Homework 3

Weight: 3%

CMPS 385 Computer Security

Submission Deadline: 12/04/2020

Spring 2020

- You need to submit Homework 2 Word document and your solution implementation on Blackboard.
- For the program and other supporting files of the program must be put in a .zip folder.
- The program must be executable.
- Copying of the answer document and copying of the program from other student will result in reporting to the University Committee.

Let **A** the state matrix of the input message to be encrypted using AES :

$$A = \begin{bmatrix} 01 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix}$$

The first 2 subkeys are:

$$K_0 = \begin{bmatrix} 2B & 28 & AB & 09 \\ 7E & AE & F7 & CF \\ 15 & D2 & 15 & 4F \\ 16 & A6 & 88 & 3C \end{bmatrix} \qquad K_1 = \begin{bmatrix} A0 & 88 & 23 & 2A \\ FA & 54 & A3 & 6C \\ FE & 2C & 39 & 76 \\ 17 & B1 & 39 & 05 \end{bmatrix}$$

Write a Java, C++ or Python program to compute the output ONLY of the **<u>first round of AES</u>** using the input state matrix A and the subkeys K_0 and K_1. Output all intermediate steps for the computation including Initial Key Addition, SubBytes, ShiftRows, and MixColumns and Round Key Addition.