Q1 Commands

10 Points

List the commands used in the game to reach the ciphertext.

Go
Back
Read

Q2 Cryptosystem

10 Points

What cryptosystem was used in this level?

Vigenère Cipher which is a simpler case of a Poly-alphabetic Substitution Cipher

Q3 Analysis

20 Points

What tools and observations were used to figure out the cryptosystem?

NOTE: Failing to provide proper analysis would result in zero marks for this assignment.

Tools used to figure out the cipher system include python code to decrypt the cipher text.

The observations to reach the cipher system are as follows:
At first, we saw some funny patterns in the distant boulder so we first type ‘go’ command to move towards the boulder where a human-face like pattern was found. Counting the lines in horizontal dimension from the bottom to top, we got the number 9292552221. We assumed the letter ‘a’ to be 0 and on counting upwards we got the keyword ‘jcjcffcccb’.
We then used the ‘back’ command to go back to the glass door, followed by the ‘read’ command to get to the ciphertext.
Next, we tried to check whether it's a simple substitution cipher or not. We checked the frequencies of individual letters but didn’t notice any similarity to the standard pattern of frequency of letters, so we assumed it wasn’t a simple substitution cipher.
We know that there are some ciphers that work on the frequencies of poly-alphabetic rather than individual letters.
We noticed ‘cjjwg’ and ‘vjg’ were repeating in the ciphertext at a gap of 20 and 40 respectively. So, all factors of these are the possible candidates for keyword length. But we got some keyword of length 10 earlier and it's a factor of 20 and 40 both. Thus, we got the idea that it's a poly-alphabetic substitution cipher with the given keyword repeating cyclically with the ciphertext up till the length of the given cipher text.
Then, the job was simple. After that we coded a python script to decrypt the ciphertext.

Q4 Decryption Algorithm

15 Points

Briefly describe the decryption algorithm used. Also mention the plaintext you deciphered. (Use less than 350 words)

The key used in this cipher is a repeating sequence of letters, also known as a keyword. The keyword is repeated until the key is of the length of the given ciphertext. The ciphertext is then created by shifting the plaintext letters based on the corresponding letters in the key.

If the key length is known, finding the original text from the cipher text in the cipher is relatively straightforward.

The decryption formula is:
Di = (Ei - Ki) mod 26
Di denotes decrypted letter, Ei denotes the encrypted letter, and Ki denotes the corresponding letter from the key. The numbering starts from 0, i.e., a is 0, b is 1 and so on.
To eliminate negative values of Di, we further modify the formula as Di = (Ei - Ki + 26) mod 26.
It is important to note that the subtraction of letters should be done in modulo 26 (the number of alphabets) to handle the wrap-around case. For example, if the key letter is 'a' and the ciphertext letter is 'z', then according to our new formula, the original letter in the plaintext would be ('z' - 'a' + 26) mod 26 = 25.

Here is a step-by-step algorithm to find the original text from the cipher text from a given keyword : (Here, the key length is 10, and the keyword is "jcjcffcccb")
1) Divide the ciphertext into blocks of length 10, each corresponding to one repetition of the keyword.
2) For each block, use the key to decrypt the ciphertext letter by subtracting the corresponding key letter from it. (As the decryption formula suggests)
3) The result will be a block of original letters from the plaintext.
4) Repeat the process for each block to get the complete plaintext.

Plaintext:
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.

Q5 Password

10 Points

What was the final command used to clear this level?

the_cave_man_be_pleased

Q6 Codes

0 Points

Upload any code that you have used to solve this level

▾ **Decryption_using_key_Level2.py** Download

```

def Decrypted_Text(cipher_text, key):
    orig_text = []
    j=0
    for i in range(len(cipher_text)):
        if cipher_text[i].isalpha():
            if cipher_text[i].isupper():
                x = (ord(cipher_text[i]) -
                     ord(key[j%10].upper()) + 26) % 26
                x += ord('A')
            else:
                x = (ord(cipher_text[i]) -
                     ord(key[j%10]) + 26) % 26
                x += ord('a')
            orig_text.append(chr(x))

            j+=1
        else:
            orig_text.append(cipher_text[i])
    return("" . join(orig_text))
string="Kg fcwd qh vin pnzy hjcocnt, cjjwg ku wnth nnyvng kxa cjjwg. Urfjm xwy yjg rbbufqwi \"vjg_djxn_ofs_dg_rmncbgi\" yq iq uqtxwlm. Oca zxw qcaj vjg tctnplyj hqs cjn pjcv ejbvdnt. Yt hkpe cjn gcnv, aqv okauy bknn ongm vt zvvgs vcpkh bqtft cjntj."

print(string)
keyword="jcjcffcccb"
print("Decrypted Text :",
           Decrypted_Text(string, keyword))
```

Q7 Team Name

0 Points

ela

Assignment 2

● Graded