ooxWord://word/media/image2.jpeg**Quiz1**

**Department: 資工系 Student ID:110550126 Name:曾家祐**

1. Please write a program to find out the frequencies of letters in the ciphertext down below.

find\_text = """T ZJDMBYFS VZRFGYRVY DBVY JIYFG

FKMFSRFGZF T IFFARGL JI GJY

ITS SFDJEFC ISJD TATSD JG

TGTANQRGL TGC FKMAJSF

YOF IAJJC JI TCETGZFC XGJHAFCLF HORZO

FTZO NFTS WSRGLV HRYO RY

"""

freq = [0]\*26

total = 0

for i in find\_text:

    if i!=" "and i!='\n':

        total +=1

        freq[ord(i)-ord('A')]+=1

for i in range(0,26):

    print(chr(ord('A')+i)+':',end = " ")

    print(freq[i])

2. Use these plaintext frequency count information as a reference to break this encrypted messages.

A COMPUTER SCIENTIST MUST OFTEN

EXPERIENCE A FEELING OF NOT

FAR REMOVED FROM ALARM ON

ANALYZING AND EXPLORE

THE FLOOD OF ADVANCED KNOWLEDGE WHICH

EACH YEAR BRINGS WITH IT

3. Assume C is Ciphertext, P is Plaintext. Can you find out a particular relationship in

between C and P?

依照下面我們所填的表格可得知

Ciphertext 🡪 Plaintext:

A 🡪 L

B 🡪 U

…

Z 🡪 C

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cipher** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| **Plaintext** | **L** | **U** | **D** | **M** | **V** | **E** | **N** | **W** | **F** | **O** | **X** | **G** | **P** |
|  | **11** | **20** | **3** | **12** | **21** | **4** | **13** | **22** | **5** | **14** | **23** | **6** | **15** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** |
| **Y** | **H** | **J** | **Z** | **I** | **R** | **A** | **Q** | **S** | **B** | **K** | **T** | **C** |
| **24** | **7** | **9** | **25** | **8** | **17** | **0** | **16** | **18** | **1** | **10** | **19** | **2** |

4. Suppose f(x) = ax + b (mod 26) where x is plaintext, please solve the value of a and b.

A to T: 0 to 19 -> b(mod26) = 19 ->b= 19

B to W: 1 to 22 ->a +19 = 22 ->a = 3

f(x) = 3x +19 (mod26) a = 3, b= 19

5. What is the key size of the mono alphabetic substitution cipher? Such size make exhaustive search becomes difficult?

26!

6. (Bonus) What is the key space in this affine substitution cipher we solved

f(x)= ax+b ?

a 有12種可能，與26互質的數(1,3,5,7,9,11,15,17,19,21,23,25)，

若a與26不互質可能出現不同x對應到相同的f(x)

b 有 26 種可能，(0~25)

🡪key space = 12\*26 = 312

Ciphertext:

T ZJDMBYFS VZRFGYRVY DBVY JIYFG

FKMFSRFGZF T IFFARGL JI GJY

ITS SFDJEFC ISJD TATSD JG

TGTANQRGL TGC FKMAJSF

YOF IAJJC JI TCETGZFC XGJHAFCLF HORZO

FTZO NFTS WSRGLV HRYO RY

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| **6** | **2** | **6** | **5** | **2** | **19** | **12** | **3** | **7** | **12** | **2** | **4** | **3** | **2** | **5** | **0** | **1** | **9** | **9** | **12** | **0** | **4** | **1** | **1** | **9** | **6** |

Ciphertext’s letter frequency count:

(H是3 不是0)

一張含有 桌 的圖片

自動產生的描述

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cipher** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| **Plaintext** | **L** | **U** | **D** | **M** | **V** | **E** | **N** | **W** | **F** | **O** | **X** | **G** | **P** |
|  | **11** | **20** | **3** | **12** | **21** | **4** | **13** | **22** | **5** | **14** | **23** | **6** | **15** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** |
| **Y** | **H** | **J** | **Z** | **I** | **R** | **A** | **Q** | **S** | **B** | **K** | **T** | **C** |
| **24** | **7** | **9** | **25** | **8** | **17** | **0** | **16** | **18** | **1** | **10** | **19** | **2** |