姓名：洪继耀 学号:2014150120

计算机安全导论作业1

第一章

- 1.1
  - **安全性**要求：
    - 能用数据库存储用户资料，查询时需要密码
    - 用户资料经过加密
  - **可用性**要求：
    - 受到黑客攻击时，系统不崩溃
  - **完整性**要求：
    - 存取的信息实时更新
    - 数据库有备份
    - 修改信息时有记录
    - 修改信息需要一定权限和认证
- 1.4
  - (a)影响比较低，因为是内部管理的**公开信息**，不需要保密，也容易恢复
  - (b)影响中等左右，因为属于**敏感信息**，但来源又是**调查信息**。
  - (c)影响比较低，同(a)
  - (d)影响都比较高，属于**商业机密**，必须保证保密和准确安全可靠。
  - (e)非常高，这属于**军事机密**。

第二章

- 2.2

  仿射密码的公式：$d(x) = a^{-1}(x-b) \pmod m$

  其中

  - a和m互质。
  - m是字母的数目。这里假设是26

  那么a的取值可能是 1 3 5 7 9 11 15 17 19 21 23 25共12种，

  b可取26种

  则有12*26=312种密码

- 2.3
  假设密码频率和明文频率一一对应，则明文->密文有e->b t->u

  而e=4 b=1 t=19 u=20 则：
  $1 \ = \ (4a+b) \ mod \ 26$
  $20 = \ (19a+b) \ mod \ 26$
  两式相减消去b有
  $19 \ = \ (15a) \ mod \ 26$
  对于上式，代入a=0,a=1,a=2,a=3，在代入a=3的情况下成立。
  因此a的最小解为3，代入得到b=15

  故破解得到$m = (3p+15) \ mod \ 26$
- 2.5
  - 加密的算法是**一一对应**替代密码，即t->a，h->b，e->c，以此类推
  - 单表密码，非常不安全
  - 因为**一句话里可能不覆盖所有字母——**第一句话不够长还可以往后面取句子补密码表，最后一句话就没辙了
- 2.6
  - 根据推理小说的套路，这种 数字+字母+有意义的单词 的密文，很大几率不过是整词替换罢了。
  - 观察第一个数字，三位数，根据套路，很可能是书的页码。而第二个字符串C2很可能表示column-2，也就是第二列。
  - 后面的内容，数字表示该列的第几个单词，英文直接照抄，这样就能得到正确的明文了。

第四章

- 4.15
  - $gcd(24140, 16762)$
    - $24140 = 16762 * 1 + 7378$
    - $16762 = 7378 * 2 + 2006$
    - $7378 = 2006 * 2 + 1360$
    - $2006 = 1360 * 1 + 646$
    - $1360 = 646 * 2 + 68$
    - $646 = 68 * 9 + 34$
    - $68 = 34 * 2 + 0$
    - 因此$gcd(24140, 16762) = 34$
  - $gcd(4655, 12075)$
    - $12075 = 4655 * 2 + 2765$
    - $4655 = 2765 * 1 + 1890$
    - $2765 = 1890 * 1 + 875$
    - $1890 = 875 * 2 + 140$
    - $875 = 140 * 6 + 35$
    - $140 = 35 * 4 + 0$
    - 因此$gcd(4655, 12075) = 35$
- 4.16
  - (a)利用反证法：
    1. P：$m/2 <= r$ 即$m <= 2r$

2. 假设P成立
3. 有$m-r<=r$
4. 也就是$qn<=r$
5. 另一方面$q>0$且$r<n$且q,r,n为整数
6. 也就是$qn>r$
7. 4和6得出矛盾，即2是不对的，P不成立
8. 原命题得证

- (b)利用(a)的结论
  - 欧几里得算法是形如$m=qn+r$的迭代
  - 假设第i次迭代$A=B*X+C$
  - 则第i+1次迭代$B=C*Y+D$
  - 则第i+2次迭代$C=D*Z+E$
  - 由(a)的结论有$A>2C$
  - 也就是$A_{i+2}<A_i/2$ 命题得证
- (c)利用(b)的结论
  1. 因为$n\leq 2^n$ 经过$2n$轮变换之后，根据(b)的结论，有$n_{2n+1}<2$
  2. 也就是说这个时候等式$m=qn+r$左边的m非0即1
  3. 如果是0，说明在$2n$轮之前就已经求得结果
  4. 如果是1，说明qn是1，那么r必然是0 也就是求得结果
  5. 所以无论如何肯定求得结果了

- 4.19
  - (a) 1234 mod 4321
    - 也就是求$1234x\equiv 1 \pmod{4321}$的$x$
    - 也就是求解 $1234x+4321y=1$
    - 求$gcd(1234,4321)$
    - $4321=1234*3+619$
    - $1234=619*1+615$
    - $619=615*1+4$
    - $615=4*153+3$
    - $4=3*1+1$
    - $3=1*3+0$
    - 也就是$gcd(1234,4321)=1$ 模逆元存在
    - 改写上面各式子
    - $(1)\ 619=4321+1234*(-3)$
    - $(2)\ 615=1234+619*(-1)$
    - $(3)\ 4=619+615*(-1)$
    - $(4)\ 3=615+4*(-153)$
    - $(5)\ 1=4*1+3*(-1)$
    - 联立$(4)(5)$得到
    - $1=4+(615+4*(-153))*(-1)$
    - $(6)\ 1=4*154+615*(-1)$
    - 联立$(3)(6)$得到
    - $1=(619+615*(-1))*154+615*(-1)$
    - $(7) 1=619*154+615*(-155)$
    - 联立$(2)(7)$得到
    - $1=619*154+(1234+619*(-1))*(-155)$

