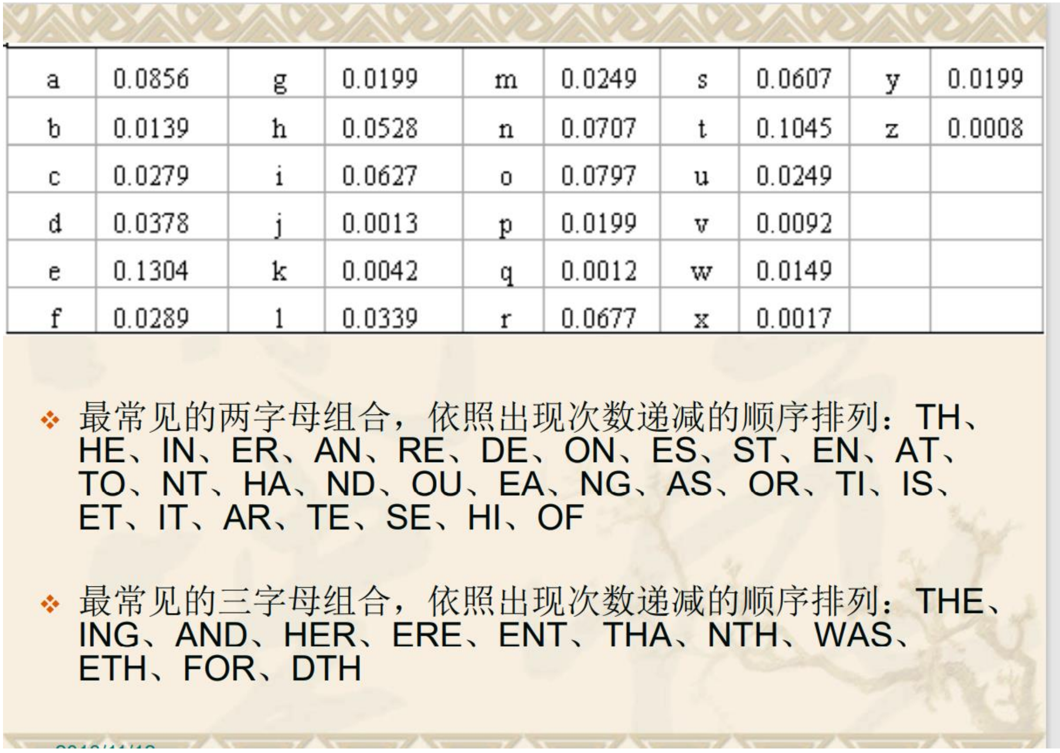
# 信息安全作业

## 通信一班 孙留羿 202000120166 提交时间 2021 年 12 月 10 日

1.（统计频率代码见附录）

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEPHZHMDZSHZQWSFP
APPD TSVPQUZWYMXUZUHSXEPYEPOPPZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

```
频次： 2 2 0 5 6 4 2 7 1 1 0 0 8 0 8 17 4 0 10 3 10 5 4 5 2 14
```



| a | 0.0856 | g | 0.0199 | m | 0.0249 | s | 0.0607 | y | 0.0199 |
|---|---|---|---|---|---|---|---|---|---|
| b | 0.0139 | h | 0.0528 | n | 0.0707 | t | 0.1045 | z | 0.0008 |
| c | 0.0279 | i | 0.0627 | o | 0.0797 | u | 0.0249 | | |
| d | 0.0378 | j | 0.0013 | p | 0.0199 | v | 0.0092 | | |
| e | 0.1304 | k | 0.0042 | q | 0.0012 | w | 0.0149 | | |
| f | 0.0289 | l | 0.0339 | r | 0.0677 | x | 0.0017 | | |

- 最常见的两字母组合，依照出现次数递减的顺序排列：TH、HE、IN、ER、AN、RE、DE、ON、ES、ST、EN、AT、TO、NT、HA、ND、OU、EA、NG、AS、OR、TI、IS、ET、IT、AR、TE、SE、HI、OF
- 最常见的三字母组合，依照出现次数递减的顺序排列：THE、ING、AND、HER、ERE、ENT、THA、NTH、WAS、ETH、FOR、DTH

