# ASSIGNMENT 3

CS-642

TEAM- Bullshot

Members –

Aman Tayal(180074)

Rohit Ranjan(180629)

Rishabh Kothary(180608)

For this assignment we had to crack the following cipher:

“ fjpebzb pi wgcd wsdx bvaj vj vbbbsxs cj mbi bsrftoe mdsppd bidsdqxi ud cqv bcbw. cu wbfqf, xxf xzdf qwaf zm fjpebidq cub bsvoc vw dqs lgif cj mbi vbyh dffzpz. sic obidpw db zig clfy fbf qd vssafa mmdi wcq. tzxd lic fbaud fgcq xfiv iavd mvb wii tww tb zig csfyd. bt iavwe xlbf fmw l tgfuddwf, qv qibs csff qzhizf! wp cu wpicwts, ueobi ffc bsopsaxw:

dni_hziad_ij ”

First, we ran a relative frequency test on the following cipher and the results we obtained were as follows (in %):

Frequency of f is 9.964

Frequency of b is 9.964

Frequency of i is 8.897

Frequency of d is 8.185

```
Frequency of w is 6.406
Frequency of c is 6.406
Frequency of s is 6.050
Frequency of v is 4.626
Frequency of q is 4.270
Frequency of z is 3.915
Frequency of p is 3.559
Frequency of x is 3.559
Frequency of a is 3.203
Frequency of j is 2.847
Frequency of m is 2.847
Frequency of t is 2.491
Frequency of u is 2.491
Frequency of g is 2.135
Frequency of e is 1.779
Frequency of o is 1.779
Frequency of l is 1.779
Frequency of y is 1.068
Frequency of h is 1.068
Frequency of r is 0.356
Frequency of n is 0.356
```

This was very close to a English text so our it was some kind of substitution cipher but looking at the cipher there wasn’t any common 2 letter or 3 letter words made us believe that it isn’t a simple substitution cipher but the text may have been broken up into blocks of some arbitrary size and some kind of permutation has been performed. The fact that letter frequency does not vary too much from actual English text made us believe that the if the block of data if seen as a vector and the linear transformation applied(Linear assumed that as there were 25 different types of characters and thus there was a one-one correspondence) as a matrix, then matrix has to be a permutation matrix, else if we assume that the matrix is denoting some arbitrary linear transformation then the relative letter frequency of the data would reach very close to random which is not seen here. Now to find the block-size we counted the entire text length which turned out to be 280 and “dni_hziad_ij ” written at bottom which we speculated to be the password for next level was 10 index long. We assumed that the blocks would be a divisor of 270 ,280 and 10, as it seemed likely that the block that contained the password would not have elements from the above paragraph. So we concluded that block-size is either 2 or 5. However if the block-size was 2 we would find at least some common diaphragms but that was not the case. So we started working with block-size 5. Now we took a leap of hope and going according to the theme of the game assumed maybe the “bsopsaxw :” (the last word of the passage) was the word “password :”. But then when we saw the that if our data was broken into blocks of 5 then the blocks that encompassed the words were like:

(fc bso) (psaxw). Now with the help of letter frequencies possible inverse permutations for decryption seemed(represented as a matrix here was):

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 |

And

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 |

If we assume data as a vector belonging to $Z_{26}$ (Residue Class of 26) then if multiply the vector with the above matrix then the permutation should occur on it. After the permutation occurs on it, we apply the approach similar to assignment 1 and play hangman. When we applied the first possible permutation matrix then we didn’t seem to be getting satisfactory results, so we tried the second permutation matrix and applied similar approach to decrypting and finally we got our plaintext which is as follows:

“breaker of this code will be blessed by the squeaky spirit residing in the hole. go ahead, and find away of breaking the spell on him cast by the evil jaffar. the spirit of the cave man is always with you. find the magic wand that will let you out of the caves. it would make you a magician, no less than jaffar! to go through, speak the password:

xtf_ijwib_tt”

This is how if finally cracked the cipher. The code we used to crack is attached in the folder.