范围

题型分布

小题 10x3：

- 五个填空
- 五个选择
- 五个判断

大题 10x4 40

综合题 15x2 30

小题

乘积密码题

乘积密码加密，算法1加密，算法2加密，是否等效，可交换吗？

```
错误 不可交换
```

DS函数

```
正确 48比特
```

随机变量X的熵

```
正确 随机变量熵与概率有关
```

f和sp谁是谁的推广

```
没说 SP是F的推广
```

平均长度

```
正确 一个密码体制的唯一解距离定义为使得伪密钥的期望数目sn 等于零的密文长度n，记录作为n0（P39，定义3.6）
```

单表的反射加密变换

熵是，不确定性的数学度量

公钥密码的基础是，xx单项函数

```
公钥密码的理论基础是陷门单向函数    P83
```

现代分组密码的设计基础

```
扩散与混淆
```

蒙尼兹（椭圆） 安全性在于

```
椭圆对数问题的难解性
```

古典密码加法乘法置换密码置换量

```
加法密码的密钥量
乘法的密钥量
置换密码的密钥量 26!     ??
```

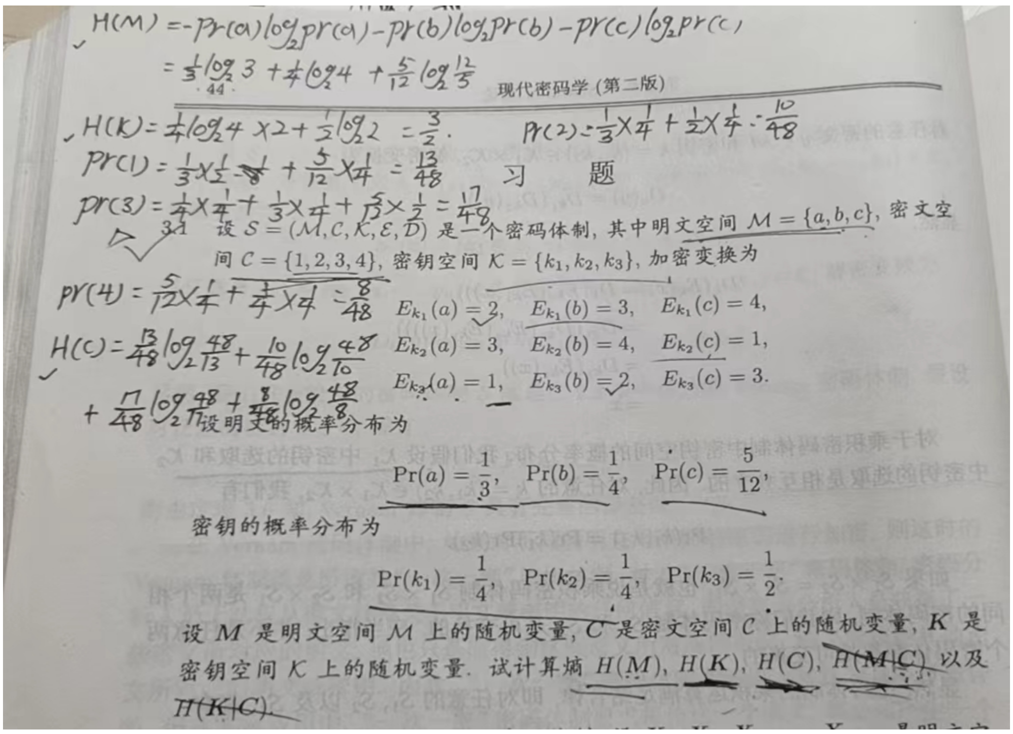
密码体制包括什么

```
明文空间 密钥空间 密文空间 解密算法 加密算法
不包括密钥源头
```

