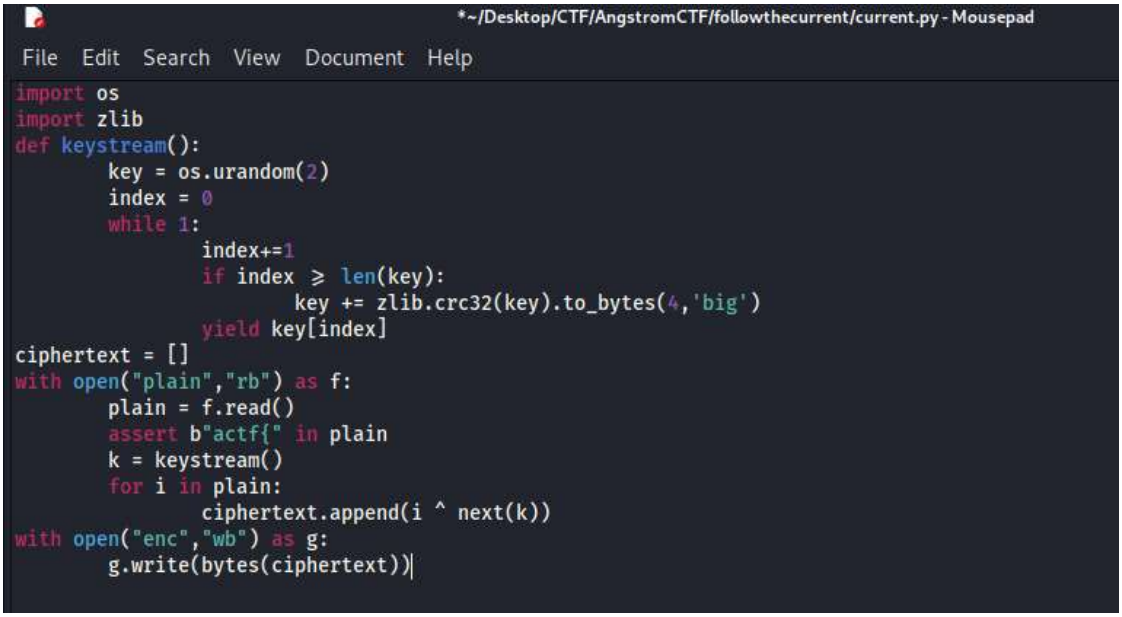
Crypto: Follow the Currents

We are given the source code + encrypted message (ciphertext). Here is the source code:

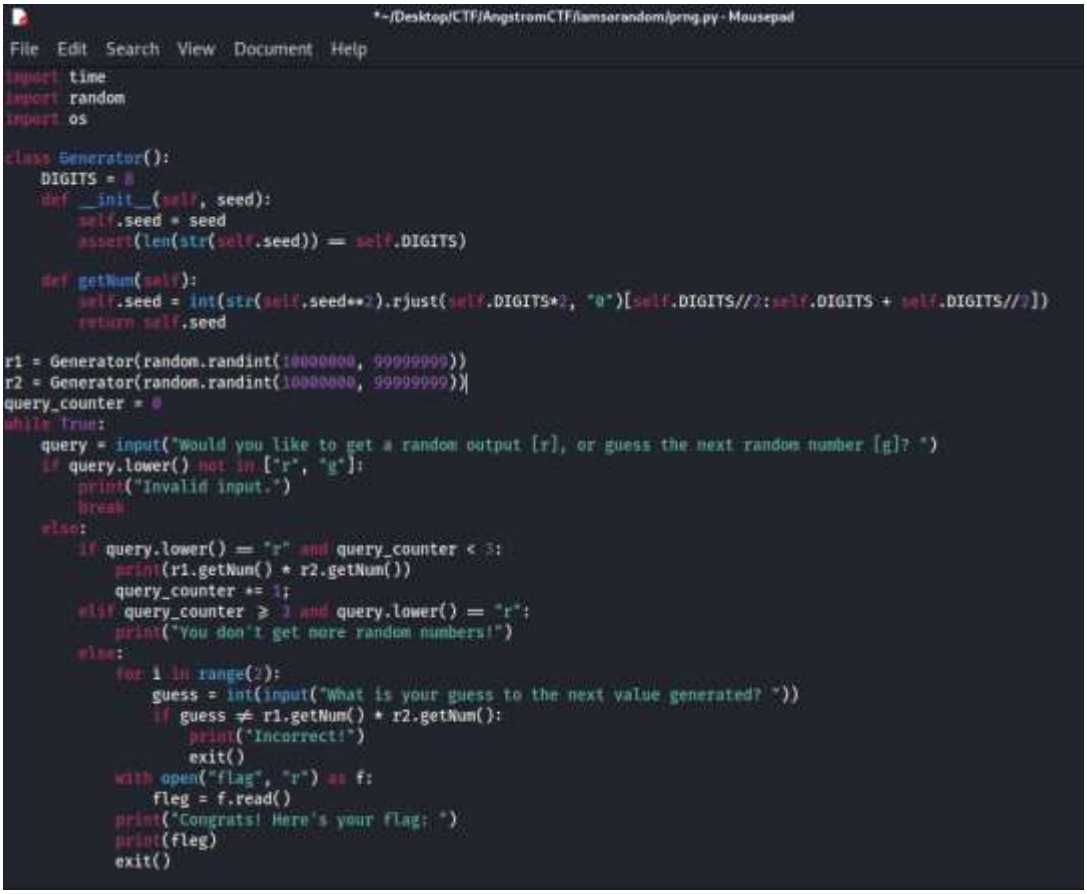


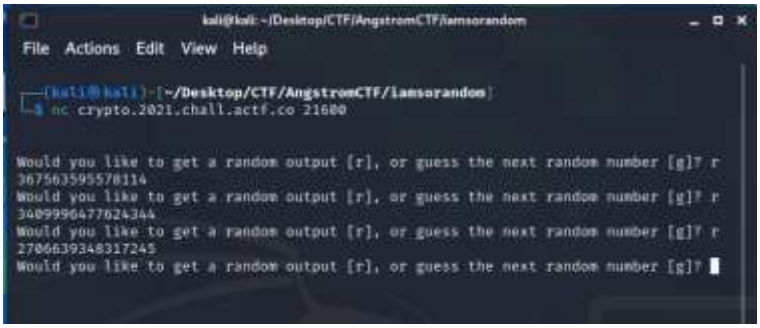
What vulnerable is that the **key** is urandom of length of 2. Brute Force it is 😊 256*256 = 65536 cases.

Flag is: `actf{low_entropy_keystream}`

Crypto: I'm so RANDOM

Here is the source code:





We are given 3 random numbers, and we will have to guess the next random numbers. Each random number is a product of two numbers with PNRG function.
Here the pseudorandom generator (PRNG) function generates new random by squaring its input + padding 0s on the right side, then only choose from digit 4:12 (8 digits).

As we know the seed is 8 digits and given the first random number, we can factorize it to a product of two numbers of length 8. Then for each pair as new seeds, generate new PNRG number to see if it matches. ☺ Here is the flag: **actf{middle_square_method_more_like_middle_fail_method}**