密码学习题提示

姓名：　杨礼珍

说明：　黑体表示的练习编号为本学期布置的

目　录

第一章　习题提示

1.1 第1章作业

练习1.1：(a)51 (b)30 (c)81 (d)7422

练习1.2：令$x = m - (a \bmod m)$。由$0 < a \bmod m < m$得到$0 < x < m$；且$(x - (-a \bmod m)) \bmod m = 0$，由此得证。

练习1.3：设$a \bmod m = x$，$a = km + x$，$b \bmod m = y$，$b = k'm + y$。

必要性：若$a \bmod m = b \bmod m$，则$x = y$。那么$(a - b)\bmod = (km + x - k'm - y) \bmod m = 0$，因此$a \equiv b \bmod m$.

充分性：若$a \equiv b \bmod m$，则存在整数t使得$a - b = tm$。另一方面有$x - y = (a - km) - (b - k'm) = a - b + (k - k')m = (t + k - k')m$。因为$0 \leq x, y < m$，那么$-m < x - y < m$，因此$x - y = 0$，即$a \bmod m = b \bmod m$。

练习1.4：根据$\lfloor x \rfloor$的定义得到：（1）$a - \lfloor \frac{a}{m} \rfloor \geq a - \frac{a}{m} \cdot m = 0$；（2）$a - \lfloor \frac{a}{m} \rfloor > a - (a/m - 1)m = m$。因此有

$$0 \leq a - \lfloor \frac{a}{m} \rfloor < m.$$

另一方面由$a - \lfloor \frac{a}{m} \rfloor m - a = \lfloor \frac{a}{m} \rfloor m$得到$a \equiv a - \lfloor \frac{a}{m} \rfloor \bmod m$。那么根据练习1.3知道

$$a \bmod m = a - \lfloor \frac{a}{m} \rfloor.$$

练习1.5：穷搜索解密密钥，直到解密出来的明文有意义。

练习1.6：设仿射密码的加密密钥为$(a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$，如果该密钥为对合密钥，那么有

$$d_K(y) = (ay + b) \bmod 26 = (a(ax + b) + b) \bmod 26 = (a^2x + ab + b) \bmod 26 = x$$

因此有

$$(a^2 - 1)x + ab + b \equiv 0 \pmod{26}$$

那么有

$$a^2 - 1 \equiv 0 \pmod{26} \Rightarrow a^2 \equiv 1 \pmod{26} \Rightarrow a = 1, 25$$

及

$$ab + b \equiv 0 \pmod{26}$$

那么当$a=1$时，$b=13$，当$a=25$时，b可取$\mathbb{Z}_{26}$上任意值。

练习1.7：令$\varphi(\cdot)$表示欧拉函数。

当$m=30$时，仿射密码的密钥量为$\varphi(30)30=(2-1)\times(3-1)\times(5-1)\times30=240$。

当$m=100$时，仿射密码的密钥量为$\varphi(100)100=2(2-1)\times5(5-1)\times100=4000$。

当$m=1225$时，仿射密码的密钥量为$\varphi(1225)1225=5(5-1)\times7(7-1)\times1225=1029000$。

练习1.10：(a)加密函数为$y=5x+21 \bmod 29$，解密函数$d_K(y)=5^{-1}(x-21) \bmod 29=6(x-21) \bmod 29=6x+19 \bmod 29$

(b)$d_K(e_K(x))=6(5x+21)+19) \bmod 29=(6\times5x+6\times21+19) \bmod 29=x$

练习1.9：

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$a^{-1} \bmod 29$	1	15	10	22	6	5	25	11	13	3	8	17	9	27
a	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$a^{-1} \bmod 29$	2	20	12	21	26	16	18	4	24	23	7	19	14	28

练习1.10：已知$K=(5,21)$是定义在$\mathbb{Z}_{29}$上的仿射密码的密钥。

(a)以$d_K(y)=a'y+b'$的形式给出解密函数，这里$a',b'\in\mathbb{Z}_{29}$。

(b)证明对任意的$x\in\mathbb{Z}_{29}$，都有$d_K(e_K(x))=x$。

解答：(a)$5^{-1} \bmod 26=21$。由$y=(5x+21) \bmod 26$，可得$x=5^{-1}(y-21) \bmod 26=21(y-21) \bmod 26=(21y+1) \bmod 26$。因此$d_{(5,21)}=(21y+1) \bmod 26$。

(b)对任意$x\in\mathbb{Z}_{29}$，有

$$\begin{aligned} d_{(5,21)}(e_{(5,21)}(x)) &= (21(5x+21)+1) \bmod 26 \\ &= (105x+442) \bmod 26 \\ &= x \bmod 26 \\ &= x \end{aligned}$$

