Q1 Team Name

0 Points

Goldfish

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.)

Upon entering read command,we found following sequence of number appearing on screen
23 5 47 55 19 32 115 112 56 75 72 67 74 92 39 37 22 69 107 91 89 59 66 11 41 48 28 30 33 29 3 66
We got following information from the screen
1. Password contains letters from f and u and it is sorted in non-decreasing order
2.Password is hashed and It can be represented by sequence of numbers as $x_1, x_2, ., x_m$ in the field f_{127} .
3. i_{th} term of password can be represented by
$\sum_{j=1}^{m} x_j^{i-1}$
As there are total 32 terms , value of i varies from 1 to 32
As we put i=1, the power raised on every terms becomes zero, thus total number of terms present in equation ,becomes equal 23. Thus value of m is 23.
As characters present in password ranges from f to u, we considered there ASCII value for determining password. thus x_j ranges from [102,117].

To decrypt password, we generated every combination of letters from 'f' to 'u' of length 23 in non-decreasing manner and we raised them by a power i-1 , then we performed 127 modulus operation on them , the resultant expression is then compared with the i th term in the sequence. If it matches with the corresponding given sequence number, we increased the value of i by 1 otherwise we considered next sequence in order for password decryption.

We performed above operation till a particular sequence of numbers ranging from 102 to 117 matched with all numbers in the given sequence.
The final password we obtained is
$102, 103, 106, 107, 107, 108, 108, 108, 109, 110, 111, 111, 112, 1$

when converted them back to their character form, we got

No files uploaded

Q4 Password

15 Points

What was the final command used to clear this level?

fgjkkllllmnooppppqrsstuu

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.