密码学习题提示

姓名：　杨礼珍

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1.5：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$\varphi(30)30 = (2-1)\times(3-1)\times(5-1)\times 30 = 240$。

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

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

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)$d_K(e_K(x)) = 6(5x+21)+19) \bmod 29 = (6\times 5x + 6\times 21 + 19) \bmod 29 = x$

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)：

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

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！

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。

1.4 第4章作业

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5.10： 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

$$x^{ab} \equiv x \pmod{p} \tag{1.1}$$

同理可证

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

因为p,q互素，联合等式(1.1)和(1.2)，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5.14： 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$y = y_1 y_2 \bmod n$。若知道y_1, y_2的明文为x_1, x_2，设y 的明文为x，则有

$$\begin{aligned} x &= y^a \bmod n \\ &= (y_1 y_2)^a \bmod n \\ &= x_1^{ba} x_2^{ba} \bmod n \\ &= x_1 x_2 \bmod n \end{aligned}$$

因此RSA对选择密文攻击是不安全的。

特别地，对于给定密文y，敌手选择密文$\hat{y} = y^{-1} \bmod n$，若获得$\hat{y}$的明文$\hat{x}$，那么密文y的明文$x = \hat{x}^{-1} \bmod n$。

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$0 \leq x < n/2$时$half(y) = 0$；且有$0 \leq 2x < n$，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$n/2 < x \leq n-1$时$half(y) = 1$；且有$n < 2x \leq 2n-2$，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

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

■

E6.2：设在ElGamal密码体制中，私钥$a \in \mathbb{Z}_{p-1}$，公钥为(p, α, β)，其中p为素数，α为模p本原元，$\beta = \alpha^a \bmod p$。如果加密运算中泄露了随机数k，会带来什么安全问题？

答：如果泄露了随机数k，敌手可计算出明文：

$$x = y_2 \beta^{-k} \bmod p$$

1.7 第7章作业

E7.1：RSA'签名方案如下：公钥(n, b)，其中$n = pq$，p和q为素数，$b \in \mathbb{Z}_n$。私钥$a \in \mathbb{Z}_n$，满足

$$ab \equiv 1 \pmod{(p-1)(q-1)}.$$

签名算法(x)：对消息$x \in \mathbb{Z}_n$计算

$$y = x^{2a} \bmod n$$

验证算法(x, y)：如果$x^2 = y^b \bmod n$，则输出true，否则输出false。

请给出RSA'签名算法的一个安全分析，并指出是哪种类型的分析（如已知消息攻击的存在性伪造）。

答：敌手如果获得消息x_1, x_2的签名y_1, y_2，则可伪造$x = x_1 x_2 \bmod n$的签名

$$y = y_1 y_2 \bmod n$$

这是已知消息的存在性伪造。