统计单字母出现频率与已知字母出现频率进行对照，得 P 为 E，Z 为 T，S 为 A，U 为 I 依照单词出现频率，推测 W 为 H，对剩余字母逐渐猜测匹配得到

:

itwasdisclosedyesterdaythatseveralinformalbutdirectcontactshavebeenmadewithpoliticalrepresentativesofthevietconginmoscow

```
频次

A B  C D  E  F  G  H I J  K  L M  N O  P  Q   R  S T U  V  W  X  Y Z

51 24 35 9 10 13 18 2 9 39 10 1 39 0 20 31 73 28 47 8 1 28 14 20 8 6
```

JXQCEFMPJASOQMDPQABCSTYSMGRQBTQOASKQAOUWCPQBDPMEEASIVMWPOQVJXQVQCSORW
BQKMMYVJQAOXQPVASBFPAOJCOARQHFQPCQSOQASBQAOXXAVCJVMGSABZASJATQVJXQYSM
GRQBTQGQTACSDPMEKMMYVASBDMPEARQBWOAJCMSQSAKRQVWVJMRQAPSAKMWJJXCSTVXAJ
GQXAZQSMMFFMPJWSCJIJMQHFQPCQSOQCSBACRIRCDQGOOASVJWBIARRJXQFRAOQVCSJXQ

GMPRBASBRQAPSDPMEFQMFRQGQGCRRSQZQPEQQJCSMWRCDQJCEQLWVJKIPQABCSTJXQCPK
MMYVGQOASARVMBQZQRMFMWPASARIJCOARVYCRRVASBRQAPSXMGJMZCQGASBCSJQPFPQJJ
XQGMPRBAPMWSBWVCSBCDDQPQSJGAIVGQOASRQAPSJXQFAVJKIPQABCSTKMMYVCSJXCVGA
IGQGMSJPQFQAJJXQECVJAYQVMMJXQPVASBOASKWCRBMSJXQCPAOXCQZQEQSJV

| | | |
|---|---|---|
| 73 | Q | E |
| 51 | A | T |
| 47 | S | A |
| 39 | M | O |
| 39 | J | N |
| 35 | C | R |
| 31 | P | I |
| 28 | V | S |
| 28 | R | H |
| **24** | B | D |
| 20 | X | L |
| 20 | O | F |
| 18 | G | C |
| 14 | W | M |
| 13 | F | U |
| 10 | K | G |
| 10 | E | Y |
| 9 | I | P |
| 9 | D | W |
| 8 | Y | B |
| 8 | T | V |
| 6 | Z | K |
| 2 | H | J |
| 1 | U | X |
| 1 | L | Q |
| 0 | N | Z |

（注）以下将大写字母作为替换前字母，小写字母作为替换后字母

(1) 假设 Q 为 E 那么统计前三个字母出现频率已知 JX 其为 th，故密文并不完全按照频率统计规律排列，

(2) 观察剩余部分发现有 eet 组合，易猜测常用单词 meet ，故 E 对应 m.

(3) 按频率开始对 A 进行处理，则在大概范围内，A 应为 a 或 o。

(4) 与同样出现频率较高的 M 联合猜测，有多个重复出现的 MM 组合，按照英文出现频率应为 oo，故 A 为 a

(5) 继续按频率将 C 替换为 r 但并没有很多明显词汇出现故暂时搁置。

(6) 按照多字母出现频率进行修改，出现大量 DPom，在对应频率范围内寻找常用组合字，找到了 from，故将 DP 分别替换为 fr 进行尝试

(7) 因 r 已被占用，在频率范围内寻找未被占用的字母，C 可能为 nish。逐一进行尝试
为 n 时有 mn,hn 等不常用组合，故暂时不选，替换为 i 时有 their，it 等常用词组，故暂时认为为 i

(8) 开头部分出现 the+imFortaSOe。与 the importance 相似，故将 FSO 替换为 pnc 进行尝试

(9) 同理将之后出现的 theimportanceofreaBinT，替换为 the importance of reading，即 BT 转

换为 dg

(10)teacherV，在名词后出现单一无关联字母，考虑为复数形式，故为 s

(11)eHperience　experience H 应为 x

(12)Rearn　　learn R 应为 l

(13)indailIlife in daily life　I 应为 y

(14)YnoGledge knowledge　YG 应为 kw

(15)soWrces sources　W 应为 u

(16)educationenaKlesus　education enables us　K 应为 b

(17)itsownadZantages　its own advantages　Z 应为 v

(18)canbeacUuiredfrom　　can be acquired from　U 应为 q

得到

theimportanceofreadingknowledgecanbeacquiredfrommanysourcestheseincludebooksteachersandpracticalexperienceandeachhasitsownadvantagestheknowledgewegainfrombooksandformaleducationenablesustolearnaboutthingshatwehavenoopportunitytoexperienceindailylifewccanstudyalltheplacesintheworldandlearnfrompeoplewewillnevermeetinoulifetimeLustbyreadingtheirbookswecanalsodevelopouranalyticalskillsandlearnhowtoviewandinterprettheworldaroundusindifferentwayswecanlearnthepastbyreadingbooksinthiswaywewontrepeatthemistakesoothersandcanbuildontheirachievements

