# CS641: Homework 1
# Team name: Team7 (chaos)

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

January 20, 2019

## Chapter 2

How we reahed the cipher text:

- At the first cave in chapter 2 we used the command *read*.
- Then we arrived at the cave with the ciphertext.

In this ciphertext, we performed frequency analysis but that did not match that of the usual texts in the English language. We concluded that it couldn't be a simple substitution cipher. Then we started to think of some polyalphabetic ciphers and started with the very famous Viginere cipher.

To crack the viginere cipher, we need to have the key, but that is not known. Therefore we tried to estimate the key length of the cipher by looking for repetitions of plaintext that are encoded with the same part of the key (that will give the same ciphertext).

First we tried with 3 letter substring repetitions which were only four with distances of $4, 4, 54$, and 15. Then we tried with 2 letter substrings which were approximately 30 and the offsets between most of them were multiples of 9. From this we guessed that the length of the key could be 9 or 18. Therefore we started with the guess of 9. For 4 letter substrings also, only 1 repetition was observed.

To determine the key, we divided the ciphertext into nine parts that were encoded with the same letter of the key and tried to solve this divided text using caeser cipher. First, we performed frequency analysis of the divided ciphertext from which we got to know that in groups 9 and 7, some letters have frequency distribution similar to English. Therefore replaced the most frequent letter in group 9 as, $f \rightarrow e$, and in group 7, $g \rightarrow e$. From there, we got to know the key used for group 9 (by subtracting e from $f \rightarrow b$) and group 7 (by subtracting e from $g \rightarrow c$). Given below is the observation we found from the text and the substitution we made:

- In group 9, frequency distribution matched to English alphabet and most frequent letter is f, therefore f-e gives b as the key. So we shifted all group 9 letters with b.
- In group 7 also frequency distribution matched to English alphabets and most frequent letter is g, therefore g-e gives c as the key. So we shifted all group 6 letters with c.
- After all this, we got a word as M_y, which we guessed to be May, letter corresponding to this in ciphertext was c, therefore we get the key as c(c-a). So we shifted all group 8 letters with c.
- We observed a word as nex_, which we guessed to be next, letter corresponding to this in ciphertext was d, therefore we get the key as k(d-t). So we shifted all group 1 letters with k.
- Then we observed a word as litt__, which we guessed to be little, letter corresponding to l (at position 5) in ciphertext was n, therefore we get the key as c (n-l). So we shifted all group 2 letters with c.
- Then letter corresponding to e (at position 6) in ciphertext was k, therefore we get the key as g (k-e). So we shifted all group 3 letters with g.

- Then we observed a word as __ssword, which we guessed to be password, letter corresponding to p (at position 1) in ciphertext was s, therefore we get the key as d (s-p). So we shifted all group 5 letters with d.
- Then,letter corresponding to a (at position 2) in ciphertext was f, therefore we get the key as f (f-a). So we shifted all group 6 letters with f.
- Now, we got almost all of the message. We got the key of the only remaining group, group 4, from the word chambe_, we guessed to be chamber, letter corresponding to r (at position 7) in ciphertext was t, therefore we get the key as c (t-r). So we shifted all group 4 letters with c.

Now, we got the password as **the_cave_man_be_pleased**.