CS641
Modern Cryptology
Indian Institute of Technology, Kanpur

Assignment 7

Group Name: Cryptomaniacs
Vishesh Kaushik (170805), Tarun Kanodia (190902), Kaustubh Verma (190924)

Submission Deadline:
April 23, 2022, 23:59hrs

Question 1

You see the following written on the panel:

22 90 38 112 67 52 25 17 45 91 110 20 82 47 115 12 124 92 120 42 6 87 45 49 34 46 98 70 82 79 7 40

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 i^{th} 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."

Solution

Cryptanalysis:

We have assumed that every letter used in the password is converted to its ASCII before applying hashing. It is given that the password is made of letters between $'f'$ and $'u'$ which means any the value of any x_i in the password is an integer and it lies in $[102, 117]$. One more point to note is that if we take $i = 1$ in the hash function, we get $x_1^0 + x_2^0 + ... + x_m^0 = m = 22$ in the field F_{127} (assuming that $m < 127$). It means that there are 22 characters in the password lying between $'f'$ and $'u'$.

As we are given summation of different power (from 0 to 31) of roots in in the field F_{127},

we have used Newton's identities to find out the actual polynomial in the field F_{127}.
If we are given $P_i = \sum_{j=1}^{j=22} x_j^i$ in the field F_{127} for $i \in [0, 31]$ then the coefficients of polynomial having roots $x_1, x_2, \ldots, x_{22}$ in the field F_{127} is related to $P_i's$ as follows:

For $i \leq k-1$, where k is the degree of polynomial and e_i is the coefficient of $(-1)^i a_{k-i}$ in the polynomial (assuming polynomial is of form $\sum_{i=0}^{k} {}_i x^i$).

$$\begin{aligned}
P_0 &= k, \\
P_1 &= e_1 \times 1 \\
P_2 &= e_1 P_1 - e_2 \times 2 \\
P_3 &= e_1 P_2 - e_2 P_1 + e_3 \times 3 \\
&\vdots \\
P_{k-1} &= e_1 P_{k-2} - e_2 P_{k-3} + \cdots + (-1)^{k-3} e_{k-2} P_1 + (-1)^{k-2} e_{k-1}(k-1)
\end{aligned}$$

For $i \geq k$

$$P_i = \sum_{j=1}^{k} (-1)^{j+1} e_j P_{i-j} \tag{1.1}$$

These equations are also valid for field F_{127} and corresponding modulo arithmetic is applied while finding e_i where $1 \leq i \geq 32$.
Once we have found the coefficients of the polynomial, then we found the roots of the polynomial by simply checking for each integer value in $[102, 117]$ whether the integer equates the polynomial to zero (in F_{127}). On the first run, we found 12 roots, which gave us the 12 distinct characters our password contains. We have to repeat the whole process of finding polynomial and finding roots thrice to get all 22 roots as we were getting repeated roots. We did it by subtracting the sum of powers of already calculated roots from each P_i's where $0 \leq i \leq 32$. After getting all the 22 integer roots lying in $[102, 117]$, we converted them to their character values and arrange them in alphabetical order to get the password as it is given in the question that the letters in the password are in alphabetic order.
The password we got is **fggghhhiijjkllmnrrrssu**. We have referred this web-page to understand Newton's Identities that we have used in our solution.