练习1.15(a)：

$$\begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix}^{-1} = (2\times5-9\times5)^{-1}\begin{pmatrix} 5 & -9 \\ -5 & 2 \end{pmatrix} = 17^{-1}\begin{pmatrix} 5 & -9 \\ -5 & 2 \end{pmatrix} = 12\begin{pmatrix} 5 & -9 \\ -5 & 2 \end{pmatrix} = \ldots$$

练习1.16：

(a)

x	1	2	3	4	5	6	7	8
$\pi(x)$	2	4	6	1	8	3	5	7

(b)有的同学混淆了置换密码和代换密码，注意，置换密码是对下标进行变换（即打乱位置），代码密码是对一个字母变换成另一个字母。

练习1.18：当初始向量为$(0,0,0,0)$时，生成全0序列，因此周期为1。

当初始向量为$(1,0,0,0)$时，生成序列如下：

$$1,0,0,0,1,1,0,0,0,\ldots$$

因此当初始向量为$(1,0,0,0),(0,0,0,1),(0,0,1,1),(0,1,1,0),(1,1,0,0)$时，周期为5。

当初始向量为$(0,1,0,0)$时，生成序列如下：

$$0,1,0,0,1,0,1,0,0\ldots$$

因此当初始向量为$(0,1,0,0),(1,0,0,1),(0,0,1,0),(0,1,0,1),(1,0,1,0)$时，周期为5。

当初始向量为$(1,1,1,0)$时，生成序列如下：

$$1,1,1,0,1,1,1,1,0,\ldots$$

因此当初始向量为$(1,1,1,0),(1,1,0,1),(1,0,1,1),(0,1,1,1),(1,1,1,1)$时，周期为5。

练习1.19方法类似于练习1.18。

思考题1：把应用于维吉尼亚密码的重合指数法应用到仿射密码的惟密文密码分析中，请写出分析算法步骤，及实现代码。测试明文（测试时请去掉空格），或使用课本第1章习题1.21中的仿射密码密文(c)来测试：

This is an essay I wrote for a mathematics essay prize We had a number of possible topics to choose from and I choose cryptology because I already had a passing interest in thanks to my attempts to code encryption algorithms for my computer programs It won by the way This is the original essay with a few corrected spelling mistakes though there are probably some left I am currently studying at Imperial College my home page is here

提示：

1 有的同学把维吉尼亚密码的划分子序列应用到仿射密码中，这是没必要的，维吉尼亚密码需要划分子序列，是因为每个密文不一定由相同密钥字母加密得到，划分后，每个子序列都用相同密钥字母加密得到。而仿射密码的所有密文都由相同的密钥加密得到。

2 某些类型的仿射密码是可以看成维吉尼亚密码的特殊情形。设仿射密码的密钥为$k=(a,b)$，加密函数为$e_k(x)=ax+b \bmod 26$，如果$a=1$时，可以看成是$m=1$的维吉尼亚密码，我们直接套用维吉尼亚密码的分析步骤来分析出b：

1. 对b的每一可能值g计算其重合指数估计值：

$$M_g = \sum_{j=0}^{25} \frac{p_j f_{(aj+g) \bmod 26}}{n}$$

2. 如果M_g最大，那么认为$b = g$

3 对一般的$k = (a, b)$呢？对于(a, b)的每一可能值(h, g)，如何推导出合理的$M_{h,g}$来区分正确密钥值和错误密钥值？

4 你的方法是否合理？要编程检验过。

1.2 第2章作业

练习2.3：仿照课本中的思路证明。

设仿射密码的加密函数为$e_K(x) = ax + b \bmod 26$，解密函数为$d_K(y)$。要证明具有完善保密性，即证明$Pr(X = x|Y = y) = Pr(X = x)$，这里$X, Y, K$分别表示明文、密文和密钥随机变量。

(a)

仿照定理2.3的证明。对于任意密文$y \in Z_{26}$

$$\begin{aligned} Pr(Y = y) &= \sum_{a \in Z_{26}^*, b \in Z_{26}} Pr(K = (a, b)) Pr(X = d_K(y)) \\ &= \frac{1}{312} \sum_{a \in Z_{26}^*} \sum_{b \in Z_{26}} Pr(X = d_K(y)) \\ &= \frac{1}{312} \sum_{a \in Z_{26}^*} \sum_{b \in Z_{26}} Pr(X = a^{-1}(y - b)) \end{aligned}$$

(作业中存在问题：

1. 少部分同学没搞清楚仿射密码的解密函数$X = d_K(y)$，写成$x = y - a$，应该是$x = a^{-1}(y - b)$！
2. 红色部分大部分同学都没有给出正确值，如果把求和符号写成$\sum_k$将不会那么容易分析出结果来，如果写成更细致的$\sum_{a \in Z_{26}^*} \sum_{b \in Z_{26}}$则很容易计算出来。)

