UTM
UNIVERSITI TEKNOLOGI MALAYSIA

School of Professional and Continuing Education (SPACE)

DEPARTMENT OF COMPUTER SCIENCE & SERVICES

CENTRE FOR DIPLOMA STUDIES, SPACE

DSPD 2343

Computer Security

Lab Skill 1

LECTURER NAME
Mr. Sajid Shah
SECTION 44

STUDENT NAME & MATRIC ID
LEE XUAN HUI
A24DW0423

NGOO JUN YU
A24DW0429

Magen A/L Srinivasan
A24DW0105

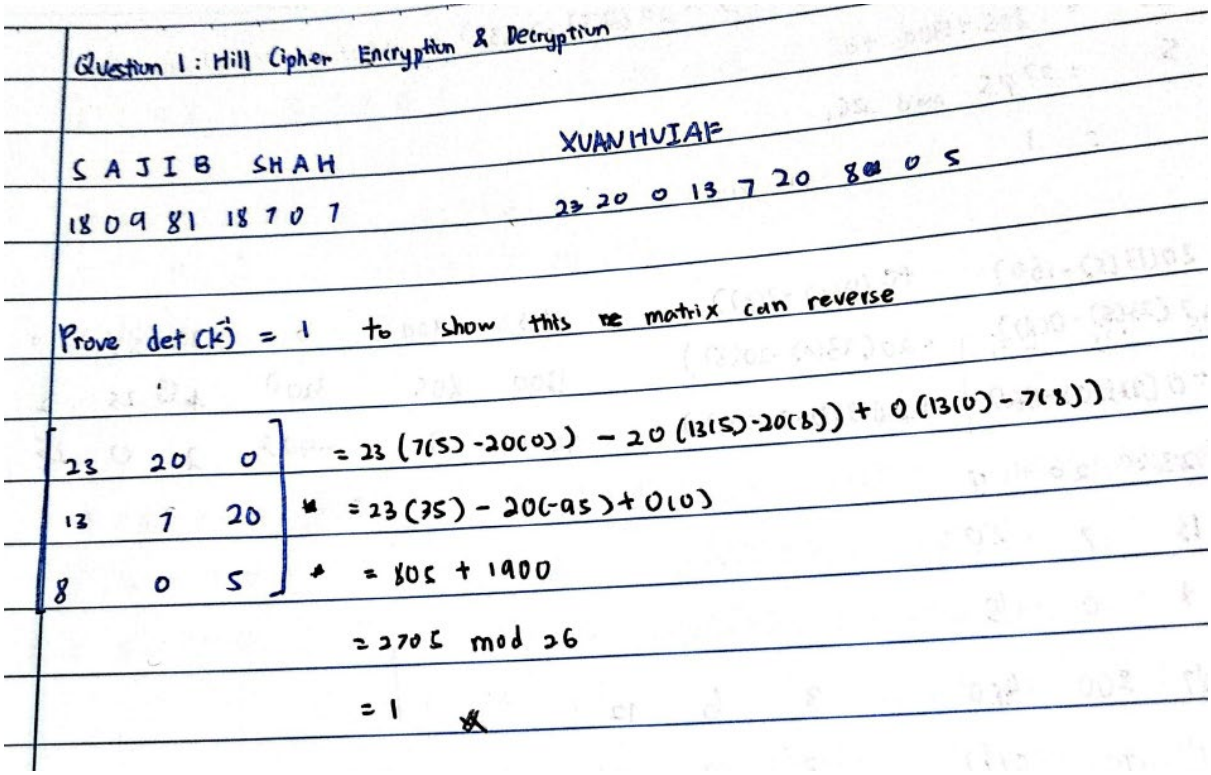
Thenamuthean A/L Manimaran
A24dw1382

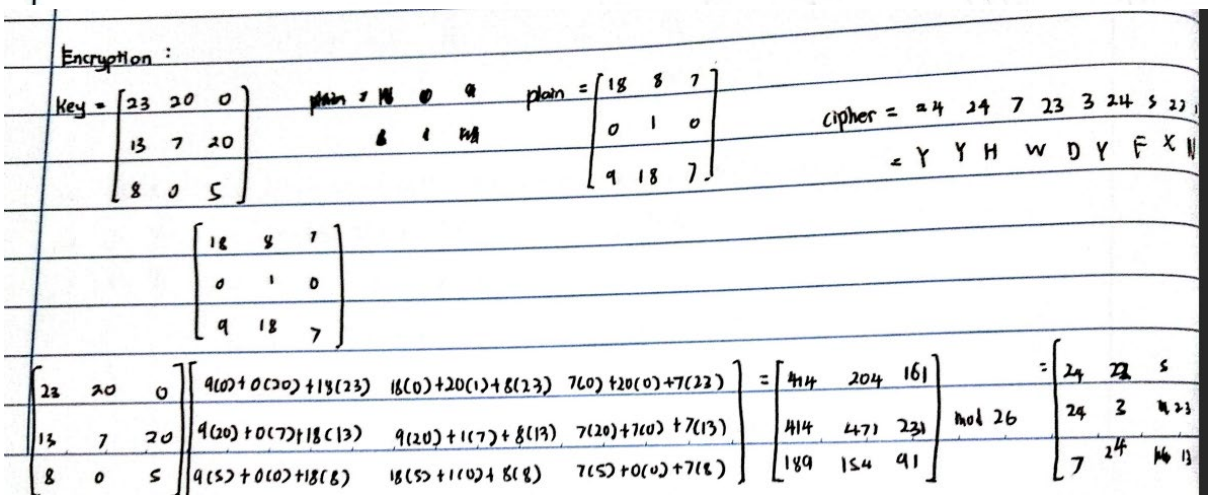
Lab 2 - Cryptography & Cryptanalysis (80 Marks)

The UTM-Space cybersecurity team has implemented the Hill Cipher for securing lecturer records. You have been asked to test its strength and attempt cryptanalysis on substitution ciphers to find vulnerabilities.

Question 1: <u>Hill Cipher Encryption & Decryption (30 Marks)</u>

- Use **3×3 Hill Cipher** matrix.
- **Plain Text:** "Lecturer Name"
- **Key:** "Student Name"
  Hint: (derive numeric key matrix from ASCII-to-0–25 mapping)
- Show **step-by-step**:
  1. Convert letters to numbers.
  2. Form key matrix.
