# 考 试 试 卷 册

（2007-2008 学年第 2 学期）

考试科目 密码学导论

出卷教师 李卫海

使用班级 PB0621801

考试日期 2008 年 7 月 4 日

中国科学技术大学教务处

装订线 答题时不要超过此线

# 中 国 科 学 技 术 大 学

## 2007--2008 学年第 2 学期考试试卷

考试科目: 密码学导论　　得分:_____

学生所在系:_____ 姓名:_____ 学号:_____

## 一、多项选择题（16 分）

1、 下列哪个是针对数据完整性的攻击？（ AD ）

A．改变数据包的顺序　　B．线路噪声造成误码
C．窃取数据包　　D．篡改数据包内容

2、 单表代换密码的可用密钥空间为（ D ）

A．26　　B．26!　　C．26!-1　　D．小于(26!-1)

3、 通过压缩清除消息中的冗余，将使得敌手（ BC ）

A．更容易破译密文　　B．更容易伪造消息
C．更难于破译密文　　D．更难于伪造消息

4、 AES 允许的消息分组长度为（ A ）

A．128　　B．192　　C．256　　D．以上都可以

5、 消息认证可以抵抗下列哪些攻击？（ ABC ）

A．内容篡改　　B．数据包顺序篡改　　C．伪造消息　　D．计时攻击

6、 下列哪些算法可以用于制作消息摘要？（ABCD）

A．DES　　B．SHA　　C．MD5　　D．Blowfish

7、 “黑手党骗局”是针对身份认证的（ B ）

A．重放攻击　　B．交织攻击　　C．反射攻击　　D．强迫延时攻击

8、 流量分析攻击可以获得哪些信息？（ BCD）

A．加密算法　　B．消息长度　　C．通信频度　　D．通信人的关系

## 二、判断题（12 分）

1、 越复杂的密码编码技术，其安全性就越强。（ × ）

2、 DES 密码中的轮函数即使是不可逆的，也不影响解密。（ √ ）

3、 密钥扩展可以增加密码系统的复杂性，对抗穷举攻击更有效。（ × ）

4、 通信双方可以使用旧密钥协商更长的新密钥，来提高安全性。（ × ）

5、 消息认证码可以替代数字签名防止第三方假冒。（ √ ）

6、 与链路加密相比，端到端加密要生成和分配的密钥比较少（ √ ）

## 三、计算题（30 分）

1. 用欧几里得算法求解 gcd(2345,6789)。（6 分）

解：gcd(6789,2345)=gcd(2345,2099)=gcd(2099,246)=gcd(246,131)
=gcd(131,115)=gcd(115,16)=gcd(16,3)=gcd(3,1)=1

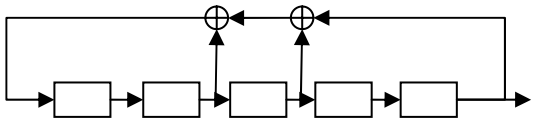
2. 用扩展欧几里得算法求解$(111)_2$在 GF($2^3$)中的逆元，模$(1011)_2$。（6 分）

解：逆元为 100

| Q | A2 | A3 | B2 | B3 |
|---|---|---|---|---|
| | 0 | 1011 | 1 | 111 |
| 10 | 1 | 111 | 10 | 101 |
| 1 | 10 | 101 | 11 | 10 |
| 10 | 11 | 10 | 100 | 1 |

3. 画出 LFSR<5,1+$D^2$+$D^3$+$D^5$>的结构，当初始状态为 0,0,0,0,1 时，写出其输出的前 15 个比特。其周期是多少？（6 分）

解：



00001->10000->01000->10100->11010->
11101->11110->01111->10111->01011->
00101->00010->00001

，

前 15 个比特为 10000,10111,10100，周期 12。

4. 分别利用欧拉定理、快速指数算法计算 $5^{73}$ mod 216。（6 分）

解：(1)Φ(216)=$2^2$*1*$3^2$*2=72，gcd(5,216)=1， $5^{73}$ mod 216=$5^{72+1}$ mod 216=5

(2)73=64+8+1=1001001，

$5^{73}$ mod 216=(((((5$^2$)$^2$)$^2$*5)$^2$)$^2$)$^2$*5 mod 216=(((97*5)$^2$)$^2$)$^2$*5 mod 216=5

5. 求解方程 7x mod 12 = 1, 0≤x≤11。（6 分）

解：$d_1$=3, $d_2$=4

7x mod 3=1 => $x_1$=1, 7x mod 4=1 => $x_2$=3

$y_1$=$4^{-1}$ mod 3=1, $y_2$=3 mod 4=3

所以，x=4*1*1+3*3*3 mod 12=7

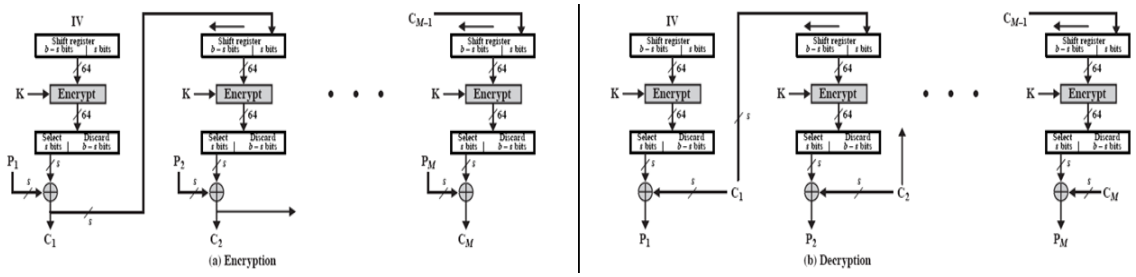
（或用求逆元等方法求解）

## 三、综合题（*42 分*）

1、为了解决校园自行车被盗问题，中国科学技术大学保卫处决定在每个停车点安放监控设备，毕竟一次性设备投入的预算比长期雇佣保安人员的费用更低。为了保护学生隐私，这些监控视频数据将在加密后再通过校园网络传送至监控中心，以防被人搭线窃听。请帮助他们完成这个系统的设计。*(24 分)*

i. 假定加密算法将采用 AES 标准、CFB 工作模式，请画出 CFB 工作模式的加密、解密框图。*(4 分)*

答：




ii. 若采用 CFB-8 模式，请分析当某个密文分组 $C_i$ 传输出错时，这个错误将影响哪些分组明文的正确解密？共计影响多少比特明文的正确解密？ *(4 分)*

答：将影响 $P_i, P_{i+1}, P_{i+2}, P_{i+3}, \ldots, P_{i+16}$ 分组的解密；共计影响 17*8=136 比特明文

iii. 若采用 CFB-128 模式，重新回答问题 b。从正确率考虑，哪个模式更有利？ *(4 分)*

答：将影响 $P_i, P_{i+1}$ 分组；共计影响 2*128=256 比特。

显然，CFB-8 模式对明文的影响更小。

为了定期给各监控点设备更换会话密钥，将利用 RSA 公钥密码给各监控点分配密钥。具体方案为：各监控点保存各自的私钥，将公钥交给监控中心管理；同时保存监控中心的公钥，以便验证监控中心的签名。

iv. 假设某监控点 A 的公钥为(35,7)，监控中心的公钥为(21,5)，求他们各自的私钥是多少？ *(4 分)*

答：$\Phi(35)=24$，A 的私钥是 $7^{-1} \bmod 24=7$；

$\Phi(21)=12$，监控中心的私钥是 $5^{-1} \bmod 12=5$。

v. 更换密钥的方式是：监控中心产生新密钥，对新密钥先加密、签名后，再传送给各监控点。请给出，为给监控点分配新密钥 K=11，监控中心所需进行的计算。*(4 分)*

答：$(11^5 \bmod 21)^7 \bmod 35=2^7 \bmod 35=23$

vi. 请给出，监控点 A 为获得更新的密钥所需进行的计算。*(4 分)*

答：$(23^7 \bmod 35)^5 \bmod 21=2^5 \bmod 21=11$

2、为了严格考试纪律，防止考卷泄露，中国科学技术大学教务处决定于 2008 年 7 月 4 日开始实行试卷锁存制度。规定：

i. 每门课程试卷由一个密码锁锁存；
ii. 开锁密钥分为若干片，其中一部分交给教务处各巡考老师，另一部分交给各监考老师；
iii. 至少两名巡考老师和至少两名监考老师正确输入各自密钥片后，方能开锁；
iv. 密钥分片及重建采用拉格朗日插值多项式方案，其重建公式为

$$h(x)=\sum_{i=1}^{t} h(x_i)\prod_{j=1,j\neq i}^{t}\frac{(x-x_j)}{(x_i-x_j)}$$

请问：*（18 分）*

a) 简述实现上述功能的密钥分片方案，并给出最终多项式的阶数？*（6 分）*
答：使用的是 2 阶多项式。该多项式是两个一阶多项式的乘积 $h(x)=h_1(x)*h_2(x)$。（也可以用加法等其它方法合成两个多项式，后面的答案也相应地不同）其中 $h_1(x)$用于给巡考老师分配密钥片，$h_2(x)$用于给监考老师分配密钥片。

b) 如果教务处对所有的密码锁使用了相同的开锁密钥，则会存在一些漏洞。有一个很“聪明”的学生，为了偷看课程 S 的试卷，假冒监考老师参与了课程 A 的监考工作，意图窃取开锁密钥。他观察到，计算以 23 为模，两位巡考老师输入的是 $h_1(2)=7$，$h_1(4)=6$，两位监考老师输入的是 $h_2(1)=22$，$h_2(4)=15$。请恢复密钥分片使用的多项式，并给出开锁密码。*（10 分）*
答：

$$h_1(x)=h_1(2)\frac{x-4}{2-4}+h_1(4)\frac{x-2}{4-2}=11x+8\pmod{23}$$

$$h_2(x)=h_2(1)\frac{x-4}{1-4}+h_2(4)\frac{x-1}{4-1}=13x+9\pmod{23}$$

$$h(x)=h_1(x)\times h_2(x)=x^2+20x+3\pmod{23}$$

开锁密码为 3

c) 当真正的老师输入了密钥片后（虽然此时开锁密钥已可以恢复），也会要求他输入的密钥片。当然，这时他已经恢复了密钥分片的多项式，因此可以输入正确的密钥片，而不泄露假冒的身份。请帮助他计算 $h_2(6)$的值。*（2 分）*
答：
$h_2(6)=18$

# 考 试 试 卷 册

（2008-2009 学年第 2 学期）

考试科目 密码学导论

出卷教师 李卫海

使用班级 PB0721801

考试日期 2009 年 5 月 26 日

中国科学技术大学教务处

装订线 答题时不要超过此线

# 中 国 科 学 技 术 大 学
# 2008--2009 学年第 2 学期考试试卷标准答案

考试科目: 密码学导论　　得分:_____

学生所在系:_____ 姓名:_____ 学号:_____

## 一、多项选择题（32 分，每个选项 1 分）

1、 数据安全包括:（ ABC ）

A．秘密性　　B．真实性　　C．完整性　　D．不可否认性

2、 下列哪些是公开密钥密码体制？（ AC ）

A．RSA　　B．ENIGMA　　C．ElGamal　　D．Blowfish

3、 下列哪些函数可以用来构造 Feistel 分组密码模型中的轮函数（仅考虑密文可以正确解密）？（ ABCD ）

A．线性函数　　B．非线性函数　　C．单向函数　　D．多对一映射

4、 双重 DES 易遭受下列哪些攻击？（ B ）

A．中间人攻击　　B．中间相遇攻击　　C．密钥全空间穷举攻击　　D．计时攻击

5、 适用于大数据量高误码率环境下的分组密码链接方式有（ CD ）

A．EBC　　B．CFB　　C．OFB　　D．CTR

6、 下列哪些是散列算法？（ BCD ）

A．Rijndael　　B．RIPEMD　　C．MD5　　D．SHA-512

7、 数字签名可以抵抗下列哪些攻击？（ BC ）

A．流量分析　　B．消息伪造　　C．信源抵赖　　D．信宿抵赖

8、 量子密钥分配技术的优点有（ AC ）

A．可获得真随机数密钥　　B．不可被窃听

C．可以发现窃听行为　　D．抗干扰性强

## 二、填空题（32 分，每空 2 分）

1、 三个圆柱体的转轮密码机最多可以提供 $26^3=17576$ 个置换表。

2、 从概率模型来讲，当已知加密算法时，密码分析员主要是利用 消息 、 密文 和 密钥 的先验概率，计算 消息 和 密钥 的后验概率。

3、 在采用 AES 密码算法的 CFB-8 链接模式中，若第 i 个密文分组在传输中出错，则该错误将影响 17 个明文分组的正确解密。

4、 计算 GCD(12345,54321)= 3

5、 计算 $14^{2162} \bmod 2025 =$ 196

6、 试列出四项随机序列统计测试方法：频率测试、序列测试、扑克测试、游程测试。（还有自相关测试、Maurer 测试等）

7、 RSA 密码算法中，若选取 p=13, q=7，公钥选取为 5，则私钥为 29 ,对消息 11 的加密密文为 72 ，对消息 11 的签名结果为 72 。

## 三、计算题*（30 分）*

1. 考虑一个包含 5 个字符（a,b,c,d,e）的文字系统。已知普通文本中各字符的出现概率分别为 a=0.1, b=0.2, c=0.3, d=0.25, e=0.15。计算明文消息的重合指数期望值（假设明文消息足够长）。（6 分）