The importance of reading knowledge can be acquired from many sources, these include books, teachers and practical experience and each has its own advantages. The knowledge we gain from books and formal education enables us to learn about things that we have no opportunity to experience in daily life. We can study all the places in the world and learn from people we will never meet in our life time. Just by reading their books, we can also develop our analytical skills and learn how to view and interpret the world around us in different ways. we can learn the past by reading books in this way we won't repeat them is takes of other sand can build on their achievements.

2.playfair（代码见附录）

（注）2 3 4 5 均用同一明文

1 转英文

ThebirthandrapiddevelopmentofquantumcommunicationsecuritytechnologymainlydependsonthefollowingtwofactorsaClassicalsecurecommunicationisfacedwiththreekeyproblemsthatataredifficulttobethoroughlysolvednamelykeynegotiationidentityidentificationandeavesdroppingdetectionTheeffectivesolutionoftheseproblemsrequiresnewtechnologiesbIntheexplorationofnewtechnologiespeoplehavediscoveredtheinherentsecuritycharacteristicsofquantumanditspossibleapplications

2 去标点和空格

ThebirthandrapiddevelopmentofquantumcommunicationsecuritytechnologymainlydependsonthefollowingtwofactorsaClassicalsecurecommunicationisfacedwiththreekeyproblemsthatar edifficulttobethoroughlysolvednamelykeynegotiationidentityidentificationandeavesdroppingdetectionTheeffectivesolutionoftheseproblemsrequiresnewtechnologiesbIntheexplorationofnewtechnologiespeoplehavediscoveredtheinherentsecuritycharacteristicsofquantumanditspossibleapplications

密钥：xinxianquan

wfucaowfqakynrabeuzbgsrocqvmlxdxxwftbptucxnbxybvqpuddmxvzvudpcsgvotrqnqhakcscqerpiwfulsggsvnihvymgndvmsmndkqmqnbqkzldbsdbptucxnbxybvanmlnduevnwfwfsddldzrsvgslomwfxydyuexggxdbfzvmcuwfpsmbhkkzmpgzueaqsukzldwablmvnqvxpiabcqvxvzabcqvxgxdnvxpiqaeuiylzkyproniheuzuuwbvxwlculluuwbilzsgfxbvipmxlczlrsvgslomsdxeaolzqcyvudpcsgvoqboenawfuqnmgsydvxpimgqcyvudpcsgvoqbmrbsshcliyueqobpzbsduylcnalcsdxwzldboavzhpdyndzuoamznbmplxdxxwftqabazmrpmqbgslnrshnbxybvqp

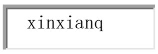
3.转轮机编写

（3 轮）

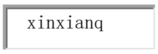
JlxjqcsuowpjfxjshkhdnqrfoztdpdnrfxfooceombdztbyojtilbdnwwpmtqhrqkxchgrtsbjawziwgvxfyogkhmwkqydjwjpnkygdmmPxzlbvotivdzjojuvrbpfbfvhvmaennoniiirmvhydhfkzfcaasvhxapvxlhpivqeisrwztrnrwflfigoxslnurlxikwqecygknrhpihilugfrruonnnpfabqguawyowdhvoukeqnbuhnztgbahqxlatbfjhnrJvjyoeayhpaxthzaxiexlnyunekdywzbugocfstxvrhfejkypbmkvntbonwNtwztkxqcyblahbpltkwxenelcsevdstjbvdsaetiyaciqrnyfqzyfwibcsuznmhigiaahwyctdfuohirabllqwpbzdoyaefipqrunbbhezgyyvcxjlqnyngcl