大题

信息论 熵

第三章P44习题3.1，计算HM HK HC，太复杂运算不需要计算结果只需要列式



$H(M) = -Pr(a)\log_2 Pr(a) - Pr(b)\log_2 Pr(b) - Pr(c)\log_2 Pr(c)$

$= \frac{1}{3}\log_2 3 + \frac{1}{4}\log_2 4 + \frac{5}{12}\log_2 \frac{12}{5}$

44 现代密码学（第二版）

$H(K) = \frac{1}{4}\log_2 4 \times 2 + \frac{1}{2}\log_2 2 = \frac{3}{2}$. $Pr(2) = \frac{1}{3}\times\frac{1}{4} + \frac{1}{2}\times\frac{1}{4} = \frac{10}{48}$

$Pr(1) = \frac{1}{3}\times\frac{1}{2} + \frac{5}{12}\times\frac{1}{4} = \frac{13}{48}$

习　题

$Pr(3) = \frac{1}{4}\times\frac{1}{4} + \frac{1}{3}\times\frac{1}{4} + \frac{5}{12}\times\frac{1}{2} = \frac{17}{48}$

3.1 设 $S = (\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ 是一个密码体制，其中明文空间 $\mathcal{M} = \{a, b, c\}$，密文空间 $\mathcal{C} = \{1, 2, 3, 4\}$，密钥空间 $\mathcal{K} = \{k_1, k_2, k_3\}$，加密变换为

$Pr(4) = \frac{5}{12}\times\frac{1}{4} + \frac{1}{4}\times\frac{1}{4} = \frac{8}{48}$

$$E_{k_1}(a) = 2,\quad E_{k_1}(b) = 3,\quad E_{k_1}(c) = 4,$$
$$E_{k_2}(a) = 3,\quad E_{k_2}(b) = 4,\quad E_{k_2}(c) = 1,$$
$$E_{k_3}(a) = 1,\quad E_{k_3}(b) = 2,\quad E_{k_3}(c) = 3.$$

$H(C) = \frac{13}{48}\log_2\frac{48}{13} + \frac{10}{48}\log_2\frac{48}{10} + \frac{17}{48}\log_2\frac{48}{17} + \frac{8}{48}\log_2\frac{48}{8}$

设明文的概率分布为

$$\Pr(a) = \frac{1}{3},\quad \Pr(b) = \frac{1}{4},\quad \Pr(c) = \frac{5}{12},$$

密钥的概率分布为

$$\Pr(k_1) = \frac{1}{4},\quad \Pr(k_2) = \frac{1}{4},\quad \Pr(k_3) = \frac{1}{2}.$$

设 M 是明文空间 $\mathcal{M}$ 上的随机变量，C 是密文空间 $\mathcal{C}$ 上的随机变量，K 是密钥空间 $\mathcal{K}$ 上的随机变量．试计算熵 $H(M)$, $H(K)$, $H(C)$, $H(M|C)$ 以及 $H(K|C)$.

欧几里得算法求逆元

P95例题5.6

例 5.6 求 13 模 35 的逆元. 因为 欧几里得算法

$35 = 2 \times 13 + 9,\quad 9 = 1 \times 35 - 2 \times 13,$

$13 = 1 \times 9 + 4,\quad 4 = 1 \times 13 - 1 \times 9 = -1 \times 35 + 3 \times 13,$

$9 = 2 \times 4 + 1,\quad 1 = 1 \times 9 - 2 \times 4 = 3 \times 35 - 8 \times 13,$

$1 = 9 - 2\times4$
$= 9 - 2(13 - 1\times9)$
$= 3\times9 - 2\times13$
$= 3\times(35 - 2\times13) - 2\times13$
$= 3\times35 - 8\times13$

所以 13 模 35 的逆元为 $(-8) \bmod 35 = 27$. □

古典密码匹配

给明文/矩阵，计算密文

P11，用profile加密，明文字符串开始加密时，插入特定的字母q。。。c2和m2同行

Playfair 体制的密钥是一个 5×5 的矩阵 $P = (p_{ij})_{5\times5}$. 构造方法如下:

1) 构造字母表 {a, b, c, d, e, f, g, h, i, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z} 的一个置换. 这里将 j 当做 i, 实际上只有 25 个字母.