  3. Multiply matrix mod 26 to get cipher.
  4. Decrypt using inverse matrix mod 26.





Tarikh : _____

Decryption :

key = $\begin{bmatrix} 22 & 20 & 0 \\ 13 & 7 & 20 \\ 8 & 0 & 5 \end{bmatrix}$

$\det(K^{-1}) = 1$

COF $(K^{-1}) = \begin{bmatrix} +[(7)5-20(0)] & -[13(5)-20(8)] & +[13(0)-7(8)] \\ -[20(5)-0(0)] & +[22(5)-0(8)] & -[22(0)-20(8)] \\ +[20(20)-0(7)] & -[22(20)-0(13)] & +[22(7)-13(20)] \end{bmatrix}$

$= \begin{bmatrix} 35 & 105 & -56 \\ -100 & 115 & 160 \\ 400 & -460 & -99 \end{bmatrix}$ mod 26

$ADJ(K^{-1}) = \begin{bmatrix} 35 & -100 & 400 \\ 105 & 115 & -460 \\ -56 & 160 & -99 \end{bmatrix}$ $\quad P = \begin{bmatrix} 24 & 23 & 5 \\ 24 & 5 & 23 \\ 7 & 24 & 13 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix}$ $\quad \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix} \begin{bmatrix} 7(10)+24(4)+24(9) & 24(10)+3(4)+23(9) & 13(10)+23(4)+5(9) \\ 8(7)+11(24)+17(24) & 24(8)+3(11)+23(17) & 13(8)+23(11)+17(5) \\ 5(7)+24(4)+24(22) & 24(5)+3(4)+23(22) & 13(5)+23(4)+5(22) \end{bmatrix}$