4. DES 密码编写;

密码 xinxianq


xinxianq

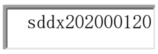
偏移量 xinxianq


xinxianq

+ExQNm/tSc6y+RRnrBTpDd1Q+pY8TeYppAt4Mr2SYNNxgAWnqmxsbvLhVMwSwLbaiCVhUmiuEDM5YPqHHLrbXT3BlWfEfIU+m3v+zKzvuLHxSZDHMDngiEABaJemcEN9jOYwPLNVsLd2EGNFbsqWcgSb+IjG+62ICSzUry07gLz2Trw/i7FKXB4DW5h2pFElLXAzW3KOpW6OvSePap4tjjsm/ZSUswBDvF1ME3TFKuyqEYbuRPMxUOO/wfV6thvpuYPhMpEoUriOJhTQDF2YdvRCkbluiHpLAKMOo5LFWkmGdJfAgUyPaYcSTtHYoJ6e//u5IzwEw+xaklfLn4CHRnR1BXSxGwi3S+4t/lmLIONFAFbpdIPNUZ2/PFWdawVK31QrutI9yuBpreIKV+xA5r4UOwoIepo9rrUDOiFeqFhdma/93/srkQBckpVPMYDiiMaYYKCiH8GF8ohFCQg56w==

5.AES 密码编写

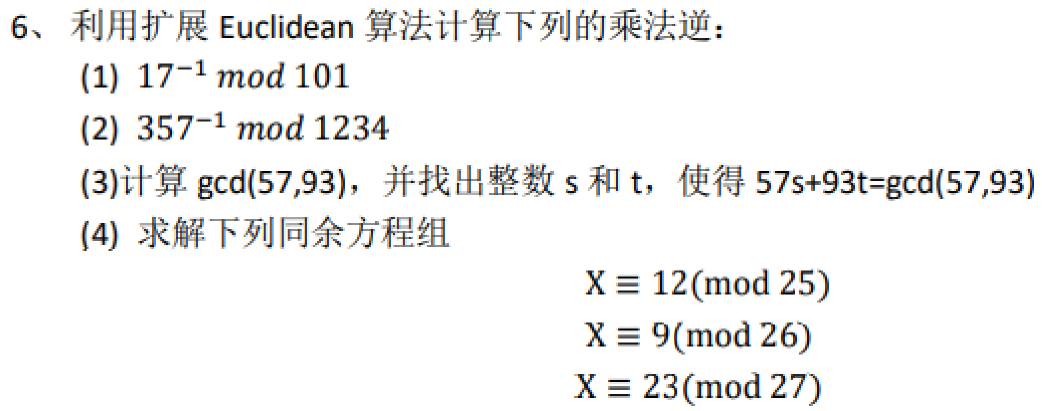
密码 sddx202000120166


sddx202000120

偏移量 sddx202000120166

sddx202000120

TwJ9ONJcsHtPAK61LV4AUzJ4TZKwJRTsbxvaUzO8gBxlYVLsB3THKYnRFeOVEsZWBGV+K
/CoM7eBa7DUqXtOFhgPVm9r1klopyj2Df8n7zTx3E8gwnqO0AxjnO1skk2gvHOmp74GAO
9COlYhOvJ+O78NLb2EhxuWIOZp2ytYef9GOovdzA9BQ/6loNraake5Tv5OILM/xephWgC
OGUudY4qOzQ9ZhhyljogBOIKeNFhlYHOh1BEC6k1OFjYAxEgFYi/RB3SuSs1QXHsKqzNE
3RCYxsIHZmqwowhGRFYTiPGUZ9ECeDu3M5TnNG2qGcsuPSn46NaGUwpLmSmeOk+E7UInZ
Y8NkKdfCda6WjeSg3aOrGLaRHyqKoCifXJMjiyoCCE8LsDs5n629AYQMYY1diCO9vrrNJ
OE+ffG7PxNbdRo2DxGtTJPjmfxhgIOH3XSY3uvO/+1myW3Xqrm5Wt95Q==



6、 利用扩展 Euclidean 算法计算下列的乘法逆：

(1) $17^{-1}\ mod\ 101$

(2) $357^{-1}\ mod\ 1234$

(3)计算 gcd(57,93)，并找出整数 s 和 t，使得 57s+93t=gcd(57,93)

