



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

Tarikh : _____

Description :

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

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

rof

$$A_{25}(K^{-1}) = \begin{bmatrix} +[(7)5 - 20(0)] & -[13(5) - 20(8)] & +[13(0) - 7(6)] \\ -[20(5) - 0(0)] & +[23(5) - 0(8)] & -[23(0) - 20(6)] \\ +[20(20) - 0(7)] & -[23(20) - 0(13)] & +[22(7) - 13(20)] \end{bmatrix}$$

$$= \begin{bmatrix} 35 & -100 & 400 \\ -100 & 115 & -460 \\ 400 & -460 & -99 \end{bmatrix} \pmod{26}$$

$$A_{25}(K^{-1}) = \begin{bmatrix} 35 & -100 & 400 \\ -100 & 115 & -460 \\ -36 & 160 & -99 \end{bmatrix}$$

$$P = \begin{bmatrix} 24 & 23 & 5 \\ 24 & 3 & 23 \\ 7 & 24 & 13 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix} \begin{bmatrix} 7(10) + 24(9) + 24(9) & 24(10) + 3(4) + 23(9) & 13(10) + 23(4) + 5(9) \\ 8(7) + 11(24) + 17(24) & 24(8) + 3(11) + 23(17) & 13(8) + 23(11) + 17(5) \\ 5(7) + 24(4) + 24(12) & 24(5) + 3(4) + 23(22) & 13(5) + 23(4) + 5(22) \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \end{bmatrix} \times 1$$

$$= \begin{bmatrix} 382 & 459 & 267 \\ 728 & 616 & 442 \end{bmatrix} \pmod{26}$$

$$A_{25}(K^{-1}) = \begin{bmatrix} 35 & -100 & 400 \\ -100 & 115 & -460 \\ -36 & 160 & -99 \end{bmatrix}$$

$$P = \begin{bmatrix} 24 & 23 & 5 \\ 24 & 3 & 23 \\ 7 & 24 & 13 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix} \begin{bmatrix} 7(10) + 24(9) + 24(9) & 24(10) + 3(4) + 23(9) & 13(10) + 23(4) + 5(9) \\ 8(7) + 11(24) + 17(24) & 24(8) + 3(11) + 23(17) & 13(8) + 23(11) + 17(5) \\ 5(7) + 24(4) + 24(12) & 24(5) + 3(4) + 23(22) & 13(5) + 23(4) + 5(22) \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix} \times 1$$

$$= \begin{bmatrix} 382 & 459 & 267 \\ 728 & 616 & 442 \\ 654 & 638 & 267 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 9 & 4 & 10 \\ 17 & 11 & 8 \\ 22 & 4 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 18 & 17 & 7 \\ 0 & 18 & 0 \\ 9 & 14 & 7 \end{bmatrix}$$

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

S A S 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 dpmcjobujpot boe uifjs pvut. Uijt qspdfstt dbo cf epof cz difsdljoh uispvhi fwfsz mjlfmz lfz.

