Q1 Team Name

0 Points

flash

Q2 Commands

5 Points

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

go/enter -> go/enter -> go/enter -> go/enter -> go/enter -> 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.)

After using the go, go, go, go, go, give, read commands respectively we were presented with the following screen:

" You see the following written on the panel:

21 7 68 86 4 50 123 5 29 110 35 23 98 36 55 4 22 109 57 52 113 52 50 58 87 13 8 35 117 96 77 24

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." "

From this message we can draw the following inferences:
1. The 32-digit number is the hash value of the password.
2. Each letter of password is between f and u.
3. Letters are in alphabetical order.
4.The ith number of the hashed sequence equals $x_1^{i-1} + x_2^{i-1} + ... + x_m^{i-1}$ where value of i is from 1 to 32.
5.password is a sequence of numbers $x_1, x_2, ..., x_m$ in the field F_{127}

$$Hashed\ value\ of\ password =$$
$$21\ 7\ 68\ 86\ 4\ 50\ 123\ 5\ 29\ 110\ 35\ 23\ 98\ 36\ 55\ 4\ 22\ 109\ 57\ 5$$

Let thei^{th} hashed value of password be p_i, so p_i can be written as:
$p_i = (x_1^{i-1} + x_2^{i-1} + ... + x_m^{i-1}) mod 127 - eqn1$ where $x_1, x_2, x_3.......x_m$ be the ascii values of the characters from 'f' to 'u'.

Putting $i = 1$ in eqn1 we get
$$p_1 = (x_1^{1-1} + x_2^{1-1} + ... + x_m^{1-1}) mod 127$$
$$21 = (x_1^0 + x_2^0 + ... + x_m^0) mod 127$$
$$21 = (1 + 1 + 1 + ...m\ times) mod 127$$
$$m = 21$$

Since we got the value of m to be 21 so our password is of length 21 characters.

We applied the brute force method to crack the password. For this we followed the following steps:

1) Generated all the possible non-decreasing sequences of 21

lengths (as our password length is 21) by considering the digits between 102 to 117 using the function "combinations_with_replacement". This function returns all combinations in sorted order allowing the repetition of elements.

2) We decided to iterate over all the possible combinations and checked whether the particular combination is generating the same hashed password digit from the 2nd to the 16th digit by varying the value of i from 2 to 16 in eqn1. We thought that if we get some options for which the first few digits of the hashed password match we can try all those options as a password in the server and can find the actual password. We didn't match all the values of the hashed password so that we can speed up our brute-force approach.

3) We obtained only one set of value which satisfies the above condition it is (102, 103, 103, 104, 104, 105, 105, 105, 107, 107, 109, 110, 111, 112, 113, 114, 114, 115, 116, 117, 117) that converts to $”fgghhiiikkmnopqrrstuu”$ when we convert ASCII values to characters. So this is the final command that is used to clear the level.

No files uploaded

Q4 Password

15 Points

What was the final command used to clear this level?

fgghhiiikkmnopqrrstuu

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.

Flash.zip Download

```
Large file hidden. You can download it using the
button above.
```

Assignment 7

● GRADED

GROUP

Ravi Shankar Das
Nimit Jain
Prashant Mishra

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