(4) 求解下列同余方程组

$$X \equiv 12(\bmod 25)$$
$$X \equiv 9(\bmod 26)$$
$$X \equiv 23(\bmod 27)$$

（代码见附录）

(1) 6

(2) 1

(3) 3  -13 8

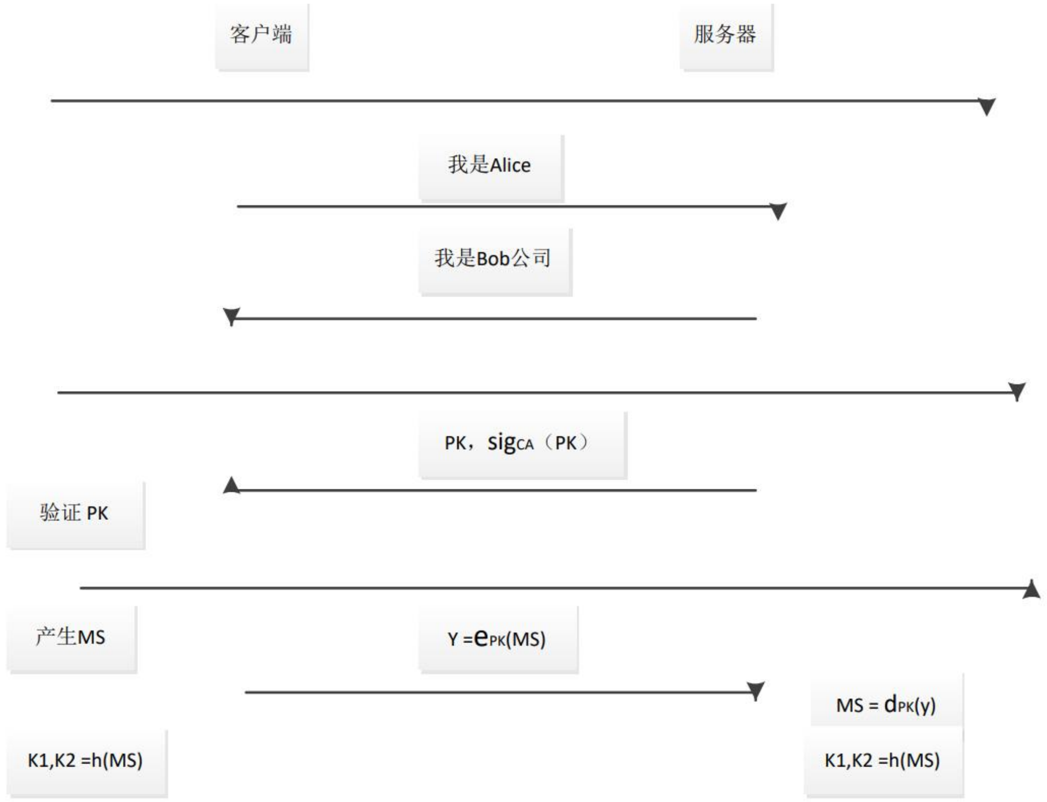
(4)14387

7、 建立一个 SSL 会话，如图 1。结合服务器到客户端的认证，但是没有客户端到服务器的 认证。设客户端（Alice）准备使用信用卡从服务器（Bob 公司）购买一些东西。图 1 协议被用来派生密钥 K1 和 K2，这两个密钥将被用来加密和认证 Alice 的信用卡号以保证 SSL 会话的安全（当卡号被发送给 Bob 公司时）。简明地讨论下面几点关于 SSL 的问题：

（a） 为什么需要 Alice 的 Web 浏览器认证 Bob 的公钥？

（b）在这个版本的协议中，Bob 没有办法建立阶段认证 Alice，这对 Bob 来说有问题 吗？为什么？

（c） 密钥 k1 和 k2 从一个由 Alice 提供的随机数 MS 派生出来，为什么随机数是由 Alice 生成而不是 Bob 公司？这种方法产生密钥 K1 和 K2 有潜在安全威胁吗？



解:
(a) Alice 的 Web 浏览器需要通过验证 Bob 公钥以确认公钥验证签名数据。
(b)可能有问题，Bob 无法确认 Alice 所处安全与否，存在一定风险。
(c)如果随机数由 Bob 公司生成，若 Bob 被攻击，MS 泄露情况，且 Alice 仍用该随机数的 hash 值作为密钥加密，则攻击者可以试探 Alice 的密文并得到 Alice 的信用卡号，导致 Alice 财产问题出现，所以应由消费者 Alice 生成，问题只会交由供货方，不会造成财产损失。

