文盛教育 2023 年计算机科学与技术专业冲刺预测

信息安全 模拟试卷（四）答案

一、选择题（每题 2 分，共 20 分）

DDBAA CDADD

二、判断题（每题 2 分，共 20 分）

FFFTF TTFTT

三、简单题（每题 10 分，共 20 分）

1.什么是防火墙，从实现形式上看分为哪些种类？从技术的角度，其功能有哪些？

1)防火墙是位于两个(或多个)网络间，实施访问控制策略的一个或一组组件集合。

2)从实现方式上来看，防火墙分为俩种：硬件防火墙和软件防火墙。

3)防火墙的功能(技术角度)：网络安全的屏障，可以强化网络安全策略，对网络存取和访问进行监控和审计，防止内部信息外泄。VPN

2.DES 加密的基本步骤是什么？

1）对 64 位明文进行 IP 置换，分为 L0 和 R0 两部分

2）密钥置换，去掉每个字节奇偶校验位，得到 56 位密钥

3）密钥的压缩置换，得到 48 位子密钥

4）对 R0 做 E 扩展置换，得到 48 位输出

5）S 盒替换，从 48 位输入到 32 位输出

6）P 盒置换。对 S 盒输出的 32 位做换位操作

7）P 盒置换的结果与最初的 64 位分组左半部分 L0 异或，然后左、右半部分交换，接着开始下一轮

8）末置换。经过上述 16 轮迭代，最后一轮后，左、右两半部分并未进行交换，而是两部分合并形成一个分组做为末置换的输入，进行 1）的逆置换。得到密文

四、计算题（其中第 1、2 题 5 分，第 3、4、5 题各 10 分，共 40 分）

1.已知凯撒密码的秘钥 k=12，密文

C=HCKAPQEADCXY

求明文：

M= Vqyodesorqlm

2.使用矩阵排列的方法加密明文，秘钥：54213，明文：

I have to study hard after the examination

解： 5 4 2 1 3

I H A V E

T O S T U

D Y H A R

D A F T E

R T H E E

X A M I N

A T I O N

密文：VTATEIOASHFHMIEUREENNHOYATATITDDRXA

3.已知 playfair 密码的密钥：jump and laugh

明文：there are so many stars in the sky

求密文：

解：

key：jumpandlgh

1）密码矩阵：

I/J U M P A

N D L G H

B C E F K

O Q R S T

V W X Y Z

2）整理明文

th er ea re so ma ny st ar si nt he sk yx

3）求出密文

ZK RX KM XR TQ PI GV TO　MT OP HO　LK TF ZY

4.假定 DES 算法中 s 盒（S 盒表见教材）的输入为（AEF2101034BA）HS 盒数据参考教材（P143 页的八个盒子数据），P 盒置换表如下，求最终输出结果

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

解：

1）s 盒输入：

101011 101111 001000 010000 000100 000011 010010 111010

2）S 盒替换

s1(101011)= (9)=(1001)B

s2(101111)= (2)=(0010)B

s3(001000)= (6)=(0110)B

s4(010000)= (1)=(0001)B

s5(000100)= (4)=(0100)B

s6(000011)= (15)=(1111)B

s7(010010)= (12)=(1100)B

s8(111010)= (3)=(0011)B

按照给定的 P 盒置换表，得如下结果：

1	1	0	1	0	0	0	0
1	0	1	1	0	1	1	1
0	0	1	0	1	0	0	0
0	0	0	0	1	1	1	1

5.假定 RSA 算法中，取 p=11，q=17，加密密钥为 e=7 求加密和解密解密秘钥。如果用该密钥来做数据加密，明文 M=2,求密文

解：

1)n=p*q=187

2) φ (n)=(p-1)×(q-1)=16×10=160

3)取 e=7，满足 1<e<φ (n)，且 gcd(φ (n),e)=1。

4)确定满足 d ·e=1 mod 160 且小于 160 的 d，

5) 因为 7*23=161 而 161 mod 160=1 ，d=23

因此公钥为{7,187}，私钥为{23,187}。

$C=M^e \bmod 160=2^7 \bmod 160=128$