CS409 CTF-01

Namish Bansal

August 2025

We are given two ciphertexts, `ciphertext1.enc` and `ciphertext2.enc`, both encrypted using the same one-time pad key. Let's say they are c1 and c2, respectively and the key used is k. The messages encrypted are p1 and p2. So, $P_1 \oplus K = C_1$ and $P_2 \oplus K = C_2$.

That gives $C_1 \oplus C_2 = P_1 \oplus P_2$

The basic idea behind the solution is to XOR c1 and c2, resulting in $P_1 \oplus P_2$. After this we know that one message is flag which starts with "cs409". Also the string we found, if we XOR it with one of our messages, we get another message. So, firstly XOR with cs409 then got "Crypta" as the starting of the other message. Then guessed Crypta to be Cryptanalysis, and then the whole sentence by XORing multiple with the flag and other sentence multiple times. English sentence we got at the end is "Cryptanalysis frequently involves statistical attempts."