

## Caesar cipher:

Ciphertext:

FBUQUIUDSHOFJOEKHDQCUMYJXJXUIQCUAUOQDTKFBEQTJEBUQHDDYDWYDPZK

Plaintext:

PLEASEENCRYPTYOURNAMEWITHTHESAMEKEYANDUPLOADTOLEARNINGINZJU

KEY:

10

What I should do:

XKQDWMUDZYU

Cryptanalysis process:

利用算法穷举 25 种偏移后的情况，筛选出合理的明文（下附部分代码和执行结果）

```
for (int i = 1; i <= 25; i++) {
    int j = 0;
    char str1[0xFF] = { '\0' };
    while (str[j] != '\0') {
        str1[j] = (str[j] - 'A' + i) % 26 + 'A';
        cout << str1[j] ;
        j++;
    }
    cout << endl;
}
```

```
*****解密ing*****
GCVRJVVETIPGKPFlierdVNZKYKYVJRDVBVPREULGCFRUKFCVRIEZEZEQAL
HDWSKWWFUJQHLQGMJFSEWOALZLZWKSEWCWQSFVMHDGSLGDWSJFAFYAFRBM
IEXTLXXGVKRIIMRHNGKTFXPBMAMAXLTFXDXTGTWNIEHTWMHEXTKGBGZBGSCN
JFYUMYYHWLSJNSIOLHUGYQCNBNBYMUGYEYSUHXOJFIUXNIFYULHCHACHTDO
KGZVNZZIXMTKOTJPMIVHZRDOCOCZNVHZFZTVIYPKGJVYOJGZVMIDIBDIUEP
LHAWOAAJYNULPUKQNJWIASPDPAOWIAGAUAJZQLHKWZPKHAWNJEJCEJVFQ
MIBXPBBKZOVMQVLRKXJBTFQEQEBPXJBHBVXKARMILXAQLIBXOKFKDFKWGR
NJCYQCCLAPWNRWMSPLYKCUGRFRFCQYKCIWYLBNSJMYBRMJCYPLGLEGLXHS
OKDZRDDMBQXOSXNTQMZLDVHSGSGDRZLDJDXZMCTOKNZCSNKDZQMFMHMYIT
PLEASEENCRYPTYOURNAMEWITHTHESAMEKEYANDUPLOADTOLEARNINGINZJU
QMFBTFFODSZQUZPVSBNFXJUUIFTBNFLFZBOEVQMPBEUPMFBFOJOHJOAKV
RNGCUGGPETARVAQWTPCOGYKVJVJGUCOGMGACPFWRNQCFVQNGCTPKPIKBLW
SOHDVHHQFUBSWBRXUQDPHZLWKWKHVDPHNHBDQGXSORDGWROHQUQLQJLQCMX
TPIEWIIRGVCTXCSYVREQIAMXLXLIWEQIOICERHYTPSEHXSPIEVMRKMRDNY
UQJFXJJSHWDUYDTZWSFRJBNYMYMJXFRJPJDFSIZUQTFIYTQJFWSNSLNSEoz
VRKGyKkTIXEVZEUAXTGSKCOZNZNKYGSKQKEGTJAVRUGJZURKGTOTMOTFPA
WSLHZLLUJYFWAFVBYUHTLDPAAOLZHTLRLFHUKBWSVHKAVSLHYUPUNPUGQB
XTMIAMVVKZGXBGWCZVIUMEQBPPMAIUMSMGIVLCXTWILBWTMIZVQVOQVHRC
YUNJBNNWLAHYCHXDAWJVNFRQCQCNBJVNTNHJWMDYUXJMCXUNJAWRWPRWISD
ZVOKCOOXMBIZDIYEBXKWOGSDDROCKWOUOIKXNEZVYKNDYVOKBXSXQSXJTE
AWPLDPPYNCJAEJZFCYLXPHTESESPDLXPVPJLYOFWZLOEZWPICYTYRTYKUF
BXQMEQQZODKBFKAGDZMYQIUFTFTQEMYQWQKMZPGBXAMPFAXQMDZUZSUZLVG
CYRNFRRAPELCGLBHEANZRVJVGUGURFNZRXLNAQHCBYBNQGBYRNEAVATVAMWH
DZSOGSSBQFMDHMCIFBOASKWHVHVSOGASYSMOBRIDZCORHCZSOFBWBWBNXI
EATPHTTTCRGNEINDJGCPBTLXIWIWTHPBTZTNPCSJEADPSIDATPGCXCVXCOYJ
明文:
PLEASEENCRYPTYOURNAMEWITHTHESAMEKEYANDUPLOADTOLEARNINGINZJU
```

## Vignere cipher:

### Ciphertext:

Ktbueluegvi nthuexmonveggmrcgxptlyhhjaogchoemqchpdnetxupbqntietiabpsmaoncnwvoutiu  
gtagmmqsxtvxaoniiogtagmbpsmtuvvihpstpdvcrxhokvhxotawswquunewcgxptlcrxtevtubvewcn  
wwsxfsnptswtagakvoyyak