$K^{-1} = \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix} \times 1$ $\quad = \begin{bmatrix} 382 & 459 & 267 \\ 728 & 616 & 442 \end{bmatrix}$ mod 26

$ADJ(K^{-1}) = \begin{bmatrix} 35 & -100 & 400 \\ 105 & 115 & -460 \\ -56 & 160 & -99 \end{bmatrix}$ $\quad P = \begin{bmatrix} 24 & 23 & 5 \\ 24 & 5 & 23 \\ 7 & 24 & 13 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix}$ $\quad \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix} \begin{bmatrix} 7(10)+24(4)+24(9) & 24(10)+3(4)+23(9) & 13(10)+23(4)+5(9) \\ 8(7)+11(24)+17(24) & 24(8)+3(11)+23(17) & 13(8)+23(11)+17(5) \\ 5(7)+24(4)+24(22) & 24(5)+3(4)+23(22) & 13(5)+23(4)+5(22) \end{bmatrix}$

$K^{-1} = \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix} \times 1$ $\quad = \begin{bmatrix} 382 & 459 & 267 \\ 728 & 616 & 442 \end{bmatrix}$ mod 26

$\begin{bmatrix} 659 & 638 & 267 \end{bmatrix}$

$= \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix}$ $\quad = \begin{bmatrix} 18 & 17 & 7 \\ 0 & 18 & 0 \\ 9 & 14 & 7 \end{bmatrix}$

plain text = 18 0 9 17 18 14 7 0 7

S A J I B S H A H

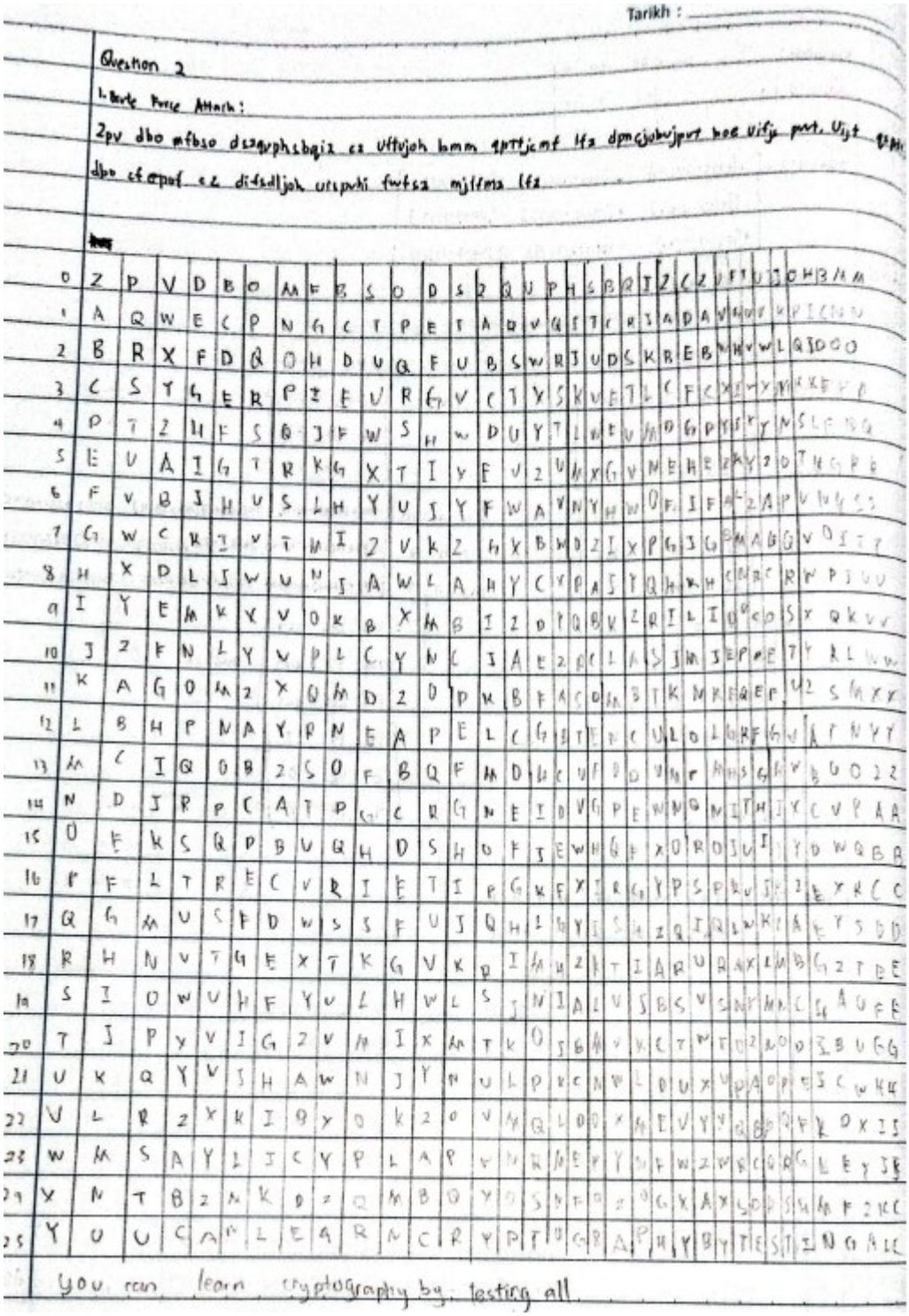
Question 2: Cryptanalysis Scenarios (20 Marks)

