2018-2019 学年第二学期期末考试

《应用密码学》试卷（B）答案与评分标准

题号	一	二	三	四	五	六	总分
得分							

姓名：_____ 线 订 装 学号：_____ 班级：_____

得分	

一、判断题（共 10 分，每题 2 分。正确填写 T, 错误填写 F）

1．17≡-3(mod11) （ F ）

2．{13,-6,-3,6,15}是整数模 5(或称 mod 5)的一个完全剩余系 （ T ）

3．设 a,b,c 是整数，若 a|c 且 b|c，则 ab|c （ F ）

4．设 a 是整数，若 12|a^2，则 12|a， （ F ）

5. 若 x 为奇数，则 $x^2 \equiv 1 \pmod 8$ （ T ）

得分	

二、填空（共 20 分，每题 2 分）

1. 移位密码中，若明文 b 被加密成 H。那么，密文 MXUAV 所对应的明文为 group

2. 仿射密码中，若密钥为： a=3，b=19，那么明文 8 对应的密文是 17

3. 在 DES 加密方案中，若替换盒 S_1 的输入为 x=000000, 则其输出 $S_1(x)$ = 1100/12 ；若替换盒 S_4 的输入是 x=111111，则其输出 $S_2(x)$ = 1001/9

4. DES 中，每一轮迭代中的分组大小为 64 比特，总共有 16 轮。

5. 利用费马小定理计算：5^{50} mod17= 8；2^{131} mod11= 2。

6. 同时满足 x=2 mod5 且 x=3 mod7 的解是 x= 17 mod 35。

7. RSA 方案的安全性基于 大整数分解 困难问题假设，

8. ElGamal 方案的安全性则基于 离散对数 困难问题假设.

9. 根据 Shannon 的理论，强对称密码算法的两个基本设计原则是 扩散 、混淆 .

10．密码技术的分类有很多种，根据加密和解密所使用的密钥是否相同，可以将加密算法分为： 对称 密码和 非对称 密码。

得分	

~~三、名词解释（共 10 分，每小题 5 分。）~~

1．无条件安全

如果从信息论的角度能够证明一个密码体制中的密文不会泄露明文的任何信息，则即使在攻击者/敌手拥有无限计算资源的情况下，它也不能被破译。我们称它是无条件安全的，或者信息理论上绝对安全的。

2．公钥证书

由证书权威中心 CA （certificate authority）向用户颁发的、用于其他用户通过验证 CA 的签名，提取证书主人的真实、有效公钥的一种证书。

四、计算题（共 40 分，每小题 10 分）

得分	

1. 利用欧几里得算法求 gcd (51,79)

79=1*51+28
51=1*28+23
28=1*23+5
23=4*5+3
5=1*3+2
3=1*2+1
2=2*1+0

--------8 分

gcd (51,79)=1

--------2 分

2. 利用扩展欧几里得算法计算 17^{-1} mod 47

47=2*17+13　　q_1=2
17=1*13+4　　q_2=1
13=3*4+1　　q_3=3

--------5 分

t_0=0，t_1=1
t_2= t_0 - t_1*q_1= 0-1*2=-2
t_3= t_1 – t_2*q_2= 1-(-2)*1=3
t_4= t_0 - t_1*q_1= 0-1*2=-2-3*3=-11

17^{-1} mod 47=-11=36 mod47

--------5 分

3. 在 RSA 方案在，假定秘密素数 p=5， q=11, 加密指数 e=23, 密文为 c=4, 首先计算私钥 d, 然后再计算 c 解密后的明文 m (要求利用平方乘算法计算模幂)

N=p*q=55, φ(N)=(p-1)*(q-1)=(5-1)*(11-1)=40
d=e^{-1} mod 40= 3^{-1} mod 40　　------2 分

40=1*23+17　　q_1 =1
23=1*17+6　　q_2=1

17=2*6+5　　$q_3=2$

6=1*5+1　　$q_4=1$

$t_1=0, t_1=1$

$t_2= t_0 - t_1 * q_1 =-1$

$t_3= t_1 – t_2 * q_2 =2$

$t_4= t_2 – t_3 * q_3 =-5$

$t_5= t_3 – t_4 * q_4 =7$

$d=23^{-1} \bmod 40=7 \bmod 40$

d=7　　------3 分

根据 RSA 解密规则，　$m=c^d \bmod N=4^7 \bmod 55$　　----------1 分

$7=(111)_2 = h_2\ h_1 h_0$

利用平方乘算法求解，t=2, r=c=4

(1) i=1, $r=r^2 = 16 \bmod 55$

$h_i=h_1=1$, $r=r*x=16*4=64=9 \bmod 55$

(2) i=0, $r=r^2 =81=26 \bmod 55$

$h_i=h_0=1$, $r=r*x=26*4=104=49 \bmod 55$

m=49

------4 分

4. 在 Diffie-Hellman 密钥交换协议中, p=29, α=2, Alice 选取的临时私钥为 a=7 ，Bob 选取的临时私钥为 b=10, 计算双方的共享密钥

$A=\alpha^a \bmod p= 2^7 \bmod 29 =12$　　------3 分

$B=\alpha^b \bmod p= 2^{10} \bmod 29 =9$　　------3 分

$K= B^a \bmod p= 9^7 \bmod 29= 28$　　------4 分

五、简答题（共 20 分，每小题 10 分）

1. 简述哈希函数的属性以及作用

任意的消息大小：　对任意大小的消息适用

固定的输出长度：生成的哈希值的长度是固定的、

有效性：计算相对简单有效

抗第一原像性：给定一个输出 z，找到满足 h(x)=z 的输入 x 是不可能的

抗第二原像性：给定一个 x_1 和 $h(x_1)$，找到满足 $h(x_1)= h(x_2)$的 x_2 在计算上不可能的

抗冲突性：找到满足 $h(x_1)= h(x_2)$的一对 x_1 和 x_2 且不等，在计算上不可行的

------6 分

作用：应用于数字签名，解决高计算负载，消息开销和安全性限制等问题；还可与对称密钥相结合，产生消息验证码，验证消息的完整性和消息源认证。------4 分

2. 简述序列密码与分组密码之间的联系与区别。

1）两者之间的联系 ------5 分

流密码:M 代表明文。流密码把 M 拆分成比特为单位的 M1,M2````MI,`````, 并用密钥流 K=K1K2```KI 中的第 i 个成分 Ki 对明文流中的第 i 个成分 Mi 进行加密，即 Ek（M）=Eki（Mi）=Ek2（M2）••• Eki（Mi）••••。如果 T 个比特后密钥序列重复，那么为周期流密码，否则就是非周期。

而分组密码是把 M 拆分成 Mi 块状，单位待定。用的是同一个密钥 K 对每个分组进行加密，分组的长度也不确定。

周期为 T 的流密码，令 K=K1K2 •••KT，这类密码可以看作是分组密码，这里的每个 Mi 都是具有 T 个比特的一个分组。T 越小，越像分组密码，T 越大则越像流密码。

2）二者之间的区别 ------5 分

分组密码每次只能处理一个固定长度的明文，不足还需要补全，分组密码的体制一般首先将 M‘进行填充得到消息 M，使其长度为固定分组长度 L 的整数倍。而流密码加密时不一定得到相同的密码，因为明文的重复部分是使用密钥流的不同部分加密的。对于分组密码，在一个固定的密钥的作用下，对相同的明文加密，一定能得到相同的密文。