Homework 1

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

https://hatimalsuwat.github.io/cryptography/textbook1.pdf

Do textbook problems:

- Problem 2.10 (Page 62)
- Problem 2.11 (a only) (Page 63)
- Problem 3.8 (a, b, c, d and e only) (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.

- In DES, if the key with parity bit (64 bits) is 0123 ABCD 2562 1456, find the first-round key.