CS641: Homework 1
Team name: Team7 (chaos)

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

January 20, 2019

Chapter 1

How we reached the ciphertext in The Caves:

- At the first cave we enterd the command: *climb*.
- At the second cave: *read*.
- Then: *enter*.
- Finally: *read*.
- Then we reached the cave with the ciphertext.

To determine what cipher the message in the first level of The Caves was encoded in, we first ran a letter frequency analysis on it. The most frequent letters in the code appeared $\approx 14\%$ (h), 9.5% (i), and 9% (l) of the time respectively. The most frequently used letters in the English alphabet are e, t, and a with frequencies (in any reasonably large piece of text) $\approx 13\%, 9\%$, and 8% respectively.

Considering the coded message is relatively small, and the top frequencies are more or less maintained, we concluded it was possibly coded using a substitution cipher.

We began by replacing $h \to e$, and $i \to t$. Because the second and third most frequent letters in the coded text did not differ by much (the number of $i's$ was 1 more than the number of $l's$), we tried instead $l \to t$. This looked more plausible because there were a lot of occurrences of common words with t and e in the right places.

Next we substituted $b \to h$ inferring a lot of the words were 'the' or 'there' or 'these' or something similar. Guessing positions of the same words we substituted $f \to r$ and $i \to s$.

From the word '*in*terest', we inferred the substitutions $w \to i$, and $e \to n$. Because we had already made the substition for i, we guessed the single-letter word must be a, and replaced $o \to a$.

We guessed other words: '*f*irst', 'shifte*d*', 'n*o*thin*g*', 'ha*v*e', '*b*een', 's*u*bstit*u*tion', 'so*m*e', '*y*ou', '*p*ass*w*ord', 'simp*l*e', '*q*uotes' and made the substitutions $d \to f$, $z \to d$, $y \to o$, $p \to g$, $c \to v$, $n \to b$, $q \to u$, $j \to m$, $g \to y$, $x \to p$, $r \to w$, $s \to l$, $k \to q$ respectively (in that order). From '*c*aves', '*c*hamber', and '*c*ipher', we inferred $m \to c$.

The code said the 'digits have been shifted by 6 places', which meant a number shifted by itself would give 6. Therefore, each digit in the code need to be shifted by 3 places.

The password has an A which does not appear in the code. We identified that the letters j, k, x, and z are also not used in the deciphered text. So a had to be the substitution for one of those. We tried all four, and only K worked.

The password we decoded is: **wyLf17Kqrv**.