解：$I_c = \sum_{1}^{5} p_i^2 = 0.1^2 + 0.2^2 + 0.3^2 + 0.25^2 + 0.15^2 = 0.225$

2. 用扩展欧几里得算法求解$(100)_2$在 GF($2^3$)中的逆元，模$(1011)_2$。*（6 分）*

解：逆元为$(111)_2$

| Q | A2 | A3 | B2 | B3 |
|---|---|---|---|---|
| | 000 | 1011 | 001 | 100 |
| 10 | 001 | 100 | 010 | 011 |
| 10 | 010 | 011 | 101 | 010 |
| 1 | 101 | 010 | 111 | 001 |

3. 求解方程 $x^2 \bmod 77 = 36$, $0<x<77$。*（12 分）*

解：$x^2 \bmod 7 = 36 \bmod 7 = 1$; $x^2 \bmod 11 = 36 \bmod 11 = 3$

可以解得

$x_1=36^{(7+1)/4} \bmod 7 = 1^2 \bmod 7 = 1$ （1 分）

$x_2=36^{(11+1)/4} \bmod 11 = 3^3 \bmod 7 = 6$ （1 分）

Z mod 7 = 1 或 6； Z mod 11 = 6 或 5（2 分）

$y_1=11^{-1} \bmod 7 =2$; $y_2=7^{-1} \bmod 11 =8$ （2 分）

$Z_1=(11*2*1+7*8*6) \bmod 77=50$ （2 分）

$Z_2=(11*2*1+7*8*5) \bmod 77=71$ （2 分）

$Z_3=77-50=27$ （1 分）

$Z_4=77-71=6$ （1 分）

4. 在 Diffie-Hellman 协议中，若公共参数取素数 q=29，本原根 α=3，用户 Alice 与 Bob 各自取私钥 $X_A=5, X_B=6$。试计算：
   a) Alice 与 Bob 在公共信道上交换的 $Y_A$、$Y_B$；
   b) Alice 与 Bob 协商得到的会话密钥；
   c) 若 Eve 进行中间人攻击，且取私钥 $X_E=9$，则他与 Alice 和 Bob 的会话密钥各是多少？
   d) 若希望由 Alice 选定密钥 $K=\alpha^{X_A}$ 并通过协议分配给 Bob，则应如何修改协议？(提示，此时 Alice 可以将原协议中的 $K_{AB}$ 发送给 Bob) *（12 分）*

解：a)$Y_A=3^5 \bmod 29=11$ （1 分）

$Y_B=3^6 \bmod 29=4$（1 分）

b)$K_{AB}=3^{5*6} \bmod 29=9$ （2 分）

c)$K_{AE}=3^{5*9} \bmod 29=2$, $K_{BE}=3^{6*9} \bmod 29=13$ （2 分）

d)

① A: $K = \alpha^{XA} \bmod P$

② B: $Y = \alpha^{XB} \bmod P \rightarrow A$ （2 分）

③ A: $X = Y^{XA} \bmod P = \alpha^{XAXB} \bmod P \rightarrow B$ （1 分）

④ B: $x'_B=x_B^{-1}$, $K' = X^{X'B} \bmod P = \alpha^{XA} \bmod P = K$ （3 分）

# 考 试 试 卷 册

（2011-2012 学年第 1 学期）

考试科目 密码学导论

出卷教师 李卫海

使用班级 PB0921801

考试日期 2011 年 12 月 1 日

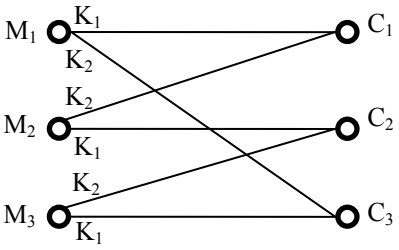
中国科学技术大学教务处

# 中 国 科 学 技 术 大 学
## 2011--2012 学年第 1 学期考试试卷标准答案

考试科目: 密码学导论　　得分:_____

学生所在系:_____ 姓名:_____ 学号:_____

一、 **有一个如图的密码系统，请计算 $P(C_i)$、$P_{M2}(C_i)$、$P_{C2}(M_i)$，$(1\leqslant i\leqslant 3)$，并回答判断：它是闭合系统么？是单纯系统么？是完美安全系统么？（10 分）**




$P(M_1)=0.2$
$P(M_2)=0.3$
$P(M_3)=0.5$
$P(K_1)=P(K_2)=0.5$

答：

$P(C_1)=0.2*0.5+0.3*0.5=0.25$　　（1 分）

$P(C_2)=0.3*0.5+0.5*0.5=0.4$　　（1 分）

$P(C_3)=0.2*0.5+0.5*0.5=0.35$　　（1 分）

$P_{M2}(C_1)=P_{M2}(C_2)=0.5$，$P_{M2}(C_3)=0$　　（2 分，错一个扣 0.5）

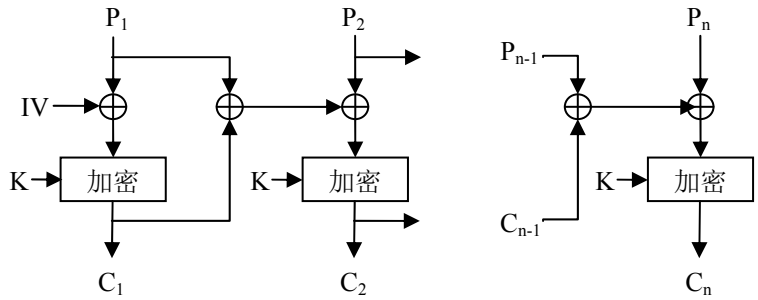
$P_{C2}(M_1)=0$，$P_{C2}(M_2)=0.375$，$P_{C2}(M_3)=0.625$　（2 分，错一个扣 0.5）

该系统是闭合系统，不是单纯系统，不是完美系统。（3 分）

二、 **扩散密码分组链接 PCBC 模式与 CBC 模式相似，区别在于它将当前明文分组与前一个分组的明文、密文分组相异或，把异或结果作为分组密码算法的输入。①请画出 PCBC 链接模式的加密、解密框图。②若某个密文分组出错，分析错误扩散情况。③若将两个相邻密文分组顺序交换，对明文有何影响？（10 分）**

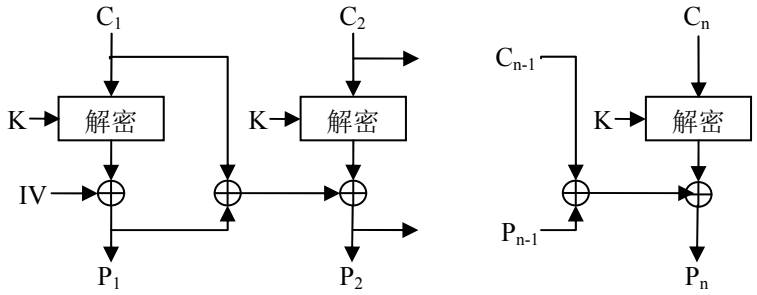
答：

① 加密：




（3 分）

解密：




（3 分）

② 当某个密文分组出错后，该分组之后的所有明文分组都将出错。　　（1 分）

③$C_i=E(P_i\oplus P_{i-1}\oplus C_{i-1})$；$D(C_i)=P_i\oplus P_{i-1}\oplus C_{i-1}$

若将两个相邻密文分组 $C_i,C_{i+1}$ 的顺序交换，则

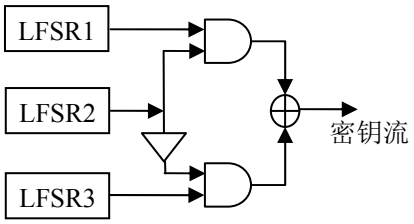
$P'_i=D(C_{i+1})\oplus C_{i-1}\oplus P_{i-1}=P_{i+1}\oplus P_i\oplus C_i\oplus C_{i-1}\oplus P_{i-1}\neq P_i$

$P'_{i+1}=D(C_i)\oplus C_{i+1}\oplus P'_i=P_i\oplus P_{i-1}\oplus C_{i-1}\oplus C_{i+1}\oplus P_{i+1}\oplus P_i\oplus C_i\oplus C_{i-1}\oplus P_{i-1}=P_{i+1}\oplus C_i\oplus C_{i+1}\neq P_{i+1}$

$P'_{i+2}=D(C_{i+2})\oplus C_i\oplus P'_{i+1}=P_{i+2}\oplus P_{i+1}\oplus C_{i+1}\oplus C_i\oplus P_{i+1}\oplus C_i\oplus C_{i+1}=P_{i+2}$

即 $P_i,P_{i+1}$ 两个明文分组会出错，但不会影响之后的明文分组。　　（3 分）

**三、 Geffe 非线性组合流密钥生成器的结构如图，**

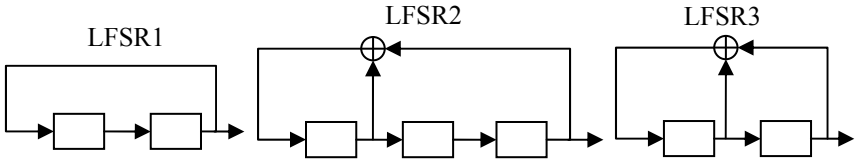



**1. 设其中三个线性移位寄存器的结构为 LFSR1<2,1+$D^2$> ， LFSR2<3,1+D+$D^3$> ， LFSR3<2,1+D+$D^2$>，画出三个 LFSR 的结构。**

**2. 已知输出密钥流为 11111010 00101011，求三个 LFSR 的初始状态。（20 分）**

答：

1.




（6 分，每个 2 分）

2.

a) 计算 LFSR1 的输出，及与系统输出的相关值，如下表：

| 初始状态 | 输出 | 相关值 |
|---|---|---|
| 00 | 00… | 3/8 |
| 01 | 10… | 3/4 |
| 10 | 01… | 1/4 |
| 11 | 11… | 5/8 |

可知 LFSR1 的初值为 01　　（4 分，用其他方法解出也给分）

b) 考虑 LFSR3，它的联接多项式是不可约的，

假设初始状态为 01，则其输出为 101…，它与系统输出的相关值为 7/16；

将输出右移一位，考虑 011…，它与系统输出的相关值为 5/8

再将输出右移一位，考虑 110…，它与系统输出的相关值为 11/16≈3/4

因此，LFSR3 的初值为 11　　（4 分，用其他方法解出也给分）

c) 考虑 LFSR2 的输出：

可求 LFSR2 的输出应为*010***101***110 的模板

LFSR2 的联接多项式是不可约的，周期为 7，对比上述模板，可知其初始状态为 101（或假设初始状态为 001，可得输出序列 1001110…，移动此序列使之与上述模板匹配，得 1010011…，也可知初始状态为 101）。　　（6 分）

**四、 在 ElGamal 系统中，取 α=7, p=13, $x_a$=4, $x_b$=11**

**1) 假定 A 加密传送 m=4 给 B，随机选择 k=7，密文是什么？**

**2) 如果 A 要签名 m=8，随机选择 k=5，签名是什么？随机选择 k=7，签名是什么？**

**3) 如果消息 m=5 附加的签名值是(2,4)，Bob 如何验证？（20 分）**

答：

1) $Y_b=\alpha^{x_b} \bmod p=7^{11} \bmod 13=2$

$c_1=\alpha^k \bmod p=7^7 \bmod 13=6$， $c_2=mY_b^{\ k} \bmod p=4\times 2^7 \bmod 13=5$，密文是(6,5)　　(5 分)

2) k=5: $r=\alpha^k \bmod p=7^5 \bmod 13=11$， $m=(x_a r+ks)\bmod(p-1)\Rightarrow 8=(4\times 11+5\times s)\bmod 12\Rightarrow s=0$
此时会泄露私钥，签名值不能使用，必须更换 k 重新计算。 （5 分）
k=7: $r=\alpha^k \bmod p=7^7 \bmod 13=6$， $m=(x_a r+ks)\bmod(p-1)\Rightarrow 8=(4\times 6+7\times s)\bmod 12\Rightarrow s=8$
签名值为(6,8)。 （5 分）
3) $Y_a=\alpha^{x_a} \bmod p=7^4 \bmod 13=9$
$\alpha^m \bmod p=7^5 \bmod 13=11$， $Y_A{}^r r^s \bmod p=9^2 2^4 \bmod 13=9$ 二者不相等，验证失败。（5 分）