以下求和公式中，y和a是固定的，b是可变的，对所有b的可能值，值$a^{-1}(y - b)$构成了Z_{26}上的一个置换，因此有

$$\sum_{b \in Z_{26}} Pr(X = a^{-1}(y - b)) = 1$$

从而，对于任意的$y \in Z_{26}$，有

$$Pr(Y = y) = \frac{1}{312} \sum_{a \in Z_{26}^*} 1 = \frac{12}{312} = \frac{1}{26}$$

接下来我们有，对于任意的x, y

$$\begin{aligned} Pr(Y = y|X = x) &= Pr(K = (a, b) : y = ax + b) \\ &= \frac{12}{312} \end{aligned}$$

$$= \frac{1}{26}$$

（这是因为，满足$y = ax + b$，等价于$b = y - ax$，因此对于每一对x, y，每一$a \in Z_{26}^*$有唯一一个$b \in Z_{26}$满足等式，因此共有12对(a, b)满足等式$y = ax + b$。）

应用Bayes定理，计算得到：

$$\begin{aligned} Pr(X = x|Y = y) &= \frac{Pr(X = x)Pr(Y = y|X = x)}{Pr(Y = y)} \\ &= \frac{Pr(X = x)\frac{1}{26}}{\frac{1}{26}} \\ &= Pr(X = x) \end{aligned}$$

证明完毕！

(b)(请注意(b)中的题意，假设a服从任意的概率分布，但很多同学给出$Pr(a) = 1/7$的结论来，而且这个结论还是从a有7个取值得到的，实际上a有$\phi(26) = 12$个取值！唯一的条件是$Pr((a, b)) = Pr(a)/26$。证明思路和(a)一样)

仿照定理2.3的证明。对于任意密文$y \in Z_{26}$

$$\begin{aligned} Pr(Y = y) &= \sum_{a \in Z_{26}^*, b \in Z_{26}} Pr(K = (a, b))Pr(X = d_K(y)) \\ &= \sum_{a \in Z_{26}^*} \sum_{b \in Z_{26}} \frac{Pr(a)}{26} Pr(X = d_K(y)) \\ &= \frac{1}{26} \sum_{a \in Z_{26}^*} Pr(a) \sum_{b \in Z_{26}} Pr(X = a^{-1}(y - b)) \end{aligned}$$

现在固定y和a，对所有b的可能值，值$a^{-1}(y - b)$构成了Z_{26}上的一个置换，因此有

$$\sum_{b \in Z_{26}} Pr(X = a^{-1}(y - b)) = 1$$

从而，对于任意的$y \in Z_{26}$，有

$$Pr(Y = y) = \frac{1}{26} \sum_{a \in Z_{26}^*} Pr(a) \cdot 1 = \frac{1}{26}$$

接下来我们有，对于任意的x, y

$$Pr(Y = y|X = x) = Pr(K = (a, b) : y = ax + b)$$

$$
\begin{aligned}
&= \sum_{a\in Z_{26}^*} \sum_{b\in Z_{26}, y=ax+b} Pr(K=(a,b)) \\
&= \sum_{a\in Z_{26}^*} \sum_{b\in Z_{26}, y=ax+b} \frac{Pr(a)}{26} \\
&= \sum_{a\in Z_{26}^*} \frac{Pr(a)}{26} \\
&= \frac{1}{26} \sum_{a\in Z_{26}^*} Pr(a) \\
&= \frac{1}{26}
\end{aligned}
$$

(以上红色部分解释：该求和公式中x, y, a的值是固定的，b是可变的，但只有唯一一个b满足$y = ax + b$)

应用Bayes定理，计算得到：

$$
\begin{aligned}
Pr(X=x|Y=y) &= \frac{Pr(X=x)Pr(Y=y|X=x)}{Pr(Y=y)} \\
&= \frac{Pr(X=x)\frac{1}{26}}{\frac{1}{26}} \\
&= Pr(X=x)
\end{aligned}
$$

证明完毕！

练习2.18：证明等概率选取的移位密码是幂等的。

注意问题：部分同学把密码体制S等同于其加密函数$x + k \bmod 26$，写出诸如$S = x - k \bmod 26$这样的错误形式来，请回顾第一章中对密码体制的定义：由明文空间、密文空间、密钥空间、加密函数和解密函数组成。

