CS641: Level 2
Team: TrojanHorse

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

January 23, 2020

Reaching the ciphertext:

The chamber consists of two important texts:

1. `read` the text on the glass panel at the first screen. This gives us the ciphertext.
2. Then, speak `go` at the first screen, to read the text on the boulder. This gives us the cryptic instructions of the Cave Man.

Ciphertext on glass panel:

```
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.
```

Identifying the encryption method:

The method is clearly an alphabet-based one, as the spaces are evenly distributed throughout the text. The method is clearly an alphabet-based one, as the spaces are evenly distributed throughout the text.

Frequency analysis results show that no letter has a frequency percentage of more than 10% (`G` has the highest frequency, 8.65%, followed by `T` with 7.03%). Such a skewed English text would be rare, and an attempt at substitution cipher indeed quickly gets stuck into contradictory swaps. Thus, substitution cipher can be eliminated. Since permutation ciphers do not change the frequency analysis, we can also eliminate permutation cipher.

We then move to polyalphabetic ciphers, the most popular of which is Vigenere cipher. Since the message of the Cave Man also hints at a number, it seemed likely that the message gives us the key length of the cipher, so we continued with an attempt at Vigenere cipher.

Breaking the cipher:

1. **Getting the key length:**

   The message of the Cave Man:

   ⟨ The face of the Cave Man ⟩

   ```
   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.
   ```

   Paying respect to the Cave Man and counting the number of lines indicated to counting the number of lines in the Cave Man's face. This turns out to be 9. Since length of the key is the most important parameter of the Vigenere cipher, we assumed the key length of the cipher to be 9 and continued.

2. **Decryption:**

   The standard method of breaking the Vigenere cipher involves breaking up the ciphertext into blocks of size equal to the key length, and then treating each column as an independent Caesar cipher, as shown below:

```
01:  LGCCUDQHU
02:  RGTGAYEJB
03:  WDKTWMGTF
04:  SUBGUDNKU
05:  DNKLRDVJF
06:  BGYRHFMQV
07:  DVNGSFUUX
08:  YTJVKJECW
09:  OOGPEJRNF
10:  KUKFWTIQU
11:  RTUWJMOCZ
12:  IQAJDAGVI
13:  OUZTHSIVI
14:  PQXVKJPGY
15:  DENCPGGTU
16:  YHOPGYJGF
17:  HKZARZHKS
18:  CVCKOQPGF
19:  NVUWWYGTN
20:  KIOEZTTFT
21:  DJKTH
```

   Firstly, we remove all the whitespaces and punctuation from the ciphertext, since they are not a part of the encryption, and can easily be replaced after decryption.

   Since the length of the key is 9, we break the ciphertext into blocks of 9, as shown. Each column is now shifted by the same offset, as the key repeats after 9 characters. Thus, each column is now an independent Caesar cipher, though not a meaningful English text, when decrypted. Following are some of the column texts:

```
1:  LRWSDBDYOKRIOPDYHCNKD
2:  GGDUNGVTOUTQUQEHKVVIJ
3:  CTKBKYNJGKUAZXNOZCUOK
          ...
```

   We could have used frequency analysis on each column text, but each column text has only 20-21 characters - too low for frequency analysis to give sufficiently accurate and reliable results, especially when the plaintext is not meaningful English.

So instead, we look for other clues.

i. Notice that the 2-letter words LG and SU in the ciphertext both occur in the first two columns, and thus are encrypted with the same first two characters of the key. Now, there are only a handful of 2-letter words commonly used in English, which are given below:

AM, AN, AS, AT, BE, BY, DO, GO, HE, HI, IF, IN, IS, IT, ME, NO, OF, OK, ON, OR, SO, TO, UP, US, WE

Observe that since L in LG and S in SU are 7 characters apart in the English alphabet, the corresponding decrypted letters will also be 7 characters apart in the alphabet. Similarly, since G in LG and U in SU are 14 characters apart in the English alphabet, the corresponding decrypted letters will also be 14 characters apart in the alphabet. The only such combination we get from the above set that follows the 7 and 14 character gap, is (BE, IS).

So, we move on with (BE, IS). This gives us that the first character of the key is

L - B $\equiv$ **K**,

and the second character of the key is

G - E $\equiv$ **C**.

ii. Now notice IQA in block no. 12 of the blockwise ciphertext. The first two letters IQ decrypt to YO. The third letter now has only one possibility, which is U. Thus, the third character of the key is A - U $\equiv$ **G**.

iii. Look at the last word, DJKTH. Now, DJK decrypts to THE. The full word can then be THESE, THERE, etc. The fifth letter is then most certainly E. Thus, we get that H decrypts to E, i.e., the fifth character of the key is H - E $\equiv$ **D**.

iv. See the word TGAY now. We know that T decrypts to N and A decrypts to X. There is then only one possibility for the full word, NEXT. Thus, G decrypts to E, and Y decrypts to T. Thus, we get fourth character of the key is G - E $\equiv$ **C**, and the sixth character of the key is Y - T $\equiv$ **F**.

With six of the nine characters of the key found, the original ciphertext partially decrypts to (spaces and punctuation replaced):

Be wary qh uhe next ejbmber, thgtf is very nkutle joy vjfre. Speam qvt the pauuxord "the_ecwe_man_be_rnfased" to iq uhrough. Ocz you havg vie strenivi for the pgyt chambgt. Uo find tjg fxit you hksst will pgfd to uttgt nagic wotft there.

Most words now start to pop out, for e.g. uhe $\equiv$ THE, pauuxord $\equiv$ PASSWORD, uhrough $\equiv$ THROUGH. With the word pauuxord itself, we can find out the remaining three characters of the key to be **CCB**. Thus, the key of the Vigenere cipher is **KCGCDFCCB**. With this key, the text fully decrypts to:

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.

Speaking the phrase the_cave_man_be_pleased in front of the glass panel, we progress to level 3.

– – – – – – – – – – – – – – – – – – – –