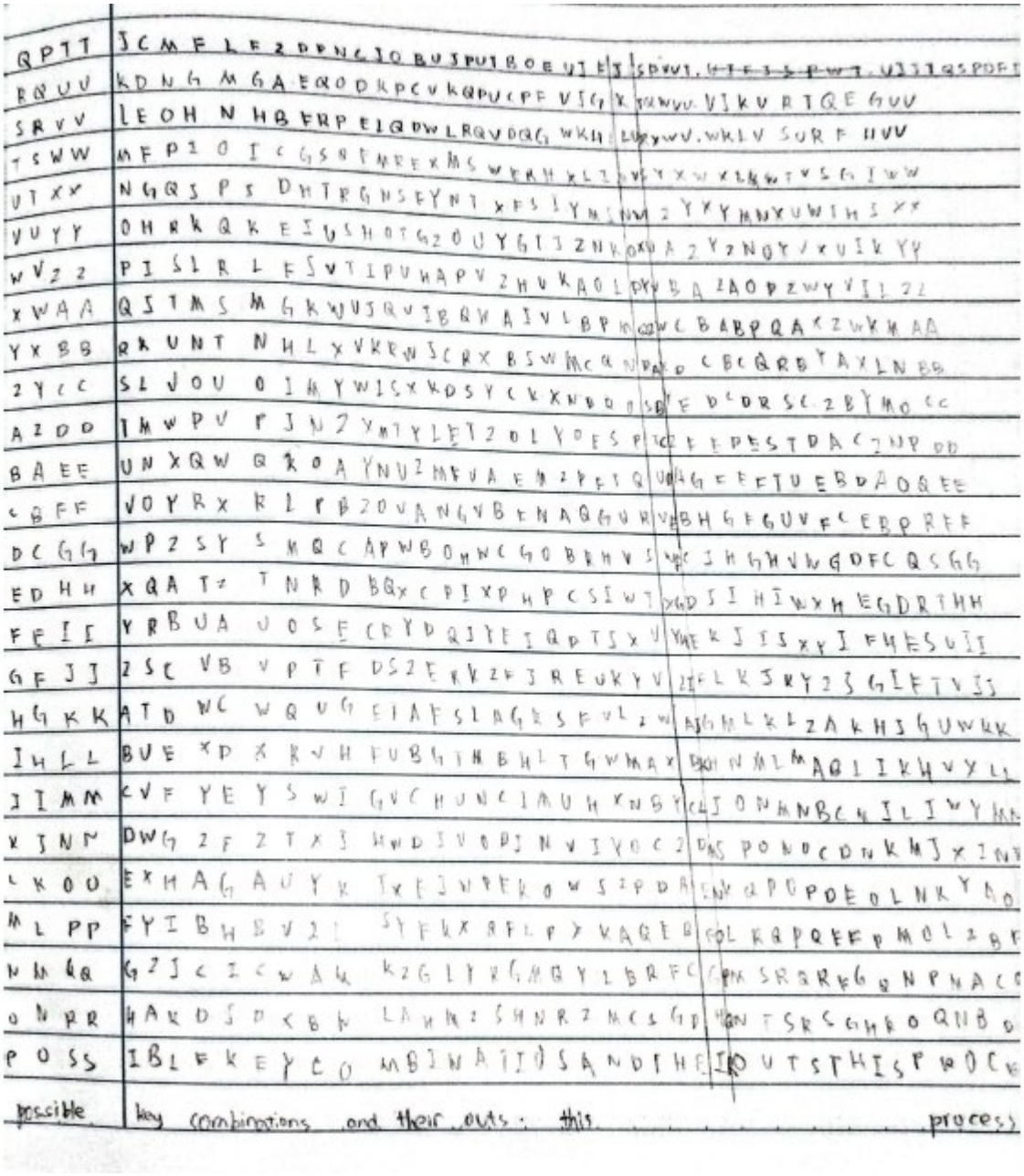
1. Brute Force Attack – Substitution Cipher (10 Marks)