这道题实质是要证明移位密码体制S等价于其乘积密码体制S^2，要证明以下两点：

1.(S^2是移位密码) 这是比较容易证明的部分，但是大部分同学的证明不严格，具体要证明以下几点：

1. S^2的明文空间、密文空间和S一样，这是显然的，注意他们的密钥空间是不一样的。
2. S^2的密钥和S的密钥存在对应关系，换言之对应的密钥对任意同一明文的加密结果一致：
   (a) 对S^2的任意密钥(k_1, k_2)存在S的密钥与之等价，可发现为S的密钥$k_1 + k_2$，因为可验证$e_{(k_1,k_2)}(x) = x + k_1 + k_2 \bmod 26$，部分同学仅证明了$S^2$的特殊形式的密钥$(k, k)$等价于$S$的密钥$2k$。

(b) 对S中的任意密钥k，可找到S^2中的密钥与之对应，可发现应为$(k, k - k_1)$，这里$k_1 \in \mathbb{Z}_{26}$。(这一步骤不可缺少，因为可能存在S中的某个密钥S^2没有密钥与之等价。从这里看到S^2中的密钥和S中的密钥不是1-1对应关系，而是S中的密钥有S^2中的26个等价密钥与之对应，课本中的例子是1-1对应关系，这意味着他们的密钥概率分布也将一致，所以到此证明可完成，但这里必须进一步证明)

2.(S^2等价的移位密码S'的密钥概率分布是均匀分布) 大部分同学都没有证明这点。提示：设S^2等价的移位密钥为S'。对S'中固定的密钥k值，$e_{k_1,k_2}(x)$对应的密钥(k_1, k_2)等价于k，当且仅当$k = k_1 + k_2 \bmod 26$，如果k_1固定，那么$k_2 = k - k_1 \bmod 26$是唯一确定的，因此有

$$Pr[k] = \sum_{k_1=0}^{25} Pr[k_1]Pr[(k - k_1) \bmod 26] = \sum_{k_1=0}^{25} \frac{1}{26^2} = \frac{1}{26}$$

1.3 第3章作业

练习3.1 注意SPN表示代换-置换网络，而不是函数名称。$\pi_S^* = \pi_S^{-1}$，$\pi_P^* = \pi_P^{-1}$

练习3.2提示：Feistel密码就是DES类型的密码，轮函数形为：

$$\begin{aligned} L^i &= R^{i-1} \\ R^i &= L^{i-1} \oplus f(R^{i-1}, K^i) \end{aligned}$$

其逆函数形为（见书p.78）形为：

$$\begin{aligned} L^{i-1} &= R^i \oplus f(L^i, K^i) \\ R^{i-1} &= L^i \end{aligned}$$

可以看到加解密函数的形式相同，当然左右分组不同。。。。。

练习3.3提示：

第一步：设密钥K产生的第i轮密钥为K^i，其补$c(K)$所产生的第i轮密钥为K'^i，证明$K'^i = c(K^i)$。

第二步：证明对函数f（观察f的结构），满足：

$$f(A, J) = f(c(A), c(J))$$

其中$c(A)$表示A的补，$c(J)$表示J的补。

第三步：证明对轮函数g成立：

$$c(g(L^{i-1}, R^{i-1}, K^i)) = g(c(L^{i-1}), c(R^{i-1}), c(K^i))$$

第四步：证明对整个加密函数结论成立。

练习3.5提示：密钥是AES的flash演示中的密钥，请自行检查。

练习3.7提示：把四种工作模式的解密模式写出来，然后证明结论。

练习3.12提示：

（b）满足

$$\bigoplus_{i=1}^{m} a_i X_i = 0$$

的$X_i \in \{0,1\}(1 \le i \le m)$个数是$2^{m-1}$。

(c)

$$\sum_{a=0}^{2^m-1} N_L(a,b) = \sum_{a=0}^{2^m-1} |\{x = (x_1, \ldots, x_m) \in \{0,1\}^m : ax \oplus b\pi_S(x) = 0\}|$$

$$= \sum_{x\in\{0,1\}^m} |\{a : 0 \le a \le 2^m - 1, ax \oplus b\pi_S(x) = 0\}| \tag{1.1}$$