### Plaintext:

it is essential to seek out enemy agents who have come to conduct espionage against you  
and to bribe them to serve you give them instructions and care for them thus doubledagents  
are recruited and used suntzutheart of war

### KEY:

CAT

### Cryptanalysis process:

上网搜索到可以利用 Friedman 测试法来确定密钥长度，其原理是找到某个  
密钥长度下的各个分组算得的平均重合因子的结果最接近 0.065。

根据迭代计算得，keylength=3 时符合。

根据密钥长度对密文进行分组。

#### 第一组:

a=2,b=0,c=6,d=0,e=1,f=1,g=7,h=1,i=3,j=1,k=1,l=0,m=1,n=2,o=2,p=8,q=4,r  
=0,s=0,t=5,u=4,v=7,w=3,x=0,y=2,z=0

#### 第二组:

a=4,b=0,c=2,d=2,e=9,f=0,g=2,h=2,i=4,j=0,k=0,l=0,m=3,n=3,o=6,p=1,q=0,r  
=2,s=7,t=10,u=3,v=1,w=0,x=0,y=0,z=0

#### 第三组:

a=4,b=5,c=0,d=0,e=0,f=0,g=2,h=5,i=0,j=0,k=3,l=3,m=4,n=5,o=2,p=0,q=0,r  
=1,s=1,t=4,u=3,v=3,w=5,x=10,y=1,z=0

标黄的字母出现频率较高，有理由猜测第一组中（e->c OR e->g OR e->P OR  
e->v），第二组中（e->e OR e->s OR e->t），第三组中（e->x），分别带  
入解密发现：第一组中 e->g，第二组中 e->e，第三组中 e->x，符合，解出  
来的密钥为 CAT

根据所得密钥利用 Caesar 解密，解出明文为 it is essential to seek out  
enemy agents who have come to conduct espionage against you and to  
bribe them to serve you give them instructions and care for them thus  
doubledagents are recruited and used suntzutheart of war

## Unknown:

### Ciphertext:

MAL TIRRUEZF CR MAL RKZYIOL EX MAL OIY UAE RICF “MAL ACWALRM DYEUPLFWL  
CR ME DYEU MAIM UL IZL RKZZEKYFLF GH OHRMLZH”

