CTF-02 Writeup

Namish Bansal

August 2025

1 Understanding the problem:

This was a challenge based on one time pad, but the problem was in the generation of the key. Here in the `encryptor.py`, it is clearly visible that the key is generated by firstly selecting a random int from (0,127) and then doing a particular set of functions to make it the same bit length as the plaintext. So there is a limited number of possible keys, i.e., 128 for a particular bit length.

2 Strategy:

- Firstly, generating the key in the same way as `encryptor.py`.
- Then decrypting the encryption logic by doing $(m1[i] - m2[i])$
- Then, using the key for all the values from (0,127) and the ciphertext, decrypt it.
- Then printing the flag which starts with cs409.