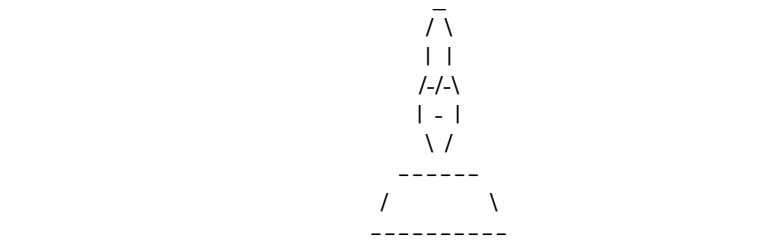
CS641A Assignment-2

Sherlocked

Bholeshwar Khurana (170214) **Yaghyesh Chouhan (170813)** **Sarthak Dubey (180674)**

1 How we reached the cipher text:

1. We were in a dark chamber, where we noticed an exit with a glass panel and a distant boulder with some funny patterns on it. We decided to check the boulder first, and went to it with the command **"go"**.
2. We saw the boulder had a human face and a message written below it, which read:



The spirit of Cave Man is the keeper of the chamber. To navigate through the chamber, you must pay respect to him first. Bow, and then slowly look up. Count the number of lines in horizontal dimension – they will stand in good stead.

3. We took a note of the face and the message, and went back with the command **"back"**.
4. We read the glass panel on the exit door by using the command **"read"**.
5. We found the ciper text:

Lg ccud qh urg tgay ejbwdkt, wmgtf su bgud nkudnk lrd vjfbg. Yrhfm qvd vng sfuuxytj "vkj_ecwo_ogp_ej_rnfkukf" wt iq urtuwjm. Ocz iqa jdag vio uzthsivi pqx vkj pgyd encpggt. Uy hopg yjg fhkz arz hkscv ckoq pgfn vu wwygt nkioe zttft djkth.

2 How we cracked the cipher text:

We found the index of coincidence of the ciphertext using the code *"freq_analysis.cpp"* which is provided along. The index of coincidence came out to be 0.044. Friedman's test says that if index of coincidence lies in the range 0.0385 to 0.065, then it is possibly **Vigenere cipher**. Vigenere Cipher uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. Mathematically, Vigenere cipher has the following form:

$$\text{Encryption: } E_i = (P_i + K_i) \mod 26 \tag{1}$$

$$\text{Decryption: } D_i = (E_i - K_i + 26) \mod 26 \tag{2}$$

1. We tried to break the Vigenere cipher but we didn't know anything about the key length.
2. We recalled the spirit of the cave man (#2 in section-1) which said us to bow down and count the number of lines in horizontal dimension. This gave us 10-2-6-2-3-5-2-2-1.

3. These numbers should definitely mean something. To know how these numbers could help us, we tried to enter these numbers and their equivalent alphabets (i.e. "jbfbcebba") in the command but all in vain.
4. These numbers could probably be the key, so we decided to decrypt the text using these numbers as the key.
5. We decrypted the text by using this $key = 10, 2, 6, 2, 3, 5, 2, 2, 1$ in equation 2. Note that the key is repeated cyclically to match the length of ciphertext. We used the code *"decrypt.cpp"* which is provided along to obtain the following decrypted text:

   Be wary of the next chamber, there is very little joy there. Speak out the password "the_cave_man_be_pleased" to go through. May you have the strength for the next chamber. To find the exit you first will need to utter magic words there.

6. The decrypted text clearly formed a meaningful text, hence our assumption of the key was correct.
7. We entered **"the_cave_man_be_pleased"** and hence proceeded to the next level.