

OTP (one-time-pad) works like this:  $\text{message XOR random\_key} = \text{ciphertext}$

What the description is hinting at is probably the fact that random key was used multiple times. In this situation, we can attempt to guess plaintexts by using the properties of xor

$C1 \text{ XOR } C2 = M1 \text{ XOR key XOR } M2 \text{ XOR key} = M1 \text{ XOR } M2$ .

Using the results can help us figure out part of each message if we get lucky enough.

There are many tools on github. After a few attempts, one which worked is

<https://github.com/andreacanepa/Many-Time-Pad/tree/master>

Just make sure to include the ciphertext mentioned in the challenge alongside the others in ciphertexts.txt

**Made with love by: AndreiCat**