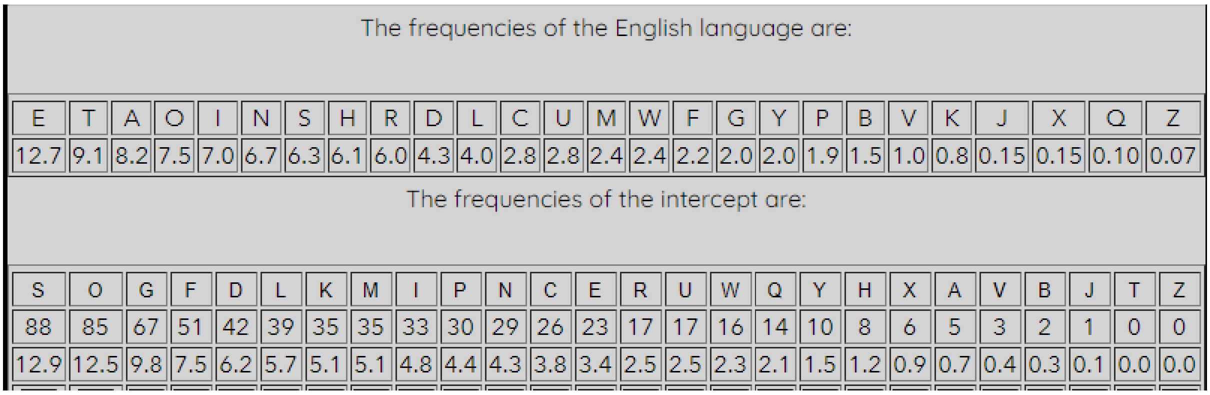
3652167, AMKELE MANDUMBU

COS738 ASSIGNMENT TASK 2

I used the frequency analysis to decrypt the cipher text.

The following diagram shows the common letters in English language and the given ciphertext.



The frequencies of the English language are:

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

The frequencies of the intercept are:

S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0
12.9	12.5	9.8	7.5	6.2	5.7	5.1	5.1	4.8	4.4	4.3	3.8	3.4	2.5	2.5	2.3	2.1	1.5	1.2	0.9	0.7	0.4	0.3	0.1	0.0	0.0

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

I began the method to replace the cipher text with the adjacent clear text attempting to make words that can be read. I looked for the words that can be read make sense when put together. Below is how we cracked he cipher text.

G	**F**	**S**
A	O	E
T	A	T
E	T	A
O	E	O
I	I	I
N	N	n

Here we can have the following words, NET, ONE and INT. And the one the make sense is **ONE**.

W	**M**	**Y**
F	S	Y
W	N	G
M	I	F

U	H	P
C	R	B
D	L	V
A	D	K
T	A	J

Here we can have the following words, WHY, WAY and DAY. And the one the make sense is **WAY**.

O	**G**
T	A
E	T
A	E
O	O
I	I
N	N

Here we can have the following words, TO, AT and IN. And the one the make sense is **TO**.

L	**G**	**D**	**V**	**S**
N	A	I	K	E
I	T	N	V	T
O	E	S	B	A
S	O	H	P	O
H	I	R	J	I
R	N	L	X	N

Here we can have the following words, SOLVE and SINKE. And the one the make sense is **SOLVE**

M	**F**
A	O
O	I
I	N

Here we can have the following words, AN and IN. And the one the make sense is **AN**.

S	**F**	**N**	**K**	**Y**	**H**	**O**	**S**	**U**
E	O	D	H	P	Y	T	E	M
T	I	C	R	Y	P	A	T	U
A	N	U	D	B	B	O	A	C
O	S	M	L	V	V	P	O	D

Here the only word that make sense is **ENCRYPTED**.

E	**S**	**L**	**L**	**M**	**R**	**S**
U	E	N	N	S	A	U
M	T	S	S	N	W	A
W	A	H	H	A	F	T
P	O	R	R	T	G	E

Here the only word that make sense is **MESSAGE**.

CIPHER TEXT	**PLAIN TEXT**
GFS	ONE
WMY	WAY
OG	TO
LGDVS	SOLVE
MF	AN
SFNKYHOSU	ENCRYPTED

ESLLMRS	MESSAGE

Now we took the cipher text charecters and write them in alphabetical order and put the plain text charecters equivalently and that’s how we produced the following table.

CT	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
PT	B	K	F	L	M	N	O	P	H	V	R	S	A	C	T	I	U	G	E	Q	D	V	W	X	Y	Z

And finally, the plain text is as follows:

ONE WAY TO SOLVE AN ENCRYPTED MESSAGE, IF WE KNOW ITS LANGUAGE, IS TO FIND A DIFFERENT PLAINTEXT OF THE SAME LANGUAGE LONG ENOUGH TO FILL ONE SHEET OR SO, AND THEN WE COUNT THE OCCURRENCES OF EACH LETTER. WE CALL THE MOST FREQUENTLY OCCURRING LETTER THE 'FIRST', THE NEXT MOST OCCURRING LETTER THE 'SECOND' THE FOLLOWING MOST OCCURRING LETTER THE 'THIRD', AND SO ON, UNTIL WE ACCOUNT FOR ALL THE DIFFERENT LETTERS IN THE PLAINTEXT SAMPLE. THEN WE LOOK AT THE CIPHER TEXT WE WANT TO SOLVE AND WE ALSO CLASSIFY ITS SYMBOLS. WE FIND THE MOST OCCURRING SYMBOL AND CHANGE IT TO THE FORM OF THE 'FIRST' LETTER OF THE PLAINTEXT SAMPLE, THE NEXT MOST COMMON SYMBOL IS CHANGED TO THE FORM OF THE 'SECOND' LETTER, AND THE FOLLOWING MOST COMMON SYMBOL IS CHANGED TO THE FORM OF THE 'THIRD' LETTER, AND SO ON, UNTIL WE ACCOUNT FOR ALL SYMBOLS OF THE CRYPTOGRAM WE WANT TO SOLVE.