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

Tarikh : _____

Question 2

1. Brute Force Attack:

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

0	Z	P	V	D	B	O	A	F	B	S	O	D	S	Z	Q	U	P	H	S	B	R	T	Z	C	Z	U	F	T	U	J	O	H	B	A	M
1	A	Q	W	E	C	P	N	G	C	T	P	E	T	A	Q	V	Q	I	T	C	R	S	A	D	A	V	H	U	V	P	I	C	H	U	
2	B	R	X	F	D	Q	O	H	D	U	Q	F	U	B	S	W	R	J	U	D	S	K	R	E	B	N	W	L	Q	I	O	O	O		
3	C	S	T	H	E	R	P	Z	F	U	R	G	V	C	T	Y	S	K	V	E	T	L	C	F	C	X	H	Y	M	K	E	V	P		
4	P	T	Z	H	F	S	B	J	F	W	S	H	W	D	U	Y	T	L	H	E	V	M	O	G	P	H	Y	M	S	L	F	B	Q		
5	E	U	A	I	G	T	R	K	G	X	T	I	Y	F	V	Z	U	H	X	G	V	M	E	H	E	Z	K	Y	Z	O	T	H	G	P	B
6	F	V	B	J	H	U	S	L	H	Y	U	J	Y	F	W	A	V	N	Y	H	W	O	F	I	F	A	Z	A	P	V	U	V	C	S	
7	G	W	C	K	J	V	T	M	I	Z	V	K	Z	H	X	B	W	Z	I	X	P	G	I	G	E	M	A	B	G	V	D	S	T	T	
8	H	X	D	L	J	W	U	N	S	A	W	L	A	H	Y	C	P	A	S	T	Q	H	K	H	C	M	R	W	P	I	U	U	U		
9	I	Y	E	M	K	Y	V	O	K	B	X	M	B	I	Z	O	P	Q	B	K	Z	R	I	L	I	U	R	C	O	S	X	Q	K	V	V
10	J	Z	F	N	L	Y	V	P	L	C	Y	N	C	I	A	E	Z	R	C	L	A	S	J	M	J	E	P	M	E	T	Y	R	L	W	W
11	K	A	G	O	M	Z	X	Q	M	D	Z	D	P	K	B	F	A	C	O	M	B	T	K	M	K	R	E	P	U	Z	S	M	X	X	
12	L	B	H	P	N	A	Y	P	N	E	A	P	E	L	C	G	P	T	E	N	C	U	L	O	L	R	E	G	W	A	T	N	Y	Y	
13	M	C	I	Q	O	B	Z	S	O	F	B	Q	F	M	D	U	C	U	F	P	O	V	N	F	A	H	S	G	W	B	O	Z	Z		
14	N	D	I	R	P	C	A	T	P	C	U	G	N	E	I	O	V	G	P	E	N	M	O	M	I	T	H	J	X	C	V	P	A	A	
15	O	F	K	S	Q	P	B	U	Q	H	D	S	H	U	F	J	E	W	H	Q	F	X	O	R	D	I	U	I	Y	O	W	Q	B	A	
16	P	F	L	T	R	E	C	V	R	I	E	T	I	P	G	K	E	X	I	R	G	Y	P	S	P	R	U	J	E	X	K	C	C		
17	Q	G	M	U	C	F	D	W	S	S	F	U	J	Q	H	L	H	Y	I	S	H	Z	Q	I	R	L	W	K	I	A	E	Y	S	D	
18	R	H	N	V	T	H	E	X	T	K	G	V	K	P	I	M	U	Z	T	I	A	R	U	R	A	K	L	M	B	G	Z	T	B	E	
19	S	I	O	W	U	H	F	Y	V	L	H	W	L	S	J	N	I	A	L	V	S	B	C	V	S	N	M	L	C	A	U	F	F		
20	T	J	P	Y	V	I	G	Z	V	M	I	X	A	N	T	K	O	J	B	H	V	K	E	T	M	T	U	Z	A	O	Z	B	U	G	
21	U	K	Q	Y	V	J	H	A	W	N	J	Y	N	U	L	P	K	C	N	W	L	D	U	X	U	P	A	O	P	E	S	C	W	K	
22	V	L	R	Z	X	K	I	B	Y	O	K	Z	O	V	M	Q	L	O	O	X	M	E	V	Y	Y	Q	B	P	Y	K	O	X	I	S	
23	W	M	S	A	Y	L	I	C	Y	P	L	A	P	V	N	R	M	E	P	Y	M	F	W	Z	M	R	C	Q	Q	L	E	Y	J	B	
24	X	N	T	B	Z	A	K	O	Z	Q	M	B	O	Y	O	S	M	F	O	Z	O	G	X	A	X	L	O	O	S	H	M	F	Z	K	
25	Y	U	U	C	A	N	L	E	A	R	N	C	R	Y	P	T	O	G	A	P	H	Y	B	Y	T	E	S	T	I	N	G	A	L	C	

You can learn cryptography by testing all.

QPTT	JCMFLFZDPNGLIOBUJPUIBOEVIET	SDWV.HTFSSFWT.UJIIQSPDE
RQVV	KDNGMGAERODKPCVKQPU(CFVIG)	XWVV.VIKVRIQEGUV
SRVV	LEOHNHBERPEIQDWLRQVGGWKH	LWVV.WKLV SURFHV
TSWW	MEPI OICGSREERXMSWERNXLZ	VYXWXLWTVSGIWW
UTXV	NHQSPTS DHTRGHSEYNTXESLYM	NWZYXYMNXUWHIXX
VUYV	OHKKQKEISUSHOTGZOUYGIZNR	QVAZYZNYVXUIKYY
WVZZ	PISLRLFSVTIPUNAPVZHUKAOL	PVBAZAOPZWYVILZZ
XWAA	QSTMSMGRVUSQVIBQVAIVLBP	QVCBABPQAQZWKHAA
YXBB	QKUNT NHLXVKRWISCRXBSWMCA	NPAQCBQRBAYXLNBB
ZYCC	SLJOUOIMYWISXKDSYCKXNB	QSEDDORSCZBYMOCC
AZDD	IMWPVFJNZYMTYLETZOLYDES	PQEFPESTDAQJNPDD
BAEE	UNXQWQKOA YNUZMVAEEDZPET	QVHGFEETUEBDAQEE
CBFF	VOYRXRLFBZOVANGVBENAGGUR	VABHGFGUVCEBPRFF
DCGG	WPZSYSMQCAPWBOHWCBOBHVS	WCIHGHVWQDFCQSGG
EDHH	XQATZTNRD BQXCPIXPHPCSIWT	XGDSIHIMXHEGDRTHH
FEII	YRBUAJOSECDYDQJYEIQDTSXU	YHEKJISXYIFHESUII
GFJJ	ZSCVBVPTEFDSZEKVZJREUKYV	ZHFLKJRYZJGIFTVJJ
HGKK	ATDWCWQUG EIAFSLAGESEFVLZW	AGHMLKLZAKHJGUWKK
IHLL	BUEXPXRVHFUBHINBHITGVMAX	BKHMLMAQLIKHVYLL
JI MM	KVFY EYSWI GVC HUNCIAUHXNB	CIJONMNBCHILIMYMM
KJNN	DWYZFZTXJHNDIVOPJNVIVOCZ	DASPOBODCNKMTJXINN
LKOO	EXHAGAU YKTXEJVPKOWSZPDA	ENWQPPQDEOLNKYOO
MLPP	FYIBH BVZISYFKXAFLEPVAGEB	COLKBPQEEPMOLZBPP
NMQA	GZJCI CWAKKZGLYKGMGYLBRFC	CPKSRQRFGGNPNACQ
ONRR	HAKDSDCBKLANKZSHNRZMCSGP	HANTSRSGHBOQNBQ
POSS	IBLEKEYCO MBIMAIIO SANDTHE	IOUTSTHISPROCQ
possible	key combinations and their outs: this process	

