

# ASSIGNMENT 1

CS-642

TEAM- Bullshot

Members –

Aman Tayal(180074)

Rohit Ranjan(180629)

Rishabh Kothary(180608)

The following was the ciphertext we needed to crack in order to complete this level:

“Gqw vpal lzelulm evl tkuje svpfclu qt evl spalj. Pj gqw spz jll evlul kj zqevkzh qt kzelulje kz evl svpfclu. Jqfl qt evl rpelu svpfcluj ikrr cl fqul kzeluljekzh evpz evkj qzl, k pf jlukqwj. Evl sqml wjlm tqv evkj fljjphl kj p jkfdrl jwcjekewekqz skdvlu kz ivksv mkhkej vpal cllz jvktelm cg 8 drpslj. Tqv evkj uqwzm dpjjiquk kj hkalz clrqj, ikevqwe evl ywqelj.

ywZr47Rzee”

In order to solve this cipher the first thing we noticed that certain three letter words continuously appeared throughout the text for eg: ‘evl’, ‘qt’, etc. This continuous appearance of certain letters made us strongly believe that this cipher was a substitution cipher, so that make our claim more sound we ran the text through a frequency test where we received the frequency of each letter.

The results we got are the following (in percentage):

Frequency of l is 14.094

Frequency of e is 10.067

Frequency of j is 9.396

Frequency of k is 8.725

Frequency of v is 7.383

Frequency of q is 6.376

Frequency of z is 5.705

Frequency of u is 5.369

Frequency of p is 5.034

Frequency of w is 3.356

Frequency of s is 3.020

Frequency of f is 2.685

Frequency of c is 2.685

Frequency of r is 2.685

Frequency of m is 2.349

Frequency of t is 2.349

Frequency of h is 1.678

Frequency of i is 1.678

Frequency of a is 1.342

Frequency of d is 1.342

Frequency of g is 1.007

Frequency of y is 0.671

Frequency of 8 is 0.336

Frequency of 4 is 0.336

Frequency of 7 is 0.336

This was very close to the frequency distribution of the English text and this gave us the hint that our assumption that the text has been encrypted by substitution seemed correct to us.

Using the frequency distribution, we got quite a lot of idea about a few letters and then we played the game of hangman to complete the words and find the key for the encryption.

Finally the output we got was:

“You have entered 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, I am serious. the code used for this message is a simple substitution cipher in which digits have been shifted by 4 places. for this round password is given below, without the quotes.

quNI03Lntt”

The code we used to crack this is attached in the File.