南 京 航 空 航 天 大 学

二〇二〇 ～ 二〇二一 学年 第 I 学期 **《密码学》考试试题**

考试日期： 2021 年 1 月 日 试卷类型： 试卷代号：

班号			学号			姓名				
题号	一	二	三	四	五	六	七	八	九	十	总分
得分											

一、 单项选择题：在下列各题中，将唯一正确的答案代码填入括号内

(本大题共 10 小题，总计 10 分)

1、在下面的密码体制中，哪一种密码在加密前首先将明文编码成（0，1）字符串（ a ）。

(a) Vernam 体制 (b) Playfair 体制 (c) Hill 体制

2、在一个密码系统模型中，只截取信道上传送信息的攻击方式被称为（ b ）。

(a) 干扰型 (b) 被动攻击 (c) 主动攻击

3、通信系统的设计目的是在信道有干扰的情况下，使接受到的信息无差错或差错尽可能地（ b ）。

(a) 不变 (b) 小 (c) 大

4、跟对称密码体制相比，公钥密码体制最大的特点是（ c ）。

(a) 速度快 (b) 加密强度高 (c) 加密密钥可公开

5、公钥密码体制的理论基础是（ a ）。

(a) 陷门单向函数 (b) 大数的素数分解 (c) 有限域上的离散对数

6、下列对 McEliece 密码体制论述不正确的是：（c）(a) 由于明文空间到密文空间有数据扩展，密文比明文长 2 倍，而不适于数字签字。

(b) 公开密钥量过大，达 2^{19}bits，这是限制此体制实用的主要因素。

(c) 加密速度低，但安全性较高。

7、“一次一密”的随机密钥序列密码体制在理论上是（ a ）破译的。

(a) 不可以 (b) 可以 (c) 很容易

8、产生序列密码中的密钥序列的一种主要工具是（ c ）。

(a) 指令寄存器 (b) 数据寄存器 (c) 移位寄存器

9、Hash 函数不可以用于（ a ）。

(a) 数据加密　　(b)数字签名　　(c) 完整性检测

10、下面对 Feistel 网络的描述不正确的是：（ c ）

(a) 它是一种代换网络。

(b) 其输出的每比特密文都和输入的明文及密钥各比特有关。

(c) 其加密过程的算法复杂度要比其解密过程的复杂度高得多。

二、 填空题：在下列各题中，将正确答案填入划线的空白处
(本大题共 10 小题，总计 10 分)

1、在保密系统中，信源是信息的发送者，离散信源可以产生字符或字符串。

2、在密码学中，没有加密的信息称为明文、加密后的信息称为密文

3、公钥密码体制的优点是 加密密钥可以公开传播，缺点是速度较慢。

4、分组密码的特点是加密密钥和解密密钥相同。

5、AES 加密算法的分组长度通常为128位，密钥长度为 128 位时，其圈变换数目为10次。

6、序列密码的加密的基本原理是：用一个随机序列与明文序列进行叠加来产生密文。

7、密码学上的 Hash 函数是一种将任意长度的消息压缩为某一固定长度的消息摘要的函数。

8、在 EIGamal 公钥密码体制中，密文依赖于明文 m 和秘密选取的随机整数 k，因此明文空间中的一个明文对应密文空间中的许多不同的密文。

9、Rabin 密码体制是利用合数模下求解平方根的困难性构造了一种公钥密码体制。

10、序列密码通常也称为流密码，密钥序列也称为密钥流。

三、设在 EIGamal 公钥密码体制中，设素数 p=71， $\alpha=7$ 是 Z^*_{71} 的生成元， $\beta=3$ 是公开的加密密

钥，①假设随机整数 k=2，试求明文 m=20 所对应的密文 ②假设选取一个不同的随机整数 k，使得明文 m=20 所对应的明文为（59，C_2），求 C_2 **(本题计 10 分)**

解: ① $c1 = \alpha^k \bmod p = 7^2 \bmod 71 = 49$

$c2 = m\beta^k \bmod p = 20 \times 3^2 \bmod 71 = 38$

密文 c= (c1,c2) = (49,38)

② 由 $59 = 7^k \bmod 71$ 得 k=3

$c2 = m\beta^k \bmod p = 20 \times 3^3 \bmod 71 = 43$

四、利用 Fermat 定理计算 $3^{501} \bmod 11$。**(本题计 10 分)**

解：由 Fermat 定理 $3^{11-1} \bmod 11 = 1$

$3^{501-1} \bmod 11 = 3 \times 3^{500} \bmod 11 = 3 \times (3^{10})^{50} \bmod 11 = 3 \times 1^{50} \bmod 11 = 3$

费马定理: $a^p \equiv a \bmod p$

P 是素数，a 和 p 互质

五、设在 EIGamal 签名方案中，p=17，g=2，①若选取 x=8，计算 y ②若选取 k=9，试对消息 m=7 进行签名。 **(本题计 15 分)**

解: ① 由 $y = g^x \bmod p$ （y,g,p 是公钥，x 是密钥）

得 $y = 2^8 \bmod 17 = 1$

② $\gamma = g^k \bmod p = 2^9 \bmod 17 = 2$

$\delta = (m - x\gamma)k^{-1} \bmod(p-1) = (7 - 8 \times 2) \times 9^{-1} \bmod 16 = 15$