**五、 在某次不经意传输中，Alice 选择 p=11, q=7, 将 n=pq 发送给 Bob。Bob 选取 a=15 并将 $a^2$ mod n 发送给 Alice。Alice 从方程 $x^2=a^2$ mod n 的四个根中任取一个发送给 Bob。请解此方程，并说明什么情况下 Bob 能确定 p 和 q，以及如何确定?（20 分）**

答：
n=77, $a^2$ mod n=71 (2 分)
解方程 $x^2=71 \bmod 77$

$\begin{cases} x^2\equiv 5 \bmod 11 \\ x^2\equiv 1 \bmod 7 \end{cases}$，解得 $\begin{cases} x=5^3 \bmod 11=4 \quad or \quad x=7 \\ x=1 \quad or \quad x=6 \end{cases}$ （4 分）

解 CRT 问题 $\begin{cases} Z_1=\mathrm{CRT}(77,11,7,4,1)=15 \\ Z_2=\mathrm{CRT}(77,11,7,4,6)=48 \\ Z_3=\mathrm{CRT}(77,11,7,7,1)=29 \\ Z_4=\mathrm{CRT}(77,11,7,7,6)=62 \end{cases}$ （各 3 分）

当 Alice 将 48 或 29 传给 Bob 时，Bob 可以计算出 p 和 q
传 48 时，Bob 计算 GCD(48+15,77)=7，77/7=11
传 29 时，Bob 计算 GCD(29+15,77)=11，77/11=7 （2 分）

**六、 将下面的基本 Fiat-Shamir 身份认证协议修改为非交互式的单向认证协议：**

**A 欲向 B 证明拥有知识 s，**

**a) 初始设置**

**1) 由可信中心 T 选择素数 p 和 q，公布 n=pq**

**2) A 选择秘密 s，GCD(s,n)=1，s≠0，计算 $v=s^2$ mod n，将 v 向 T 注册为公钥**

**b) 交互协议，执行 t 轮**

**1) A 选择随机数 r，r≠0，发送 $x=r^2$ mod n 给 B**

**2) B 随机选择比特 e=0 或 1，发送 e 给 A**

**3) A 计算 y=r (若 e=0)，或 y=r·s mod n (若 e=1)，发送 y 给 B**

**4) 若 y=0，则 B 拒绝协议；否则，验证若 $y^2=x\cdot v^e$ mod n，则接受证明。（10 分）**

答：
初始设置部分不变，交互协议部分： （每步 2 分）

1) A 选择 t 个随机数 $r_i$，$r_i\neq 0$，i=1,2,3,…,t，计算 $x_i=r_i^2$ mod n
2) A 将 $x_1$、$x_2$、$x_3$、…作为一个散列函数的输入，并保存散列函数输出的前 t 位
3) 若第 i 位为 0，则计算 $y_i=r_i$；若第 i 位为 1，则计算 $y_i=r_i\cdot s$ mod n
4) A 将 $x_i,y_i$(i=1,2,3,…,t)发送给 Bob
5) B 同样计算 $x_i$ 作为输入的散列函数的输出，并对每一个输出为 i，验证 $y^2=x\cdot v^e$ mod n，若前 t 个位都成立，则接受证明。若某位的 $y_i=0$，或等式不成立，则拒绝证明。

**以下两题任选一题解答，若两道都做，则分数累加，但总分不超过 100。**

**七、 设 Feistel 结构 3 轮分组密码系统中，第 i 轮的轮函数为 $F_i$，请用矩阵描述加/解密运算，并证明其互为逆运算。提示：左右交换操作等价于乘以矩阵 $\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}$。（10 分）**

答：

加密 $\begin{pmatrix}L'\\ R'\end{pmatrix}=\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_3\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_2\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_1\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\begin{pmatrix}L\\ R\end{pmatrix}$ (4 分)

解密 $\begin{pmatrix}L\\ R\end{pmatrix}=\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_1\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_2\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_3\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\begin{pmatrix}L'\\ R'\end{pmatrix}$ (4 分)

在 F(2)域中，

$$\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_1\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_2\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_3\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_3\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_2\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\bullet\begin{pmatrix}I & F_1\\ 0 & I\end{pmatrix}\begin{pmatrix}0 & I\\ I & 0\end{pmatrix}\begin{pmatrix}L\\ R\end{pmatrix}$$ (2 分)

$$=\begin{pmatrix}L\\ R\end{pmatrix}$$

**八、 用中国剩余定理推导（t,n）门限方案的拉格朗日插值公式（10 分）**

答：(t,n)门限方案可表示为：

$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+D$，系数均为模 p 运算，以下省略不写

已知 $\begin{cases}f(x_1)=y_1\\ f(x_2)=y_2\\ \vdots\\ f(x_t)=y_t\end{cases}$ 求解 f(x)

根据余数定理，$\begin{cases}f(x)=(x-x_1)g(x)+y_1\\ f(x)=(x-x_2)g(x)+y_2\\ \vdots\\ f(x)=(x-x_t)g(x)+y_t\end{cases}$，即 $\begin{cases}f(x)\equiv y_1 \bmod(x-x_1)\\ f(x)\equiv y_2 \bmod(x-x_2)\\ \vdots\\ f(x)\equiv y_t \bmod(x-x_t)\end{cases}$ （1）

设 $\begin{cases}Q_i(x)\equiv 1 \bmod(x-x_i)\\ Q_i(x)\equiv 0 \bmod(x-x_j)\end{cases}$ $(\text{for } j\neq i)$，$1\le i\le t$，可以令 $Q_i(x)=\prod_{j=1,j\neq i}^{t}(x-x_j)q_i(x)\equiv 1 \bmod(x-x_i)$，解得

$$q_i(x)=\left[\prod_{j=1,j\neq i}^{t}(x-x_j)\right]^{-1} \bmod(x-x_i)=\prod_{j=1,j\neq i}^{t}(x-x_j)^{-1} \bmod(x-x_i)=\prod_{j=1,j\neq i}^{t}1/(x_i-x_j)$$

所以 $Q_i(x)=\prod_{j=1,j\neq i}^{t}\frac{(x-x_j)}{(x_i-x_j)}$

将 $Q_i(x)$带入（1）式，可得 $f(x)=\sum_{i=1}^{t}y_i\prod_{j=1,j\neq i}^{t}\frac{(x-x_j)}{(x_i-x_j)}$

当方程数量少于 t 个时，恢复的多项式低于 t-1 次，无法确定 D。

# 考 试 试 卷 参 考 答 案

（2012-2013 学年第 1 学期）

考试科目 密码学导论

出卷教师 李卫海

使用班级 PB1021801

考试日期 2013 年 1 月 17 日

中国科学技术大学教务处

# 中 国 科 学 技 术 大 学
## 2012--2013 学年第 1 学期考试试卷标准答案 A 卷

考试科目:__密码学导论__ 得分:_____

学生所在系:_____ 姓名:_____ 学号:_____

**一、 考虑一个包含 3 个字符{a,b,c}的文字系统，已知普通文本中各字符的出现概率分别为 a=0.3, b=0.1, c=0.6，请分析：**

1. **分别计算明文消息和随机字符序列的重合指数期望值。**
2. **若某段密文的重合指数为 0.45，请分析可能是哪种加密算法？请列举 3 种。若密文的重合指数为 0.3，可能是哪种加密算法？请列举 3 种。**

**（本题假设明文消息/密文消息都足够长）（10 分）**

答：

1. 明文消息： $I_c = \sum_1^3 p_i^2 = 0.3^2 + 0.1^2 + 0.6^2 = 0.46$ （2 分）

随机字符序列： $I_c = \sum_1^3 \left(\frac{1}{3}\right)^2 = 0.33$ （2 分）

2. 重合指数为 0.45 时未改变频率分布，可能是置换密码，单表代换密码，移位密码，等。重合指数为 0.3 时，接近于随机分布，可能是一次一密加密，多表代换，维吉尼亚密码，等。（每种 1 分，共 6 分）

**二、 不解方程，判断 $X^2 \bmod 7*17 = 2$ 和 $X^2 \bmod 7*11*17 = 2$ 各有几个根，再求解之。（19 分）**

答：

$$X^2 \bmod 7*17 = 2 \Leftrightarrow \begin{cases} X^2 \bmod 7 = 2 \\ X^2 \bmod 17 = 2 \end{cases}$$ （2 分）

$$X^2 \bmod 7*11*17 = 2 \Leftrightarrow \begin{cases} X^2 \bmod 7 = 2 \\ X^2 \bmod 11 = 2 \\ X^2 \bmod 17 = 2 \end{cases}$$ （2 分）

$2^{(7-1)/2} \bmod 7 = 1$，2 是模 7 的二次剩余 （1 分）

$2^{(11-1)/2} \bmod 11 = -1$，2 不是模 11 的二次剩余（1 分）

$2^{(17-1)/2} \bmod 17 = 1$，2 是模 17 的二次剩余 （1 分）

因此 $X^2 \bmod 7*17 = 2$ 有 4 个根；$X^2 \bmod 7*11*17 = 2$ 无解。 （各 2 分，共 4 分）

对 $X^2 \bmod 7*17 = 2 \Leftrightarrow \begin{cases} X^2 \bmod 7 = 2 \\ X^2 \bmod 17 = 2 \end{cases}$

$$\begin{cases} X_1 \bmod 7 = 2^{(7+1)/4} \bmod 7 = 4, \quad \text{or} \quad X_1 = 7 - 4 = 3 \\ X_2 \bmod 17 = 6, \quad \text{or} \quad X_2 = 17 - 6 = 11 \end{cases}$$ （4 分）

$Z_1 = \mathrm{CRT}(119,7,17,4,6) = 4*17*5+6*7*5 \bmod 7*17 = 74$

$Z_2 = \mathrm{CRT}(119,7,17,4,11) = 4*17*5+11*7*5 \bmod 7*17 = 11$

$Z_3 = 119-74 = 45$

$Z_4 = 119-11 = 108$

（各 1 分，共 4 分）

**三、 我们知道，在使用流密码加密数据时，其中伪随机数发生器的种子不得重复使用。请问：**

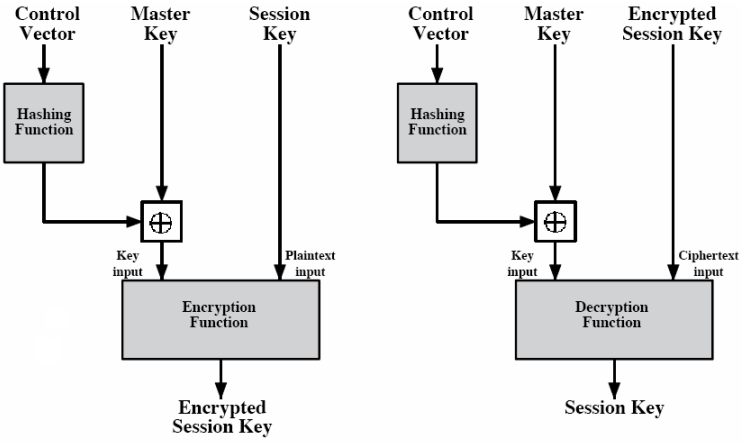
**1. 这是为了抵抗什么攻击？**

**2. 请设计两种方案，使得同一密钥多次使用时，得到不同的伪随机数发生器输出。画出方案的框图，必要时附加文字说明。（15 分）**

答：

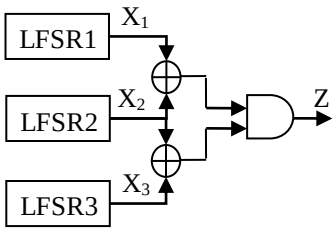
1. 已知明文攻击，选择明文攻击，选择密文攻击，等等。 （3 分）

2. 可以采用控制向量方案。




还可以使用初始向量；在状态反馈时引入时间；等等。答案不唯一，方案合理即可。 （每种方案 6 分，共 12 分）

**四、 某非线性组合流密钥生成器的结构如图，请问**




**1. 填写下面的真值表，并总结输出 Z 与输入 $X_1$、$X_2$、$X_3$ 之间关系的代数正规型表示。其非线性次数是多少？**

| $X_1$ | $X_2$ | $X_3$ | $X_1X_2$ | $X_1X_3$ | $X_2X_3$ | Z |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | | | | |
| 0 | 0 | 1 | | | | |
| … | … | … | | | | |

**2. 计算输出 Z 与输入 $X_1$、$X_2$、$X_3$ 的相关性。（15 分）**

答：1.

| $X_1$ | $X_2$ | $X_3$ | $X_1X_2$ | $X_1X_3$ | $X_2X_3$ | Z |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **1** | **0** | **1** | **0** | **1** | **0** | **1** |
| **1** | **1** | **0** | **1** | **0** | **0** | **0** |
| **1** | **1** | **1** | **1** | **1** | **1** | **0** |

