Q1 Team Name

0 Points

≡>

INFINITY

Q2 Commands

5 Points

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

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.)

On the last panel we got the text

"You see the following written on the panel:

39 116 103 29 18 91 As you wonder what do these numbers mean, you hear a whisper in your ears ...

20 21 44 68 59 82 20 50 30 28 38 51 56 50 117 67 75 35 121 6 96 126 102 93 126 60

"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."

Let the password be a sequence of integers like $x_1x_2x_3x_4....x_m$ Given,

 $x_1^0+x_2^0+x_3^0+x_4^0+\ldots+x_m^0=20$, which gives us the length of the password as

Let,

 $p_1 = x_1 + x_2 + x_3 + x_4 + \dots + x_m = 21$ $p_2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + \dots + x_{20}^2 = 44$

$$p_2 = x_1^3 + x_2^5 + x_3^3 + x_4^4 + \dots + x_{20}^5 = 44$$

$$p_3 = x_1^3 + x_2^3 + x_3^3 + x_4^3 + \dots + x_{20}^3 = 68$$

 $p_{31} = x_1^3 1 + x_2^3 1 + x_3^3 1 + x_4^3 1 + \dots + x_{20}^3 1 = 91$

General form for p_k can be defined as, $p_k = \sum_{i=1}^{i=m} x_i^k$ called as the k^{th} power sum.

Let's define $e_0 = (x_1, x_2, x_3, x_4,, x_m) = 1$ $e_0(x_1, x_2, x_3, x_4,, x_m) = x_1 + x_2 + x_3 + x_4 + + x_m$

 $e_1(x_1, x_2, x_3, x_4,, x_m) = \sum_{1 \le i \le j \le n} x_i x_j$

 $e_n(x_1, x_2, x_3, x_4, ..., x_m) = x_1 x_2 x_3 x_4 ... x_m$

 $e_k(x_1, x_2, x_3, x_4, ..., x_m) = 0$, for k > m, Then Newton's identities can be defined as

 $ke_k(x_1, x_2, x_3, x_4,, x_m) =$

 $\sum_{i=1}^k (-1)^{i-1} e_{k-i}(x_1,x_2,x_3,x_4,...,x_m) p_i(x_1,x_2,x_3,x_4,...,x_m)$, for all $n\geq 1$ and m > k > 1.

For all $k>n\geq 1$, above equation is 0.

Using the above equation we can find, $e_1, e_2, e_3, e_4, ..., e_{m=20}, ..., e_{31}$, $e_{21}=e_{22}=e_{23}=\ldots =e_{31}=0$ as it comes on the second part of the equation.

Above equations are implemented in the index.py, For multiplying by k^{-1} , using Ferma't Little Theorem we get $k^{-1}=k^{125} mod 127$

Then we get,

 $e_k, 0 \le k \le 20 =$

[1, 21, 8, 67, 98, 55, 36, 9, 63, 101, 11, 30, 95, 55, 9, 75, 77, 108, 84, 25, 108]Now we are brute-forcing from f-u for all the letters whether they will satisfy the polynomial formed by e_k $P(x) = \sum_{k=0}^{n} (-1)^k e_k x^{n-k}$, whose roots are the letters of the password

We get following letters satisfying the polynomial equation ['g', h', i', j', l', m', o', q', r', s', t', u']Thus, these are the letters which are used in the password, now we need to find their

frequencies in the password. For finding the frequency, we are defining a matrix pow_char with each row having $pow_char[i][j] = pass_char[i]^j$, where pass_char are the characters of

pass_char_list. We know the value of $\Sigma x_i^j = p[j]$, now each x_i belongs to the pass_char_list. As their are 12 distinct character we can use j from 1 to 12 so that we can use linear algebra to get

frequency of each letter. (as it has to be a square matrix). Let $pow_char.X = power_sum$, where power_sum is the array of p[j] from 1 to 12. X will contain the frequency of each letter.

We solved this equation in SAGE in Prime Field 127 using their inbuilt function $solve_right()$.

And as we know, the password contains the letters in alphabetical order we can easily find the whole password using each letters frequency.

Password: ghhhhiijjlmmoqqrrstu

References Link:

https://en.wikipedia.org/wiki/Newton%27s_identities

https://math.stackexchange.com/questions/973073/roots-of-simultaneous-power-sumequations-numerically-or-otherwise

https://www.geeksforgeeks.org/fermats-little-theorem/

No files uploaded

Q4 Password

15 Points

What was the final command used to clear this level?

will be given 0 for the entire assignment.

ghhhhiijjlmmoqqrrstu

Q5 Codes

0 Points It is MANDATORY that you upload the codes used in the cryptanalysis. If you fail to do so, you

▲ Download ▼ INFINITY.zip

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