8、说说你对信息安全的理解

信息安全是对于信息的安全问题，而我们现在处于信息化社会，身边小至当前所处的位置，今天要吃的食物，大到身份信息以及各种个人账户乃至银行卡密码都是信息，而有些信息需要高度保密，就必然存在着安全问题。

首先对于信息安全这一学科以我的理解，是基于数学的一门学科，从古典的凯撒密码以及 enigma 机作为一个简单的数学映射关系，到现在对称以及非对称密码体制和大素数分解还有哈希散列表等数据结构，和未来的量子通信，其本质都是可以看作不同的数学问题。

基于对数学的一点兴趣，我在大一下曾经尝试过网络空间安全学院的春转，可惜对于大一上知识的不使用导致迅速遗忘，使我在面试中关于线性代数的问题没有能回答上来，进而没有能转入，但我对于信息安全的重视以及看好是不会改变的，因为不管是我现在所处的通信工程专业，还是以后要从事的其他行业，都对信息安全方面提出了相当高的要求，并且，在小时候经历过 QQ 被盗号我却无能为力只能通过不断申诉进行找回的无力感，所以我依然会继续学习有关信息安全方面的问题。

最后对于这次信息安全作业，我还是认识到了自己实力的不足，对于第一题的单表代换本来以为是非常容易的一个频率统计题目，可当统计出频率之后发现现实和理想之间是有相当大的差距的，我们不能寄希望于密码总是出成符合规律的样子，只能和题解中一样，用漫

长的十八步分析对字母进行逐一的确定，play fair 还可以借助网络工具加上自己的编码能力实现， 几个简单的数论问题都是我以前做过的题目，可以直接拿以前的代码来解决。

总而言之信息安全是一个很重要的学科，尤其是现在处于一个信息化的时代，人们对于信息安全的重视也势必会逐渐加强，未来我们对于信息安全也必然会有进一步的学习以及应用。

2 附录：

***（注）代码实际编译与执行均在 acwing 在线测试平台上操作***

C + +

1.

统计频率代码

```
#include  < iostream >
#include  < cstring >
#include  < algorithm >
const int N  =  28;
int a[N];
char str[1001];
using namespace std;

int main()
{
        cin >> str;
        memset(a, 0, sizeof a);
        for(int i = 0; str[i]! = '\0'; i + +)
               a[str[i]  −  'A']  + + ;
       for (int i  =  0;  i  <  26;  i  + + )
               cout  ≪  a[i]  ≪  ' ';

}
```

2、play fair 代码

```
#include < iostream >
#include < cstring >
#include < algorithm >
const int N  =  1e8;

bool flag[25];
using namespace std;

int main()
{
char zimu[26]  = {"ABCDEFGHIKLMNOPQRSTUVWXYZ"};
memset(flag, 0, sizeof flag);
char ch[5][5];
char miyao[N];//key
char juzhen[N];//plaintext
char nonr;//non − related char
int len = 'a' − 'A';
cin >> miyao;
for(int i = 0; i < strlen(miyao); i ++ )
{
miyao[i] = toupper(miyao[i]);
if(miyao[i] == 'J' )
miyao[i] = 'I';
}
cin >> nonr;
if(nonr >= 'a')
nonr = nonr − len;

int a1 = 0, a2 = 0;
for(int i = 0 ; i < strlen(miyao); i ++ )
{
for(int j = 0; j < 25; j ++)
{
if(miyao[i] == zimu[j] && flag[j] == 0)
{
ch[i][j] = letters[j];
flag[j] = 1;
if( j < 4 ) j ++ ;
else
{
i ++;
j = 0;
}
}
}
}
cin >> juzhen;
for(int i = 0; i < strlen(juzhen); i ++)
{
juzhen[i] = toupper(juzhen[i]);
if(miyao[i] == 'J' )
miyao[i] = 'I';
}

for(int i = 0; i < strlen(juzhen); i += 2 )
{
if(juzhen[i] == juzhen[i + 1])
```

```
{
for(int j = strlen(juzhen); j > i; j -- )
{
juzhen[j + 1] = juzhen[j];
}
juzhen[i + 1] = nonr;
}
}
if(strlen(juzhen) % 2 ! = 0)
{
juzhen[strlen(juzhen) + 1] = juzhen[strlen(juzhen)];
juzhen[strlen(juzhen)] = nonr;
}
for(int i = 0; i < strlen(juzhen); i += 2 )
{
int m1,m2,n1,n2;
for(m1 = 0; m1 <= 4; m1 ++)
{
for(n1 = 0; n1 <= 4; n1 ++)
if(juzhen[i] == ch[m1][n1] ) break;
if(juzhen[i] == ch[m1][n1] ) break;
}
for(m2 = 0; m2 <= 4; m2 ++)
{
for(n2 = 0; n2 <= 4; n2 ++)
if(juzhen[i + 1] == ch[m2][n2] ) break;
if(juzhen[i + 1] == ch[m2][n2] ) break;
}
m1 = m1 % 5,m2 = m2 % 5;
if(n1 > 4)
n1 = n1 % 5,m1 = m1 + 1;
if(n2 > 4)
n2 = n2 % 5,m2 = m2 + 1;
if(m1 == m2)
{
juzhen[i] = ch[m1][(n1 + 1) % 5];
juzhen[i + 1] = ch[m2][(n2 + 1) % 5];
}
else
{
if (n1 == n2)
{
juzhen[i] = ch[(m1 + 1) % 5][n1];
juzhen[i + 1] = ch[(m2 + 1) % 5][n2];
}
else

{
juzhen[i] = ch[m1][n2];
juzhen[i + 1] = ch[m2][n1];
}
}

}
cout << juzhen << endl;
 }
```

