现代密码学

第二讲 作业

作业

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

密文：*14 25 18*

*9*3-26=1 所以 $9^{-1}=3 \bmod 26$*

2）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。

密文：rzqpmxov gdfwclqv ugmvybrj gqdtn

作业

3）用Hill密码加密明文“hill”，使用的密钥是

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

试求其密文。

P=(7,8,11,11)，密文是jiiy

作业

4）试设计实现仿射密码和单表代换密码：给出密钥生成（ 随机选择小于26的数、选择和26互素的密钥；以及生成0-25上的一个随机置换）、加解密的伪代码;

仿射密码：PRG 函数，扩展欧几里得算法

单表代换：

密钥生成：

```
void key(int *key) {
//数组 k 为 0-25 的升序排列
    Int i, j;
    for( i = 0; i < 26; i ++ ) {
    // 随机交换数字
        j = rand() %26 ;
        Int t = key[i];
        key[i] = key[j];
        key[j] = t;
    }
}
```

作业

5）给出移位、仿射、单表代换、维吉尼亚密码、多表代换（每个密钥是一个单表代换）、置换密码 穷尽搜索的复杂度（即密钥空间大小）。

- 移位密码:25
- 仿射密码：Phi(26)*26
- 单表代换：26！
- 维吉尼亚密码：密钥长为m，密钥空间为26^m
- 多表代换密码：密钥长为m，密钥空间为（26！）^{m}
- 置换密码：以m长度分组互换，密钥空间为m！

6）区分单表代换、多表代换、置换密码、希尔密码，哪个属于分组加密范畴，为什么？

置换密码和希尔密码是分组加密的范畴。

以字母代换不是：

作业

7) 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。

Per zlrracm, vxmcs r qipqlczhs. Qs fcv rihw sxx hblrxh sm nkidhvzphw. Ixxvn qsn, lysh sifecs uui jrrfyg, mk xj suvc kd ss wbrzrrz uqh jpp zyw qv ylgn osfz fin isi bpgyoj, fg dm zdqzap, cl sifecs qks cdfy iu xyxey iu tipp zcni dt. Sin lj nt rfy jszcx hi jik iyfixky iysmh hzuwwwxpk izayv; mw lv olh kfxeu nr gitrhy d afgcr qkiit vjyucsdum bdw kwv cjssiilbcwc kd wwhg e ads, ohg ewuffx fscavuy; lj nt rfy jszcx hi vemt kvy hrmxichpiei rbx giwtrh zxxlgv duqhvbzqm, wlvc ns uui xdzba ws ypms nr hf xk hijikwvf.

第二讲作业

- And finally, build a community. No one does big things by themselves. Right now, when people are scared, it is easy to be cynical and say let me just look out for myself, or my family, or people who look or think or pray like me. But if we are going to get through these difficult times; if we are going to create a world where everybody has the opportunity to find a job, and afford college; if we are going to save the environment and defeat future pandemics, then we are going to have to do it together.

现代密码学

第三讲

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？

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。

作业

2 超递增背包问题：

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

- 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；
- 计算复杂度：O(n)

作业

3 调研我国密码行业标准SM4的密钥长度，以及目前个人电脑的计算性能，从穷尽搜索的角度（已知明密文对），最坏情况下需要多久才能获得密钥。

密钥长度128，最坏搜索复杂度 2^{128}

计算机约百万次每秒

现代密码学

第四讲作业

第二节 作业

1. 证明3DES的穷举攻击复杂度为：$Time=2^{118}$，$space \approx 2^{56}$

加密部分：对每个K1加密并按密文排序

$O(2^{56}\log(2^{56}))$次加密

解密部分：对每个K2||K3解密，并查询是否有相同中间值

$O(2^{112}\log(2^{56}))= O(2^{112}*2^{6})$次解密

第二节 作业

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

例1)0x0000000000000000

- 经过 PC-1 变换后前 28 比特为全 0，后 28 比特为全 0，无论怎么移位产生的子密钥都相同 。

第三节 作业

1. 尝试推导AES的列混合操作转化为矩阵乘法

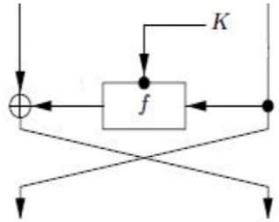
b(x)=a(x)*c(x) mod x^4+1, c(x)= $03x^3+01x^2+01x+02$

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

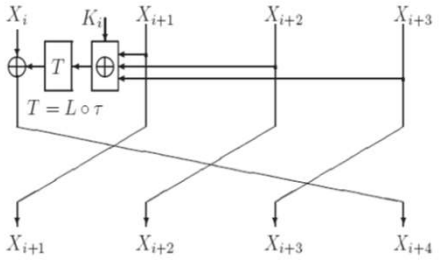
2. 快速计算法，计算0x87乘以0x03模 $m(x)=x^8+x^4+x^3+x+1$的值. ）0x92

