具有不确定性，并且它的密文长度是明文长度的两倍。(　　)

三、 已知一明文串为 00011001，相应的密文串为 10111110，密钥流序列由 3 级 m 序列生成，试破译之。**（6 分）**

四、 设多表代换密码 $C_i=AM_i+B \pmod{26}$中，A 是 2×2 矩阵，B 是 0 矩阵，又知明文“here”被加密为“szol”，求矩阵 A。**（6 分）**

五、 已知分组密码算法 AES 是建立在有限域 $GF(2^8)$上的，模多项式取为 $m(x)=x^8+x^4+x^3+x+1$，试计算$(x^6+x^2+x+1)\times(x^4+x+1) \bmod m(x)$，若该计算用 x 乘表示时，试给出计算过程。**（6 分）**

六、 设一个线性反馈移位寄存器 LFSR 为$\langle 5,1+D+D^3+D^4+D^5 \rangle$，其中联结多项式 $C(D)$为本原多项式式（即特征多项式为 $P(x)=x^5+x^4+x^3+x+1$）。求该 LFSR 输出序列的周期，并写出该周期序列。**（6 分）**

七、 RSA 算法是一种极为重要的公钥密码算法，在网络安全应用中极为广泛。

（1）试描述 RSA 算法的密钥产生、加密、解密过程**（3 分）**

（2）证明 RSA 算法中解密过程的正确性；**（5 分）**

（3）已知 RSA 的模数 $n=23\times29$，设加密指数 $e=13$，试用扩展欧几里德算法求解私钥 d；**（3 分）**

八、 求 13 的所有本原根**（6 分）**

九、 在 Shamir 秘密分割门限方案中，设 $k=3$，$n=5$，$q=17$，5 个子密钥分别是 8、7、10、0、11，从中任选 3 个，构造插值多项式并求秘密数据 s。**（6 分）**

十、 Diffie-Hellman 密钥交换协议易受到中间人攻击。

（1）详细分析攻击者如何实施攻击；**（4 分）**

（2）说明最后的攻击结果。**（2 分）**

十一、 已知 NS 协议如下

① A→KDC：$ID_A \| ID_B \| N_1$

② KDC→A：$E_{KA}[K_S \| ID_B \| N_1 \| E_{KB}[K_S \| ID_A]]$

③ A→B：$E_{KB}[K_S \| ID_A]$

④ B→A：$E_{KS}[N_2]$

⑤ A→B：$E_{KS}[f(N_2)]$

（1）分析以上协议的安全性，请问基于旧会话密钥的重放可在第几步？**（2 分）**

（2）如何进行? **（3 分）**

十二、 已知一椭圆曲线 $E_7(1,1)=x^3+x+1 \bmod 7$，设该曲线上的两个点 P＝(2，2)，Q＝(0,6)。

（1）试计算 3P，P+Q**（4 分）**

（2）利用该椭圆曲线实现的 ElGamal 密码体制中，若选择的生成元 P=(2,2)，假设接收者 Alice 的秘密钥为 $n_A=5$，求 Alice 的公开钥 P_A。**（3 分）**

说明：设 $P=(x_1, y_1)$，$Q=(x_2, y_2)$，$P \neq -Q$，则 $P+Q=(x_3, y_3)$由以下规则确定：

$$x_3 \equiv (\lambda^2 - x_1 - x_2) \bmod p;$$

$$y_3 \equiv (\lambda(x_1 - x_3) - y_1) \bmod p, \quad \text{其中 } \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & P = Q \end{cases}$$