CTF-03 writeup

Namish Bansal

August 2025

1 Understanding the problem:

In this problem, there was a small change in the generation of the key, as the key is now selected from [0x01,0xff] instead of [0x00,0xff]. Now this violates the perfect security of the system as now the ciphertext will provide some information about the message, like at a given position, the text will not be the same in the message as in the ciphertext.

2 Strategy:

- We will provide a long string with the same character (here '00').
- Then, the server will provide us with two ciphertexts, of which one is random and the other one is padded using the key. We will see if any byte of c1 matches with our original string, then that is not the ciphertext.
- If there is a case that no ciphertext contains the same character (here '00'), then we need to make the string longer.
- After enough length, there will always be a case that either of them contains the character we are looking for. At the end, It will give us flag.