Fall 2020 CIS 3362 Quiz #3 Part B: AES

Date: 10/12/2020

Directions: Please use DES/AES and Binary->Hex reference sheets, your course notes and a calculator as aids for this exam. Do NOT attempt to look up information online. Even if you use a calculator, show each step of your calculations that you would do by hand. The role of the calculator will simply be to speed up individual calculations (13 x 29, for example), not to skip whole steps, as these steps are typically awarded points in the grading criteria.

Please either type your answers. The accepted file types for submission will be .doc, .docx, .txt and .pdf. I recommend that you directly type into the posted document to save time.

Please look at Webcourses to see when your due time and late due time are. It's recommended that you stop working at the due time and start uploading at that time. Anything turned in before the late due time will be accepted for full credit. Anything that doesn't make it in by the late due time will earn a 0. A 10 minute buffer will be provided after both due times. Please don't take advantage of these buffers as it's an unnecessary risk.

1) (14 pts) If the state matrix is the following right before the Mix Columns step of AES, what is the entry in row 4, column 2, right after the Mix Columns step? ***(Note: Please be very, very, very careful that you work out the correct entry. If you find the entry of row 2, column 4, you will earn a maximum of 3 points out of 14.)***

$$\begin{pmatrix} 7B & A4 & CD & 12 \\ 2C & 3D & 96 & 4F \\ 97 & 16 & A0 & 62 \\ B2 & D7 & 7E & D3 \end{pmatrix}$$

Note that the fixed matrix multiplier for the Mix Columns step in AES is $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$.

2) (10 pts) Consider the process of AES Key Expansion. Imagine that we have:

w[36] = B1 89 C4 07 (in hex)
w[39] = 9C 2F 63 DE (in hex)

Calculate w[40], showing each of the following intermediate results: RotWord(temp), SubWord(RotWord(temp)), Rcon[i/4], and the result of the XOR with Rcon[i/4].

RotWord	SubWord	Rcon[i/4]	XOR	FinalResult

3) (1 pt) On what day of the week does the sketch comedy show Saturday Night Live air?