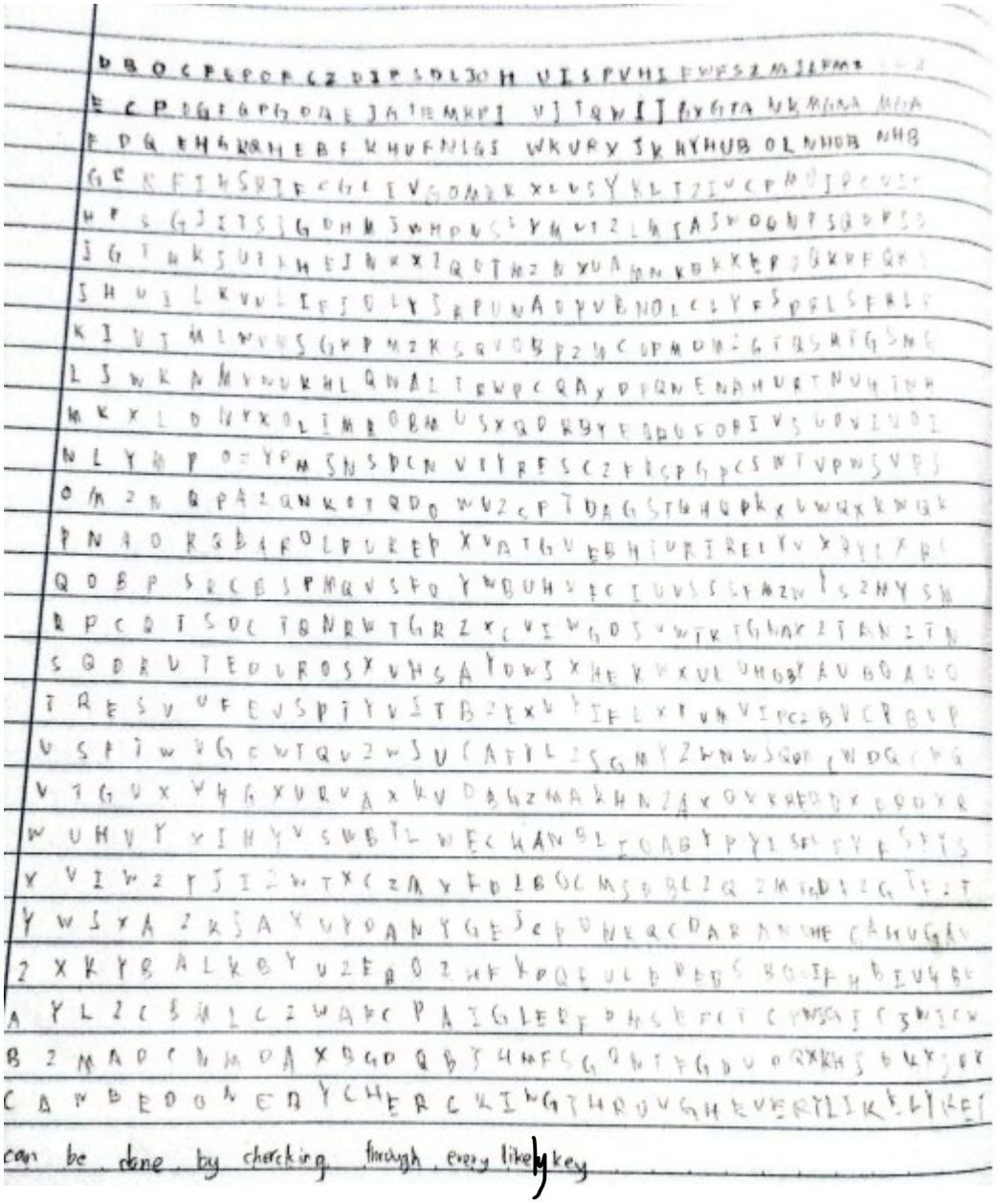
Encrypted paragraph:

```
Zpv dbo mfbso dszquphsbqiz cz uftujoh bmm qpttjcmf lfz dpncjobujpot boe uifjs
pvut. Uijt qspdftt dbo cf epof cz difsdljoh uispvhi fwfsz mjlfmz lfz.
```

