现代密码学

作业

第2次作业

1）给出仿射、单表代换、多表代换、置换及希尔密码体制的弱密钥；

2）令仿射密码的密钥k=(9,3), 且gcd(9,26)=1. 明文hot=(7,14,19)，求加解密过程。

3）用维吉尼亚密码加密明文“please keep this message in secret”，其中使用的密钥为“computer”，试求其密文。

4） 用Hill密码加密明文“hill”，使用的密钥是

$$k=\begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix}$$

第2次作业

5) 已知下列密文是通过维吉尼亚密码加密得来的，试求其明文。

“CHREE VOAHM AERAT BIAXX WTNXB EEOPH BSBQM QEQERBWRVX UOAKX AOSXX WEAHB WGJMM QMNKG RFVGX WTRZXWIAKL XFPSK AUTEM NDCMG TSXMX BTUIA DNGMG PSRELXNJEL XVRVP RTULH DNQWT WDTYG BPHXT FALJH ASVBFXNGLL CHRZB WELEK MSJIK NBHWR JGNMG JSGLX FEYPHAGNRB IEQJT AMRVL CRREM NDGLX RRIMG NSNRW CHRQHAEYEV TAQEB BIPEE WEVKA KOEWA DREMX MTBHH CHRTK DNVRZ CHRCL QOHPW QAIIW XNRMG WOIIF KEE”。

第2讲答案

（3）解：k=computer

明文每部分 7 个字母

pleaseke epthisme ssageins ecret

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q

对照维吉尼亚密码表得:

Rzqpmxov qgfwclqv ugmvybrj gqdtn

以上即密文

第2讲答案

(4)

明文 p=”hill”　k= { 8 6 9 5 }

6 9 5 10

5 8 4 9

10 6 11 4

P=(7,8,11,11)

C=p*k=(7,8,11,11)* { 8 6 9 5 }={ 9 }=j

6 9 5 10 8 i

5 8 4 9 8 i

10 6 11 4 24 y

所以加密的密文是 jiiy

第2讲答案

(5)

明文：

Chreevoahmaeratbiaxxwtnxbeeophbsbqmqeqerbwrvxuoakxaosxxweahbwgjmmqmnkgrfvgxwtrzx
wiaklxfpskautemndcmgtsxmxbtuiadngmgpsrelxnjelxvrvprtulhdnqwtwdtygbphxtfaljhasvbfxngllch
rzbwelekmsjiknbhwrjgnmgjsglxfeyphagnrbieqjtamrvlcrremndglxrrimgnsnrwchrqhaeyevtaqebbipe
ewevkakoewadremsmtbhhchrtkdnvrzchrclqohpwqaiiwxnrmgwoiifkee

观察 CHR 出现的地方

相对距离是 165,235,275,285　　gcd（165,235,275,285）=5

所以密钥长度可能是 5；

用重合指数法判断 密钥长度从 1 到 5 时在 5 的时候 IC 值估算为 0.067

所以密钥长度为 5；

利用拟重合指数测试法

$$A: p_0 = \frac{f_0}{n'}, B: p_1 = \frac{f_1}{n'}, \cdots, Z: p_{25} = \frac{f_{25}}{n'}$$

$$Correlation(P_i, Q) = \sum_{j=0}^{26} p_{(i+j) \bmod 26} \bullet q_j$$

分别在在循环计算程序中得出结果

第2讲答案

可知密钥在 9 的时候接近 0.065
同理可得之后密钥为 0　13 4　19
即 JANET
然后代入解密的
明文：
The almond tree was in tentative blossom the days were longer of ten ending with magnificent evenings of corrugated pink skies the hunting season was over with hounds and guns put away for six months the vine yards were busy again as the well organized farmers treated their vines and the more lackadaisical neighbors hurried to do the pruning they should have done in November.

第3讲作业

1 求冒泡排序法的计算复杂度, 该算法是否为多项式的?

2 超递增背包问题:

设A=(a_1,a_2,…,a_n)是由n个不同的正整数构成的n元组，且 $a_j > \sum_{i=1}^{j-1} a_i \quad j = 2,\cdots,n$

S是另一已知的正整数。

求A的子集A’，使 $\sum_{a_i \in A'} a_i = S$.

(1) 给出该问题的求解算法;

(2) 求算法的计算复杂度.