（4 分）

$Z=X_1X_2 \oplus X_2 \oplus X_2X_3 \oplus X_1X_3$ （4 分）

非线性次数为 2 （1 分）

2. 由真值表可以查得，$P(Z=X_1)=1/2$；$P(Z=X_2)=1/2$；$P(Z=X_3)=1/2$。（各 2 分，共 6 分）

**五、 某系统采用 RSA 体制传递数据，要求提供安全性并签名。已知 Alice 的公钥为(65,7)，Bob 的公钥为(91,5)。**

1. **若 Alice 欲将消息 M=11 发送给 Bob，请计算 Alice 发送的数据。**
2. **若 Bob 欲将消息 M=11 发送给 Alice，请计算 Bob 发送的数据。**
3. **Alice 可以请秘书帮助她验证 Bob 的签名而不泄露消息么？Bob 可以么？**
4. **不考虑大数分解的难度，结合上面计算，分析 Alice 的公钥选取是否存在漏洞，并证明之。（19 分）**

答：

1. 65=5*13，$\Phi(65)=4*12=48$，Alice 的私钥 $d=7^{-1} \bmod 48=7$ （2 分）

Alice 先签名，后加密：$C=(11^7 \bmod 65)^5 \bmod 91=41^5 \bmod 91=6$ （4 分）

2. 91=7*13, $\Phi(91)=6*12=72$，Alice 的私钥 $d=5^{-1} \bmod 72=29$ （2 分）

Bob 先加密，后签名：$C=(11^7 \bmod 65)^{29} \bmod 91=41^{29} \bmod 91=6$ （4 分）

3. Alice 可以请秘书验证 Bob 的签名，Bob 不可以请秘书验证 Alice 的签名。 (4 分)

4. 注意到 Alice 的公钥与私钥相同。若 Alice 对消息 M 的签名为 S（本题中 S=41），Bob 收到 M 后，若再用 Alice 的公钥加密得 R（本题中 R=41），就会发现 S=R，从而得知 Alice 的私钥与公钥相同。 （1 分）

证明，

若 e=d, $S=M^e \bmod n$, $R=M^d \bmod n=M^e \bmod n=S$。即 e=d 是 R=S 的充分条件

若 R=S，

对 R 解密，$M=R^e \bmod n=M^{de} \bmod n=M$

又，对 R 解密等于对 S 解密，即 $M=S^e \bmod n=M^{ee} \bmod n=M$。

因此，$de=ee=1 \bmod \Phi(n)$

考虑到 $GCD(e, \Phi(n))=1$，将上式除以 e，得

$d=e \bmod \Phi(n)$。即 e=d 是 R=S 的必要条件。

因此，只要 Bob 发现 R=S，就可以判定 Alice 的公钥等于私钥。 （2 分）

**六、 5 个人采用拉格朗日插值多项式方案进行秘密值分片共享，要求至少 3 个人才能共同恢复秘密值。现已知其中 3 个人的秘密分片为 h(2)=3,h(4)=11,h(1)=5，以 17 为模。请计算原始秘密值是多少。（10 分）**

答：

$$
\begin{aligned}
h(x) &= h(2)\frac{(x-4)(x-1)}{(2-4)(2-1)} + h(4)\frac{(x-2)(x-1)}{(4-2)(4-1)} + h(1)\frac{(x-2)(x-4)}{(1-2)(1-4)} \\
&= 3\times\frac{(x-4)(x-1)}{-2} + 11\times\frac{(x-2)(x-1)}{6} + 5\times\frac{(x-2)(x-4)}{3} \\
&= 3\times 8\times\left(x^2-5x+4\right) + 11\times 3\times\left(x^2-3x+2\right) + 5\times 6\times\left(x^2-6x+8\right) \\
&= 2x^2+9x+11 \pmod{17}
\end{aligned}
$$

秘密值为 11

**七、 Alice 将一副牌（去掉大小王后的 52 张）随机且秘密地分一半给 Bob。现在，Alice 准备大声地告诉 Bob 一条秘密消息 M，偷听者 Eve 可以听到 Alice 说的所有内容。**

1. **请为 Alice 设计一个具体的传讯方法。**
2. **证明，Alice 有可能找到一种方法将 48 比特的信息 M 安全地传递给 Bob，且 Eve 不能获得 M 的任何信息；但完美安全地传递 49 比特的信息则不可能实现。**

**（12 分）**

答：

1. 首先公开地约定牌的顺序，例如红桃 A-K，黑桃，…；然后对于第 i 个消息比特，Alice 大声地说出第 i 张牌是否在自己手中。若 i=1，则说真话；若 i=0，则说假话。Bob 对照自己手中的牌，就可以得知消息 M。 (6 分)

2. Alice 和 Bob 各分一半牌，共有 C(52,26)=495918532948104 种分法，即密钥量为 logC(52,26)≈48.8 比特。所以完美安全地传递 48 比特是可能的，而对 49 比特则不可能。 （6 分）

# 考 试 试 卷 参 考 答 案

（2013-2014 学年第 1 学期）

考试科目 密码学导论

出卷教师 李卫海

使用班级 PB1103301

考试日期 2014 年 1 月 7 日

中国科学技术大学教务处

装订线 答题时不要超过此线

# 中 国 科 学 技 术 大 学
## 2013--2014 学年第 1 学期考试试卷标准答案 A 卷

考试科目:__密码学导论__ 得分:_____

学生所在系:_____ 姓名:_____ 学号:_____

**一、 计算（没有计算过程不得分）**

1. **问 $33^{2013}$ 的末两位数是多少？**
2. **解方程 $(100)_2X \bmod (1011)_2 = (101)_2$ (15 分)**

答：

1. $\Phi(100)=\Phi(2^2*5^2)=2^1*(2-1)*5^1*(5-1)=40$ (4 分)

$33^{2013} \bmod 100 = 33^{50*40+13} \bmod 100 = ((33^2*33)^2)^2*33 \bmod 100 = (37^2)^2*33 \bmod 100 = 69^2*33 \bmod 100 = 13$，末位数字是 13 (3 分)

2.

利用扩展欧几里德算法解出

| q | y | D |
|---|---|---|
| | 0 | $(1011)_2$ |
| | $(1)_2$ | $(100)_2$ |
| $(10)_2$ | $(10)_2$ | $(11)_2$ |
| $(10)_2$ | $(101)_2$ | $(10)_2$ |
| $(1)_2$ | $(111)_2$ | $(1)_2$ |

$(100)_2^{-1} \bmod (1011)_2 = (111)_2$ (5 分)

$X=(111)_2*(101)_2 \bmod (1011)_2 = (110)_2$ （3 分）

**二、 设某对称加密算法 E，对应解密算法为 D，密钥 K 长度为 56bit，明文分组长度为 128bit。不考虑算法 E 本身的安全性，则对 3 重加密 $E_{K2}(E_{K1}(E_{K1}(M)))$的已知明文攻击的代价是多少？（这里的代价指当单次 E/D 的计算次数最少时，E/D 的平均计算次数和存储规模。）并简述说明攻击过程。一般而言，为得到唯一的密钥组合，需要多少明文-密文对？ （10 分）**

答：

中间相遇攻击：穷举计算 $2*2^{56}$ 次，存储空间 $2^{56}$。 （4 分）

攻击过程： （4 分）

i. 对 $2^{56}$ 个可能的密钥 $K_2$ 计算 $X=D_{K2}(C)$，将结果按 X 值排序存储。计算量 $2^{56}$ 次，存储空间 $2^{56}$。

ii. 对 $2^{56}$ 个可能的密钥 $K_1$ 计算 $Y=E_{K1}(E_{K1}(M))$，在 X 的表中查找 Y。平均计算量 $0.5*2*2^{56}$ 次。

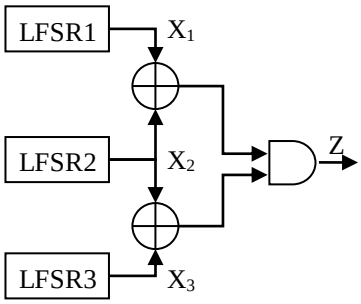
iii. 若找到匹配，则对应的 K1 和 K2 即为所求的密钥。

对任意明文 M，加密得到的密文有 $2^{128}$ 种可能，而密钥组合只有 $2^{112}$ 中可能。产生匹配的概率为 $2^{-16}$。因此，一般而言只需一个明文-密文对，即可确定密钥组合。 （2 分）

**三、 某非线性组合流密钥生成器的结构如图，请问**

1. **写出 Z 与输入 $X_1$、$X_2$、$X_3$ 之间关系的代数正规型表示。其非线性次数是多少？**
2. **列出 Z 与输入 $X_1$、$X_2$、$X_3$ 之间的真值表，计算 Z 与输入 $X_1$、$X_2$、$X_3$ 的相关性。**

**3. 该生成器能抵抗相关攻击么？它的输出适宜直接用作密钥么？ （15 分）**




1.

$Z=(X_1 \oplus X_2)(X_2 \oplus X_3)=X1X2 \oplus X1X3 \oplus X2 \oplus X2X3$（2 分）

非线性次数为 2（3 分）

2.

| $X_1$ | $X_2$ | $X_3$ | $X_1 \oplus X_2$ | $X_2 \oplus X_3$ | Z |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 |

（真值表 1 分）

$P(Z=X_1)=1/2$；$P(Z=X_2)=1/2$；$P(Z=X_3)=1/2$。（6 分）

3.

输出与输入相关性为 1/2，能抵抗相关攻击。 （2 分）

输出中 0、1 数量偏差很大，不宜直接用作密钥。 （2 分）

**四、 Alice 向 Bob 发送信息，通过 ElGamal 密码进行加密与签名。取公共大素数 p=29，本原元 α=3，Alice 的私钥为 5，Bob 的私钥为 7，Alice 选取的随机数为 6。**

**1. Alice 欲加密消息 m=11，请计算密文，并为 Bob 解密密文。**

**2. Alice 欲签名消息 m=12，请计算签名（写出所有可能），并计算 Bob 如何验证。（20 分）**

答：

1.

$Y_B = \alpha^{X_B} \bmod p = 3^7 \bmod 29 = 12$ （2 分）

Alice 加密：

$K = (Y_B)^k \bmod p = 12^6 \bmod 29 = 28$ （2 分）

$\begin{cases} c_1 = \alpha^k \bmod p = 3^6 \bmod 29 = 4 \\ c_2 = mK \bmod p = 11*28 \bmod 29 = 18 \end{cases}$，密文为（4,18） （2 分）

Bob 解密：

$K=(c_1)^{x_B} \bmod p=4^7 \bmod 29=28$ （1 分）

$m=c_2/K \bmod p=18*(28)^{-1} \bmod 29=18*28 \bmod 29=11$ （2 分）

2.

$Y_A=\alpha^{X_A} \bmod p=3^5 \bmod 29=11$ （2 分）

Alice 签名：

$r=\alpha^k \bmod p=3^6 \bmod 29=4$ （2 分）

$m=(x_A r+ks) \bmod p-1 \Rightarrow 12=(5*4+6s) \bmod 28 \Rightarrow 6s=20 \bmod 28$
$\Rightarrow s=22,8$ （2 分）

签名数据（4,22）或（4,8） （2 分）

Bob 验证：

$\alpha^m \bmod p=3^{12} \bmod 29=16$
$Y_A{}^r r^s \bmod p=11^4*4^{22} \bmod 29=25*25 \bmod 29=16=11^4*4^8 \bmod 29$ （2 分）

所以 $\alpha^m=Y_A{}^r r^s \bmod p$，通过验证。 （1 分）

**五、 Alice 和 Bob 执行不经意传输协议。假设 Alice 的秘密是两个大素数 13、19，她传给 Bob 的模数是 247。**

**1. 若 Bob 选取 x=23，并计算 $23^2$ mod 247 = 35 发送给 Alice。问，Alice 可能反馈什么数字给 Bob？反馈数字是多少时，Bob 可以解出 Alice 的秘密？**

**2. 若 Bob 碰巧选择 x=13 来执行协议（设 Bob 未注意到 13|247），会发生什么？ （20 分）**

答：

1.

$X^2 \bmod 13*19=35 \Leftrightarrow \begin{cases} X^2 \bmod 13=9 \\ X^2 \bmod 19=16 \end{cases}$ （2 分）

$\begin{cases} X_1 \bmod 13=3, \quad \text{or} \quad X_1=13-3=10 \\ X_2 \bmod 19=4, \quad \text{or} \quad X_2=19-4=15 \end{cases}$ （2 分）

$Z_1=\mathrm{CRT}(247,13,19,3,4)=3*19*11+4*13*3 \bmod 247=42$
$Z_2=\mathrm{CRT}(247,13,19,3,15)=3*19*11+15*13*3 \bmod 247=224$
$Z_3=247-42=205$
$Z_4=247-224=23$

所以 Alice 可能发送 42、224、205、23。 （各 2 分，共 8 分）

当 Alice 发送 42 或 205 时，Bob 能算出 Alice 的秘密。GCD(23+42,247)=13，GCD(23+205,247)=19 （1 分）

2.