    - $(8)\ 1 = 619 * 309 + 1234 * (-155)$
    - 联立(1)(8)得到
    - $1 = (4321 + 1234 * (-3)) * 309 + 1234 * (-155)$
    - 即$1 = 4321 * 309 + 1234 * (-1082)$
    - 解得$x = -1082$
      $y = 309$
    - 答案也就是-1082
    - 即$1234 * (-1082) \equiv 1 \pmod{4321}$
- (b) 24140 mod 40902
    - 求$gcd(24140, 40902)$
    - $40902 = 24140 * 1 + 16762$
    - $24140 = 16762 * 1 + 7378$
    - $16762 = 7378 * 2 + 2006$
    - $7378 = 2006 * 3 + 1360$
    - $2006 = 1360 * 1 + 646$
    - $1360 = 646 * 2 + 68$
    - $646 = 68 * 9 + 34$
    - $68 = 34 * 2 + 0$
    - 也就是$gcd(24140, 40902) = 34 \neq 1$
    - 结论：模逆元不存在
- (c) 550 mod 1769
    - 求$gcd(550, 1769)$
    - $1769 = 550 * 3 + 119$
    - $550 = 119 * 4 + 74$
    - $119 = 74 * 1 + 45$
    - $74 = 45 * 1 + 29$
    - $45 = 29 * 1 + 16$
    - $29 = 16 * 1 + 13$
    - $16 = 13 * 1 + 3$
    - $13 = 3 * 4 + 1$
    - $4 = 1 * 4 + 0$
    - 也就是$gcd(550, 1769) = 1$，模逆元存在
    - 整理过程，有
    - $119 = 1769 + 550 * (-3)$
    - $74 = 550 + 119 * (-4)$
    - $45 = 119 + 74 * (-1)$
    - $29 = 74 + 45 * (-1)$
    - $16 = 45 + 29 * (-1)$
    - $13 = 29 + 16 * (-1)$
    - $3 = 16 + 13 * (-1)$
    - $1 = 13 + 3 * (-4)$
    - 整理上述各式，有
    - $1 = 13 + (16 + 13 * (-1)) * (-4)$
    - $1 = 13 * 5 + 16 * (-4)$
    - $1 = (29 + 16 * (-1)) * 5 + 16 * (-4)$
    - $1 = 29 * 5 + 16 * (-9)$
    - $1 = 29 * 5 + (45 + 29 * (-1)) * (-9)$

- $1=(74+45*(-1))*14+45*(-9)$
- $1=74*14+45*(-23)$
- $1=74*14+(119+74*(-1))*(-23)$
- $1=74*37+119*(-23)$
- $1=(550+119*(-4))*37+119*(-23)$
- $1=550*37+119*(-171)$
- $1=550*37+(1769+550*(-3))*(-171)$
- $1=550*550+1769*(-171)$
- 也就是说550对1769的模逆元是550
- 即$550*550 \equiv 1 \pmod{1769}$

第三章

3.11

主密钥：0000 0001 0010 0011 0100 0101 0110 1000 1001 1010 1011 1100 1101 1110 1111

明文　：0000 0001 0010 0011 0100 0101 0110 1000 1001 1010 1011 1100 1101 1110 1111

1. 推导第一轮的子密钥
    - 选择置换1后：1111 0000 1100 1100 1010 1010 0000 1010 1010 1100 1100 1111 0000 0000
    - 选择置换2后：0000 1011 0000 0010 0110 0111 1001 1011 0100 1001 1010 0101 0000 0000
2. 推导L_0，R_0
    - L_0，R_0即IP置换后的两个半块
    - $L_0=$ 1100 1100 0000 0000 1100 1100 1111 1111
    - $R_0=$ 1111 0000 1010 1010 1111 0000 1010 1010
3. 扩展R0求E[R0]
    - $E[R0]=$0111 1010 0001 0101 0101 0101 0111 1010 0001 0101 0101 0101
4. 计算A= E[R0]^ K1
    - $A=$0111 0001 0001 0111 0011 0010 1110 0001 0101 1100 1111 0000
5. 把上题的48位结果分为6位的集合并求对应S盒代换的值
    - 011000 = 5
    - 010001 = 12
    - 011100 = 2
    - 110010 = 1
    - 111000 = 6
    - 010101 = 13
    - 110011 = 5
    - 110000 = 0
6. 利用上题的结论求32位的结果B
    - $B=S(A)=$0000 0000 1010 1010 1111 0000 1010 1010
7. 应用置换求P(B)
    - $P(B)=$0010 1001 0100 0110 0000 0101 1100 0101
8. 计算R1=P(B)^ L0
    - $R1=$1110 0101 0100 0110 1100 1001 0011 1010

9. 写出密文

    - 经过16轮次之后，变成了
    - 0100 0101 1010 1010 1001 0101 0100 0101 0001 1111 1111 1111 1010 0100 1111 1100
    - 经过最终置换变成了
    - 1110 0101 1011 0000 1110 1111 1011 0010 1010 0110 0011 1010 0110 0011 0011 1110
    - 转换为8字节的byte数组为：$\{-89, 13, -9, 77, 101, 92, -58, 124\}$