Students must try **all possible keys** to recover plaintext. Show the working in detail.




possible key combinations and their outs: this process



2. English Frequency Analysis – Substitution Cipher (10 Marks)

Encrypted paragraph:

```
Zpv dbo mfbso dszquphsbqiz cz uftujoh bmm qpttjcmf lfz dpncjobujpot boe uifjs
pvut. Uijt qspdftt dbo cf epof cz difsdljoh uispvhi fwfsz mjlfmz lfz. Jg zpv
tpnfujnft usz up csfbl uif tffdsfu, zpv xjmm offe up bqqmz dpnnpo mfuufs
gsfrvfodz tubujtujdt. Fohmjti jt uif nptu dpnnpo mbohvbhf jo uif xpsme, boe tp
nboz xpset bqqfbs jo uif dszuqufe ufyu. Cz dpnqbsjoh uif gsfrvfodz pg uif
djqifsufe ufyu xjui tusboebse Fohmjti mfuufs gsfrvfodjft, zpv dbo dpnqvuf b
tuspohtubujpo nbqqjoh boe tpmwf uif dpef xjui hjhi bddvsbdz.
```

Students must use **letter frequency tables of English** to guess mapping and find plaintext. Show the working in detail.

Tarikh :

Question 2 English Frequency Analysis

Zpv dbo mfbso dszquphsbqiz cz uftujoh bmm qpttjcmf lfz dpncjobujpot boe uifjs pvut. Uijt qspdftt dbo cf epof cz difdljoh uispvhi fwfsz mjlfmz lfz. Jg zpv tpnfujnft usz up csfbl uif djqifs, zpv xjmm offe up bqqmz dpnnpo mfuufs gsfrvfodz tubujtujdt. Fohmjti jt uif nptu dpnnpo mbohvbhf jo uif xpsme, boe tp nboz xpset bqqfbs jo uif dszqufe ufyu. Cz dpnqbsjoh uif gsfrvfodz pg uif djqifsufyu xjui tuboebse Fohmjti mfuufs gsfrvfodjft, zpv dbo dpnqvuf bttpdjbujpo nbqqjoh boe tpmwf uif dpef xjui ijhi bddvsbdz

a = 0 b = 26 c = 7 d = 23 e = 12 f = 51 g = 5 h = 13 i = 19 j = 26 k = 0 l = 5
m = 16 n = 12 o = 29 p = 30 q = 13 r = 3 s = 26 t = 25 u = 42 v = 12 w = 2 x = 5 y = 7 z = 22

