**🔓 The Plan**

Given:

cipher.encrypt(b'Slide to the left') → ciphertext1

cipher.encrypt(b'Slide to the right') → ciphertext2

You are provided:

ini

ciphertext1 = 1257c09aeb79f5883818c6947524bce955

ciphertext2 = 3b64eb9faf54bdf56e0511985d793d33f903

The goal is to submit the ciphertext of:

bash

b'Criss cross, criss cross'

So we’ll:

1. Recover the keystream by XORing the known plaintext and ciphertext.
2. Use that keystream to encrypt the target message.

**🧮 Step-by-Step**

**1. Get the keystream from a known pair**

We use the shorter known pair:

vbnet

plaintext: b'Slide to the left' → 17 bytes

ciphertext: 1257c09aeb79f5883818c6947524bce955

XOR each byte of plaintext with the corresponding ciphertext byte to recover the keystream.

**2. Encrypt b'Criss cross, criss cross' using the recovered keystream.**

If the recovered keystream is long enough (the message is 23 bytes), we need at least one of the ciphertexts to be 23 bytes long. Let’s check the second ciphertext:

3b64eb9faf54bdf56e0511985d793d33f903 → 24 bytes

So use this one.

Plaintext:

b'Slide to the right' → len = 18 bytes

But we need to encrypt:

b'Criss cross, criss cross' → 23 bytes

So that ciphertext won't help us unless we know how to continue the stream.

⚠️ **Solution**: Instead, treat the process as:

* Decrypt ciphertext1 using plaintext1 to get the keystream for those 17 bytes.
* Decrypt ciphertext2 using plaintext2 to get 18 more bytes of keystream.
* Combine them to make a 35-byte keystream.
* Encrypt b'Criss cross, criss cross' (23 bytes) with the first 23 bytes of the keystream.

Here's a complete **Python script** that automates the exploitation of this challenge. It will:

1. Connect to the challenge using nc (via pwn library for automation).
2. Read the two ciphertexts from the server.
3. Recover the keystream using known plaintexts ("Slide to the left" and "Slide to the right").
4. Encrypt "Criss cross, criss cross" with the keystream.
5. Send the ciphertext.
6. Print the server response (which should contain the flag if successful).