D B O C P R P O P C Z D I P S D L J O H U I S P V H I F W F S Z M J L F M Z L F Z
 E C P R D G I G R G D A E J A T H M K P I U J T Q W I J A X G T A M K M G N A M H A
 F D Q E H A R R H E B F K H V F N I G S W K V R Y J K H Y H U B O L N H O B M H B
 G E K F I H S R I F C G I E V G O M A R K X L V S Y K L T Z I V C P H O J P C O S I
 H F S G J I T S I G O H M J W H P N S Y M V I Z L H I A J W O G N P S O D P S S
 I G T A K S U I T H E I N X X I Q O T H Z N X U A H N K B K X E P O B K V F Q K S
 J H U S L K V U L I F I O L Y S A P U N A D Y V B N O L C L Y F S P R L S F A L P
 K I V T M L W V S G Y P M Z K S Q V O B P Z M C O P M O H Z G T A S A I G S M E
 L S W K N M V W K H L Q N A L T W P C Q A X P Q M E N A H U A T N U H T H
 M K X L O H X O L I M R O B M U S X Q D W B Y E D D U F O P I V S U P V I U D I
 N L Y H P O Y P M S H S P E N V I T R E S C Z F K S P G P C S W T V P N S V P S
 O M Z N Q P A Z Q N K O T Q D O W U Z C F T O A G S T H Q P K X U W X K W I K
 P N A O K S B A F O L V U E P X V A T G U E B H I U R I R E I V X H Y I X P I
 Q O B P S R C B S P M Q V S F O Y W D U H V E C I U V S C F M Z W I S Z H Y S H
 R P C Q T S O C T B N R W T G R Z X C V I W G O S V W T R I G H A X Z I A N Z I N
 S G D R U T E D U R O S X V H S A Y O W S X H E K W X U L U H O B Y A U B O A U O
 T R E S V U F E U S P I Y V I T B Z E X V Y I F L X T V H V I P C B V C P B V P
 U S F T W V G C W T Q U Z W S U C A T I L I S G M Y Z H N W S Q O P W D Q C W G
 V T G U X Y H G X V R V A X K V D A G Z M A K H N Z A X O V F E D O X E P O Y R
 W U H V Y X I H Y V S W B I L W E C H A N G L E C A B Y P Y I S F I Y F S F I S
 Y V I W Z F J I Z W T X C Z A Y F D I B O C M S D Q L Z Q Z M T D I Z G T E S T
 Y W S X A Z K S A X U Y P A N Y G E S C P D N E R C D A R A N H E C A H U G A V
 Z X K Y B A L K B Y U Z E A O Z H F Y P Q E U L B P E B S B O I F H B E U H B V
 A Y L Z C B M L C Z W A F C P A I G L E R F H S E F I T C Y M S A I C S M I C W
 B Z M A D C N M O A X B G D Q B T H M F C G O H T F G D U O R X H S B K Y J Y
 C A V B E O O H E A Y C H E R C K I N G T H R O U G H E V E R I L I K E L I H E I
 can be done by checking through every likely key

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

Encrypted paragraph:

Zpv dbo mfbso dszquphsbqiz cz uftujoh bmm qpttjcmf lfz dpncjobujpot boe uifjs
 pvut. Uijt qspdfstt dbo cf epof cz difsdljoh uispvhi fwfsz mjlfmz lfz. Jg zpv
 tpfufjntf usz up csfbl uif tffdsfu, zpv xjmm offe up bqgmz dpnnpo mfuufs
 gsfrvfodz tubujtdt. Fohmjti jt uif nptu dpnnpo mbohvbhf jo uif xpsme, boe tp
 nboz xpset bqgfbs 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 bddvshdz.

