# CS641: Level 2
# Team: TrojanHorse

*Members:*
*Ayush Kumar, 180174*
*Rishav Kumar, 180612*
*Nilay Majorwar, 180483*

*February 1, 2020*

### Reaching the ciphertext:

The inner chamber has two holes.

1. `enter` the smaller hole and `pick` some mushrooms.
2. Go back to the previous chamber and now `give` the mushrooms to the man in the bigger hole.
3. The man gives us the secret keyword to open the hidden door. Go `back` to the main chamber, and speak the secret keyword `'thrnxxtzy'`.
4. `read` the ciphertext on the glass panel.

### Ciphertext on glass panel:

```
xwygjmf pg ypdu likl ryok jy jkoyuuy yi mzj wyqnulb uzxygm lgtlolui mt lcy kpiy.  yi
wpcot, wow wotl ffpz wr xwygjimc tlk ybuyl it pkm uwds yi mzj aklv ygwffw.  buy impmlg
ld yim fwsy vwk wu ltruzw rpzi mlo.  tlfq wsy imwrd lcwi motk klrm pzm ykp mqp qd yim
fluyv.  wk qprmy xwso swq p zldlcwkp, tt wimu uyfw atwpmg!  wf gi mpcuicq, pmxwy buw
byiogpru:

pih_gtqls_us
```

### Identifying the encryption method:

The method is clearly an alphabet-based one, as the spaces are evenly distributed throughout the text. We need to check now if the cipher is a monoalphabetic one or a polyalphabetic one.

We can calculate the index of coincidence of the given ciphertext, which turns out to be 0.05728. Since normal English text has an index of coincidence of around 0.06, we can conclude that the given cipher is a monoalphabetic cipher, most probably substitution or permutation.

Trying direct substitution cipher, we quickly ran into a deadend. So the given cipher is not a direct substitution cipher. But then, the letterwise frequencies differ a lot from frequencies in English text (Y and Z are the most common letters in ciphertext, with 10.37%), thus it cannot be just a permutation cipher. Thus, the most probable possibility left was a combination of substitution and permutation, which are interchangeable in order.

```
01:  XWYGJ
02:  MFPGY
03:  PDULI
04:  KLRYO
05:  KJYJK
06:  OYUUY
07:  YIMZJ
08:  WYQNU
09:  LBUZX
10:  YGMLG
11:  TLOLU
12:  IMTLC
13:  YKPIY
14:  YIWPC
15:  OTWOW
16:  WOTLF
17:  FPZWR
18:  XWYGJ
19:  IMCTL
20:  KYBUY
21:  LITPK
22:  MUWDS
23:  YIMZJ
24:  AKLVY
25:  GWFFW
26:  BUYIM
27:  PMLGL
28:  DYIMF
29:  WSYVW
30:  KWULT
31:  RUZWR
32:  PZIML
33:  OTLFQ
34:  WSYIM
35:  WRDLC
36:  WIMOT
37:  KKLRM
38:  PZMYK
39:  PMQPQ
40:  DYIMF
41:  LUYVW
42:  KQPRM
43:  YXWSO
...
46:  KPTTW
47:  IMUUY
48:  FWATW
49:  PMGWF
50:  GIMPC
51:  UICQP
52:  MXWYB
53:  UWBYI
54:  OGPRU
```

**Breaking the cipher:**

1. **Undoing the permutation:**

   Considering that the last phrase and the rest of the text is encrypted differently, we can guess that the period of permutation is a divisor of the length of the last phrase. The length of the last phrase is 10 (excluding the underscores), so the possibilities of period of permutation are $\{2, 5, 10\}$. We can try to rule out a possibility by observation.

   Consider that the period of permutation is 2. Then the permutation is uniquely determined as `12` → `21`. Now note, in the original ciphertext, the word `wf` (line 4). The word occurs at index `244-245`, which means that the `w` gets exchanged with its preceding character `g` at 243rd position, while `f` gets exchanged with the next character `g`. This makes the word `wf` to decrypt (un-permute) to `gg`, which cannot be a valid English word after any substitution. Thus, 2 is not the permutation cipher.

   So we now check the possibility 5. Notice that the pair of words `yi mzj` occur twice in the ciphertext, and also when the ciphertext is broken into pieces of 5, the corresponding pair of phrases `YIMZJ` occur in individual blocks (see block 7 and 23). This is a huge indication that 5 is the required period of permutation.

   Now we need to find the permutation. Consider the last few words of the main text: `buw byiogpru`. We can easily guess that the last word is `password`. Thus, after the permutation, the 3rd and 4th letter of the last word must be same. Now the last two 5-blocks of the text are `UWBYI` and `OGPRU`, which have only `U` in common. Thus, in the required permutation, `5` → `1` and `1` → `5`. We have now $3! = 6$ possibilities for the rest three slots.

   Consider block 46 now, which contains the word `tt`. Again, the two letter of a two-letter word cannot be same. Thus we can remove the two possibilities `123` → `132` and `123` → `123`.

   Similarly notice block 5, which contains the word `jy`. The two letters must not be the same after the un-permutation, thus we can remove one more possibility, `123` → `312`. We are left with three possibilities: `321, 213, 231`. We can try each possibility one by one.

After undoing the permutation, we just need to undo the substitution. The unpermuted version is:

```
JGYWXYGPFMILUDPOYRLKKJYJKYUUYOJZMIYUNQYWXZUBLGLMGYULOLTCLTMIYIPKYCPWIY
WOWTOFLTOWRWZPFJGYWXLTCMIYUBYKKPTILSDWUMJZMIYYVLKAWFFWGMIYUBLGLMPFMIYDW
VYSWTLUWKRWZURLMIZPQFLTOMIYSWCLDRWTOMIWMRLKKKYMZPQPQMPFMIYDWVYULMRPQKOS
WXYZPQWSWCLDLWTTPKYUUMIWTAWFFWGMPCPMIGPQCIUBYWXMIYBWUURPGO
```

This is an easy step. Since the last word probably stands for PASSWORD, we already get the key for 7 alphabets. We can proceed with the standard way of breaking the substitution, to get:

```
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
CAVEMAN 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
```

The letter H has not been used in the main text, and is necessary to decrypt the passphrase. We checked all the possibilities for H, and got the right passphrase.