信息安全原理 作业1

姓名：庄毅非 学号：3200105872

1. Caesar: FBUQIUUDSHOFJOEKHDQCUMYJXJXUIQCUAUOQDTKFBEQTJEBUQHDYDWYDPZK

- 解密方式：对上述字符串的每一位增加x，x表示从1到26的所有自然数，观察输出的所有字符串，找出其中可读性最高的字符串。得到的key值为10
- 以下是我的解密过程
  - 使用的python代码：

```python
def caeser(string):
    strlist = [i for i in string]
    for i in range(26):
        for k in range(len(strlist)):
            strlist[k] = chr(ord(strlist[k]) + 1)
            if strlist[k] > 'Z':
                strlist[k] = chr(ord(strlist[k]) - 26)
        print("".join(strlist))

caeser("FBUQIUUDSHOFJOEKHDQCUMYJXJXUIQCUAUOQDTKFBEQTJEBUQHDYDWYDPZK")
```

  - 得到输出如下

```
GCVRJVVETIPGKPFLIERDVNZKYKYVJRDVBVPREULGCFRUKFCVRIEZEXZEQAL
HDWSKWWFUJQHLQGMJFSEWOALZLZWKSEWCWQSFVMHDGSVLGDWSJFAFYAFRBM
IEXTLXXGVKRIMRHNKGTFXPBMAMAXLTFXDXRTGWNIEHTWMHEXTKGBGZBGSCN
JFYUMYYHWLSJNSIOLHUGYQCNBNBYMUGYEYSUHXOJFIUXNIFYULHCHACHTDO
KGZVNZZIXMTKOTJPMIVHZRDOCOCZNVHZFZTVIYPKGJVYOJGZVMIDIBDIUEP
LHAWOAAJYNULPUKQNJWIASEPDPDAOWIAGAUWJZQLHKWZPKHAWNJEJCEJVFQ
MIBXPBBKZOVMQVLROKXJBTFQEQEBPXJBHBVXKARMILXAQLIBXOKFKDFKWGR
NJCYQCCLAPWNRWMSPLYKCUGRFRFCQYKCICWYLBSNJMYBRMJCYPLGLEGLXHS
OKDZRDDMBQXOSXNTQMZLDVHSGSGDRZLDJDXZMCTOKNZCSNKDZQMHMFHMYIT
PLEASEENCRYPTYOURNAMEWITHTHESAMEKEYANDUPLOADTOLEARNINGINZJU
QMFBTFFODSZQUZPVSOBNFXJUIUIFTBNFLFZBOEVQMPBEUPMFBSOJOHJOAKV
RNGCUGGPETARVAQWTPCOGYKVJVJGUCOGMGACPFWRNQCFVQNGCTPKPIKPBLW
SOHDVHHQFUBSWBRXUQDPHZLWKWKHVDPHNHBDQGXSORDGWROHDUQLQJLQCMX
TPIEWIIRGVCTXCSYVREQIAMXLXLIWEQIOICERHYTPSEHXSPIEVRMRKMRDNY
UQJFXJJSHWDUYDTZWSFRJBNYMYMJXFRJPJDFSIZUQTFIYTQJFWSNSLNSEOZ
VRKGYKKTIXEVZEUAXTGSKCOZNZNKYGSKQKEGTJAVRUGJZURKGXTOTMOTFPA
WSLHZLLUJYFWAFVBYUHTLDPAOAOLZHTLRLFHUKBWSVHKAVSLHYUPUNPUGQB
XTMIAMMVKZGXBGWCZVIUMEQBPBPMAIUMSMGIVLCXTWILBWTMIZVQVOQVHRC
YUNJBNNWLAHYCHXDAWJVNFRCQCQNBJVNTNHJWMDYUXJMCXUNJAWRWPRWISD
```

```
ZVOKCOOXMBIZDIYEBXKWOGSDRDROCKWOUOIKXNEZVYKNDYVOKBXSXQSXJTE
AWPLDPPYNCJAEJZFCYLXPHTESESPDLXPVPJLYOFAWZLOEZWPLCYTYRTYKUF
BXQMEQQZODKBFKAGDZMYQIUFTFTQEMYQWQKMZPGBXAMPFAXQMDZUZSUZLVG
CYRNFRRAPELCGLBHEANZRJVGUGURFNZRXRLNAQHCYBNQGBYRNEAVATVAMWH
DZSOGSSBQFMDHMCIFBOASKWHVHVSGOASYSMOBRIDZCORHCZSOFBWBUWBNXI
EATPHTTCRGNEINDJGCPBTLXIWIWTHPBTZTNPCSJEADPSIDATPGCXCVXCOYJ
FBUQIUUDSHOFJOEKHDQCUMYJXJXUIQCUAUOQDTKFBEQTJEBUQHDYDWYDPZK
```

可以发现，当每个ascii位增加10时，能够得到解密之后的句子：“PLEASEENCRYPTYOURNAMEWITHTHESAMEKEYANDUPLOADTOLEARNINGINZJU”,我的姓名（**ZHUANGYIFEI**）按照相同方式加密后的结果是**JREKXQISPOS**