	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
8.16	~~8.16~~	1.49	2.78	4.253	12.70	2.23	2.02	6.09	7	0.15	0.77	4.03	2.41	6.75	7.50	1.929	0.1	5.99	6.33	9.06	2.76	0.98	2.36	0.15	1.97	0.07
	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	A

You can learn cryptography by testing all possible key combinations and their outs. This process can be done by checking through every likely key. If you sometimes ~~be done by~~ try to break the you will need to apply common letter frequency statistics English is the most common language in world and so many words appear in the crypted text By comparing the frequency of the cipher text with standard accuracy English letter frequencies you can compute a strongstation mapping code with ~~graph~~ high accuracy

Question 3: Programming / Pseudocode and Flowchart (30 marks)

Write a **program in any language** or **pseudocode** and draw the **flowchart** for:

- Cryptanalysis of substitution cipher using **English frequency analysis**.
- Input: Cipher text (as in part Q2b)
- Output: Probable plaintext and mapping table.
- Draw the **flowchart** showing the frequency calculation, mapping, and substitution steps.

Note: 30 Marks for Each (15 Marks for Code and 15 Marks for FlowChart)

Coding :

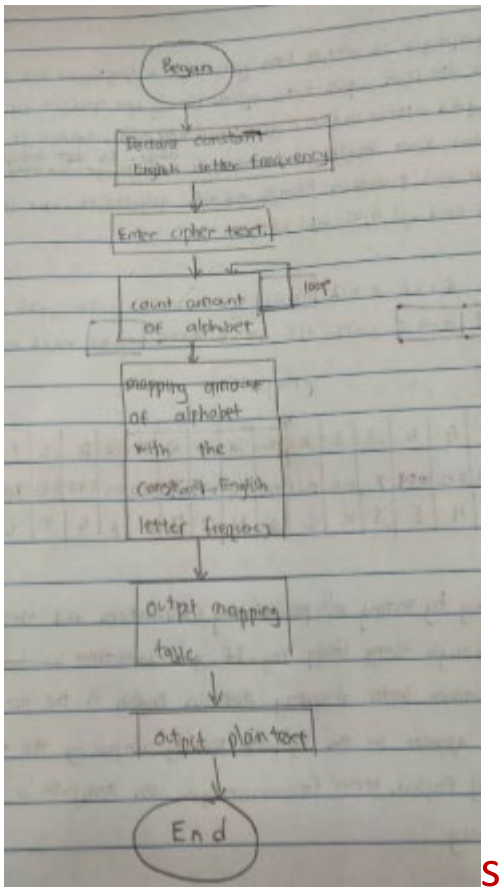
```
#include<iostream>
#include<cctype>
#include<iomanip>
using namespace std;

struct block{
   char alpha;
   int count;
   char mapping;
   float percent;
};

const string letterFrequency = "ETAOINSHRDLCUMWFGYPBVKJXQZ";

int main() {
   block letter[26];
   int count = 0;

   for(int i = 0; i < 26; i++){
      letter[i].alpha = 'A' + i;
      letter[i].count = 0;
      letter[i].mapping = 'A' + i;
   }
```

```
string sequence;
cout<<"please enter a sequence :";
getline(cin,sequence);

for(char &c : sequence){
   if(isalpha(c)){
   count++;
     c = toupper(c);
     letter[c-'A'].count++;
   }
}

for(int i = 0; i < 25;i++){
   for(int j = 0; j < 25 - i ;j++){
      if (letter[j].count < letter[j+1].count){
         swap(letter[j],letter[j+1]);
      }
   }
}

for(int i = 0; i < 26; i++){
   letter[i].mapping = letterFrequency[i];
}

cout <<"============================================\n";
cout << left<< setw(10)<< "Letter" << setw(10)<< "Count" << setw(10)<< "Mapping" <<"\n";
cout <<"============================================\n";

for(int i = 0; i < 26; i++){
   cout<<left<<setw(10)<<letter[i].alpha<<setw(10)<<letter[i].count<<letter[i].mapping<<"\n";
```

```
    }

    cout <<"============================================\n";

    string result = "";
    for(char c : sequence){
        if(isalpha(c)){
