Q1 Team Name

0 Points

DECODERS

Q2 Commands

5 Points

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

go, go, go, go, go, give, read

Q3 Analysis

30 Points

Give a detailed description of the cryptanalysis used to figure out the password. (Use Latex wherever required. If your solution is not readable, you will lose marks. If necessary the file upload option in this question must be used TO SHARE IMAGES ONLY.)

The screen on the last door gave us the hash values of our password. The sequence of hash values is as follows:
20 22 116 8 88 110 54 118 94 123 80 6 11 44 43 123 101 84 91 83 30 8 1 7 77 102 10 22 115 6 54 64
It was given that the password contained the letters in the range 'f' to 'u' and they were in alphabetic order. There were 32 hash values which were generated from the password. To generate the ith hash value in the sequence, the password is viewed as a sequence of numbers $x_1, x_2, ..., x_m$ in the field F_{127} and the value $x_1^{i-1} + x_2^{i-1} + ... + x_m^{i-1}$ gives the ith hash value in the sequence. Since the password contained the letters 'f' to 'u' and it is viewed as a sequence of numbers in the field F_{127}, we mapped the letters from 'f' to 'u' to their corresponding ASCII values i.e.

from 102 to 117 and proceeded with the cryptanalysis.

The first hash value ($i = 1$) in the hashed sequence was 20 and it is calculated as $x_1^0 + x_2^0 + ... + x_m^0$ i.e. $1 + 1 + ... + 1 = 20$. From this equation we found out that the length of the password (m) is 20 since each character in the password contributed 1 when raised to the power 0.

Now, to find the complete password, we started iterating over all possible values of the password starting from a sequence which contains all 'f's i.e. [102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102] and generated all possible combinations in which the ASCII values were in increasing order because it was given that the letters in the password are in alphabetic order. After this, we checked for each one of these combinations whether they produced the hash sequence that was available to us. We applied this brute force mechanism for all the combinations until we got the sequence which produced the same hash values that were given on the screen and we stopped iterating for further combinations.

The sequence which produced the given hash values is given below:
$102, 102, 104, 104, 105, 105, 107, 107, 107, 108, 109, 111, 111$

These are the ASCII values of the corresponding letters in the password. Hence, we converted these ASCII values to their corresponding character representations and got the following string:
$ffhhiikkklmoopqqrssu$

When we entered this string as the password on the panel near the door, it got accepted and we cleared this level and escaped from the caves.

No files uploaded

Q4 Password

15 Points

What was the final command used to clear this level?

ffhhiikkklmoopqqrssu

Q5 Codes

0 Points

It is MANDATORY that you upload the codes used in the cryptanalysis. If you fail to do so, you will be given 0 for the entire assignment.

DECODERS.ipynb Download

In [6]:
```
from itertools import
combinations_with_replacement
```

In [7]:
```
l=[i for i in range(102,118)]
```

In [8]:
```
hashes=
[20,22,116,8,88,110,54,118,94,123,80,6,11,44,43,12
```

In [9]:
```
ans=combinations_with_replacement(l,20)
```

In [10]:
```
def found(l):
    for i in range(16):
        add=sum([pow(j,i,127) for j in
l])%127
        if add!=hashes[i]:
            return False
    print(l)
    return True
```

In [ ]:
```
for i in ans:
    if found(i):
        li=list(i)
        break
```

```
(102, 102, 104, 104, 105, 105, 107, 107, 107, 108,
```

In [9]:
```
s=""
for i in li:
    s+=(chr(i))
print("Password is",s)
```

```
Password is ffhhiikkklmoopqqrssu
```

In [ ]:

Assignment 7

GRADED

GROUP

Akash Gajanan Panzade
Manthan Kojage
Abhishek Dnyaneshwar Revskar
View or edit group

TOTAL POINTS

50 / 50 pts

QUESTION 1

Team Name — **0** / 0 pts

QUESTION 2

Commands — **5** / 5 pts

QUESTION 3

Analysis — **30** / 30 pts

QUESTION 4

Password — **15** / 15 pts

QUESTION 5

Codes

0 / 0 pts