若 Bob 选择 x=13，则 $13^2$mod 247 = 169，发送给 Alice。

$$X^2 \bmod 13*19 = 169 \Leftrightarrow \begin{cases} X^2 \bmod 13 = 0 \\ X^2 \bmod 19 = 17 \end{cases}$$

$$\begin{cases} X_1 \bmod 13 = 0 \\ X_2 \bmod 19 = 17^{(19+1)/4} \bmod 19 = 6, \quad \text{or} \quad X_2 = 19 - 6 = 13 \end{cases}$$

此时 Alice 只能解出两个解 $\begin{matrix} Z_1 = 6*13*3 \bmod 247 = 234 \\ Z_2 = 247 - 234 = 13 \end{matrix}$ （5 分，也可以直接写出结果）

若 Alice 返回 13，Bob 可以计算 GCD(13+13,247)=13；但 Bob 也可能因为返回值与他任取的 x 相同而放弃计算。 （1 分）

若 Alice 返回 234，Bob 计算 GCD(13+237,247)=247，Bob 仍不会发现 Alice 的秘密。 （1 分）

**六、 设变换 H 将 m 位二进制串{0,1}$^m$ 映射到 n 位二进制串{0,1}$^n$，其中 m 远大于 n。问：**

1. **假设变换 H 是抗弱碰撞的，那么 H 是单向的么？如果是，请解释为什么；如果不是，请给出反例。**
2. **假设变换 H 是单向的，那么 H 是抗弱碰撞的么？如果是，请解释为什么；如果不是，请给出反例。 （10 分）**

答：

1.

若 H 抗弱碰撞，则 H 是单向的。（2 分）

否则求解 $x=H^{-1}(y)$将是容易的；又因为映射是多对一的，其解必为多个，因而可以找到多个碰撞。这与假设矛盾。 （3 分）

2.

若 H 的单向的，H 未必是抗弱碰撞的。 （2 分）

例如：大素数（模三余一）域中的平方运算是单向的，但不抗弱碰撞（x 与 p-x 碰撞）。 （3 分）

**七、 在 Diffie-Hellman 密钥协商协议中，通信双方在未更新私钥之前，产生的会话密钥总是相同的。但要求用户经常更换私钥，将会给用户带来很多麻烦。为此，可以用随机数代替 Diffie-Hellman 协议中的私钥，从而获得可变的会话密钥，私钥仍用于身份认证。请具体设计该协议。要求协议能抵抗中间人攻击，并进行双向认证。 （10 分）**

答：

A: 私钥 xa，公钥 $Ya=\alpha^{xa}$；B: 私钥 xb, 公钥 $Yb==\alpha^{xb}$

公钥可由 AS 签发证书。Alice 公钥证书为 Sa，bob 公钥证书为 Sb

1) A: 选择私钥 ra<q，计算 $Ta=\alpha^{ra}$
2) A→B: $ID_A$, $ID_B$, $PR_{xa}(Ta)$, Sa, $N_1$
3) B: 选择私钥 rb<q，计算 $Tb=\alpha^{rb}$
4) B: 计算 $K=(Ta)^{rb}$
5) B→A: $PR_{xb}(Tb)$, Sb, $E_K(N_1+1 \parallel N_2)$,
6) A: 计算 $K=(Tb)^{ra}$
7) A→B: $N_2$

也可用可信第三方授权发送公钥。 （密钥协商部分 4 分，抵抗中间人攻击 3 分，双向认证 3 分）

装订线 答题时不要超过此线

# 中 国 科 学 技 术 大 学
## 2014--2015 学年第 1 学期考试试卷标准答案 A 卷

考试科目: 密码学导论　　得分:_____

学生所在系:_____ 姓名:_____ 学号:_____

**一、 计算（必须写明计算过程）（25 分）**

1. **若将 $11^{2046}$ 表示为十六进制数，其最末一位是什么？**
2. **解方程 $X^2$ mod 7*19 = 18**

答：

1. Φ(16)=8　　(4 分)

$11^{2046}$ mod 16=$11^{255*8+6}$ mod 16=9，末位数字是 9　　(6 分)

2.

$$X^2 \bmod 7*19 = 18 \Leftrightarrow \begin{cases} X^2 \bmod 7 = 4 \\ X^2 \bmod 19 = 18 \end{cases}$$ （6 分）

$$\begin{cases} X_1 \bmod 7 = 2, \quad \text{or} \quad X_1 = 7-2 = 5 \\ X_2 \bmod 19 = -1 \text{无解} \end{cases}$$ （8 分）

因此方程无解（1 分）

**二、 在某加密系统中，先对明文进行单表代换操作，再对代换结果进行置乱操作。问：如何对该系统进行选择明文攻击？请描述你的攻击方法。若明文/密文字符集都是英文字母集合，对于一段长 15 个字符的密文，需要选择多少个明文就能保证破译？（10 分）**

**（附加一问：仍是这段密文，最少需要多少个选择明文？答出加 5 分，答不出不扣分）**

答：首先破译置乱操作。改变一个明文字符，观察密文中哪个字符发生了变化，从而获知一个置乱位置；重复此操作，直至置乱表完全获得。然后，对明文字母表进行一次加密操作，结合置乱表即可获知代换表。对于长 15 个字符的密文，选择 15 个明文（第 2-15 个明文的第 1-14 个字符与第 1 个明文不同），即可破译置乱表，再由 1 个明文破译代换表，共需 16 个选择明文。

附加部分：只需 3 个选择明文。第一个明文为：abbccccddddeeeee，根据字符数量的不同，判断出若干个置乱的段，并确定 a-e 的代换表。第二个明文为：ffgfghfghifghij，根据字符数量不同，结合前面获得的置乱分段，可以分析出完整的置乱表，并确定 f-j 的代换表。第三个明文为 klmnopqrstuvwxy，获得 k-y 的代换结果，最后推测出 z 的代换结果。

**三、 设 Alice 有长度为 n 比特的密钥 $k_1$，Bob 有长度 n 比特的密钥 $k_2$。他们希望加密消息 M，使得密文必须使用双方的密钥才能解密。他们考虑使用某个分组密码算法 E，并采用如下方案：**

**a. $C=E_{k1}[E_{k2}[M]]$**

**b. $C=E_{k1 \oplus k2}[M]$**

**c. $C=(E_{k1}[r], E_{k2}[r \oplus M])$，这里 r 是每次更换的随机数。**

**问：**

1. **假设攻击者已获得若干明文/密文分组对{M,C}，和待破译密文 C'，则以上三种方案都可以在 $O(2^n)$时间内破译，请说明攻击方法。**

**2. 哪种方案的攻击代价最小？哪种方案的攻击代价最大？ （20 分）**

答：

1.

a. 采用中间相遇攻击。 （5 分）

b. $k_1$ 与 $k_2$ 异或等价于一个新密钥 $k_3$，穷举 $k_3$ 即可。 （5 分）

c. 穷举 $k_1$，编写 $k_1$ 与 r 的表；穷举 $k_2$，编写 $k_2$ 与 $r \oplus M$ 的表。按照已知的 M，找出 $k_1$ 与 $k_2$ 的配对，再用其他分组进行验证。 （5 分）

2.

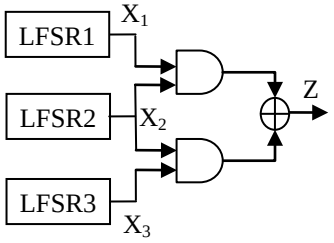
b 方案需要穷举 $2^n$ 次，无需存储

a 方案需要穷举产生两张表（第二张表无需完整），再做少量验证，存储代价 $2^n$

c 方案需要穷举产生两张完整表，并验证每个密钥对，存储代价 $2*2^n$

b 方案的攻击代价最小，c 方案的攻击代价最大。 （5 分）

**四、 某非线性组合流密钥生成器的结构如图，请问**




**1. 写出 Z 与输入 $X_1$、$X_2$、$X_3$ 之间关系的代数正规型表示。其非线性次数是多少？**

**2. 计算输出 Z 与输入 $X_1$、$X_2$、$X_3$ 的相关性。（10 分）**

答：

1. $Z=X_1X_2 \oplus X_2X_3$ （2 分）

非线性次数为 2 （2 分）

2.

| $X_1$ | $X_2$ | $X_3$ | $X_1X_2$ | $X_2X_3$ | Z |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 1 | 0 |

$P(Z=X_1)=1/2$；$P(Z=X_2)=3/4$；$P(Z=X_3)=1/2$。（6 分）

**五、 某系统采用 RSA 体制传递数据，要求提供安全性并签名。已知 Alice 的公钥为(55,7)，Bob 的公钥为(65,5)。**

**1. 若 Alice 欲将消息 M=3 发送给 Bob，请计算 Alice 发送的数据。**

**2. 若 Bob 欲将消息 M=3 发送给 Alice，请计算 Bob 发送的数据。（15 分）**

答：

1. $55=5*11$，$\Phi(55)=4*10=40$，Alice 的私钥 $d=7^{-1} \bmod 40=23$ （3 分）

Alice 先签名，后加密：$C=(3^{23} \bmod 55)^5 \bmod 65=27^5 \bmod 65=27$ （4 分）

2. $65=5*13$, $\Phi(39)=4*12=48$，Bob 的私钥 $d=5^{-1} \bmod 48=29$ （4 分）

Bob 先加密，后签名：$C=(3^7 \bmod 55)^{29} \bmod 65= 42^{29} \bmod 65=22$（4 分）

六、 **5 个人采用拉格朗日插值多项式方案进行秘密分享，要求至少 3 个人才能共同恢复秘密值。在某次秘密重建时，一个骗子观察到 3 个合法使用者的秘密分片为 h(2)=5, h(4)=3, h(1)=10，以 17 为模，并为自己计算了一个合法分片 h(5)。问秘密值和 h(5)分别是多少？（10 分）**

答：

$$h(x)=h(2)\frac{(x-4)(x-1)}{(2-4)(2-1)}+h(4)\frac{(x-2)(x-1)}{(4-2)(4-1)}+h(1)\frac{(x-2)(x-4)}{(1-2)(1-4)}$$

$$=5\times\frac{(x-4)(x-1)}{-2}+3\times\frac{(x-2)(x-1)}{6}+10\times\frac{(x-2)(x-4)}{3}$$ （7 分）

$$=5\times8\times(x^2-5x+4)+3\times3\times(x^2-3x+2)+10\times6\times(x^2-6x+8)$$

$$=7x^2+8x+12(\mathrm{mod}17)$$

秘密值为 12 (1 分)

h(5)=6 （2 分）

七、 **假设用户 A 准备向用户 $B_i$(i=1,2,…,n)广播消息。这里秘密性并不重要，但所有用户 $B_i$ 需要能够验证他所接收的消息来自 A。A 决定使用 MAC。问：**

1. **若 A 和所有的 $B_i$ 共享一个密钥 k，用户 A 使用密钥 k 计算消息的 MAC 值，并发送给所有 $B_i$。如此，所有的 $B_i$ 都可以验证 MAC 值。请用一句话解释，为什么这个方案是不安全的。**
2. **假设用户 A 有密钥集 $S=\{k_1,k_2,\cdots,k_m\}$，每个用户拥有 S 的一个子集 $S_i\subseteq S$。当用户 A 广播消息时，她使用每个密钥分别计算一个 MAC 值，并将这 m 个 MAC 值附加在消息后面。当用户 $B_i$ 收到消息后，他验证他的密钥子集 $S_i$ 中每个密钥对应的 MAC 值，若都正确则确认消息来自用户 A。问 $S_i$ 应满足什么条件，才能保证该方案不会收到问题 1 中的攻击。（假设所有的 $B_i$ 不会共谋）**
3. **当 n=6 时，用户 A 的密钥集 S 中最少应包含几个密钥？构造此时的 $S_1$~$S_6$。（10 分）**

答：

1. $B_i$ 无法确认消息是否来自其他 $B_j$。或，任意 $B_i$ 都有能力伪造该 MAC 值。 (3 分)
2. $S_i$ 应互不相等或包含。 （3 分）
3. S 中至少有 4 个密钥。 （2 分）

   $S_1=\{k_1,k_2\}$; $S_2=\{k_1,k_3\}$; $S_3=\{k_1,k_4\}$; $S_4=\{k_2,k_3\}$; $S_5=\{k_2,k_4\}$; $S_6=\{k_3,k_4\}$ （2 分）