可得（2，15）是对消息 m=7 的签名。

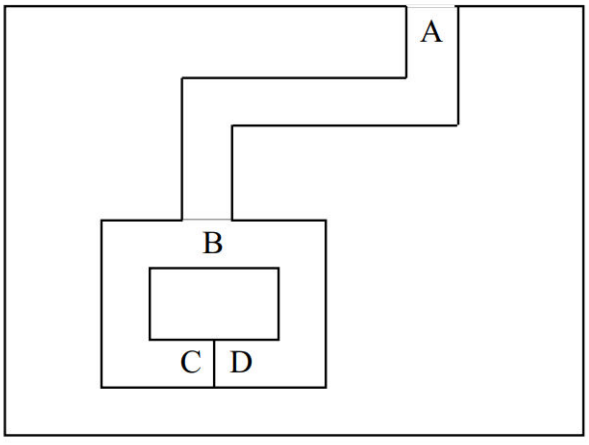
六、设 E 是由 $y^2 \equiv x^3 + x + 8 (\bmod 17)$ 所确定的有限域 Z_{17} 上的椭圆曲线，试确定 E 上四个点。**(本题计 15 分)**

解:

X	$y^2 \equiv x^3 + x + 8 (\mathrm{mod}\ 17)$	是否为模 17 的平方剩余	Y
0	8	不是	
1	10	不是	
2	1	是	1，16
3	4	是	2，15
4	8	不是	
5	2	不是	
6	9	是	3，14
7	1	是	1，16
8	1	是	1，16
9	15	不是	
10	15	不是	

点有（2，1）（2，16）（3，2）（3，15）（6，3）（6，14）
（7，1）（7，16）（8，1）（8，16）……

七、下图所示，在洞穴深处的位置 C 和位置 D 之间有一道门，只有知道秘密咒语的人才能打开位置 C 和位置 D 之间的门，假设 P 知道打开门的咒语，P 想向 V 证明自己知道咒语，但又不想向 V 泄露咒语，请写出 P 向 V 证明自己知道咒语的协议。**(本题总计 15 分)**



零知识洞穴示意图

解：(1) V 停留在位置 A ；

(2) P 从位置 A 走到位置 B，然后随机选择从左通道走到位置 C 或从右通道走到位 D ；

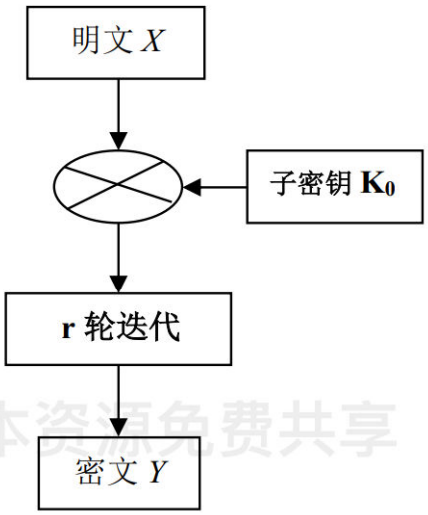
(3) P 消失后，V 走到位置 B ；

(4) V 命令 P 从位置 C 经左通道或从位置 D 经右通道返回位置 B ；

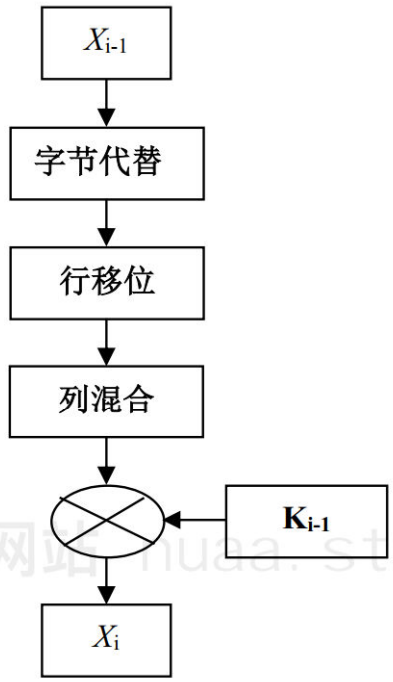
(5) P 服从 V 的命令，必要时 P 可以利用咒语打开位置 C 和位置 D 之间的门 ；

(6) P 和 V 重复执行第(1)步至第(5)步 n 次 。

八、下图是 AES 算法结构示意图，请在下图空白框中，写出相应文字说明。**(本题总计 15 分)**



AES 算法框图



一轮 AES 结构图

AES 加密算法的分组长度通常为 128 位，当密钥长度为 128 位时，其轮变换数目为 10 次。

把一个信息分组 State 分成四行 *x* 列的矩阵形式，一轮 AES 算法包含 4 种变换：

1. 字节代换 SubBytes(State)。使用一个 S 盒 π_S 对 State 进行非线性变换，其中 π_S 是有限域 $\{0,1\}^8$ 的一个置换。SubWord(A0, A1, A2, A3) = (B0, B1, B2, B3)，其中 Bi = SubBytes(Ai)。

2. 行移位变换 ShiftRow(State)。分组长度为 128 或 192 b 时，State 下三行分别循环左移 1、2、3 字节。

3. 列混合变换 MixColumn(State) = *CState 是有限域 $GF(2^8)^4$ 上的一个线性变换。**

4. 轮密钥加法变换 AddRoundKey(State，RoundKey)。将由函数 KeyExpansion(key)生成的轮密钥 RoundKey 中的一个字与 State 的每一个列向量进行异或运算 。