[CS641] The Caves: Chapter 3
Team name: team7 (chaos)

Komal Kalra (18111032) Riya James (18111054) Sristi Jaiswal (18111074)

January 31, 2019

1 Arriving at the Cipher

We *entered* the main chamber, and *put* our hand into the small hole in the ground in the second chamber. We got bitten by something in the hole. So we *entered* the third chamber from the second. We found mushrooms there and *plucked* a few. Not finding a way out, we went *back* to the previous chamber. Here, we remembered the thing that bit us and tried to *give* it the smelly mushrooms. We were greeted by the grateful spirit that had previously bitten us. The spirit told us to go *back* to the main chamber and utter the magic word *'thrnxxtzy'*. So we did just that. And we entered through a hidden door to a different cave with a glass panel in it. We *read* the writing on the panel to discover a cipher. This is how we proceeded to decode it.

2 Guessing the Cipher

At first we considered some classical ciphers and tried guessing if any of them could be applied to the cipher text, but we were unable to come to any conclusion.

But then we guessed that the last few words of the cipher could be: *'To go through, speak the password'*. We first guessed the last word had to be password. The letter-count and the context (a password immediately following) matched. Most previously decoded ciphers were instructions on how to proceed. Knowing this we tried to match letter-counts of words with possible sentences.

We assumed it was encoded with a block cipher. Also as the size of cipher text was 280 we guessed it might have a block length of 5, 7, or 10. Because the size of the password was also 10, we tried a block length of 10 initially. Looking at the cipher text and the (guessed) plain text, and considering all the classical ciphers we knew, we quickly concluded it was encoded using a combination of a transposition and a substitution cipher.

3 Inferring the Key

Matching the number of occurrences of a letter within a block, we inferred the following permutation and substitution rules within a block (in order):

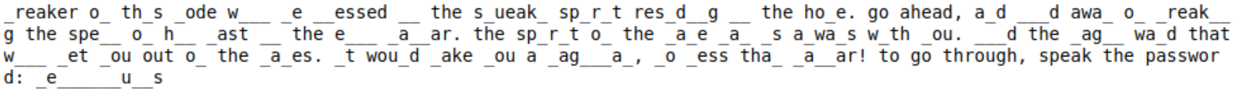
- From the two s's in the second full-block of text we had, and the 1-s in the first block, we inferred the rules: position-3 → position-5; position-7 → position-6.
- We mirrored the permutation position-7 → position-6 in the first full-block of text. This gave us $w \rightarrow o$.
- Both full-blocks had a, o, and h in common (in our guessed plain text). Since we had already mapped $w \rightarrow o$, a and h had to be mapped to f and c in some order. The half-block of text had a h, so we guessed the substitutions to be $f \rightarrow a$ and $c \rightarrow h$. The permutation rules that we got from this: position-1 → position-4, position-9 → position-8, and position-2 → position-1 confirmed the substitutions were right.

- Mirroring these rules in both blocks and continuing similarly we inferred the following rules:

  position-1 → position-4; position-2 → position-1; position-3 → position-5; position-4 → position-3; position-5 → position-2; position-6 → position-9; position-7 → position-6; position-8 → position-10; position-9 → position-8; position-10 → position-7;

- On looking closer at the permutations, we realized the block size was actually 5. We also got the corresponding part of the substitution key for the letters in the sentence we guessed.

- The partially deciphered text we had at this point (using just the key for the letters in the last sentence) looked like like this:



```
_reaker o_ th_s _ode w___ _e __essed __ the s_ueak_ sp_r_t res_d__g __ the ho_e. go ahead, a_d ___d awa_ o_ _reak__
g the spe__ o_ h__ _ast __ the e___ _a__ar. the sp_r_t o_ the _a_e _a_ _s a_wa_s w_th _ou. ___d the _ag__ wa_d that
w___ _et _ou out o_ the _a_es. _t wou_d _ake _ou a _ag___a_, _o _ess tha_ _a__ar! to go through, speak the passwor
d: _e______u__s
```

- From here it was easy to guess the rest of the substitution key.

- For the password, we didn't have the key for the letter n. So it had to be for a letter that wasn't present in the decoded text. That left two possibilities: j, and x. We tried both, and x worked.

  The password: **nej_jmvyu_xs**