            result += letter[c -'A'].mapping;
        }else{
            result +=c;
        }
    }

    cout<<"plain text"<<sequence;
    cout<<"\n\ncipher text"<<result;

    return 0;
}
```

```
please enter a sequence :Zpv dbo mfbso dszquphsbqiz cz uftujoh bmm qpttjcmf lfz dpncjobujpot boe uifjs pvut. Uijt qspdftt dbo cf epof cz difsdljoh uispvhi fwfsz mjlfmz lfz. Jg zpv tpnfujnft usz up c
sfbl uif tffdsfu, zpv xjmm offe up bqqmz dpnnpo mfuufs gsfrvfodz tubujtujdt. Fohmjti jt uif nptu dpnnpo mbohvbhf jo uif xpsme, boe tp nboz xpset bqqfbs jo uif dszuqufe ufyu. Cz dpnqbsjoh uif gsfrvfo
dz pg uif djqifsufe ufyu xjui tusboebse Fohmjti mfuufs gsfrvfodjft, zpv dbo dpnqvuf b tuspohtubujpo nbqqjoh boe tpmwf uif dpef xjui hjhi bddvsbdz.
==============================================
Letter    Count     Mapping
==============================================
F         51        E
U         42        T
P         30        A
O         29        O
B         26        I
J         26        N
S         26        S
T         25        H
D         23        R
Z         20        D
I         19        L
M         16        C
Q         14        U
H         13        M
E         12        W
N         12        F
V         12        G
C         7         Y
G         5         P
L         5         B
X         5         V
R         3         K
W         2         J
Y         2         X
A         0         Q
K         0         Z
==============================================
plain textZPV DBO MFBSO DSZQUPHSBQIZ CZ UFTUJOH BMM QPTTJCMF LFZ DPNCJOBUJPOT BOE UIFJS PVUT. UIJT QSPDFTT DBO CF EPOF CZ DIFSDLJOH UISPVHI FWFSZ MJLFMZ LFZ. JG ZPV TPNFUJNFT USZ UP CSFBL UIF TFFDSF
U, ZPV XJMM OFFE UP BQQMZ DPNNPO MFUUFS GSFRVFODZ TUBUJTUJDT. FOHMJTI JT UIF NPTU DPNNPO MBOHVBHF JO UIF XPSME, BOE TP NBOZ XPSET BQQFBS JO UIF DSZUQUFE UFYU. CZ DPNQBSJOH UIF GSFRVFODZ PG UIF DJQIF
SUFE UFYU XJUI TUSBOEBSE FOHMJTI MFUUFS GSFRVFODJFT, ZPV DBO DPNQVUF B TUSPOHTUBUJPO NBQQJOH BOE TPMWF UIF DPEF XJUI HJHI BDDVSBDZ.

cipher textZFK OTW UNTPW OPZGVFHPTGRZ AZ VNBVDWH TUU GFBBDAUN CNZ OFMADWTVDFWB TWI VRNDP FKVB. VRDB GPFONBB OTW AN IFWN AZ ORNPOCDWH VRPFKHR NJNPZ UDCNUZ CNZ. DS ZFK BFMNVDMNB VPZ VF APNTC VRN BNNOP
NV, ZFK XDUU WNNI VF TGGUZ OFMMFW UNVVNP SPNYKNWOZ BVTVDBVDOB. NWHUDBR DB VRN MFBV OFMMFW UTWHKTHN DW VRN XFPUI, TWI BF MTWZ XFPIB TGGNTP DW VRN OPZVGVNI VNQV. AZ OFMGTPDWH VRN SPNYKNWOZ FS VRN ODGR
NPVNI VNQV XDVR BVPTWITPI NWHUDBR UNVVNP SPNYKNWODNB, ZFK OTW OFMGKVN T BVPFWHBVTVDFW MTGGDWH TWI BFUJN VRN OFIN XDVR HDHR TOOKPTOZ.
PS C:\Users\User\OneDrive\Desktop\coding>
```

Flow Chart:



s