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

**Department: 資工14 Student ID: 110550091 Name: 吳承瑀**

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

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?

See the graph below. The relationship between C and P is “A 🡪 L”, “B 🡪 U”, etc.

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

a = 3+26k, b = 19+26m, where k and m are integers.

We can solve this by using when x=0, f(x) = 19, so b=19. Next, use 0 = 11a + 19 (mod 26) is equivalent to 7 = 11a (mod 26) to solve that a = 3.

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

26!, this is a super big number which is equivalent to about 2^88.

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

f(x)= ax+b ?

Since there are 12 numbers that are less than 26 and co-prime to 26, there are thus 12 possible numbers for the value of a. The value of a must be co-prime to 26 because if not, there would not be a unique number for each element within 26. As for b, there are no constraints so there are 26 possible numbers from 0 to 25. Therefore, the key space would be 12x26=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** | **0** | **7** | **12** | **2** | **4** | **3** | **2** | **5** | **0** | **1** | **9** | **9** | **12** | **0** | **4** | **1** | **1** | **9** | **6** |

Ciphertext’s letter frequency count:

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 | 16 | 8 | 17 | 0 | 25 | 18 | 1 | 10 | 19 | 2 |