6.

快速幂求解

```
#include < iostream >
#include < cstring >
#include < algorithm >

using namespace std;

typedef long long LL;

int qmi(int a , int k, int p)
{
  int res = 1 ;
  while (k)
  {
    if (k & 1) res = (LL)res * a % p ;
    k >>= 1 ;
    a = (LL)a * a%p;
  }
  return res;
}

int main()
{
  int n;
  scanf("%d", &n);
  while (n −− )
  {
    int a, p;
```

```
        scanf("%d%d",&a,&p);
        int res = qmi(a,p - 2,p);
        if(a%p)
        printf("%d\n",res);
        else puts("impossible");
    }
}
```

拓展欧几里得

```
#include <iostream>
#include <cstring>
#include <algorithm>
using namespace std;

int exgcd(int a , int b , int &x,int &y )
{
    if(!b)
    {
        x = 1,y = 0;
        return a ;
    }
    int d  =   exgcd(b,a%b,y,x);
    y-= a/b * x;
    return d;
}

int main()
{

    int n;
    scanf("%d",&n);
    while (n  - - )
    {
        int a,b,x,y;
        scanf("%d%d",&a,&b);
        exgcd(a,b,x,y);
        printf("%d %d\n",x,y);
    }
}
```

求解同余方程

```
#include <iostream>
#include <cstring>
#include <algorithm>
using namespace std;
```

```
typedef long long LL;

int exgcd(int a , int b , int &x, int &y )
{
  if(! b)
  {
    x = 1, y = 0;
    return a ;
  }
  int d  =  exgcd(b, a%b, y, x);
  y -=  a / b  *  x;
  return d;
}


int main()
{

  int n;
  scanf("%d", &n);
  while (n  -- )
  {
    int a, b, m, x, y;
    scanf("%d%d%d", &a, &b, &m);
    int d  =  exgcd(a, m, x, y);

    if(b % d) puts("impossible");
    else printf("%d\n", (LL)x * (b/d)%m);
  }
}
```

求解同余方程组

```
#include  < iostream >
#include  < cstring >
#include  < algorithm >
using namespace std;

typedef long long LL;
int n;
LL exgcd(LL a, LL b, LL &x, LL &y)
{
  if(! b)
  {
    x  =  1, y  =  0;
    return a;
  }

  LL d = exgcd(b, a % b, y, x);

  y -= a / b * x;

  return d;
}

int main()
{
  int n;
  cin >> n;

  LL flag = 0 , a1, m1;
  cin >> a1 >> m1;
  for (int i = 0; i < n - 1; i ++ )
  {
    LL a2, m2;
    cin >> a2 >> m2 ;
    LL k1, k2;
    LL d = exgcd (a1, -a2, k1, k2);
    if((m2 - m1)%d)
    {
        flag = 1;
        break;
    }
    k1 *= (m2 - m1) / d;
    LL t = a2 / d;
    k1 = (k1 % t + t) % t;

    m1 = a1 * k1 + m1;
    a1 = abs(a1 / d * a2);


  } if(! flag)
    {
        cout << (m1 % a1 + a1) % a1 << endl;
    }
    else puts(" - 1");
}
```