证明对$x \neq 0$有：

$$|\{a : 0 \le a \le 2^m - 1, ax \oplus b\pi_S(x) = 0\}| = 2^{m-1}$$

证明对$x = 0, b\pi_S(x) = 0$有：

$$|\{a : 0 \le a \le 2^m - 1, ax \oplus b\pi_S(x) = 0\}| = 2^m$$

证明对$x = 0, b\pi_S(x) \neq 0$有：

$$|\{a : 0 \le a \le 2^m - 1, ax \oplus b\pi_S(x) = 0\}| = 0$$

把以上证明的三个结论代入式(1.1)可以证明(c)中结论。

(d)分两种情况讨论：

情况1：$x = 0$时$\pi_S(x) = 0$，应用(c)证明中的结论可以证明：

$$\sum_{a=0}^{2^m-1}\sum_{b=0}^{2^n-1} N_L(a, b) = 2^{n+2m-1} + 2^{n+m-1}$$

情况2：$x = 0$时$\pi_S(x) \neq 0$，应用(c)证明中的结论，并加上一些复杂点的讨论可以证明：

$$\sum_{a=0}^{2^m-1}\sum_{b=0}^{2^n-1} N_L(a, b) = 2^{n+2m-1}$$

练习3.14提示：

(a)根据N_L的定义计算即可，参考例子：图3.2。

(b)题目要求使用3个活动S盒，共有三轮，那么每轮应该只有一个活动S盒。每个S盒的偏差绝对值应该尽可能大，才能准确的估计出随机变量的偏差。有必要编写程序搜索合适S盒。

练习b3：如果AES算法没有列混合运算，请给出一个比穷搜索更加有效的攻击算法。

提示：以分组长度为128比特的AES为例。假设明文为

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}$$

其中$s_{i,j}$为一个字。

对应的密文为

$$\begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}$$

其中$c_{i,j}$为一个字。

如果没有列混合运算，那么明文中第i行的4个字只影响到密文中第i行的4个字。如果敌手获得以下2^{32}个密文的对应明文，那么他就可以解密出用同样密钥加密的所有密文：

$$\begin{pmatrix} c'_0 & c'_1 & c'_2 & c'_3 \\ c'_0 & c'_1 & c'_2 & c'_3 \\ c'_0 & c'_1 & c'_2 & c'_3 \\ c'_0 & c'_1 & c'_2 & c'_3 \end{pmatrix}$$

其中c'_0, c'_1, c'_2, c'_3取尽所有可能值。

1.4 第4章作业

习题4.5：

注意问题：两道题的证明关键在于给出第二原像问题的解，不是证明解的存在性！存在解不意味着容易解。

(a)(难点：考虑到所有情况)设$x' \neq x$，且$x^2+ax+b \equiv x'^2+ax'+b \pmod{2^m}$，那么等价于$(x-x')(x+x'+a) \equiv 0 \pmod{2^m}$，因为$x \neq x'$可令$x+x'+a \equiv 0 \pmod{2^m}$，解得：

$$x' = \begin{cases} 2^m - x - a & \text{若} x \leq 2^m - a \\ 2^{m+1} - x - a & \text{若} x > 2^m - a \end{cases}$$

下面分两种情况讨论：

情况1：以上解如果还满足$x' \neq x$则为第二原像问题的解。

情况2：以上解如果满足$x' = x$(即在$x \equiv -a/2 \pmod{2^m}$且a为偶数时)，并不是第二原像问题的有效解。

把$x \equiv -a/2 \pmod{2^m}$代入$x^2 + ax + b \equiv x'^2 + ax' + b \pmod{2^m}$得到$-a^2/4 \equiv x'^2 + ax' \pmod{2^m}$，等价于$(x' - a/2)^2 \equiv 0 \pmod{2^m}$，其中两个模$2^m$的平方根为0和$2^{m-1}$，那么得到其中2个解：

$$x' = \begin{cases} 2^{m-1} - a/2 \\ a/2 \end{cases}$$

如果以上2个解都不同，则必然有一个与x不同的值为第二原像问题的解。

如果以上2个解相同，则需进一步讨论，这时意味着$a = 2^{m-1}$，$x = -2^{m-2} \bmod 2^m = 2^m - 2^{m-2} \neq 2^{m-2}$，因此$x' = a/2 = 2^{m-2}$仍然是第二原像问题的解。

(b) 注意条件$n > m$。如果$x' \equiv x \pmod{2^m}$，就可满足

$$h(x) \equiv h(x') \pmod{2^m}$$

如可令$x' = (x + 2^m) \bmod 2^n$，即可满足$x' \equiv x \pmod{2^m}$，且$x \neq x' \bmod 2^n$。

习题4.6： 证明$h(x)$不是原像稳固的，即证明对$x_1 = x_1'||x_1''$，可计算出$x_2 = x_2'||x_2''$，有$f(x_1' \oplus x_1'') = f(x_2' \oplus x_2'')$，只需令$x_1' \oplus x_1'' = x_2' \oplus x_2''$，即为第二原像问题的解，例如可令$x_2' = x_1' \oplus b, x_2'' = x_1'' \oplus b$其中$b \neq 0$(注意$b \neq 0$是必须的)。