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

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 = "ETAOINSHRDLCLUMWFGYPBVKJXQZ";

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 dpcncjobujpot boe uifjs pvut. Uijt qspdfitt dbo cf epof cz difsdljoh uispmhi fwfsz mjlfmz lfz. Jg zpv tpmfujnft usz up c sfbt uif tffdsf, zpv xjmm offe up bqgmz dppno mfuufs gsfrvfodz tubujtjdt. Fohajtj jt uif nptu dppno mbobvhf jo uif xpsme, boe tp nboz xpsset bqgbs jo uif dszuqfe ufyu. Cz dpmqbsjoh uif gsfrvfo dz pg uif djqifsfufe ufyu xjui tusboebse Fohajtj mfuufs gsfrvfodjft, zpv dbo dpmqub b tuspohtubujpo nbqajoh boe tpmf 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
=====

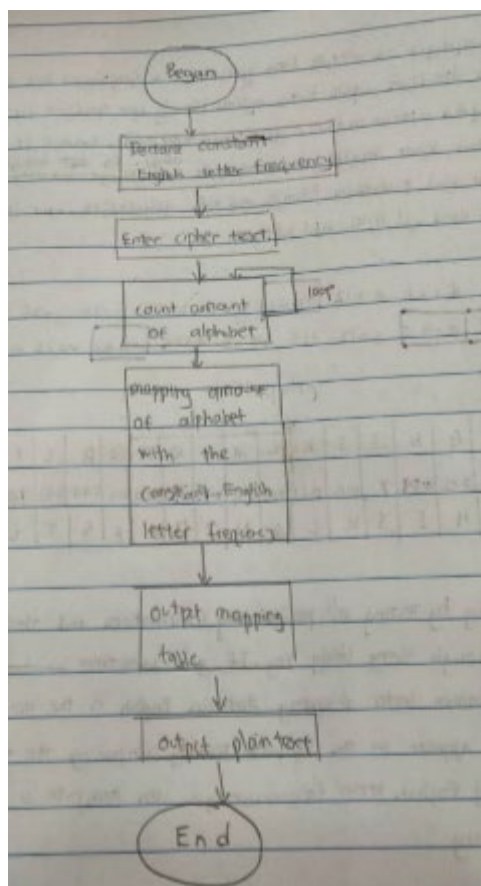
```

plain text:ZPV DBO MFB SO DSZQUPHSBQIZ CZ UFTUJOH BMM QPTTJCMF LFZ DPCNCJOBUIPOT BOE UIFJS PVUT. UIJT QSPDFTT DBO CF EPOF CZ DIFSDLJOH UISPMHI FWFSZ MJLFMZ LFZ. JG ZPV TPMFUJNFT USZ UP CSEBTL UIF TFFDSF U, ZPV XJMM OFFE UP BQGMZ DPPNO MFUUPS GSFRVFOZ TUBUJTJDT. FOHAJTI JT UIF NPTU DPPNO MBOBVHF JO UIF XPSME, BOE TP NBOZ XPSET BQGBS JO UIF DSZUQFE UFYU. CZ DPMQBSJOH UIF GSFRVFOZ PG UIF DQJIF SUE UFYU XJUI TUSBOEBSE FOHAJTI MFUUPS GSFRVFOZJFT, ZPV DBO DPMQUB B TUSPOHTUBUJO NBQJOH BOE TPMF UIF DPEF XJUI HJHI BDDVSDZ.

cipher text:ZFK OTW UNTPW OPZGVHPTGRZ AZ VNBVDNH TUJ GEBBDAUN CNZ OFMADWTVDFWB TWI VRNDP FKVB. VRDB GPFONBB OTW AN IFWN AZ ORNPOCDWH VRPEKHR NONPZ UDCNUZ CNZ. DS ZFK BFMNDVMB VPZ VF APNTC VRN BNNOP NV, ZFK XDUI WNNI VF TGGUZ OFMFEW UNVNP SPNYKMOZ BVTVDVDOB. NWHUDBR DB VRN MFBV OFMFEW UTHKTHN DW VRN XFPUI, TWI BF MTWZ XFPIB TGGNTP DW VRN OPZGVNIZ VNOV. AZ OFMGTDMH VRN SPNYKMOZ FS VRN ODGR NFWII VNOV XDVR BVPTWITPI NWHUDBR UNVNP SPNYKMOONB, ZFK OTW OFMGKN T BVPFMHBVTVDWF MTGGDWH TWI BFUJN VRN OFIN XDVR HDHR TOOKPTOZ.

PS C:\Users\User\OneDrive\Desktop\coding>

Flow Chart:



S