# CS641 - Assignment 1
## Nishtha - 180489

Text on the wall :

**"wsam ie pjo ysgtm eyipbya .P axg niphay y,**
**mey syw ahgm ewhrg tw hmysyam wh meyiepjo**
**ys .Ag jygtmeyk pmys ie pjo ysavw kkoyjgsy**
**whmy sy amwh rmephmewagh y!Me yigu ynay utg**
**smew ajya apr ywap awjfkya no a mwmnmw**
**ghiwfeyswhve wieuwr wm aepby oyyhae wtmy**
**uox8 fkpiya. Me y fpaavgs uwa mxSrN03u wd**
**dvwmegnmmey dngmya. Mew awameyt"**

# Cryptanalysis

---

- **Commands to get to cipher**

    go -> read -> enter -> read

- **Figuring out the Cryptosystem**

    We have used frequency analysis to figure out the plaintext. First, we located the letters with high frequency then we try to figure out some common words that match approximately with their frequency and then the subsequent words. Now after getting the text part we have to find the shift of digits and there were only 10 possibilities of the shift from 0 to 9. We tried all the 10 passwords and found the correct one and the shift was 4 so tyRgU03diqq was actually tyRgU69diqq.

- **Mapping between plaintext and ciphertext**

    **Ciphertext**

    wsam ie pjo ysgtm eyipbya .P axg niphay y,
    mey syw ahgm ewhrg tw hmysyam wh meyiepjo
    ys .Ag jygtmeyk pmys ie pjo ysavw kkoyjgsy
    whmy sy amwh rmephmewagh y!Me yigu ynay utg
    smew ajya apr ywap awjfkya no a mwmnmw
    ghiwfeyswhve wieuwr wm aepby oyyhae wtmy

uox8 fkpiya. Me y fpaavgs uwa mxSrN03u wd
dvwmegnmmey dngmya. Mew awameyt

## Plaintext

This is the 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 than this one!  The
code used for this message is a simple
substitution cipher in which digits have
been shifted by 4 places. The password is
tyRgU69diqq without the quotes.

## Mapping (without shift)

[(wsam,irst),(ie,ch),(pjo,amb),(ysgtm,eroft),(eyipbya,hecaves),(P,A),(axg,syo),(nip
hay,ucanse),(y,e),(mey,the),(syw,rei),(ahgm,snot),(ewhrg,hingo),(tw,fi),(hmysyam,
nterest),(wh,in),(meyiepjo,thechamb),(ys,er),(Ag,So),(jygtmeyk,meofthel),(pmys,
ater),(ie,ch),(pjo,amb),(ysavw,erswi),(kkoyjgsy,llbemore),(whmy,inte),(sy,re),(amw
h,stin),(rmephmewagh,gthanthison),(y!Me,e!Th),(yigu,ecod),(ynay,euse),(utg,dfo
),(smew,rthi),(ajya,smes),(apr,sag),(ywap,eisa),(awjfkya,simples),(no,ub),(a,s),(m
wmnmw,tituti),(ghiwfeyswhve,oncipherinwh),(wieuwr,ichdig),(wm,it),(aepby,sha
ve),(oyyhae,beensh),(wtmy,ifte),(uox8,dby4),(fkpiya,places),(Me,Th),(y,e),(fpaavg
s,passwor),(uwa,dis),(mxSrN03u,tyRgU69d),(wd,iq),(dvwmegnmmey,qwithoutthe
),(dngmya,quotes),(Mew,Thi),(awameyt,sisthef)]