装订线 答题时不要超过此线

# 中 国 科 学 技 术 大 学
## 2017--2018 学年第 1 学期考试试卷标准答案 A 卷

考试科目: 密码学导论　　得分:_____

学生所在系:_____ 姓名:_____ 学号:_____

**一、单项选择题 （15 分）**

**1. 以下哪一条描述，不是对“实际安全密码系统”的要求？ （ A ）**

**A. 即使有无限的资源和时间，都无法唯一地破译密文**

**B. 破译密码的难度与数学上某个困难问题的难度相同**

**C. 破译密码所需成本超出密文信息的价值**

**D. 破译密码所需时间超出密文信息的有效生命期**

**2. 设计与使用密码系统时，以下描述恰当的是（ C ）。**

**A. 即使是低安全级别的信息，也应使用最高级别的加密技术给予保护**

**B. 密码系统在不过分增加运算负担的条件下，应尽可能复杂，就可以提供高安全性**

**C. 若已验证密文被 Alice 私钥签名，即使已知该私钥安全，也不能推断 Alice 了解消息内容**

**D. 当发觉旧密钥可能已不安全时，应尽快利用旧密钥加密传递新密钥**

**3. 密文反馈分组工作模式的缩写是（ B ）。**

**A. ECB　B. CFB　C. CBC　D. OFB**

**4. 以下是公开密钥密码算法的是（ B ）。**

**A. Blowfish　B. Robin　C. RC4　D. RC5**

**5. 关于 Diffie-Hellman 协议，下列表述错误的是（ C ）。**

**A. 用于双方协商密钥**

**B. 基于离散对数难题**

**C. 易受中间相遇攻击**

**D. 不能用于交换确定消息**

**二、填空题 （14 分）**

**6. 利用 重合指数法 或 Kasisky 法 可以推算维吉尼亚密码的密钥长度。**

**7. 冗余是表达信息时语言中附加的部分，当冗余变为 零 （零、无穷大）时，任何闭合密码系统都是完美安全的，其密钥的模糊度随着密文数量的增加 不降低 （不降低、降低但不为零、降为零）。通过 压缩 技术可以减少冗余。**

**8. 高级加密标准 AES 算法的一轮运算中包括四步操作， 轮密钥加 操作与密钥有关， 行移位 操作相当于置乱， 字节代换 操作相当于单表代换，后两种操作与 列混淆 操作一起提供了混淆、扩散和非线性功能。**

**9. MD5 的分组长度为 512 比特，摘要长度为 128 比特，SHA-1 的分组长度为 512 比特，摘要长度为 160 比特，SHA-256 的摘要长度为 256 比特。**

**三、简答与计算题：**

**10. 在 Shannon 概率模型下，简要说明**

**a) 密码分析者破译了某密文的含义；**

**b) 密码分析者破译了某密钥的含义；**

**b) 柯克霍夫原则/香农箴言。（12 分）**

答：

a) 攻击者计算消息的后验概率/模糊度，当某一消息的后验概率接近 1，或消息模糊度为零时，即完成破译。 （4 分）

b) 攻击者计算密钥的后验概率/模糊度，当某一密钥的后验概率接近 1，或密钥模糊度为零时，即完成破译。 （4 分）

c) 攻击者知道消息、密文的先验概率，知道加密和解密映射族/密钥的先验概率，知道实际密文的情况下，仍无法分析出实际的消息和密钥。 （4 分）

**11. 五个人采用拉格朗日插值多项式方案进行(3，5)门限秘密分享。已知其中三份分享为 H(x=2)=7，H(x=3)=3，H(x=5)=8，模数为 17，问秘密值是多少？（10 分）**

答：

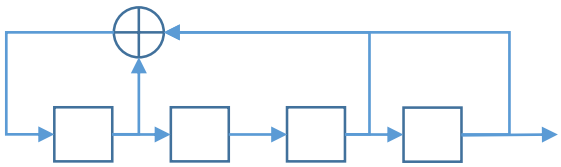
$$\begin{aligned}\mathrm{H(x)} &= 7\times\frac{(x-3)(x-5)}{(2-3)(2-5)}+3\times\frac{(x-2)(x-5)}{(3-2)(3-5)}+8\times\frac{(x-2)(x-3)}{(5-2)(5-3)}\\ &= 7\times\frac{(x-3)(x-5)}{3}+3\times\frac{(x-2)(x-5)}{-2}+8\times\frac{(x-2)(x-3)}{6}\\ &= 8\times(x-3)(x-5)+7\times(x-2)(x-5)+7\times(x-2)(x-3)\\ &= 5x^2+5x+11\end{aligned}$$

（8 分）

秘密值为 11 （2 分）

**12. 画出 LFSR<4,1+D+$D^3$+$D^4$>的结构，并列出所有非全零初值对应的周期（并不需要穷举每个初值）。（11 分）**

答：



初值为 0001 的输出序列为 1000 1110 00…，周期为 6，包括的状态有(0001 1000 1100 1110 0111 0011)

初值为 0010 的输出序列为 0100 100…，周期为 3，包括的状态有(0010 1001 0100)

初值为 0101 的输出序列为 1010 10…，周期为 2，包括的状态有(0101 1010)

初值为 0110 的输出序列为 0110 110…，周期为 3，包括的状态有(0110 1011 1101)

初值为 1111 的输出序列为 1111…，周期为 1，包括的状态有(1111) （前 4 个每个 2 分，最后 1 个 1 分）

综上，

初值(1111)的周期为 1

初值(0101 1010)的周期为 2

初值(0010 0100 0110 1001 1011 1101)的周期为 3

初值(0001 0011 0111 1000 1100 1110)的周期为 6 （2 分）

**13. 当使用 RSA 算法实现即加密又签名功能时，需要考虑通信双方的模数大小。为避免这种约束，Alice 和 Bob 决定使用相同的模数 n（但两人均不知道如何分解 n），不同的私钥和公钥。已知 n=65，Alice 的私钥 $d_A$=5，Bob 的私钥 $d_B$=7。**

**a) 若你能分解 n，请计算 Alice 和 Bob 的公钥。该公钥在 b）和 c）问中为已知条件。**

**b) 若 Alice 将消息 m=2 先签名再加密后发送给 Bob，求她发送的数据。**

**c) 若有第三方将一个消息分别用 Alice 和 Bob 的公钥加密后发送给他们，其中发给 Alice 的密文是 $C_A$=48，发送给 Bob 的密文是 $C_B$=42，请破译该消息（你不能分解 n，也无法算出 Alice 和 Bob 的私钥）。（20 分）**

答：

a)

n=5*13，Φ(n)=4*12=48 （2 分）

$e_A=5^{-1} \bmod 48=29$ （2 分）

$e_B=7^{-1} \bmod 48=7$ （2 分）

b)

签名 $2^5 \bmod 65=32$ （3 分）

加密 $32^7 \bmod 65=33$ （3 分）

发送的数据是 33

c）

由扩展欧几里得算法，解 r*29+s*7=1

| | | | |
|---|---|---|---|
| | 1 | 0 | 29 |
| | 0 | 1 | 7 |
| 4 | 1 | -4 | 1 |

1*29-4*7=1 （3 分）

由扩展欧几里得算法，解 42 模 65 的逆元

| | | |
|---|---|---|
| | 0 | 65 |
| | 1 | 42 |
| 1 | -1 | 23 |
| 1 | 2 | 19 |
| 1 | -3 | 4 |
| 4 | 14 | 3 |
| 1 | -17 | 1 |

$42^{-1} \bmod 65=48$ （3 分）

消息为 $48^1 \times 48^4 \bmod 65=3$ （2 分）

**14. Rabin 于 1978 年提出了一种散列算法：对于消息 $M=M_1||M_2||\cdots|M_N$，使用 AES 分组加密算法，令 $H_0$=初始值，迭代计算 $H_i=E(M_i,H_{i-1})$ (i=1,2,3,⋯,N)，散列值 $G=H_N$。问，这种算法安全么？如安全，解释理由；如不安全，请给出一种攻击方法。（10 分）**

答：

基于生日悖论的“中间相遇”攻击

i. 计算消息 M 的散列值 G

ii. 构造新消息 $Q_1||Q_2||\cdots||Q_{N-2}$，并计算 $H_{N-2}$ （4 分）

iii. 产生 $2^{m/2}$ 个随机分组，对每一分组 X，计算 $E(X,H_{N-2})$；再产生 $2^{m/2}$ 个随机分组，对每一分组 Y，计算 D(Y,G)

iv. 根据生日悖论，存在 X 和 Y 满足 $E(X,H_{N-2})=D(Y,G)$的概率大于 0.5 （4 分）

v. 构造消息 $Q_1||Q_2||\cdots||Q_{N-2}||X||Y$，其散列码也为 G （2 分）

**15. 时间锁安全服务。在该服务下，Alice 能够加密一个秘密 S，它只能在若干天后才能被解密（比如 10 天，1 年，100 年）。假设现在有一个可信机构愿意提供服务，但该机构只愿意定期发布一些信息，而不愿意与用户交互。请利用该可信机构设计一种时间锁安全服务。 （8 分）**

答：参考答案，不唯一

可信机构产生一批公钥 $PU_i$、私钥 $PR_i$ 对，在时刻 0 将所有公钥发布，并保存好所有私钥。之后，在每天凌晨发布一条私钥 $PR_i$。Alice 可以查询公钥，若希望 x 天后解密，则用 $PU_x$ 加密她的秘密并公开。x 天后，$PR_x$ 被可信机构发布，则公众可以解秘该秘密。 （8 分）

装订线 答题时不要超过此线

# 中 国 科 学 技 术 大 学
## 2018--2019 学年第 1 学期考试试卷标准答案 A 卷

考试科目: 密码学导论　　得分:_____

学生所在系:_____ 姓名:_____ 学号:_____

### 一、单项选择题 （15 分）

1. 关于冗余的作用，下列表述错误的是（ **C** ）
   A. 冗余决定了压缩可能达到的极限
   B. 自然语言中的冗余无法彻底消除
   C. 冗余是描述消息性质的，与密码系统的安全性无关
   D. 如果能在消息中消除冗余，那么即使采用凯撒密码加密也可以获得完美安全

2. 以下哪一种情况不是实际安全的? （ **B** ）
   A. 密码破译被证明等价于解数学难题，且问题规模足够大
   B. 使用现有的计算资源不能破译
   C. 在消息失效前不能破译
   D. 破译消息的代价远超过消息本身的价值

3. 以下哪一个不是对称密钥算法？（ **B** ）
   A. DES　B. ECC　C. RC5　D. RC4

4. 在 Shannon 的概率模型下，攻击者截获密文后所要进行的分析不包括以下那一条？（ **B** ）
   A. 可能的明文的后验概率
   B. 可能的密文的后验概率
   C. 可能的密钥的后验概率
   D. 实际的密钥

5. 用于认证的可信时间戳不能由发信人自行添加的原因，不包括（ **D** ）
   A. 发信人可以撒谎
   B. 发信人可以抵赖
   C. 发信人可以自由设定自己系统时间
   D. 时间戳可以被篡改

### 二、填空题 （15 分）

6. AES 加密标准的分组长度是 **128** 比特，密钥长度是 **128/192/256** 比特；SMS4 加密标准的分组长度是 **128** 比特，密钥长度是 **128** 比特。

7. MD5 标准的摘要长度是 **128** 比特，抗强碰撞的能力是 2 的 **64** 次方；SHA-1 标准的摘要长度是 **160** 比特，抗强碰撞的能力是 2 的 **80** 次方；SHA-384 标准的摘要长度是 **384** 比特，抗强碰撞的能力是 2 的 **192** 次方。

8. 传统密码算法采用的两类基本加密方法是 **代换** 和 **置乱** ，交替使用这两种方法，并在其中插入一个简单变换，就可以实现 **扩散** 和混淆的效果，增加统计分析的难度。

9. n 级最长 LFSR 输出的是 m 序列，在一个周期内，长为 n-1 的 0 游程最多有 **1** 个，长为 n 的 1 游程最多有 **1** 个。

## 三、问答与计算题

10. 仿射密码本质上是定义在模运算上的一元一次线性函数 C=am+b mod 26，其中常数 a 和 b 是密钥。若已知字母“f”(5)被加密为字母“V”(21)，字母“t”（19）被加密为字母“T”（19），且密文可以唯一解密，求解所有可能的密钥。（10 分）