第3讲答案

（1）

冒泡排序

依次比较相邻的两个数，将大数放在前面，小数放在后面。

1）首先比较第 1 个和第 2 个数，将大数放前，小数放后。然后比较第 2 个数和第 3 个数，将大数放前，小数放后，如此继续，直至比较最后两个数，将大数放前，小数放后，此时第一趟结束，在最后的数必是所有数中的最小数。

2）重复以上过程，仍从第一对数开始比较（因为可能由于第 2 个数和第 3 个数的交换，使得第 1 个数不再大于第 2 个数），将大数放前，小数放后，一直比较到最小数前的一对相邻数，将大数放前，小数放后，第二趟结束，在倒数第二个数中得到一个新的最小数。如此下去，直至最终完成排序。

用二重循环实现，外循环变量设为 i，内循环变量设为 j。外循环重复 n 次，内循环依次重复 n-1，n-2，...，1 次。共循环 $n(n-1)/2$, 即复杂度为 $O(n^2)$次比较和交换操作。

（2）超递增背包：从 n 到 1，S 和 aj 一次比较，大于则减去 aj，xi=1；否则，xi=0 进行下次循环；复杂度 O（n）比较和减法操作。

第4讲作业

1. 证明3DES的穷举攻击复杂度为：Time=2^{118} , space ≈ 2^{56}
2. 如果16轮使用的子密钥K16＝K1，K15＝K2，…，K9＝K8, 则加密所用的子密钥与解密所用的子密钥相同, 对一个明文X加密两次,得到的还是明文X. 弱密钥的定义：若k使得加密函数与解密函数一致，则称k为弱密钥. 证明下列密钥为弱密钥（偶校验：就是让原有数据序列中（包括你要加上的一位）1的个数为偶数）：

   1) 0x0000000000000000　2) 0x1E1E1E1E 0F0F0F0F

   3) 0x E1E1E1E1F0F0F0F0　4) 0xFFFFFFFFFFFFFFFF

第4讲答案

（1）$c=E_{k3}(E_{k2}(E_{k1}(m)))$

All k_1 加密存储排序 $O(2^{56}\log(2^{56}))$；　对 all k_2k_3 解密，对比 $O(2^{112}\log(2^{56}))= O(2^{112}*2^6)$

（2）解：密钥经过 PC-1 置换，使得 C 和 D 寄存器中的数据为（0x0000000, 0x0000000）（0xFFFFFFF, 0x0000000）（0x0000000, 0xFFFFFFF）（0xFFFFFFF, 0xFFFFFFF）四种状态；每轮的密钥生成：为 C 和 D 分别的自循环移位，各选 24 比特，所以选出的密钥 K1=K2=K3=...=K16

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

2) 0x1E1E1E1E 0F0F0F0F →

0x 0001 1110　8　0001 1110　16　0001 1110　24　0001 1110　32

0000 1111　40　0000 1111　48　0000 1111　56　0000 1111　64

第4讲答案

（2） 计算 0x87 乘以 0x03 模 $m(x)=x^8+x^4+x^3+x+1$ 的值.

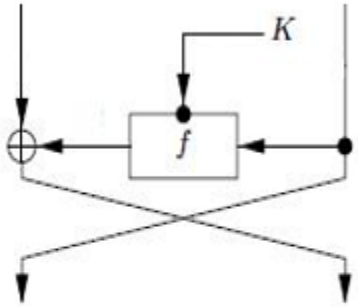
0x87: 1000 0111　　0x03:0x02 ^0x01

所以 1000 01110 ^ 10000111=110001001

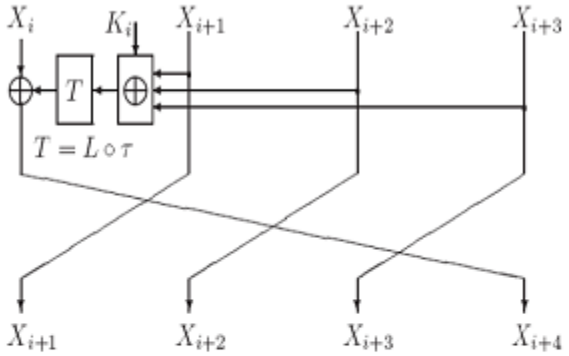
模 m：100011011

110001001 ^ 100011011=10010010: 0x92

(3)



