Q1 Team Name
0 Points

Noobs

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 following message,

"You see the following written on the panel:

22 26 79 117 81 116 56 41 110 0 102 57 50 109 107 89 59 102 15 121 91 116 89 56 47 91 6 54 92 67 43 122

As you wonder what do these numbers mean, you hear a whisper in your ears ... "I am so happy that he went away without noticing me. He is the one who bound me to the hole. Oh, I was so scared that he will notice me!

You must be wondering about these numbers. These are hash values of your password which is made of letters between 'f' and 'u'. Also, the letters in the password are in alphabetic order. For hashing, your password is viewed as a sequence of numbers x_1, x_2, ... x_m in the field F_{127}. The ith number of the hashed sequence equals x_1^{i-1} + x_2^{i-1} + ... + x_m^{i-1}. As you can see, there are 32 such numbers for i = 1 to 32."

Thus the sequence of hash values corresponding to our password is 22 26 79 117 81 116 56 41 110 0 102 57 50 109 107 89 59 102 15 121 91 116 89 56 47 91 6 54 92 67 43 122. We mapped the characters from 'f' to 'u' to their respective ASCII values, i.e., from 102 to 117, and proceeded with the cryptanalysis because the password contained the letters 'f' to 'u' and was regarded as a sequence of integers in the field F_{127}.

So basically we had to find that combination of letters in range [f,u] in alphabetical order such that the sequence of 32 numbers given to us should follow the rule: $sequence[i-1] = x_1^{i-1} + x_2^{i-1} + ... + x_m^{i-1}\ for\ i = 1 to 32$ (here $x_1, x_2, ..., x_m$ are ASCII values of letters chosen).

Now, the first hash value $i = 1$ in the hashed sequence was 22 and it is calculated as $x_1^0 + x_2^0 + ... + x_m^0$. i.e. $1 + 1 + ... + 1 = 22$. From this equation we found out that the length of the password is 22 since each character in the password contributed 1 when raised to the power 0.

Now we have to find the right combination of length 22 that satisfies the above equation. In order to do so we just used brute force method starting from the first possible combination of length 22 , i.e. $fffffffffffffffffffff$ basically [102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102, 102], second $ffffffffffffffffffffg$, to the last possible combination $uuuuuuuuuuuuuuuuuuuuu$. In simple words, if the current password satisfies the above equation we stop our execution and if not then we backtrack and insert a new letter such that ASCII(new letter) >= ASCII(previous letter)

Our recursive solution stopped at the sequence [102, 104, 104, 106, 106, 108, 108, 108, 109, 111, 111, 112, 112, 113, 114, 114, 115, 116, 116, 116, 117, 117] which when converted back to letters gives $fhhjjlllmoopppqrrstttuu$. When we used this as password it got accpeted.

No files uploaded

Q4 Password
15 Points

What was the final command used to clear this level?

fhhjjlllmoopppqrrstttuu

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.

A7.ipynb Download

```
In [1]:
import sys

codes = [22, 26, 79, 117, 81, 116, 56, 41, 110, 0, 102, 57, 50, 109,
107, 89, 59, 102, 15, 121, 91, 116, 89, 56, 47, 91, 6, 54, 92, 67,
43, 122]

def hash_function(arr):
    for i in range(2,14):
        res = sum(map(lambda x : x ** i, arr))
        res = res%127
        if(res != codes[i]):
            return False
    return True

def gen(n,arr,i,c):
  if i == n:
    if hash_function(arr):
      print(arr)
      #since we used system exit the program will stop as an
exception after printing the answer array
      sys.exit()
    return

  for j in range(c,118):
    arr[i] = j
    gen(n,arr,i+1,j)

n = 22
arr = [None] * n
gen(n,arr,0,102)
```

```
[102, 104, 104, 106, 106, 108, 108, 108, 109, 111, 111, 112, 112, 113, 114,

An exception has occurred, use %tb to see the full traceback.
SystemExit

/usr/local/lib/python3.7/dist-packages/IPython/core/interactiveshell.py:285
  warn("To exit: use 'exit', 'quit', or Ctrl-D.", stacklevel=1)
```

```
In [ ]:
```

Assignment 7

GRADED

GROUP
Manu Shukla
Rishabh Lakhwani
Divyansh Bisht
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