Writeup for c4

August 9, 2025

1 Understanding the problem

This challenge is quite interesting as we are trying to demonstrate that a different approach in the faulty one-time-pad which doesn't use the 0 byte may end up in giving a perfect secure encryption. For capturing the flag we are given with the ciphertext as well as the keystream and the task is largely to run the decryption algorithm.

2 Perfect Security for this algorithm

Here we are converting to base255 then performing some operation and again converting to base 256. If we pay close attention to the operation we are performing it is just adding the integer representing for the byte at that position in the key - 1 and then taking modulo 255. The interesting thing which is happening is that any byte in the key can have all values among 1 to 255 so subtracting 1 from it, we can have all values among 0 to 254. So, this is basically acting as a one-time-pad between plaintext and ciphertext in base 255 representations which is perfectly secure as per our previous knowledge. So, we can view our algorithm as a one-time-pad which involves two base conversion steps.

3 Solution

Firstly I created a simple base conversion function which uses mathematical approach of converting the base from initial base to final base. Also, we would need to subtract during decryption as encryption involved adding so I created a function to subtract taking care of modular arithmetic involved. Now, as we have the key all that remains is to convert the base of cipher text then subtract the key from it and then again convert from base 255 to 256 in order to get the plaintext.

4 Conclusion

This is kind of a one-time-pad only with changed bases and base conversion involved at both ends. As we are given with key and ciphertext, we just have to construct the decrypting algorithm which is quite evident from the specifications of the encryption algorithm.