Writeup for c3

August 9, 2025

1 Understanding the problem

Here, the encryptor is not using \x00 as a byte in the one-time-pad algorithm and we need to show that we can differentiate the cipher obtained by running on a string given by us from the cipher obtained by running this algorithm on some random string with some new random key.

2 Solution

Here, we will not be getting the same character as in ciphertext as 0 is never in the key of the encryption algorithm. So, naturally we should check whether there is any character which matches in the ciphertext with the plaintext I gave if it does, the other ciphertext is the answer otherwise this one is the answer. The chance for having a same character highly increases as we increase the length of the string being given by us. So, I have given a long string of As in hex form which is something 41414141... . To check for any same character, I have simply XORed c1 with my payload text and check whether there is any 0 byte in the result. If there's then c2 is the encryption and if there is not c1 is likely the encryption which becomes nearly sure given the large size of my payload

3 Conclusion

We observe that simply by omitting 0 byte in the key generation, we have provided chance to distinguish between encryptions from two different messages and so it doesn't follow definition of perfect security and is a faulty one-time-pad.