2) 将上述置换按行排列成一个 5×5 的矩阵 $P = (p_{ij})_{5\times5}$.

用 Playfair 体制对明文字母串进行加密时, 首先在明文字母串的适当位置插入一些特定的字母, 譬如字母 q, 使得明文字母串的长度为偶数, 并且将明文字母串按两个字母一组进行分组, 每组中的两个字母不同. 对任意的明文字母对 m_1m_2, 设它们对应的密文对为 c_1c_2, 加密方法如下:

1) 如果 m_1 和 m_2 在 P 中同一行, 则密文 c_1 和 c_2 分别为紧靠 m_1 和 m_2 的右端的字母. 这里将第一列看作是在最后一列的右端.

2) 如果 m_1 和 m_2 在 P 中同一列, 则密文 c_1 和 c_2 分别为紧靠 m_1 和 m_2 的下方的字母. 这里将第一行看作是在最后一行的下方.

3) 如果 m_1 和 m_2 既不在 P 中的同一行, 也不在同一列, 则密文 c_1 和 c_2 分别为由 m_1 和 m_2 确定的矩形的其他两个角上的字母. c_1 和 m_1 同行, c_2 和 m_2 同行.

例 2.1 设密钥矩阵

$$P = \begin{pmatrix} c & i & p & h & e \\ r & a & b & d & f \\ g & k & l & m & n \\ o & q & s & t & u \\ v & w & x & y & z \end{pmatrix},$$

明文为

Playfair cipher was actually invented by Wheatstone.

将明文分组为

pl ay fa ir ci ph er wa sa ct ua lq
ly in ve nt ed by wh ea ts to ne

则密文为

bs dw rb ca ip he cf ik qb ho qf ks
mx ek zc mu hf dx yi if ut uq uf □

例子2.1

用费马小定理计算高幂

P132习题5.6

钥 $1 < e < \phi(n)$, 使得对任意明文 x 都有 $x^e \equiv x \pmod n$. $3^{\varphi(11)} = 3^{10} \equiv 1\ (11)$

5.6 利用 Fermat 定理计算 $3^{201} \bmod 11$. 3 $3^{201} = 3\cdot3^{200} = 3\cdot(3^{10})^{20} = 3$.

