2018-2019 学年第二学期期末考试

《应用密码学》试卷答案与评分标准（A）

题号	一	二	三	四	五	六	总分
得分							

姓名：　　线　　装　　订　　学号：　　班级：

得分	

一、判断题（共 10 分，每题 2 分）

1．77≡7 (mod 7)　　（ T ）

2．{13,-6,-3,7,15}是整数模 5 (或称 mod 5)的一个完全剩余系　　（ F ）

3．若 a 是整数，7|a^2，则 7|a　　（ T ）

4．若 a,b,c 是整数，ab|c, 则 a|c　　（ F ）

5. 若 c 与 m 互素，则 a ≡b(mod m)等价于 ac ≡bc(mod m)。　　（ T ）

二、填空（共 20 分，每题 2 分）

1．基本的安全服务包括：保密性、完整性、消息验证、不可否认性

2．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（或公钥）密码。

3. 对称密码体制可分为两类，按比特逐位加密的序列密码和按固定数据块大小加密的分组密码

4. 古典密码学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：置换和代换（替换）仍是构造现代对称分组密码的核心方式。

5. 移位密码中，若明文 e 被加密成 O。那么，密文 WYXNKI 所对应的明文为 monday

6. 仿射密码中，若密钥为： a=5，b=10，那么明文 7 对应的密文是 19

7. 利用费马小定理计算：8^{48} mod13= 1 ; 4^{131} mod17= 13 ;

8. 在 DES 加密方案中，若替换盒 S_1 的输入为 x=111111, 则其输出 $S_1(x)$ = 13 (或 1101) ;若替换盒 S_4 的输入是 x=000000，则其输出 $S_4(x)$ = 07(或 0111)

9. DES 中，每一轮迭代中的分组大小为 64 比特，总共有 16 轮。

10.能够被证明绝对安全的密码是一次一密（或 one time pad）.

~~三、名词解释（共 10 分，每小题 5 分。）~~

得分	

1．科克霍夫准则（Kerckhoff's Principle）。

即使除密钥外的整个系统的一切都是公开的，这个密码体制也必须是安全的。尤其是即使攻击者知道整个系统的加密算法和解密算法，此系统也必须是安全的。

2．公钥基础设施（ PKI）

认证中心(CA)形成的整个实体系统与所需的支持机制一起形成了公钥基础结构，也称为 PKI

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 (48,67)

67=1*48+19

48=2*19+10

19=1*10+9

10=1*9+1

9=9*1+0

--------8 分

gcd (48,67)=1

----------2 分

2. 利用扩展欧几里得算法计算 $17^{-1} \bmod 40$

40=2*17+6 $q_1=2$

17=2*6+5 $q_2=2$

6=1*5+1 $q_3=1$

--------5 分

$t_1=0, t_1=1$

$t_2= t_0 - t_1 * q_1 =-2$

$t_3= t_1 - t_2 * q_2 =5$

$t_4= t_2 - t_3 * q_3 =-7$

$17^{-1} \bmod 40=-7 \bmod 40 =33$

--------5 分

3. 在 RSA 方案在，假定秘密素数 p=5， q=11, 加密指数 e=7, 密文为 c=3, 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

$d=e^{-1} \bmod 40= 7^{-1} \bmod 40$ ------2 分

40=5*7+5 $q_1=5$

$7=1*5+2$ $q_2=1$

$5=2*2+1$ $q_3=2$

$t_1=0, t_1=1$

$t_2= t_0 - t_1 * q_1 = -5$

$t_3= t_1 - t_2 * q_2 = 6$

$t_4= t_2 - t_3 * q_3 = -17$

$d=7^{-1} \bmod 40 = -17 \bmod 40 = 23$

$d=23$ ------3 分

根据 RSA 解密规则， $m=c^d \bmod N=3^{23} \bmod 55$ ----------1 分

$23=(10111)_2=h_4\ h_3\ h_2\ h_1 h_0$

利用平方乘算法求解，t=4, r=x=3

(1)i=3, $r=r^2=9 \bmod 55$

$h_3=0$

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

$h_2=1$, $r=r*x=26*3=78=23 \bmod 55$

(3)i=1, $r=r^2=23\text{^}2=529=34 \bmod 55$

$h_1=1$, $r=r*x=47 \bmod 55$

(4)i=0, $r=r^2=9 \bmod 55$

$h_0=1$, $r=r*x=27$

$m=27$ -------4 分

4. 在 Diffie-Hellman 密钥交换协议中, p=31, α=3, Alice 选取的临时私钥为 a=8 ，Bob 选取的临时私钥为 b=11, 计算双方的共享密钥

$A=\alpha^a \bmod p= 3^8 \bmod 31 = 20$ ------3 分

$B=\alpha^b \bmod p= 3^{11} \bmod 31 = 13$ ------3 分

$K= B^a \bmod p= 13^8 \bmod 31= 7$ ------4 分

五、简答题（共 20 分，每小题 10 分）

1. 对称与非对称密码的区别与联系有哪些?

对称密码是指双方共享一个密钥，并使用相同的加密方法和解密方法。

非对称密码是指双方使用不同的密钥：一个公钥和一个私钥。---4 分

对称加密算法的优点：加密安全快速，密钥短。

存在一些缺点：无法解决密钥分配问题，密钥个数多，对对方的欺骗没有防御机制。

非对称密码的优点：可以解决密钥分配问题，能够提供消息验证，完整性和不可否认等安全性

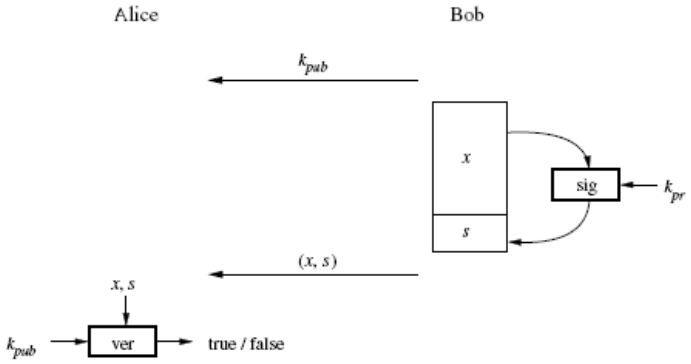
---4 分

非对称密码的缺点：加密速度慢，密钥长。

联系：在安全系统中，常常同时需要对称密码和非对称密码算法，两者相结合使用，可以有效的解决安全问题。---2 分

2. 简述数字签名的基本原理与作用

数字签名的基本思想是：对消息签名的一方使用私钥，接收者则使用对应的公钥（3 分）。数字签名方案的基本思想如下图



这个过程从 Bob 对消息 x 进行签名开始，而签名算法是 bob 的私钥的一个函数。因此假设 bob 的私钥是保密的，只有他本人才能对消息 x 进行签名。为了将一个签名与一个消息对应，x 也必须是数字签名的一个输入，Bob 对消息进行签名后，将得到的签名 s 附加到消息 x 之后,并将得到的（x,s）对发送给 Alice, .Alice 通过 Bob 的公钥进行验证签名是否是 Bob 的有效签名。------4 分

签名的作用：可以提供消息验证，不可否认性和消息完整性。------3 分