

# XOR Cipher Challenge

## Introduction

For the new semester, the TUM security office sends new login credentials to each student and staff member. Since these credentials are very sensitive, they are encrypted using a 24-byte-long pre-shared key. Your key is (hex encoded):

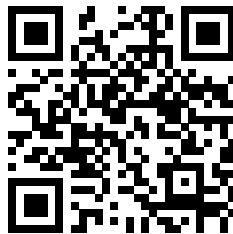
5a6935554b655a4a4b37696e353379584a397a32657071

The message that contains your credentials is 48 bytes long. To decrypt it, you need to split it into two 24-byte halves and apply the bitwise XOR operator to each byte of the message and the key. The message you got from the TUM security office is (hex encoded):

030640276b09352d2259490d47561d3d244d135309034b

3d060c62331c20651f5f001d7c403a37384b1f51114a58

To make the conversion of hex to ASCII and the calculation of XOR more convenient, you can use this website:



<https://set-xor-challenge.dorian.im>

With this website, copy and paste is enough to solve both challenges.

## Challenge 1 (2 points)

To decrypt this message, you need to use the bitwise XOR operator to combine the ciphertext and key byte-by-byte. For more information about the XOR cipher, see: [https://en.wikipedia.org/wiki/XOR\\_cipher](https://en.wikipedia.org/wiki/XOR_cipher)

**Decrypt the message to find out your login credentials!**

## Challenge 2 (8 points + 3 bonus points)

A mail server security flaw allowed you to read your professor's emails! You were able to find his email from the TUM security office which contained his encrypted credentials (hex encoded):

3d061001451f3c1e1a1a450e3b161036071701041e2777

0306514111063e562a1b102e3b1217380c07211153756c

However, you don't have access to their decryption key.

**Can you still find out their login credentials?**

## Hints

Properties of bitwise XOR:

- commutative:  $A \oplus B = B \oplus A$
- associative:  $A \oplus (B \oplus C) = (A \oplus B) \oplus C$
- identity element:  $A \oplus 0 = A$
- self-inverse:  $A \oplus A = 0$

Definition of XOR cipher:

- Encryption:  $Plaintext \oplus Key = Ciphertext$
- Decryption:  $Ciphertext \oplus Key = (Plaintext \oplus Key) \oplus Key = Plaintext \oplus (Key \oplus Key) = Plaintext$

If you get stuck and don't know how to proceed, you can ask your tutor for more hints in exchange for some points.