Writeup for c1

August 9, 2025

1 Understanding the problem

This challenge demonstrates the security issues that arise by using the key for a one-time-pad. If we both the messages are using a particular language(here english), we can easily exploit the language's patterns to obtain the messages. We are given ciphertext1 and ciphertext2 as two cipher texts made using one-time-pad technique using the same key. Also, we are given that the flag is contained in ciphertext1 and starts with cs409{.

2 Solution

If we simply XOR the two cipher texts, we obtain the XOR of the two messages(let this be called XORED). Now, if we have some hint about one message, we can simply XOR it with the value XORED by padding the remaining part as zero and get something about the other message. Now, we can guess by knowledge of english language how the sentence can be completed and then try XORing it and select the one which gives a sensible output for the other text. For Example, when I started XORing with cs409{, I obtained Crypta in the other message. Now I try XORing with words like Cryptanalysis or Cryptanalyst and try until I get some sensible output. Now, I get something like cs409{one_t by using the word Cryptanalysis and then I can guess what can complete cs409{one_t and it becomes pretty obvious that the word may be one_time. Now this reveals something about the other message and I continue doing the same process until I obtain the whole flag.

3 Conclusion

Here, I have used patterns in the english language which are quite easy to recognize as a frequent english speaker to keep guessing the next words and obtain the flag.