Q1 Team Name

0 Points

Lazarus

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.)

After typing in the "read" command we got the password hash as

$$24\ 69\ 53\ 32\ 23\ 40\ 36\ 117\ 20\ 16\ 65\ 121\ 96\ 113\ 27\ 43\ 83\ 80\ 91\ 48\ 115\ 2\ 42\ 74\ 122$$

Hash function formula was stated as $\sum_{j=1}^{m} x_j^{i-1}$ is equivalent to ith value in above password hash. Where x_j is an element of F_{127} and $i \in [1, 32]$

So when $i = 1$ is substituted in above formula, all x_j are raised to 0 and thus we get password length to be first element in password hash, which is 24 , i.e. $m = 24$

Another hint was that password contains only English lowercase letters from f to u and the characters in the password are in ascending alphabetical order. As ASCII value of 'f' is 102 and that of 'u' is 117. Therefore $x_j \in [102, 117]$ and this also satisfies that x_j is an element of F_{127}

For the given password hash formula order of letters does not matter as all password characters are raised to same power at a time to calculate ith element of password hash. So we generated all possible combinations of length 24 from integers value $\in [102, 117]$ and for each generated combination, summation of elements raised to power $i - 1$ was calculated then $\mod 127$ was performed and checked with i^{th} element of password hash. If same then next power was checked else next combination was checked from beginning. This was done for i = 1 to 32.

Combination satisfying all password hash values is given below

$$[102, 104, 106, 108, 109, 109, 104, 107, 111, 113, 113, 116, 117, 105, 106, 106, 108, 112, 113]$$

which after sorting in ascending order

$$[102, 102, 104, 104, 105, 105, 106, 106, 106, 107, 108, 108, 112, 113, 113, 113, 113, 116, 117]$$

which on converting to English lowercase characters using ASCII code comes out to be

$$\mathrm{ffhhiijjjkllmmmoopqqqqtu}$$

which is the password to clear this level

No files uploaded

Q4 Password

15 Points

What was the final command used to clear this level?

ffhhiijjjkllmmmoopqqqtu

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.

▾ Lazarus.zip Download

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

Assignment 7

● GRADED

GROUP

Aditya Loth

Varun Vankudre
Harsh Agarwal
View or edit group

TOTAL POINTS

40 / 50 pts

QUESTION 1

Team Name **0** / 0 pts

QUESTION 2

Commands **5** / 5 pts

QUESTION 3

Analysis R **20** / 30 pts

✓ **+ 5 pts** Encoding used for the input is ASCII encoding, i.e., $f - u$ maps to $102 - 117$

✓ **+ 5 pts** Finding the value of m, i.e, password length

✓ **+ 20 pts** Finding password:
Solution 1: Brute forcing over non-decreasing combinations of length m only
Solution 2: Using Newton Identities: Finding distinct roots and their multiplicities

+ 25 pts *Solution 3:* Form a system of modular equations. No need to explicitly compute m

+ 0 pts Incorrect or NA

− 10 pts Upper bound too much

Regrade Request Submitted on: **May 08**

We have script execution output from 21st April screenshot. Could you please share your email address, so we can share the image with you

I have your image. And it does not provide any credibility. You may have used the submitted code to get your password. But, it is not true every time.

Reviewed on: **May 08**

Regrade Request Submitted on: **May 07**

It is brute force and also stocashtic in nature,so sometimes it may take longer.

That is the thing. In the worst case, the total number of permutations is just too much to brute force. There is no credibility that the challenge was solved by the submitted code.

Reviewed on: **May 07**

Regrade Request Submitted on: **May 06**

It's possible. We have used submitted code to Brute Force the password. You can check by executing the script, in most cases the password comes out in an hour

I ran the Python script. And it has been 3 hours since it's running and yet not finished.

Reviewed on: **May 07**

Regrade Request Submitted on: **May 05**

Our method of choosing input randomly gives lesser decryption cases without compromising on the possible input combinatios. I dont think our method will give incorrect input text as order of numbers dont matter while taking sum and at the end we have taken sorted plaintext and outputted the password

The number of combinations for length 6 are 54264 which is the size of your variable a. Now in your while loop, you concatenate 4 random elements of a with replacement. That brings a total of $54264^4 = 8670561364418236416$ permutations which are not possible to brute force.

Reviewed on: **May 06**

QUESTION 4

Password

15 / 15 pts

QUESTION 5

Codes

0 / 0 pts