第三节 作业

3. 调研SM4算法，其迭代结构属于何类型？并详细描述加解密及密钥编排的步骤。



1轮Feistel

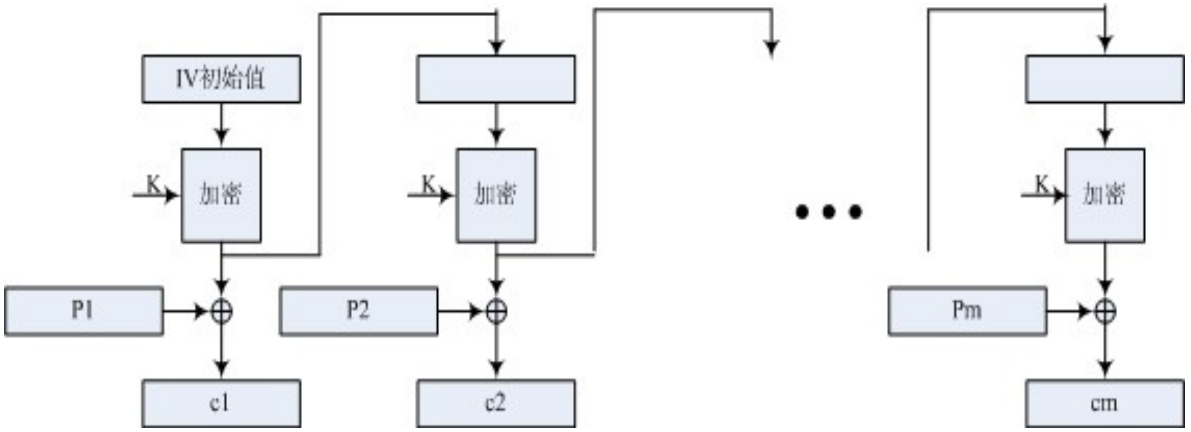


1轮SMS4

4. （选作）使用 乘法逆元及仿射方法实现AES字节代换操作 的快速运算方法。

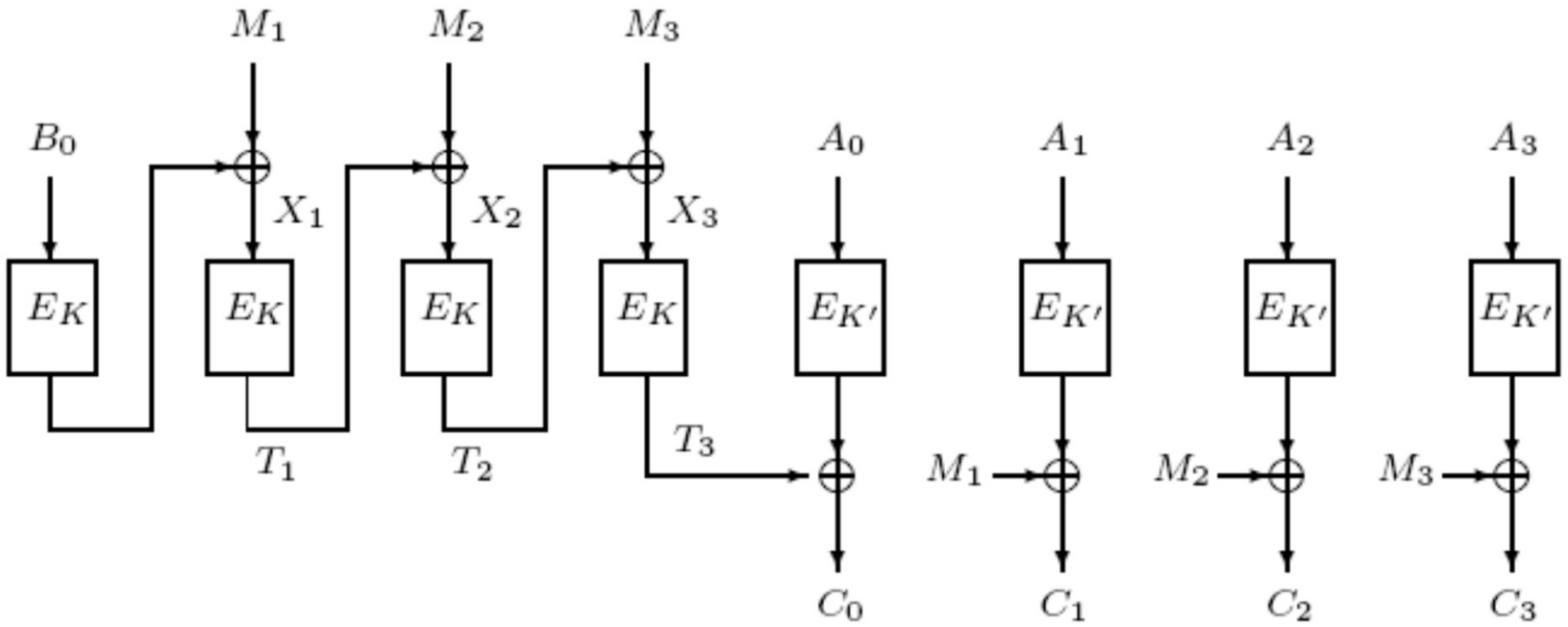
第四节 作业

1.调研OFB模式及CCM模式，并分析其各自性质。



第四节 作业

- CCM认证加密模式



现代密码学作业

第五讲

第一节

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.

输出为 000111101011001 输出周期为 15

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.

最终输出序列11011，周期为5

第一节

3 设RC4每次输出的字符为0-3中的数，初始密钥为123，设a-z分别对应0-25，计算“ok”的加解密过程。

OK: 01110 01010

S：0123，K：1231

4试构造一个输出小m序列的5级LFSR。

- 5次本原多项式：p(x)=$x^5 + x^4$+1
- 即$b_6=b_2 \oplus b_1$

第一节

5 （选做）调研GM/T 0005-2012随机性检测规范，对你熟悉的随机数生成函数进行伪随机性测试

现代密码学

第六讲作业

第一节作业

1 SHA-256处理的消息最大长度为$2^{64}-1$比特，为什么？预留了64比特，用于填充消息的长度

2 SHA系列的压缩函数中，轮迭代之后，为什么要与输入链接变量（初始变量）模加

否则可以用中间相遇攻击求出二次原像，复杂度仅为O(2^{n/2})

第一节作业

3 （选作）调研国标GM/T 0004-2012

SM3密码杂凑算法

4（选作）调研区块链中Merkle tree的作用，是否可以直接将所有交易信息输入某hash算法，hash值放在区块中？为什么？

第二节作业

1　对上述选择消息攻击（攻击二），三种填充方法是否可以防止？选择处理（截断）是否可以抵抗上面攻击？