**答:**

**5a+b=21 mod 26 (1), 19a+b=19 mod 26 (2)　　（1 分）**

**两式相减，得 14a=24 mod 26　　（2 分）**

**7a=12 mod 13**

**a=12*2=24, 或 a=24+13=11　　（3 分）**

**舍弃 a=24　　(2 分)**

**将 a=11 带入（1）可得 a=11, b=18　　（2 分）**

11. 若已知一个 6 阶线性反馈移位寄存器自时钟为 0 时起的输出为 001001001001…，问

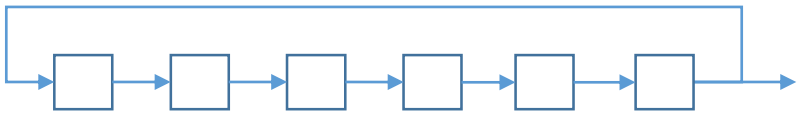
a) 时钟为 0 时，各寄存器的状态是什么（从第 5 级至第 0 级顺序写出）？
b) 时钟为 5 时，各寄存器的状态是什么（从第 5 级至第 0 级顺序写出）？
c) 画出一个满足条件的线性反馈移位寄存器结构。
d) 该输出序列中，前 2 个比特的线性复杂度是多少？前 3 个比特的线性复杂度是多少？
e) 该输出序列中前 12 个比特的线性复杂度是 6 吗？为什么？（10 分）

**答：**

**a) 100100　　（2 分）**

**b) 001001　　（2 分）**

**c)**



**（2 分）**

**d) 前 2 个比特的线性复杂度是 0，前 3 个比特的线性复杂度是 3。　　（2 分）**

**e) 线性复杂度不是 6。因为该序列周期为 3，线性复杂度至多为 3。　　（2 分）**

12. 五个人采用拉格朗日插值多项式方案进行（3,5）门限秘密分享。已知其中三份分享为 H(x=1)=1，H(x=2)=3，H(x=3)=4，模数为 11，问秘密值是多少？（10 分）

**答：**

$$\mathbf{H(x)} = \mathbf{1}\times\frac{(x-2)(x-3)}{(1-2)(1-3)} + \mathbf{3}\times\frac{(x-1)(x-3)}{(2-1)(2-3)} + \mathbf{4}\times\frac{(x-1)(x-2)}{(3-1)(3-2)}$$

$$= \frac{(x-2)(x-3)}{2} + \mathbf{3}\times\frac{(x-1)(x-3)}{-1} + \mathbf{4}\times\frac{(x-1)(x-2)}{2}$$

$$= \mathbf{6}\times(x-2)(x-3) - \mathbf{3}\times(x-1)(x-3) + \mathbf{4}\times\mathbf{6}\times(x-1)(x-2)$$

$$= \mathbf{27}x^2 - \mathbf{90}x + \mathbf{75} = \mathbf{5}x^2 + \mathbf{9}x + \mathbf{9}\ \ mod\ \ \mathbf{11}$$

**（8 分）**

**秘密值为 9　（2 分）**

13. 分组密码的明文反馈链接与标准的 CFB 模式相似，区别仅在于它将该分组的明文而不是密文反馈进入移位寄存器中。

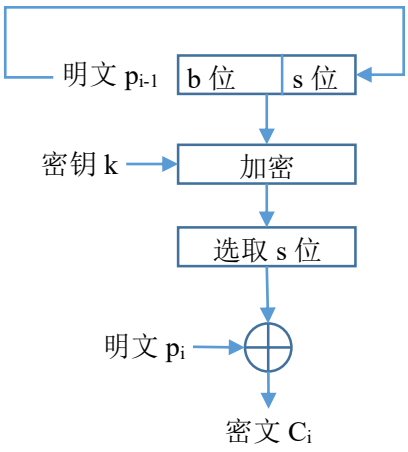
a) 请画出明文反馈链接模式的加密和解密框图。

b) 若某个密文分组在传输中发生错误（即 0 或 1 发生翻转），分析错误扩散情况。

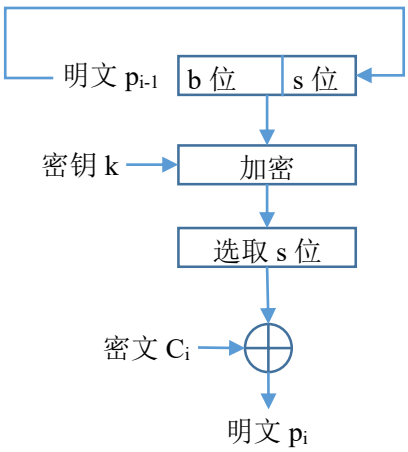
c) 请分析明文反馈链接与 CFB 相比的优缺点。（10 分）

**答：**

**a)**




加密




解密

**（3 分）**

**b) 该密文错误将导致后面所有分组无法正确解密。　　（3 分）**

**c) 优点是将明文反馈至移位寄存器中，窃听者不能直接获得移位寄存器的内容，无法进行字典攻击。缺点是错误扩散太严重。　　（4 分）**

14. Alice 和 Bob 使用 RSA 算法实现保密和签名。已知 Alice 的 $n_A$=55，Alice 的公钥 $e_A$=27，Bob 的 $n_B$=65，公钥 $e_B$=11。

a) 请计算 Alice 和 Bob 的私钥。

b) 若 Alice 欲将消息 m=2 加密发送给 Bob，求她发送的数据。

c) 若 Alice 收到 Bob 发来的密文 C=7，及对明文的签名 S=2，求明文并验证签名。（10 分）

**答：**

**a)**

**$n_A$=5*11，Φ(n)=4*10=40**

**$d_A=27^{-1}$ mod 40=3　（2 分）**

**$n_B$=5*13=65，Φ(n)=4*12=48**

**$d_B=11^{-1}$ mod 48=35　（2 分）**

**b)**

**发送密文 $C=2^{11}$mod65=33　（2 分）**

**c）**

**明文 $m=7^3$mod 55=13　（2 分）**

**用 Bob 的公钥验证签名 $2^{11}$ mod 65=33**

**签名验证不通过　（2 分）**

15. 分组密码算法可用于构造 Hash 函数。假设有一个分组密码算法 E(k,m)，分组长度为 n 比特，密文不扩展，我们可以如下构造一个 Hash 函数：将消息分组为 $M_1, M_2, \cdots, M_m$，采用 CBC 模式加密，即 $H_i=E(k, H_{i-1} \oplus M_i)$，$H_0$ 是 n 比特全零分组，$H_m$ 为最终的散列函数结果，

k 是一个公开的常数。但这样构造的 Hash 函数是不抗碰撞的。

a) 给出一种基于生日悖论的复杂度为 $2^{n/2}$ 的构造强碰撞的方法

b) 给出一种基于生日悖论的复杂度为 $2^{n/2}$ 的构造弱碰撞的方法

c) 给出一种不基于生日悖论的复杂度为 1 的构造弱碰撞的方法 （20 分）

**答：**

**a)**

**构造消息 $P_1,P_2,\cdots P_{m-1}$ 和 $Q_1,Q_2,\cdots,Q_{m-1}$，**

**构造 $2^{n/2}$ 个随机分组 $P_m$ 和 $2^{n/2}$ 个随机分组 $Q_m$**

**根据生日悖论，存在一对 $P_m$ 和 $Q_m$ 使得 $H_m(P)=H_m(Q)$的概率为 50%**

**强碰撞的消息为 $P_1,P_2,\cdots P_m$ 和 $Q_1,Q_2,\cdots,Q_m$ （7 分）**

**b）**

**已知消息 $M_1,M_2,\cdots M_m$ 和构造消息 $Q_1,Q_2,\cdots,Q_{m-2}$，计算 $H_{m-2}(Q)$**

**构造 $2^{n/2}$ 个随机分组 X 和 $2^{n/2}$ 个随机分组 Y**

**分别计算 $E(k,H_{m-2}\oplus X)$和 $D(k,H_m)\oplus Y$**

**根据生日悖论，存在一对 X 和 Y 使得 $E(k,H_{m-2}\oplus X)= D(k,H_m)\oplus Y$ 的概率为 50%**

**弱碰撞的消息为 $Q_1,Q_2,\cdots,Q_{m-2},X,Y$ （7 分）**

**c)**

**已知消息 $M_1,M_2,\cdots M_m$ 和构造消息 $Q_1,Q_2,\cdots,Q_{m-1}$，计算 $H_{m-1}(Q)$**

**计算 $H_{m-1}(M)\oplus M_m$ 和 $H_{m-1}(Q)$**

**令 $Q_m=H_{m-1}(M)\oplus M_m\oplus H_{m-1}(Q)$**

**则 $E(k,H_{m-1}(Q)\oplus Q_m)=E(k,H_{m-1}(M)\oplus M_m)=H_m$，即可使得散列值相同**

**弱碰撞的消息为 $Q_1,Q_2,\cdots,Q_m$ (6 分)**

装订线 答题时不要超过此线

# 中 国 科 学 技 术 大 学
## 2019--2020 学年第 1 学期考试试卷标准答案 A 卷

考试科目: 密码学导论　　得分:_____

学生所在院系:_____ 姓名:_____ 学号:_____

### 一、单项选择题 （18 分）

1. 下列哪一个性质不属于密码学关注的范畴？（ **D** ）
   A. 保密性　　B. 完整性　　C. 访问控制　　D. 可视性

2. AES 的密钥长度不能选择下面哪一个？（ **A** ）
   A. 512 比特　　B. 256 比特　　C. 192 比特　　D. 128 比特

3. 采用公开密钥加密体制，用私钥对数据进行加密运算，可以提供哪些安全服务？（ **C** ）
   A. 数据保密性、来源认证　　B. 来源认证、隐私保护
   C. 不可否认、完整性保护　　D. 来源认证、访问控制

4. 关于 Feistel 框架，描述不正确的是？（ **D** ）
   A. 框架采用了 S-P 迭代结构
   B. 从安全角度，轮函数可以采用散列函数
   C. 从可解密角度，轮函数可以取消
   D. 解密过程与加密过程完全一致

5. 以下哪一个不是用于序列加密的伪随机数必须具有的性质？（ **B** ）
   A. 不可预测性　　B. 不可重复性　　C. 分布一致性　　D. 统计独立性

6. 采用拉格朗日插值多项式实现（t,n）秘密分享门限方案，当设定为由 9 个用户中的 3 个协作可重建秘密时，多项式的次数应当为（ **A** ）
   A. 2　　B. 3　　C. 8　　D. 9

### 二、填空题 （14 分）

7. DSA 是 **数字签名** 算法，RC4 是 **序列密码** 算法，RC5 是 **分组密码** 算法，RIPEMD 是 **散列** 算法，SMS4 是 **分组密码** 算法（填分组密码，序列密码，散列，或数字签名）

8. SHA-1 标准的分块大小为 512 比特，包括 4 轮运算，每轮 20 步，输出摘要长度是 **160** 比特，抗强碰撞的能力是 2 的 **80** 次方；SHA-256 标准输出的摘要长度是 **256** 比特，抗强碰撞的能力是 2 的 **128** 次方。

9. 对于具有良好雪崩效应的密码算法，字符频率统计攻击 **无效** （有效/无效）。这是因为 **良好雪崩效应意味着具有良好的扩散和混淆性，无法对密文字符进行切分和独立统计** 。

10. n 级最长 LFSR 包含 **n** 个延迟存储单元，输出比特序列的周期是 **2^n-1** 。在一个周期内，长为 k（k≤n-2）的 0 游程最多有 **2^(n-k-2)** 个。

## 三、问答与计算题

11. 请从密码系统的概率模型角度，简要说明“敌人了解系统”是指什么？什么是无条件安全，什么是实际安全？ （8 分）

**答：**

**“敌人了解系统”是指攻击者知道明文集合、密文集合、密钥集合、加密和解密映射，以及它们的先验概率，和实际的密文。 （2 分）**

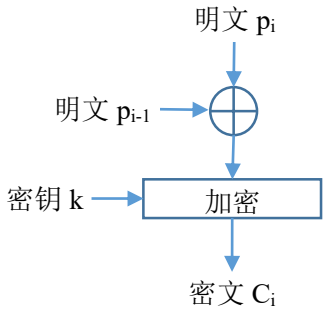
**无条件安全是指获得任意长度密文，两个（或以上）的明文或密钥的后验概率不为零（或模糊度不为零）。 （3 分）**

**实际安全是指虽然某个明文或密钥的后验概率可以降为零，但达到此目标所需的密文长度、计算量或计算时间足够大（或唯一解距离足够大，工作特性足够大）。 （3 分）**

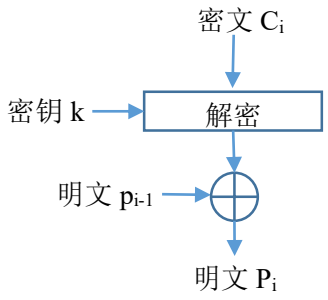
12. 分组密码的明文分组链接模式与标准 CBC 模式相似，区别仅在于它链接的是前一个分组的明文，而不是密文。请（1）画出明文分组链接模式的加密和解密框图；（2）若某个密文分组在传输中发生错误（即 0 或 1 发生翻转），分析错误扩散情况；（3）分析明文分组链接模式的优缺点。 （10 分）

