CS641 Assignment 1

January 23'20

objectStrongly
Dewansh Singh 170241
Nikhil Naidu 170758
Parv Jain 170241

CHAPTER 1: "The Entry"

- We tend to **GO** on the carved out trail. Hence the command **GO.**
- The message written tempts us to **READ** it, hence the command **READ.**
- We try **Go** ing in but we fail to push the wall.
- We try to **ENTER** the cave. Hence the command **ENTER.**
- To **READ** the secret message weenier the **READ** command.
- The text we get : "Gyq boch helhfhz lbh dwfil mbojnhf yd lbh mochi. Oi gyq moe ihh lbhfh wi eylbwep yd welhfhil we lbh mbojnhf. Iyjh yd lbh solhf mbojnhfi rwss nh jyfh welhfhilwep lboe lbwi yeh, w oj ihfwyqi. Lbh myzh qihz dyf lbwi jhiioph wi o iwjxsh iqnilwlqlwye mwxbhf we rbwmb zwpwli boch nhhe ibwdlhz ng 6 xsomhi. Dyf lbwi fyqez xoiiryfz wi pwche nhsyr, rwlbyql lbh kqylhi."
- The password : "rgSd40Akfc"

H	I	L	W	B	Y	F	O	E	M	Q	N	J	D	Z	S	P	R	X	C	G	K
42×	28×	27×	26×	22×	19×	16×	15×	15×	9×	9×	8×	8×	7×	7×	6×	5×	5×	4×	4×	3×	1×
14.69%	9.79%	9.44%	9.09%	7.69%	6.64%	5.59%	5.24%	5.24%	3.15%	3.15%	2.8%	2.8%	2.45%	2.45%	2.1%	1.75%	1.75%	1.4%	1.4%	1.05%	0.35%

SOLVING THE CIPHER

E	T	A	O	I	N	S	R	H	D	L	U	C	M	F	Y	W	G	P	B	V	K	X	Q	J	Z
12.0	9.10	8.12	7.68	7.31	6.95	6.28	6.02	5.92	4.32	3.98	2.88	2.71	2.61	2.30	2.11	2.09	2.03	1.82	1.49	1.11	0.69	0.17	0.11	0.10	0.07

To start with, we assume it to be a very basic cipher i.e. **substitution cipher,** so we try basic frequency analysis.
We get :
Actual English letter frequency:

As per this table we get H in our text is E.
We have two single letter words in our text, w and o. They have to be amongst a or i.
Two letter words: yd, oi, oj, wi, we, ng and nh.
Words with double letters: ihh, rwss and nhhe.
And lbh word is repeated very frequently, this may be 'the' (satisfies h -> e).

Our deductions in a table:

Cipher Text	Actual Text	Reason
H	E	Highest frequency
L	T	Letters in THE
B	H	Letters in THE

Cipher Text	Actual Text	Reason
I	S	IHH -> _EE -> SEE
W	I	WI -> _S -> IS
O	A	W is I so O has to be A (only two single letter words)
Y	O	Frequency matches, also assumed GYQ -> YOU
E	N	WE -> I_ -> can be N or S, S already discovered.
F	R	HELHFHZ -> ENTE_E_ should be R
Z	D	HELHFHZ -> ENTERE_ should be D
D	F	DWFIL -> _IRST -> FIRST
G	Y	GYQ -> YOU
Q	U	GYQ -> YOU
C	V	BOCH -> HA_E -> HAVE
M	C	MOCHI -> _AVES -> CAVES
N	B	MBOJNHF -> CHA__ER -> CHAMBER
J	M	MBOJNHF -> CHAM_ER -> CHAMBER
P	G	EYLBWEP -> NOTHIN_ -> NOTHING
S	L	SOLHF -> _ATER -> LATER
R	W	RWSS -> _ILL -> WILL/BILL (B already discovered)
X	P	XSOMHI _> _LACES -> PLACES
K	Q	KQYLHI -> _UOTES -> QUOTES

So the text says:
You have entered first chamber of the caves. As you can see there is nothing of interest in the chamber. Some of the later chambers will be more interesting, I am serious. The code used for this message is a simple substitution cipher in which digits have been shifted by 3* places. For this round password is given below, without the quotes.

* In the given text it is given that it is shifted by 6 places. But the actual number would also be shifted. Hence number + number = 6. Hence number = 3.
* We still don't have the match for the letter a. We can try amongst J, K, X and Z.

Hence the obtained Password is :

rsgSd40Akfc -> wyLf17Kqrv

Since the password satisfies, we don't go further in the analysis of cipher text.