2.Vignere:ktbueluegvitnthuexmonveggmrcgxptlyhhjaogchoemqchpdnetxupbqntietiabpsmaoncnwvoutiugtagmmqsxtvxaoniiogtagmbpsmtuvvihpstpdvcrxhokvhxotawswquunewcgxptlcrxtevtubvewcnwwsxfsnptswtagakvoyyak

解密思路：首先获取原字符串中多次出现的长度为三的子字符串之间的距离，获取其公因数为3，所以猜测密钥长度为3，之后在三层循环中暴力破解密码，找到其中含有最多"THE"的字符串即为所求字符串

```python
import re

class Vignere:
    encrypted = ""

    def __init__(self, astring):
        self.encrypted = astring

    #   计数每三个连续的词出现的个数
    def findRepeat(self):
        result = {}
        for i in range(len(self.encrypted) - 2):
            curStr = self.encrypted[i:i + 3]
            iniPos = self.encrypted.find(curStr)
            if self.encrypted.find(curStr, iniPos + 1) == -1:
                continue
            if result.get(curStr) is None:
                result[curStr] = 1
            else:
                result[curStr] = result.get(curStr) + 1
        return result

    def getDistance(self, strdict):
        distanceDist = {}
        for i in strdict.keys():
            newList = []
            prePos = self.encrypted.find(i)

```

```
            while prePos != -1:
                behPos = self.encrypted.find(i, prePos + 1)
                if behPos != -1:
                    newList.append(behPos - prePos)
                prePos = behPos
            distanceDist[i] = newList
        return distanceDist

    def decrypt(self, keylist):
        charlist = [i for i in ciper]
        for i in range(len(charlist)):
            charlist[i] = chr((ord(charlist[i]) + keylist[i % 3] - 97 + 26) % 26 + 97);
        result = "".join(charlist)
        if result.find("the") != -1:
            return True, result
        return False, None


if __name__ == '__main__':
    ciper = "ktbueluegvitnthuexmonveggmrcgxptlyhhjaogchoemqchpdnetxupbqntietiabpsmaoncnwvoutiugtagmmqsxtvxaoniiogtagmbpsmtuvvihpstpdvcrxhokvhxotawswquunewcgxptlcrxtevtubvewcnwwsxfsnptswtagakvoyyak"

    vig = Vignere(ciper)
    repDict = vig.findRepeat()
    #通过输出结果发现重复单元的间距都是3的倍数，猜测密钥长度为3
    print(vig.getDistance(repDict))

    bestResult = ""
    maxThe = -1
    #暴力破解qwq
    for i in range(26):
        for j in range(26):
            for k in range(26):
                find, result = vig.decrypt([i, j, k])
                if find:
                    countThe = len(re.findall(r"the", result))
                    # print(countThe)
                    if countThe > maxThe:
                        bestResult = result
                        maxThe = countThe
    print(bestResult)

```

输出是

```
itisessentialtoseekoutenemyagentswhohavecometoconductespionageagainstyouandtobribethemtoserveyougivetheminstructionsandcareforthemthusdoubledagentsarerecruitedandusedsuntzutheartofwar
```

#

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

解密思路：MAL在句子中多次出现，将其替换为THE，之后根据常见英文词语进行替换，即得到结果 `THE PASSWORD IS THE SURNAME OF THE MAN WHO SAID THE HIGHEST KNOWLEDGE IS TO KNOW THAT WE ARE SURROUNDED BY MYSTERY`

解密程序：

```
1
2  def replace(ciper,repDict):
3      result = ""
4      charlist = [chr(ord(i)) for i in ciper]
5      for i in range(len(ciper)):
6          if chr(ord(ciper[i])) not in repDict.keys():
7              result += '_'
8          else:
9              result += repDict[ciper[i]]
10     return result
11
12 if __name__ == '__main__':
13     ciper = "MAL TIRRUEZF CR MAL RKZYIOL EX MAL OIY UAE RICF “MAL ACWALRM DYEUPLFWL
   CR ME DYEU MAIM UL IZL RKZZEKYFLF GH OHRMLZH”"
14     repDict = {
15         ' ':' ',
16         '\"':'\"',
17         'M':'T',
18         'A':'H',
19         'L':'E',
20         'I':'A',
21         'Z':'R',
22         'C':'I',
23         'R':'S',
24         'W':'G',
25         'E':'O',
26         'F':'D',
27         'T':'P',
28         'U':'W',
29         'O':'M',
```

```
        'Y':'N',
        'D':'K',
        'P':'L',
        'K':'U',
        'G':'B',
        'H':'Y',
        'X':'F'
    }
    print(ciper)
    print(replace(ciper,repDict))
#最终输出

#MAL TIRRUEZF CR MAL RKZYIOL EX MAL OIY UAE RICF “MAL ACWALRM DYEUPLFWL CR ME DYEU MAIM UL IZL RKZZEKYFLF GH OHRMLZH”
#THE PASSWORD IS THE SURNAME OF THE MAN WHO SAID _THE HIGHEST KNOWLEDGE IS TO KNOW THAT WE ARE SURROUNDED BY MYSTERY_
```

搜索可知，说这句话的人是 `Albert Schweitzer` 所以密码是 `Schweitzer`