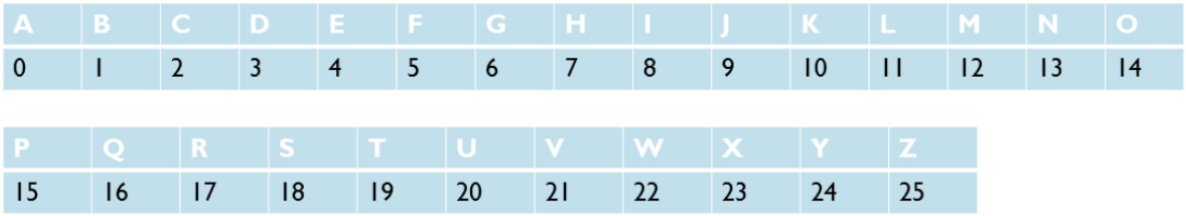
Advanced Security 1 – DT211-4, DT282-4 and DT228-4

Lab Sheet 3 (2 Mark)

Part A

Write a Java program (or any other programming language you are happy to use) to encrypt plaintext using a 2 * 2 Hill cipher.

Example



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

Key = BAKE

$$\begin{pmatrix} B & A \\ K & E \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 10 & 4 \end{pmatrix}$$

PlainText =CAKE

$$\begin{pmatrix} C & A \\ K & E \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 10 & 4 \end{pmatrix}$$

C = PK mod 26

$$C = \begin{pmatrix} 1 & 0 \\ 10 & 4 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 10 & 4 \end{pmatrix} mod\, 26$$

Part B

Write a Java program (or any other programming language you are happy to use) to perform a letter frequency attack on any monoalphabetic substitution cipher without human intervention. Your software should produce possible plaintexts in rough order of likelihood. It would be good if your user interface allowed the user to specify “give me the top 5 possible plaintexts.”

Example

Cipher Text = UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOMBZ WPFUPZHMDJUDTMOHMQ

Calculate letter frequency

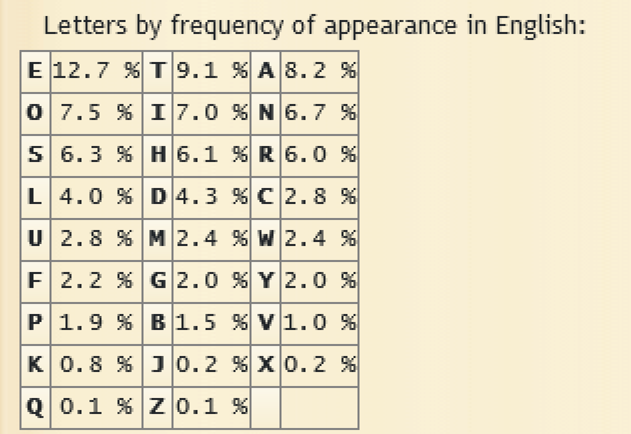
$$\text{Freq} = \frac{\text{number of occurrence}}{\text{Total Element}} \times 100$$

$$J = \frac{1}{120} \times 100 = 0.83$$

$$Y = \frac{2}{120} \times 100 = 1.67$$

P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

Swap it with the English Frequency and generate five possible plaintext.



Letters by frequency of appearance in English:

E	12.7 %	T	9.1 %	A	8.2 %
O	7.5 %	I	7.0 %	N	6.7 %
S	6.3 %	H	6.1 %	R	6.0 %
L	4.0 %	D	4.3 %	C	2.8 %
U	2.8 %	M	2.4 %	W	2.4 %
F	2.2 %	G	2.0 %	Y	2.0 %
P	1.9 %	B	1.5 %	V	1.0 %
K	0.8 %	J	0.2 %	X	0.2 %
Q	0.1 %	Z	0.1 %		