

Homework 1
2022-2023 3rd Trimester
Due on Saturday April 1, 2023, 11:59 p.m. via Blackboard.

If you do not have the textbook, use the following link to download it

<https://emadalsuwat.github.io/cryptography/textbook1.pdf>

Do textbook problems:

- Review Questions (3.1, 3.2, 3.5, 3.7, 3.8) (Page 97)

- Problem 3.8 (b, c, d and e) (Page 99)

- Answer the following questions about S-boxes in DES:
 - Show the result of passing 110111 through S-box 3.
 - Show the result of passing 001100 through S-box 4.
 - Show the result of passing 000000 through S-box 7.
 - Show the result of passing 111111 through S-box 2.

- Show the results of the following hexadecimal data

0110 1023 4110 1023

after passing it through the initial permutation box.

- Show the results of the following hexadecimal data

AAAA BBBB CCCC DDDD

after passing it through the final permutation box.