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

**Department: 資工系 Student ID: 109550135 Name: 范恩宇**

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

“109550135.py” in the same fold

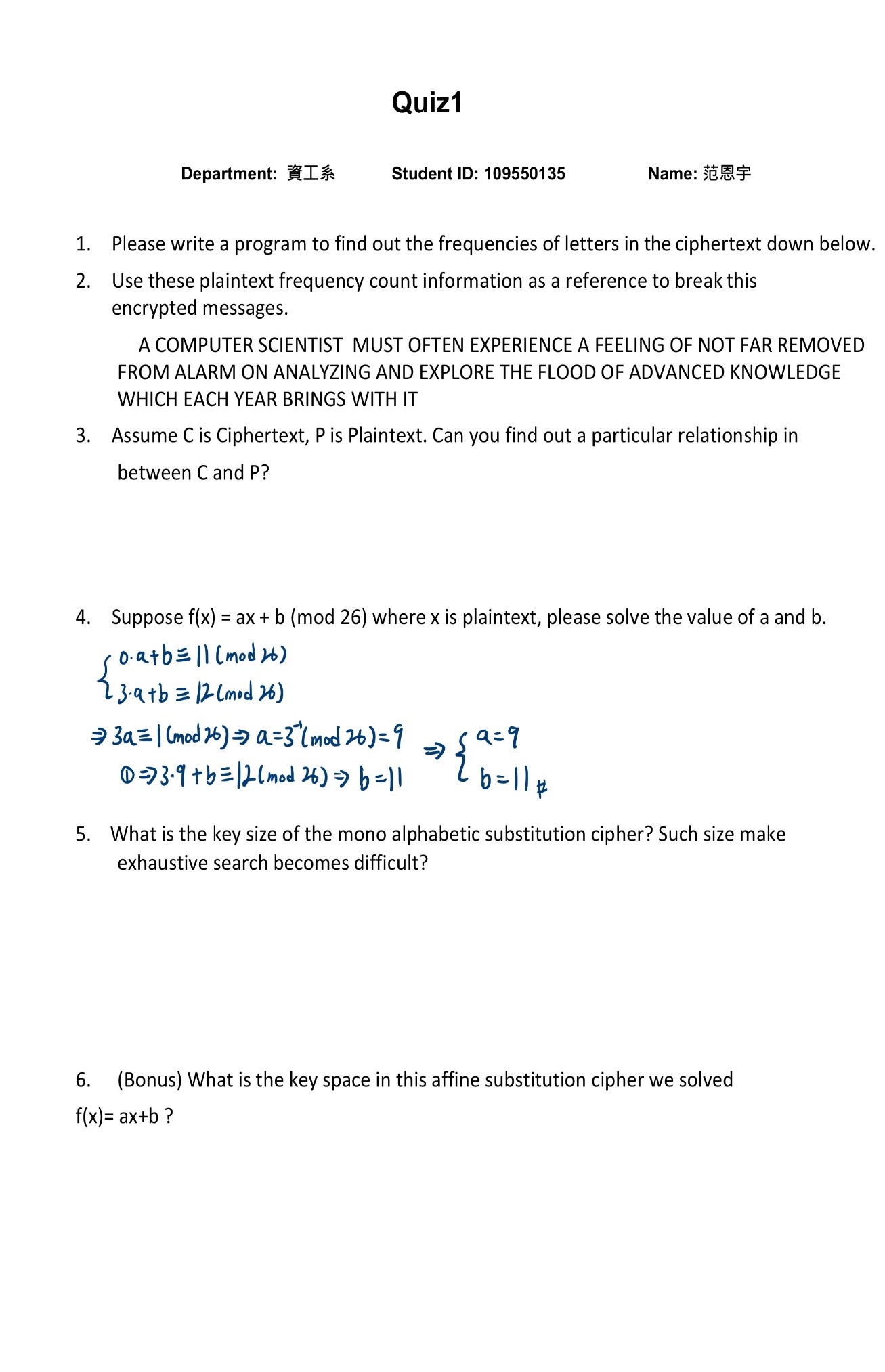
**2. Use these plaintext frequency count information as a reference to break this encrypted messages.**

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

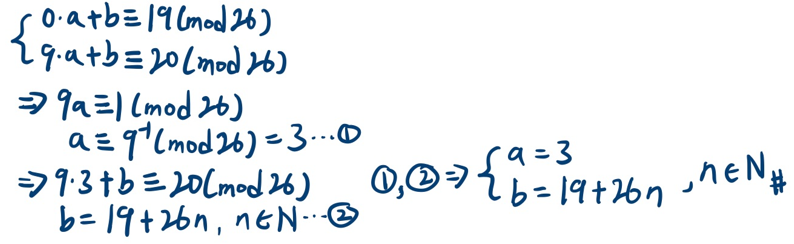
**3. Assume C is Ciphertext, P is Plaintext. Can you find out a particular relationship in**

**between C and P?**

As the chart at the bottom (P = 9\*C + 11 (mod 26)



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



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

26! , which does make exhaustive search becomes difficult .

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

f(x)= ax+b ?

The key space consists of all pairs (a, b) where a is relatively prime to 26 , which means there are 12 possible values for a (1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25) , and for each “a” , there are 26 possible values for b . So , the key space is 312(26\*12).

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(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** | **Q** | **Z** | **I** | **R** | **A** | **J** | **S** | **B** | **K** | **T** | **C** |
| **24** | **7** | **16** | **25** | **8** | **17** | **0** | **9** | **18** | **1** | **10** | **19** | **2** |