Cryptographic Engineering Quiz4

109550025 謝翔丞

密文: EOEYE GTRNP SECEH HETYH SNGND DDDET OCRAE RAEMH TECSE USIAR WKDRI RNYAR ANUEY ICNTT CEIET US

明文:GREECE ANNOUCED YESTERDAY IT HAD REACHED AGREEMENT WITH TURKEY TO END THE CYPRUS CRISIS NS

這次的密文總共有 77 個字，所以我研判應該是 7*11 或是 11*7 的矩形，因此，我先建立兩個 list 用來存他們每行分別有幾個母音，然後再去跟平均的機率 0.4 算差距，得出 7*11 的矩形是 11.2,而 11*7 的矩形是 7.2，可知，加密的方法應該是 11*7 的方形。

```
cp=""
cp = str(input())

cypher=""

for i in range(len(cp)):
    if cp[i].isalpha():
        cypher+=cp[i]

print(cypher)

ia = ord('A')
ie = ord('E')
ii = ord('I')
io = ord('O')
iu = ord('U')
ll711=11*0.4
ll117=7*0.4

vector711 = [0 for i in range(7)]
vector117 = [0 for i in range(11)]

for i in range(7):
    for j in range(11):
        t = ord(cypher[i+j*7])
        if (t == ia or t == ie or t == ii or t == io or t == iu):
            vector711[i]+=1.0
    vector711[i] = vector711[i]-ll711
    if (vector711[i]<0): vector711[i] *=-1.0

for i in range(11):
    for j in range(7):
        t = ord(cypher[i+j*11])
        if (t == ia or t == ie or t == ii or t == io or t == iu):
            vector117[i]+=1.0
    vector117[i] = vector117[i]-ll117
    if (vector117[i]<0):vector117[i] *=-1.0

t711=0.0
t117=0.0
for i in range(7): t711 += vector711[i]
for i in range(11): t117 += vector117[i]

print(t711)
print(t117)
```

下頁還有

接下來，我在程式一開始有建立一個字典，將參考文章每三個字就當作一個 key 放入字典並且 value 為該 Key 的數量，檢查如果已經存在則把該 key 的 value+1。然後計算每個 key 出現的頻率方便後續比對。

```
inp = """WITHM ALICE TOWAR DNONE WITHC HARIT YFORA LLWIT
HFIRM NESSI NTHER IGHTA SGODG IVESU STOSE ETHER
IGHTL ETUSS TRIVE ONTOF INISH THEWO RKWEA REINT
OBIND UPTHE NATIO NSWOU NDSTO CAREF ORHIM WHOSH
ALLHA VEBOR NETHE BATTL EANDF ORHIS WIDOW ANDHI
SORPH ANTOD OALLW HICHM AYACH IEVEA NDCHE RISHA
JUSTA NDLAS TINGP EACEA MONGO URSEL VESAN DWITH
ALLNA TIONS GREEC EANNO UNCED YESTE RDAYT HEAGR
AGREE MENTW ITHTR UKEYE NDTHE CYPRU STHAT THEGR
EEKAN DTURK ISHCO NTING ENTSW HICHA RETOP ARTIC
IPATE INTHE TRIPA RTITE HEADQ UARTE RSSHA LLCOM
PRISE RESPE CTIVE LYGRE EKOFF ICERS NONCO MMISS
IONED OFFIC ERSAN DMENA NDTUR KISHO FFICE RSNON
COMMI SSION EDOFF ICERS ANDME NTHEP RESID ENTAN
DVICE PRESI DENTO FTHER EPUBL ICOFC YPRUS ACTIN
GINAG REEME NTMAY REQUE STTHE GREEK ANDTU RKISH
GOVER NMENT STOIN CREAS EORRE DUCET HEGRE EKAND
TURKI SHCON TINGE NTSIT ISAGR EEDTH ATTHE SITES
OFTHE CANTO NMENT SFORT HEGRE EKAND TURKI SHCON
TINGE NTSPA RTICI PATIN GINTH ETRIP ARTIT EHEAD
QUART ERSTH EIRJU RIDIC ALSTA TUSFA CILIT IESAN
DEXEM PTION SINRE SPECT OFCUS TOMSA NDTAX ESASW
ELLAS OTHER IMMUN ITIES ANDPR IVILE GESAN DANYO
THERM ILITA RYAND TECHN ICALQ UESTI ONSCO NCERN
INGTH EORGA NIZAT IONAN DOPER ATION OFTHE HEADQ
UARTE RSMEN TIONE DABOV ESHAL LBEDE TERMI NEDBY
ASPEC IALCO NVENT IONWH ICHSH ALLCO MEINT OFORC
ENOTL ATERT HANTH ETREA TYOFA LLIAN CE """

string = ""
for i in range(len(inp)):
    if(inp[i].isalpha()):
        string+=inp[i]

dict={}

for i in range(len(string)-2):
    str_tmp = string[i]+string[i+1]+string[i+2]
    if(dict.__contains__(str_tmp)):
        dict[str_tmp] += 1
    else:
        dict2 = {str_tmp:1}
        dict.update(dict2)

for key in dict:
    dict[key] = float(dict[key]/len(dict))
```

(圖中 string 為去掉空格的 inp)

最後一步就是，根據已有的 GRE 去推論後面的明文，我的程式碼寫法是每次都拿已有的後兩字母去當作 key[0]與 key[1]，並且會印出字典中，所有以這兩字母為首的連續三字母及其頻率，因此便挑選頻率最大者為第三字母，然後再接續前步驟持續到找出所有順序。即可完成解密。

```
for i in range(11):
    for j in range (7):
        print(cypher[i+j*11],end=' ')
    print('\n')



for key in dict:
    if(key[0]=='E' and key[1]=='E'):
        print(key," ",dict[key])
```