习题4.7.代入公式直接计算。

习题4.12： (a)观察到如果$i_1, \ldots, i_n$是$1, 2, \ldots, n$的置换，那么$h_K(x_1, \ldots, x_n) = h_K(x_{i_1}, \ldots, x_{i_n})$。下面将证明如果$(x_1, \ldots, x_n)$不是$(x, x, \ldots, x)$的形式就可以获得假冒。假定$x_i \neq x_j, i > j$，令

$$(i_1, i_2, \ldots, i_n) = (1, 2, \ldots, i-1, j, i+1, \ldots, j-1, i, j+1, \ldots, n)$$

则$(x_1,\ldots,x_n)\neq(x_{i_1},\ldots,x_{i_n})$，那么$(x_{i_1},\ldots,x_{i_n})$是$(1,1)$假冒者。

(b)除了考虑(a)中的情况外，还需考虑$(x,x,\ldots,x)$的情况：

$$h_K(x,x,\ldots,x)=\begin{cases}0 & n\text{为偶数}\\ e_K(x) & n\text{为奇数}\end{cases}$$

可如下构造假冒者：

如n为偶数 对任意$x'\neq x$，$(x',x',\ldots,x')$是假冒者。

如n为奇数 对任意$x'\neq x$，$(x,x',\ldots,x')$是假冒者。

1.5 第5章作业

习题5.3：参考例5.1,p.130 (a)6 (b)1075 (c)1844

习题5.6：根据中国剩余定理计算

$x = 14387$

习题5.10： 对任意x有，因为$ab \equiv 1 \pmod{(p-1)(q-1)}$，因此$ab \equiv 1 \pmod{p-1}$，可设$ab = 1 + k(p-1)$。以下分情况讨论：

情况1）当$\gcd(x,p) \equiv 1 \pmod{p}$时，那么根据Fermat小定理推论得到：

$$x^{ab} \equiv x^{1+k(p-1)} \equiv x \pmod{p}$$

情况2）当$\gcd(x,p) \equiv 0 \pmod{p}$时，则有

$$x^{ab} \equiv 0 \equiv x \pmod{p}$$

因此恒有

$$x^{ab} \equiv x \pmod{p} \tag{1.2}$$

同理可证

$$x^{ab} \equiv x \pmod{q} \tag{1.3}$$

因为p, q互素，联合等式(1.2)和(1.3)，根据中国剩余定理得到

$$x^{ab} \equiv x \pmod{pq = n}$$

现在我们证明了$d(e(x)) \equiv x^{ab} \equiv x \pmod{n}$。

习题5.13：(a) 因为p, q互素，根据中国剩余定理得到RSA的解密消息$x = d_k(y) = y^d \bmod pq$ 等价于以下方程组的解：

$$\begin{aligned} x &\equiv y^d \equiv y^{d_p} \pmod{p} (d\text{可改为}d_p\text{是根据费马小定理}) \\ x &\equiv y^d \equiv y^{d_p} \pmod{q} (d\text{可改为}d_q\text{是根据费马小定理}) \end{aligned}$$

根据中国剩余定理，以上方程的唯一解，即为题目所给的解。

(b)$d_p = 907, d_q = 1345, M_q = 777, M_p = 973$

(c)$x = 1443247$

习题5.14： 设RSA的公钥为(n,b)，私钥为a。对于给定密文y，选择密文y_1,y_2满足$y=y_1y_2 \bmod n$。若知道y_1,y_2的明文为x_1,x_2，设y 的明文为x，则有

$$\begin{aligned} x &= y^a \bmod n \\ &= (y_1y_2)^a \bmod n \\ &= x_1^{ba}x_2^{ba} \bmod n \\ &= x_1x_2 \bmod n \end{aligned}$$

因此RSA对选择密文攻击是不安全的。

习题5.34 设x,y是一对RSA明文和密文。由RSA加密的乘法性质有

$$(y \times e_K(2)) \bmod n = e_K(2x \bmod n)$$

当$0 \le x < n/2$时$half(y)=0$；且有$0 \le 2x < n$，则$2x \bmod n = 2x$，那么$2x \bmod n$为偶数，则有$parity((y \times e_K(2)) \bmod n)=0$。

当$n/2 < x \le n-1$时$half(y)=1$；且有$n < 2x \le 2n-2$，则$2x \bmod n = 2x-n$，那么$2x \bmod n$为奇数，则有$parity((y \times e_K(2)) \bmod n)=1$。

综上所述有

$$half(y) = parity((y \times e_K(2)) \bmod n).$$

上式中用$(y \times e_K(2^{-1})) \bmod n$代替$y$得到

$$half((y \times e_K(2^{-1})) \bmod n) = parity(((y \times e_K(2^{-1})) \bmod n \times e_K(2)) \bmod n) = parity(y)$$