1轮Feistel

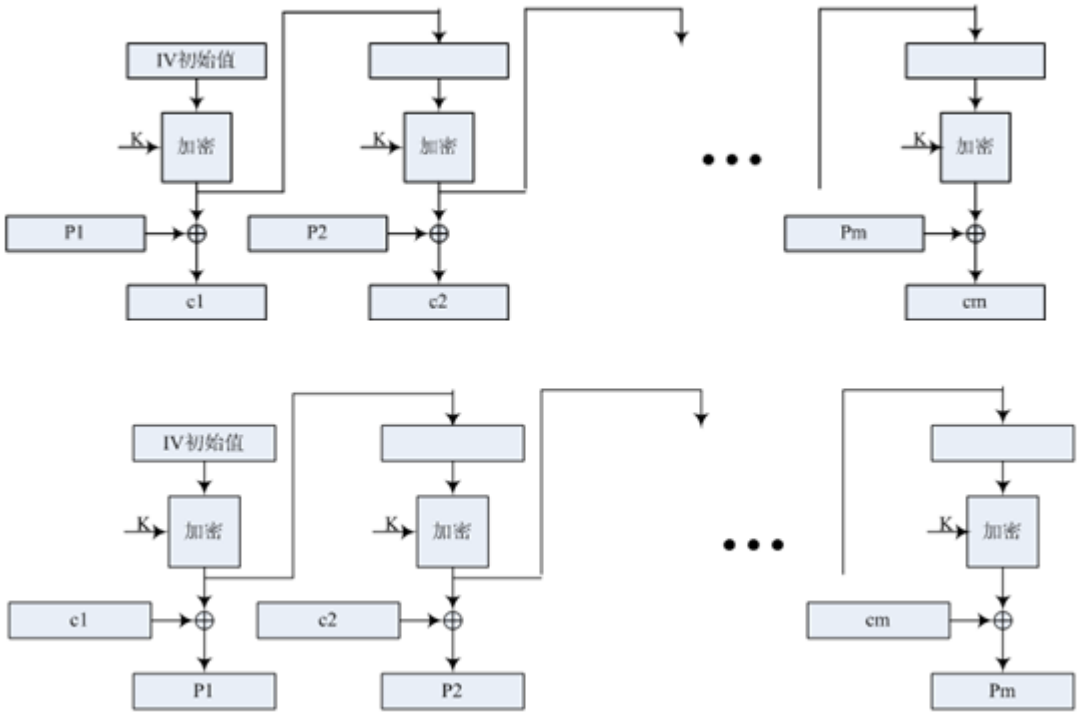


1轮SMS4

加解密和密钥编排步骤略

第4讲答案

(1)



第4讲答案

- 消息被看作比特流，无须分组填充.
- 只使用 DES 加密算法，且所有加密都使用同一密钥.
- 需要额外的初始向量，若初始向量公开，攻击者可以通过篡改，使所有明文解密错误.
- 密钥流可以在已知消息之前计算，不需要按顺序解密.
- 密钥相同时，明文中相同的 64 比特分组产生不相同的 64 比特密文块(与初始值相关).
- 不存在比特错误传播.
- 发送者和接收者必须保持同步.

CCM 略（AE 模式讲）

第5讲作业

1 设4级线性移位寄存器的反馈函数为 $f(b_4,b_3,b_2,b_1)=b_4\oplus b_1$，初始状态 $(b_4b_3b_2b_1)=(1000)$，写出该移位寄存器的输出.

2 设 $n=4$，$f(b_4,b_3,b_2,b_1)=b_4\oplus b_2b_3\oplus b_1\oplus 1$，初态为 $(b_4b_3b_2b_1)=(1011)$，试求此非线性移位寄存器的输出序列及周期.

3 设RC4每次输出的字符为0-3中的数，初始密钥为23，计算“ok”的加密过程.

4 试构造一个输出小m序列的5级LFSR。

第5讲答案

1、：

（01）1000 ⟹ 0
（02）1100 ⟹ 0
（03）1110 ⟹ 0
（04）1111 ⟹ 1
（05）0111 ⟹ 1
（06）1011 ⟹ 1
（07）0101 ⟹ 1
（08）1010 ⟹ 0
（09）1101 ⟹ 1
（10）0110 ⟹ 0
（11）0011 ⟹ 1
（12）1001 ⟹ 1
（13）0100 ⟹ 0
（14）0010 ⟹ 0
（15）0001 ⟹ 1
（16）1000 ⟹ 0

因此最终的输出是 0001111010110010，输出周期为 15 个拍子

2、：

（01）1011 ⟹ 1
（02）1101 ⟹ 1
（03）1110 ⟹ 0
（04）1111 ⟹ 1
（05）0111 ⟹ 1
（06）1011 ⟹ 1

因此最终的输出是 11011，输出周期为 5 个拍子

第5讲答案

(3)、

解：

依题意可得，使用 2 位的 RC4，其操作对 4 取模。初始数据表 S 只有 4 个元素，初始化为 S：

0	1	2	3

将初始密钥填入密钥数据表为 T：

1	2	3	1

利用下左程序可将 S 盒进行初始置换，过程如下右所示。

```
j=0;
for(i=0;i<4;i++)
{
        j=(j+s[i]+T[i])%4;
        temp=s[j];
        s[j]=s[i];
        s[i]=temp;
}
```

1	0	2	3

1	3	2	0

2	3	1	0

2	0	1	3

0, 1; 1,3; 2,0; 3,1

最终 S 表被随机化为：

2	0	1	3

第5讲答案

经过左下图程序，选取出密钥序列如右下图所示：输出的 k 值分别为：1，1，1，2，1

```
i=0;
j=0;
for(l=0;l<4;l++)
{
    i=(i+1)%4;
    j=(j+s[i])%4;
    swap(s[i],s[j]);
    t=(s[i]+s[j])%4;
    k=s[t];

}
```

2	0	1	3
0	1	2	3
0	1	3	2
3	1	0	2

转换成二进制序列为：　　0101011001

明文“OK”换成二进制序列为：0111001010

两者异或的结果为：0010010011，换回字线即“ET”