第一、二种可以攻击成功，第三种和选择处理不行

2 试给出CFB运行模式的选择密文攻击？

- 假设已知（C1||C2）j 为 IV 加密后的值
- 构造一个 C2’=C2’⊕r
- 将(C1||C2’)输入 oracle 得到(m1||m2’)
  推导出m1||m2=m1||m2’⊕r

现代密码学

第七讲作业

第七讲

1. 若通信双方使用RSA单向陷门函数加解密信息，已知接收方公钥 (e,n)=(5,35)，截获密文为C=10，求明文M.

由n = 35,知p=7，q=5.所以Φ（35）=24，易知d = 5

- 因此$M = 10^5 \bmod 35 = 5$

第七讲

2. 若使用ElGamal单向陷门函数加解密信息，已知接收方B的公钥($p=71, g=7, y_B=3$).

1) 设发送方A选择的随机整数k=3，求明文M=10所对应的密文. C=59,57

2) 若截获到A发送的密文是C=(59,29)，求M.

K=3 m=30

3) 若截获到A发送的密文是C=(49,29)，求M.

K=2 m=19

第七讲

3. (选做)调研SM2加密标准的密钥生成、加密、解密详细步骤
4. (选做) 调研密码库函数中模幂运算的快速实现方法.
5. (选做) 调研椭圆曲线上点乘运算kG的快速实现方法.

现代密码学

第八讲作业

作业

1. 在DSS数字签名标准中，取 p=83=2×41+1，q=41，h=2，$g \equiv 2^2 \equiv 4 \bmod 83$，若取x=16，则 $y \equiv g^x \equiv 4^{16} = 77 \bmod 83$.

   在对消息M=56签名时(忽略压缩过程)，选择k=23，计算签名并进行验证.签名值为（10，29）

2. （选做）利用椭圆曲线签名体制，设椭圆曲线是 $E_{23}(1,1)$, 一个7阶生成元为G=(17,20). 接收方A的秘密钥x=3，A欲对消息e=h(m)=5签名，选择随机数k=2，求签名 (6,1)为消息的签名

3 （选做）调研密码标准SM2数字签名算法

现代密码学

第九讲作业

作业

1. 试设计一个基于公钥系统的密钥分配方案，保证密钥的一致和新鲜性。

2. 运用密钥安全管理的理念，描述如何在现实生活中管理好自己的各种口令。