### Plaintext:

THE PASSWORD IS THE SURNAME OF THE MAN WHO SAID THE HIGHEST KNOWLEDGE IS TO  
KNOW THAT WE ARE SURROUNDED BY MYSTERY

### substitution table:

明文	A	C	E	F	I	K	L	M	O
密文	H	I	O	D	A	U	E	T	M
明文	R	T	U	X	Y	Z			
密文	S	P	W	F	N	R			

### Cryptanalysis process:

#### 1. 猜测是 Caesar cipher，将所有情况列举后发现不是。

```
NBMUJSSVFAGDSNBMSLAZJPMFYNBMPJZVBFSJDCGNBMDXBMSNEZVQMGXMSNFEZVFNBJNVMJAMSLAAFLZGMGHIPISNMAI
OCNVKTTWGBHETOCNTMBAKQNGZOCNQKAWCGTKEHOCNCEYCNTOFAGWRNHYNETOAGWOCKOWNKBNTMBBGMANHIIJQJTONBJ
PDOWLUXHCIFUPDOUNCBLROHAPDORLBXDHULFIPDODFZDOUPGBHXSOIZOFUPHGBHXPDLXPOLCOUNCCCHNBIOIJKRKUPOCK
QEPXMVVYIDJGVQEPVODCMSPIBQEPSCMYEIVMGJQEPGEAEPVQHCIYTPJAPGVQIHCYQEMQYPMDPVODDIIOCJPJKLSLVQPD
RFQYNWWZJEKHWRFPQWEDNTQJCRFQTNZDFJWNHKKRFQFHBQWRIDJZUQKBQHWRIJZJRFNRZQNEQWPEEJPDQKQKLTMTWRQEM
SGRZOXXAKFLIXSGRXQFEOURKDSGRUOEAGKXOILSGRGICGRXSJEKAVRLCRIXSJEKASGOSAROFRXQFFKQELRLMNUNXSRFN
THSAPYYBLGMJYTHSYRGFPVSLETHSVPFHLYPMJTHSHJDHSYTKFLBWSMDSJYTLKFLBTHPTBSPGSGYRGGLRFMSMNOVOYTSGO
UITBQZZCMHNKZUITZSHGQWTFUITWQGCIMZQKNUITIKEITZULGMCXTNETKZUMLGMCUIQUCTQHTZSHHMSGNTNPPWPZUTHP
VJUCRAADNIOLAVJUATIHXRUNGVIJXRHDJNARLOVJULFJUAVMHNDYUOFULAVNMHNDVJRVDIRIUAITINTHOUPQXQAVUIQ
WKVDSBBEOJPMBWKVBUIJSYVOHWKVYSIEKOBSPWKVKMGVBWNIQEZVPGVMBWONIOEWSWEVSJVBUIJJOUIPVPPQRYRBWVJR
XLWETCCFPKQNCXLWCVKJTWPIXLWZTJFLPCTNQXLWNLHLCXOJPPAQHWNXCPOJPFXLTXFWTKWCVKKPVJQWQRSZSCXWKS
YMXFUDDGQLRODYMMDWLKUXAQJYMXAUKGMQDUORYMXMOIMXDYPKQGBXRIXODYQPKQGYMUYGXULXDWLLQWKXRSTATDYXLT
ZNYGVEEHRMSPEZNYEXMLVBYRKZNYBVLHNREVPSZNYNPNJYEZQLRHCYSJYPEZRQLRHZNZVHYVMYEXMRLXSYSTUBUEZYMU
AOZHWWFISNTQFAOZFYNNWCZSLAOZCWMIOSFQTAOZOQKOFARMSIDZTKZQFASRMSIAOWAIZWNZYNNSYMZTUVCFVFAZNV
BPAIXGGJTOURGPAGZONXDATMBPADXNJPTGXRUBPAPRLPAGBSNTJEAULARGBTSNTJBXPBJAXOAGZOOTZNUAUVWDWGBAOW
CQBHYHHKUPVSHQCQBHAPOYEBUNCQBEOYOKUHYSVQCQBQSBQHBCTOUKFBVMBSHCUTOUKCYCKBYPBHAPPUAOVVWVXEXHCBPX
DRCKZIIILVQWITDRCTBQPFZFCVODRCFZPLRVIZTWDRCTNRCIDUPVLGCWNCTIDVUPVLDRLZDLZCQIBQQVBPWCWXYFYIDCQY
ESDLAJJMWXRUIJESDJCRQAGDWPESDGAQMSWJAUXESDSUOSDJEVQWMDXODUJEWVQWMSAEMDARDJCRRCQXDXYZGZJEDRZ
FTEMBKKNXSYVKFTEKDSRBHEXQFTEHBRNTXKBVYFTETVTEKFWRNIEYPEVKFXWRXNFTBFNEBSEKDSXDRYEYZAHAKFESA
GUFNCLLOYTZWLGFULETSCIFYRGUFIOSUYLWCWZGUFUWUFLGXSYOJFZQFWLGYXSYOGUCGOFCTFLETTYESZFZABIBLGFTB
HVGODMMPZUAXMHVGMFUTDJGZSHVGJDTVPZMDXAHVGVXRVGMHYZTPKGARGXMHYZTPHVDHPGDUGMFUUZFTAGABCJCMHGUC
IWHPENNAQVBYNTHWNGVUEKHATIWHKEUQWANEYBIWHWYSWHNIZUAQLHBSHYNIAZUAQIWEIQHEVHNGVAVAGUBHBCDKDNIHVD
JXIQFOORBWCOJXIOHWWFLIBUJXILFVRXBOPZCJXIXZXIOJAVBRMICTIZOJBABVRJXJIRIFWIOHWWBHVCICDELEOJIWE
KYJRGPPSCXDAPKYJPIXWGMJCVKYJMGWSYCPGADKYJYAUYPJBKBCSNJDUJAPKCBWCSKYGKSJGXJPIXXCIWDJDEFMFPKJXF
LZKSHQQTDEYBQLZKQJYXHNKDWLZKNHXTZDQHBELZKZBVZKQLCXDTOKEVKBQLDCXDTLZHLTKHYKQJYYDJXEKEFGNGQLKYG
```

#### 2. 猜测是 Vignere cipher，利用 Friedman 测试法穷举后找不到合适的 keylength。

#### 3. 猜测是单表加密

频率分析得，

A=4,B=0,C=2,D=0,E=3,F=2,G=0,H=0,I=4,J=0,K=1,L=4,M=3,N=0,O=2,P=0,  
Q=0,R=5,S=0,T=1,U=2,V=0,W=0,X=1,Y=2,Z=2

同时，观测到 MAL 出现频率较高，猜测又处于句子开头，故猜测是 THE，  
M->T, A->H, L->E

观察到文中出现了 MAIM,其对应 TH\_T，猜测 I->A，则 MAIM->THAT

同理根据 IZL->A\_E，猜测 Z->R，则 IZL->ARE

MAIM UL IZL->TAHT \_E ARE 猜测 U->W, 即 THAT WE ARE  
UAE ->WH\_ ME->T\_ 猜测 E->O 即 UAE ->WHO ME->TO  
EX->O\_ 猜测 X->F 即 EX->OF

再根据主谓宾结构猜测 CR->IS

进而可根据 ACWALRM->HI\_HEST 推出 W->G ACWALRM->HIGHEST  
同理可推出其他对应关系。