5.7 在 ElGamal 公钥密码体制中, 设素数 $p = 71$, $\alpha = 7$ 是 Z_{71}^* 的生成元, $\beta = 3$

综合题

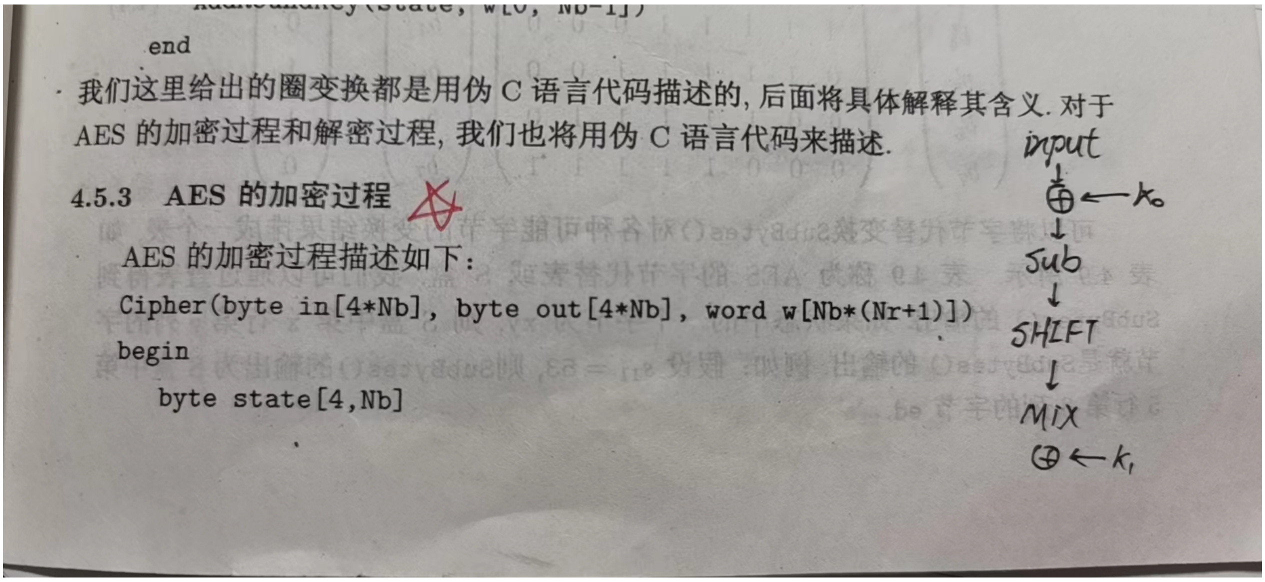
AES DES

变换P65-66 四个函数的意义 subbytes？四个横线（算法代码循环体）

AES DES常见的分组密码结构，xx网络

AES：SP网络

DES：Feistel网络



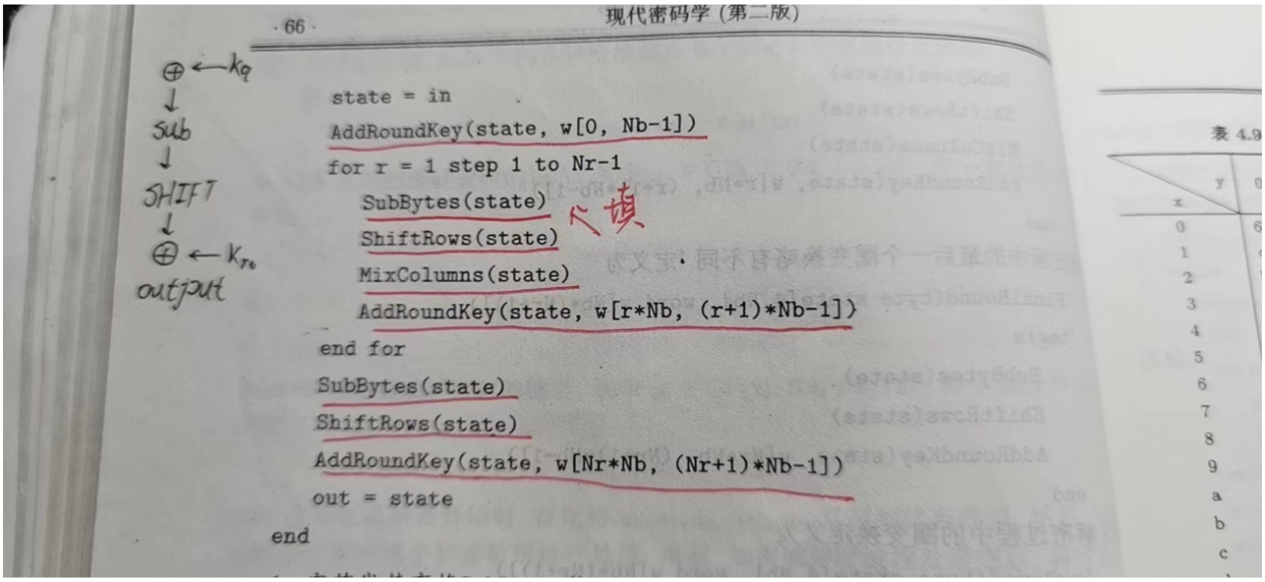
```
    AddRoundKey(state, w[0, Nb-1])
  end
```

我们这里给出的圈变换都是用伪 C 语言代码描述的，后面将具体解释其含义. 对于 AES 的加密过程和解密过程，我们也将用伪 C 语言代码来描述.