**答：**

**（1）**




加密




解密

**（6 分）**

**（2） 密文错误将扩散，导致后面所有分组无法正确解密。 （2 分）**

**（3） 优点是明文异或后可以并行加密运算。缺点是错误扩散太严重。 （2 分）**

***以其它合理的优缺点作答的，可以酌情得分。***

13. 线性同余生成器 $X_n=(aX_{n-1} + b) \bmod M$ （$0 \le a,b < M$）是一种具有良好统计特性的序列发生器，常用来生成用于仿真目的的伪随机数序列，但它的安全性很差。通过观察某个发生器的输出，发现它输出的数字均小于 99，且序列的前 3 个数字是 “15，75，93”。求：（1）系数 a 和 b；（2）输出序列的周期。 （12 分）

**答：**

**（1）**

**M=99 （1 分）**

**15a+b=75 mod 99 (1)**

**75a+b=93 mod 99 (2) （2 分）**

**两式相减，得 60a =18 mod 99**

**20a=6 mod 33 （1 分）**

**a=30+33t (t=0,1,2) （即 a=30, 63, 96） （3 分）**

**b=75-15(30+33t) = 21 （3 分）**

**（2）**

**$X_n=(30+33t)X_{n-1}+21 \bmod 99$**

**注意到 $X_n$ 都是 3 的倍数，33t 项可去掉。整理得 $X_n+69=30(X_{n-1}+69) \bmod 99$**

**令 $Y_n=X_n+69$**

**$Y_n=30Y_{n-1}=30^{n-1}Y_1 \bmod 99$**

**$Y_n=3^{n-1}Y_1 \bmod 9$ 且 $Y_n=8^{n-1}Y_1 \bmod 11$**

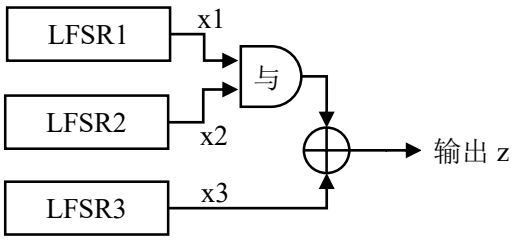
**$Y_n=3^n*2 \bmod 9$ 且 $Y_n=4*8^{n-1} \bmod 11$**

**第一式除 n=1 时 $Y_1=2 \bmod 9$ 外，均为 $Y_n=0 \bmod 9$，周期为 1**

**第二式可验证 8 是模 11 的生成元，周期为 10**

**因此 $X_n$ 从第二个数字开始形成周期，周期为 10**

14. 考虑如右图的非线性组合生成器，它的输出是 z 序列，三个 LFSR 的输出分别是 x1,x2,x3 序列。z 序列是将 x1 和 x2 相与后，再与 x3 异或得到。问：（1）各 LFSR 的输出泄露到 z 的概率是多大？（2）如何进行相关攻击？（3）假定各 LFSR 都是长度为 L 的最长线性反馈移位寄存器，则相关攻击的穷举工作量是多少？ （14 分）




**答：**

**（1）**

**P(L1 泄露) = P(z=x1)**

**= P(x3=0)*(P(x2=1)+P(x2=0)*P(x1=0))+P(x3=1)*(P(x1=1)*(P(x2=0))**

**=0.5*(0.5+0.5*0.5)+0.5*(0.5*0.5)=0.5 没有泄露 （2 分）**

**P(L2 泄露) = P(L1 泄露) = 0.5 没有泄露 （2 分）**

**P(L3 泄露) = P(z=x3)**

**= P(x1=0)*P(x2=1)+P(x1=0)*P(x2=0)+P(x1=1)*P(x2=0)**

**=0.5*0.5+0.5*0.5+0.5*0.5=0.75 （2 分）**

**但应注意到，P(z=x1 | x3=0)=0.75, P(z≠x1 | x3=1)=0.75，x2 类似。故当 LFSR3 被攻破后，LFSR1 和 LFSR2 都有 75%的概率被泄露出去。 （2 分）**

**（2）**

**首先穷举 LFSR3 的初始状态，当 x3 与 z 相同（碰撞）的比特数占 75&时，即获得了 LFSR3 的初始状态。 （2 分）**

**将 x3=1 所对应的 z 中比特取反，然后分别穷举 LFSR1 和 LFSR2 的初始状态，使之与修改后的 z 有 75%碰撞，即可得到 LFSR1 和 LFSR2 的初始状态。 （2 分）**

***若第（1）问中未发现 LFSR1 和 LFSR2 的泄露，则本问答 LFSR1 和 LFSR2 进行了联合的穷举可以得分。***

**（3）**

**穷举工作量为 3*2^L（答 2^L 不扣分） （2 分）**

***若第（1）问中未发现 LFSR1 和 LFSR2 的泄露，且第（2）问对 LFSR1 和 LFSR2 进行了联合的穷举，则本问答 2^L+2^2L 或 2^2L 可以得分。***

15. Alice 和 Bob 使用 ElGamal 算法实现保密和签名。已知公共大素数 P=23，本原元素 α=5。已知 Alice 的私钥 $X_A=5$，Bob 的私钥 $X_B=6$。

（1）计算 Alice 和 Bob 的公钥 $Y_A$ 和 $Y_B$。

（2）若 Alice 欲将消息 m=2 加密发送给 Bob，她选择的随机数 k=3，求密文数据。

（3）若 Alice 欲将消息 m=2 签名发送给 Bob，她选择的随机数 k=3，求签名数据。

（4）若 Carol 对消息 m=2 的签名为（4,16），且她选择的随机数 k=4 发生泄露，求 Carol 的私钥。　（14 分）

**答：**

**（1）**

**$Y_A$=5^5 mod 23=20　（2 分）**

**$Y_B$=5^6 mod 23=8　（2 分）**

**（2）**

**K=8^3 mod 23=6　（1 分）**

**C1=5^3 mod 23=10　（1 分）**

**C2=2*6 mod 23=12　（1 分）**

**Alice 发送密文（10，12）　（1 分）**

**（3）**

**r=5^3 mod 23=10　（1 分）**

**解 2=(5*10+3s) mod 22 得 s=6　（2 分）**

**签名为（10，6）　（1 分）**

**（4）**

**解 2=($X_C$*4+4*16) mod 22 得 $X_C$=1（舍去）或 12　(2 分)**

16. Alice 有 N 个秘密，她想将其中一个传给 Bob。Bob 只能获得一个秘密，但不能选择是哪一个秘密。除 Bob 外，包括 Alice 在内的任何人都不知道 Bob 获得了什么秘密。请设计一个完成该任务的协议，并分析该协议的安全假设和所用到密码算法的约束。（说明：你无需默写课堂介绍的协议。可以自行设计并分析）　（10 分）

**答：**

**协议如下：**

**（1）Alice 产生一对公钥 e/私钥 d，N 个随机数 $X_i$，将公钥 e 和所有随机数 $X_i$ 发给 Bob；**

**（2）Bob 选择一个对称密码算法 E 的密钥 k，用公钥加密 k 后，再用 $X_i$ 盲化，计算 $V=X_i+PU(e, k)$发给 Alice；**

**（3）Alice 分别用 $X_i$ 去盲化后，用私钥解密得到 N 个随机数（其中一个等于 k）$k_i=PR(d, V-X_i)$；**

**（4）Alice 分别用每个 $k_i$ 去加密她的每个秘密 $M_i$，$C_i=E(k_i, M_i)$，将密文发给 Bob；**

**（5）Bob 用 k 解密每份密文，有意义的那一份明文就是他获得的秘密**

**安全假设是 Alice 必须忠实执行她的任务，否则很容易欺骗 Bob（例如，在第 4 步加密的是同一个秘密）**

**该协议对公钥算法和对称密码算法没有特殊约束，可以抵抗唯密文攻击就行。**

***协议设计合理，关键的安全假设和约束列出即可得分。***

# 中 国 科 学 技 术 大 学
## 2019--2020 学年第 2 学期考试试卷 A 卷

考试科目: 密码学导论　　得分:_____

学生所在院系:_____ 姓名:_____ 学号:_____

**一、单项选择题 （15 分）**

1. 用于身份认证的哈希函数必须具备下列（　　）性质。

   A. 单向性　　B. 抗弱碰撞

   C. 抗强碰撞　　D. 以上全部

2. 关于 RSA 算法，下列说法正确的是（　　）。

   A. RSA 属于分组密码

   B. RSA 可以使用一对足够大的素数 p 和 q 来为所有人建立共同的公共模数 n=pq

   C. RSA 可以设置较小的私钥，例如 65537，以方便自己解密运算和签名运算

   D. RSA 名称的含义是分别以 R、S 字母开头的两个人设计的 Algorithm

3. Alice 和 Bob 拥有一对对称密钥，下列说法正确的是（　　）。

   A. 若 Bob 收到该密钥加密的一段消息，则可确认该消息是 Alice 加密的

   B. 若 Bob 收到该密钥加密的一段消息，则可确认发信方是 Alice

   C. Alice 能够否认自己发送过的加密消息

   D. Alice 可以将时间戳与明文一同加密，来作为时间证据

**线 答题时不要超过此线**

4. 根据密码分析者所掌握的信息多少，可将密码分析分为：唯密文攻击、已知明文攻击、选择明文攻击和（　　）。

   A. 已知密文攻击

   B. 选择密文攻击

   C. 猜测部分明文攻击

   D. 猜测部分密钥攻击

5. 下面关于数字签名（私钥未丢失）的描述**不正确**的是（　　）。

   A. 数字签名是不可抵赖的　　B. 数字签名是不可伪造的

   C. 数字签名是不可替换的　　D. 被签名文件是不可更改的

**二、填空题 （15 分）**

6. 分组密码的计数器工作模式英文缩写为_____，它_____（支持/不支持）预处理和并行处理，_____（支持/不支持）分组的随机加密或解密，_____（存在/不存在）错误传播。

7. 密码学意义安全的伪随机序列生成器应能通过多项式时间统计测试和续位测试。多项式时间统计测试是指，任何_____算法均不能以大于 1/2 的概率正确区分该生成器的输出序列和一个同等长度的_____序列；续位测试是指不存在_____算法，能够根据_____以大于 1/2 的概率有效预测下一个比特。

8. RSA 算法依赖的数学难题是_____， ElGamal 算法依赖的数学难题是_____， ECC 算法依赖的数学难题是_____，Diffie-Hellman 协议依赖的数学难题是_____。

9. 密码协议中常用的 nonce 有_____、_____、_____。

## 三、问答与计算题

10. 什么是密钥的唯一解距离？什么是消息的唯一解距离？一般而言，二者谁更大？当恰好满足消息的唯一解距离要求时，密钥被破译的概率是否大于 50%？为什么？ （10 分）

11. 为抵抗选择明文攻击，有人提出这样一个方案：先用算法 H 对明文计算摘要，然后用算法 F 将摘要与密钥 K 进行运算，得到一个新的密钥，用新密钥加密明文。当然，摘要算法 H、算法 F 以及加密算法 E 都是公开的。请问：
（1）若要使该方案可行，假设明文为 M，写出加密方发送给解密方的数据。
（2）该方案与二战时期德国使用 Enigma 的哪个操作过程有异曲同工之处？
（3）请设计一个比题中方案效率更高的方法来达到同样的效果。
本题解答时不应引入 H、F、E 之外的运算。（10 分）

12. 加密和签名是两种重要的安全机制，在应用中可以先加密后签名，也可以先签名后加密。试举例分析这两种不同的顺序各有什么便利和局限？（10 分）

13. 某 RSA 系统中，密钥管理中心为用户 A 和用户 B 分配了相同的模数 n=77。已知用户 A 的公钥 $e_A$=5，用户 B 的公钥 $e_B$=7。攻击者从某个途径获知：有人向用户 A 和用户 B 分别加密传输了同一个消息 m，给用户 A 的密文 $c_A$=10，给用户 B 的密文 $c_B$=68。试破解消息 m。注意，你不能对模数分解质因数，因而也无法求解两个用户的私钥。当然，你也不可以靠猜测。（15 分）

14. 在 ElGamal 系统中，取本原元 α=7，模数 p=13，Alice 的私钥 xa=4, Bob 的私钥 xb=11
（1）假定 Alice 加密传送 m=4 给 Bob，随机选择 k=7，密文是什么？
（2）如果 Alice 要签名 m=8，随机选择 k=5，签名是什么？随机选择 k=7，签名是什么?
（3）如果消息 m=5 附加的签名值是(2,4)，Bob 如何验证？（15 分）

15. 结合以下密钥分配协议，说明已过期的旧密钥为何必须妥善销毁？如何修改此协议以避免这种威胁？（10 分）

A→KDC: $ID_A \| ID_B \| N_1$

KDC→A: $E(K_A, K_S \| ID_A \| ID_B \| N_1) \| E(K_B, K_S \| ID_A)$

A→B: $E(K_B, K_S \| ID_A)$

B→A: $E(K_S, N_2)$

A→B: $E(K_S, f(N_2))$