1.6 第6章作业

E6.1：对$\mathbb{Z}_p^*$上的ElGamal公钥加密体制做如下变形：
公钥α, β, p，私钥a如ElGamal体制所定义，加密如下定义：
选取随机数$x \in \mathbb{Z}_p^*$，

$$e_k(x,k) = (y_1, y_2)$$

其中

$$y_1 = \alpha^k \pmod p$$

且

$$y_2 = x + \beta^k \pmod p$$

要求：
（1）给出解密运算
答：$e_k(x) = y_2 - y_1^a \bmod p$
（2）课本中已证明ElGamal体制具有如下结论：任何解CDH的算法，都可以用于解密密文，反之亦然。请证明该结论对以上所定义的加密体制同样成立。
证明：仿照ElGamal体制的证明。我们姑且称该加密体制为RElGamal。
1.证明：任何解CDH的算法，都可以用于解密RElGamal密文

1. 假设OracleCDH是解CDH的一个算法
2. 假设：RElGamal的公钥为α, β, p，私钥a
3. 设$y_1 = \alpha^k \bmod p, y_2 = x + \beta^k \bmod p$是RElGamal密码的密文，如下计算明文$x$：

$$\delta = OracleCDH(\alpha, \beta, y_1) = OracleCDH(\alpha, \alpha^a, \alpha^k) = \alpha^{ak}$$

计算

$$x = y_2 - \delta \equiv x + \beta^k - \alpha^{ak} \bmod p$$

2.证明：任何解密RElGamal密文的算法，都可以用于解CDH

1. 假设Oracle-RElgamal-Decrypt是解密RElGamal密文的一个算法
2. 假设：CDH的输入为：$\alpha, \beta = \alpha^a, \gamma = \alpha^b$
3. 可如下计算CDH的输出α^{ab}: 令RElGamal的参数如下：公钥α, β，密文$y_1 = \gamma, y_2 \in \mathbb{Z}_p^*$为随机数，计算：

$$x = Oracle - RElgamal - Decrypt(\alpha, \beta = \alpha^a, (y_1 = \alpha^b, y_2))$$

$$\begin{aligned} &= y_2 - y_1^a \\ &= y_2 - \alpha^{ab} \end{aligned}$$

然后计算

$$\delta = y_2 - x = y_2 - (y_2 - \alpha^{ab}) = \alpha^{ab}$$

■

6.11：$f(x) = x^5 + x^2 + 1$

(a)

$$\begin{aligned} (x^4 + x^2) \times (x^3 + x^2 + 1) &= (x^7 + 2 \cdot x^5 + x^4 + x^3 + x^2) \bmod f(x) \\ &= (x^7 + x^4 + x^3 + x^2) \bmod f(x) \\ &= (x^7 + x^4 + x^3 + x^2) - x^2 f(x) \\ &= x^3 \end{aligned}$$

(b) 求$x^3 + x^2$的逆元。根据扩展Euclidean算法，得到

i	r_j	q_j	s_j	t_j
0	$x^5 + x^2 + 1$	0	1	0
1	$x^3 + x^2$	$x^2 + x + 1$	0	1
2	1	$x^3 + x^2$	1	$x^2 + x + 1$

那么$(x^3 + x^2)^{-1}$为$x^2 + x + 1$

(c)求x^{25}。指数$25 = (11001)_2$，根据平方-乘算法计算：

i	b_i	
5	1	$1^2 \cdot x = x$
4	1	$x^2 \cdot x = x^3$
3	0	$(x^3)^2 = x^3 + x$
2	0	$(x^3 + x)^2 = x^6 + x^2 = x^3 + x^2 + x$
0	1	$(x^3 + x^2 + x)^2 \cdot x = x^7 + x^5 + x^3 = x^4 + x^3 + 1$

节省运算的小技巧：如$a_i \in \mathbb{Z}_2$，则

$$(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_i x^i + \ldots + 1)^2 = a_n x^{2n} + a_{n-1} x^{2(n-1)} + \ldots + a_i x^{2i} + \ldots + 1$$

习题6.20：可编程计算。

1.7 第7章作业

练习7.1：ElGamal签名中，$p = 31847, \alpha = 5, \beta = 25703$

注意$x = 8990$的签名$(23972, 21396)$，$x = 31415$的签名$(23972, 20481)$相同的部分。对x的签名为$(\gamma = \alpha^k \bmod p, \delta = (x - a\gamma)k^{-1} \bmod p - 1)$，这意味着两次签名的随机数$k$一样，那么可利用p.229（或者相关课件）介绍的方法给出k的可能值，并通过验证等式$23972 = \alpha^k \bmod p$来唯一确定出k值。

