CTF-04 Writeup

Namish Bansal

August 2025

1 Understanding the problem:

This is a nice way to correct the problem created in ctf-03. The given system is perfectly secure because we can say that the representation of m in base-255 is unique for every m. Then the base-255 message p is getting encrypted by a key whose every bit is randomly selected from [1,255], so there is even possibility of having any bit after the encryption at a given position. Thus, it forms a secure ciphertext c. And for every base-255 c, we can uniquely convert it to base-256 bytes.

2 Strategy:

- The strategy is simple, by just reversing the encryption logic completely, as we have both ciphertext and keyfile.
- So, for that, I firstly converted the ciphertext into base-255.
- Then, as I know k has bytes from [1,255], so I reversed the encryption by $(c - k + 1)\%255$.
- Then, to get the flag, we have to just convert this base-255 message into bytes.