Assignment 3

Task (10 marks). The task of this assignment is to implement the symmetric block cipher PRESENT-80 in bitsliced format in C language. The program should

- Include key schedule (no need to be bitsliced)
- Bitsliced encryption algorithm for PRESENT-80
- Allow the user to provide master key
- Be able to encrypt a user specified plaintext in hexadecimal format (up to 64 × 64 bit) uploaded as a file (see the file sampleplaintext.txt)
- Utilize algebraic normal form for implementing sBoxLayer
- Output the ciphertext blocks in hexadecimal format, similar to the sampleciphertext.txt file

Test vectors can be found in the following link `https://eprint.iacr.org/2009/516.pdf` at page 170 - note that this contains test vectors for just block of plaintext

Grading criteria:

- Correctness (5 marks)
- Answer questions when presenting the code (5 marks)
- Example questions:
  - Where is pLayer implemented
  - What is the meaning of a certain variable in the code
  - How is algebraic normal form implemented
- Note that you will get a 0 grade if your implementation is not bitsliced.

What to submit. The submission should include

- Source code of the program with *proper* comments
- A readme file describing how to run the encryption
  - How to compile the program
  - Format of input file

When to submit: by Week 4 Thursday 8 am