计算出k值后，如果$\gcd(\gamma, p-1) = 1$，可根据p.229（或者相关课件）介绍的方法，给出a值，即根据以下公式计算：

$$a = (x - k\delta)\gamma^{-1} \bmod p - 1$$

但要注意这里$\gcd(\gamma, p-1) = 2$，无法根据上面公式唯一确定出a值来，因为不存在$\gamma^{-1} \bmod p$。

但这里求a的方法仍然一样，由

$$\delta = (x - a\gamma)k^{-1} \bmod p - 1$$

得到

$$a\gamma \equiv x - k\delta \bmod p - 1$$

两边除以$\gcd(\gamma, p-1) = 2$，得到

$$a\gamma' \equiv \frac{x - k\delta}{2} \bmod \frac{p-1}{2}$$

这里$\gamma' = \gamma/2$，那么得到a的两个可能解

$$a = \gamma'^{-1}\frac{x - k\delta}{2} \bmod \frac{p-1}{2} + i\frac{p-1}{2}, i = 0, 1$$

最后通过验证$\delta = (x - a\gamma)k^{-1} \bmod p - 1$来唯一确定出正确的$a$值。

练习7.4 (a)代入验证即可，课件中给出了推导的方法。

(b)代入ElGamal的第二种伪造方法计算。

练习7.5(a) 对ElGamal签名，如果$\delta = 0$，由$\delta = (x - a\gamma)k^{-1} \bmod p - 1$得到

$$(x - a\gamma) \equiv 0 \pmod{p-1}$$

因此

$$a\gamma \equiv x \pmod{p-1}$$

如果$\gcd(\gamma, p-1) = 1$，那么

$$a = x\gamma^{-1} \pmod{p-1}$$

如果$\gcd(\gamma, p-1) = d \neq 1$，类似于p.229后面的讨论，有

$$a = x'\gamma'^{-1} \pmod{p'} + ip', i = 0, 1, \ldots, d-1$$

这里

$$x' = \frac{x}{d}, \gamma' = \frac{\gamma}{d}, p' = \frac{p-1}{d}$$

最后根据$\beta = \alpha^a \bmod p$唯一确定出a值。

对DSA方案的讨论类似以上讨论，但注意对指数的模数改为q。

练习7.7：直接代入DSA算法计算。

1.8 第8章作业

练习1.18,见p.31。

答：LFSR为$z_{i+4} = (z_i + z_{i+1} + z_{i+2} + z_{i+3}) \bmod 2$，有：

(1)初始向量0000生成的周期序列为：0000

(2)初始向量0001生成的周期序列为：00011000，这也是初始向量0110,1100,1000,0011,0110生成的周期序列生成的周期序列为(初始位置不同)

(3)初始向量0111生成的周期序列为：0111101111，这也是初始向量1111,1110,1101,1011,0111生成的周期序列(初始位置不同)

(4)初始向量0010生成的周期序列为：00101，这也是初始向量0101,1010,0100,1001生成的周期序列(初始位置不同)

1.9 第9章作业

练习9.2：

假设Olga观察到Alice和Bob运行协议9.13的认证会话

Alice　　Bob

选择r_1

$y_1 = sig_{Bob}(r_1)$

$Cert(Bob), r_1, y_1$ ⟵ – – – – – –

验证$Cert(Bob)$

$ver_{Bob}(r_1, y_1) = true?$

$y_2 = sig_{Alice}(r_1)$

选择r_2

$y_3 = sig_{Alice}(r_2)$

$Cert(Alice), r_2, y_2, y_3$ – – – – – – ⟶

验证$Cert(Alice)$

$ver_{Alice}(r_1, y_2) = true?$

$ver_{Alice}(r_2, y_3) = true?$

$y_4 = sig_{Bob}(r_2)$

y_4 ⟵ – – – – – –

$ver_{Bob}(r_2, y_4) = true?$

Olga对协议9.13的并行会话攻击，成功向Alice冒充Bob：

Alice　　Olga　　Bob

重放：$Cert(Bob), r_1, y_1$ ⟵ – – – – – –

验证$Cert(Bob)$

$ver_{Bob}(r_1, y_1) = true?$

$y_2 = sig_{Alice}(r_1)$

选择r_2

$y_3 = sig_{Alice}(r_2)$

$Cert(Alice), r_2, y_2, y_3$ – – – – – – ⟶

$Cert(Alice), r_2, y_2$ – – – – – – ⟶

$Cert(Bob), y_4 = sig_{Bob}(r_2), r'_2, sig_{Bob}(r'_2)$ ⟵ – – – – – –

y_4 ⟵ – – – – – –

$ver_{Bob}(r_2, y_4) = true?$