4.5.3 AES 的加密过程

AES 的加密过程描述如下：

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte state[4,Nb]
```

·66· 现代密码学（第二版）

```
   state = in
   AddRoundKey(state, w[0, Nb-1])
   for r = 1 step 1 to Nr-1
      SubBytes(state)
      ShiftRows(state)
      MixColumns(state)
      AddRoundKey(state, w[r*Nb, (r+1)*Nb-1])
   end for
   SubBytes(state)
   ShiftRows(state)
   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
   out = state
end
```


ElGamal算法

1. 密文依赖于什么？P111中间考下三分之一

```
密文依赖于明文m和秘密选取的随机整数k
```

2.安全性基于什么？P112

```
关于有限域 Zp 上离散对数问题的难解性
```

3.计算m对应的密文c：P111，用余来算更好

5.4 EIGamal 公钥密码

5.4.1 EIGamal 公钥密码体制

EIGamal 公钥密码体制是由 T. EIGamal 于 1985 年提出的. 它至今仍然是一个安全性能良好的公钥密码体制.

EIGamal 公钥密码体制描述如下:

1) 选取大素数 p, $\alpha \in Z_p^*$ 是一个$\boxed{\text{本原元}}$. p 和 α 公开.

2) 随机选取整数 d, $1 \leqslant d \leqslant p-2$, 计算

$$\beta = \alpha^d \bmod p.$$

β 是公开的加密密钥, d 是保密的解密密钥.

3) 明文空间为 Z_p^*, 密文空间为 $Z_p^* \times Z_p^*$.

4) 加密变换: 对任意明文 $m \in Z_p^*$, 秘密随机选取一个整数 k, $1 \leqslant k \leqslant p-2$, 密文为

$$c = (c_1, c_2),$$

其中

$$\boxed{\begin{aligned} c_1 &= \alpha^k \bmod p, \\ c_2 &= m\beta^k \bmod p. \end{aligned}}$$

$\beta = \alpha^d$

5) 解密变换: 对任意密文 $c = (c_1, c_2) \in Z_p^* \times Z_p^*$, 明文为

$$m = c_2(c_1^d)^{-1} \bmod p.$$

现在我们来证明解密变换能正确地从密文恢复相应的明文.

因为

$$\begin{aligned} c_1 &= \alpha^k \bmod p, \\ c_2 &= m\beta^k \bmod p, \\ \beta &= \alpha^d \bmod p, \end{aligned}$$

所以

$$\begin{aligned} c_2(c_1^d)^{-1} &\equiv m\beta^k(\alpha^{dk})^{-1} \pmod p \\ &\equiv m\alpha^{dk}(\alpha^{dk})^{-1} \pmod p \\ &\equiv m \pmod p. \end{aligned}$$

因此, 解密变换能正确地从密文恢复相应的明文.

在 EIGamal 公钥密码体制中, 密文依赖于明文 m 和秘密选取的随机整数 k. 因此, 明文空间中的一个明文对应密文空间中的许多不同的密文.

例 5.11 设 $p = 2579$, $\alpha = 2$, $d = 765$. 容易计算

$$\beta = 2^{765} \bmod 2579 = 949.$$

对于明文 $m = 1299$, 秘密随机选取整数 $k = 853$. 容易计算密文为 $c = (c_1, c_2)$, 其中

$$c_1 = 2^{853} \bmod 2579 = 435,$$

$$c_2 = 1299 \times 949^{853} \bmod 2579 = 2396.$$

反过来, 对于密文 $c = (435, 2396)$, 容易计算明文为

$$m = 2396 \times (435^{765})^{-1} \bmod 2579 = 1299.$$

显然, 解密变换正确地从密文恢复出了明文.