现代密码学作业——第二讲

1)

加密 $C = E(p) = (7\times9+3, 14\times9+3, 19\times9+3) \bmod 26$

$= (14, 25, 18)$

$= OZS$

由欧几里得除法可知 $a^{-1}=3$

解密 $P = D(C) = [(14-3)\times3, (25-3)\times3, (18-3)\times3] \bmod 26$

$= (7, 14, 19)$

$= hot$

2)

明文 $P = (15, 11, 4, 0, 18, 4, 10, 4, 4, 15, 19, 7, 8, 18, 12, 4, 18, 18, 0, 6, 4, 8, 13, 18, 4, 2, 17, 4, 19)$

密钥 $K = (2, 14, 12, 15, 20, 19, 4, 17)$

密文 $C = (15+2, 11+14, 4+12, 0+15, 18+20, 4+19, 10+4, 4+17, 4+2, 15+14, 19+12, 7+15, 8+20, 18+19, 12+4, 4+17, 18+2, 18+14, 0+12, 6+15, 4+20, 8+19, 13+4, 18+17, 4+2, 2+14, 17+12, 4+15, 19+20) \bmod 26$

$= (17, 25, 16, 15, 12, 23, 14, 21, 6, 3, 5, 22, 2, 11, 16, 21, 4, 6, 12, 21, 24, 1, 17, 9, 6, 16, 3, 19, 13)$

$= rzqpmxovgdfwclqvemvybrjgqdtn$

3)

明文 $p = (7, 8, 11, 11)$

密文 $C = (7, 8, 11, 11)\begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix} \bmod 26 = (9, 8, 8, 24) = jiiy$

4）单表代换密码：

```
import random
#单表代换加密
def encode(plaintext,key):
    print(plaintext,key)
    for p in plaintext:
        temp=key[ ord(p.upper())-ord("A")]
        print(chr(ord("A")+temp),end="")
#单表代换解密
def decode(cipher,key):
    print(cipher,key)
    for c in cipher:
        cnum= ord(c.upper())-ord("A")
        for i in range(0,26):
            if(key[i]==cnum):
                break
        print((chr(i+ord("A"))),end="")
#key=random.sample(range(0,26),26)
key= [3, 15, 24, 20, 23, 25, 1, 4, 21, 2, 5, 17, 22, 14, 11, 6, 8, 10
, 18, 19, 9, 0, 7, 13, 12, 16]
encode("abcdef",key)
print()
decode("DPYUXZ",key)
```

仿射密码：

```
#key=(a,b)
import random
#欧几里得判断两数最大公因数是不是 1
def gcd(a,b):
    if(a<b):
        return gcd(b,a)
    while(a%b!=0):
        temp=b
        b=a%b
        a=temp
    return b
#遍历求逆
def qiuNi(a):
    for i in range(1,26):
         if((a*i-1)%26==0):
            return i
#仿射加密
def encode(plaintext,a,b):
```

```
    print(plaintext,a,b)
    for p in plaintext:
        if(p==" "):
            print(" ",end="")
        pnum=ord(p.upper())-ord("A")
        temp=(pnum*a+b)%26
        print(chr(temp+ord("A")),end="")
#仿射解密
def decode(cipher,a,b):
    print(cipher,a,b)
    a_Ni=qiuNi(a)
    for c in cipher:
        if(c==" "):
            print(" ",end="")
        cnum=ord(c.upper())-ord("A")
        temp=(cnum-b)*a_Ni%26
        print(chr(temp+ord("A")),end="")

a=random.randint(1,25)
b=random.randint(1,25)
#plaintext=input()
while  gcd(a,26)!=1:
         a=random.randint(1,25)
#encode(plaintext,a,b)
encode("hot",9,3)
print()
decode("ozs",9,3)
```

5)

密码	穷尽搜索的复杂度
移位	O(25)
仿射	O(12*26)
单表代换	O(26!)
维吉尼亚密码	$O(26^m)$
多表代换	$O((26!)^m)$
置换密码	O(m!)

6）多表代换，置换密码，希尔密码属于分组加密。多表代换要将明文 m 个分组成一段，不足 m 的元素填充按密钥对应不同的密码表加密。置换密码和希尔密码分组后不足 m 的要进行补齐，然后进行换位或与矩阵做乘法。

7)

密钥：prouder

解密：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.