Fall 2020 CIS 3362 Quiz #3 Part B: AES Solution

Date: 10/12/2020

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 $\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$.

Solution

The appropriate entry is equal to 03 x A4 + 01 x 3D + 01 x 16 + 02 x D7.

Let's work out the first and last product individually:

03 x A4 = 02 x A4 + 01 x A4

02 x A4 = 02 x (1010 0100) = 1 0100 1000 = 0100 1000
+ 1 1011

0101 0011 (53)

Using the Hex XOR chart, we find that 53 + A4 = F7.

02 x D7 = 02 x (1101 0111) = 1 1010 1110 = 1010 1110
+ 1 1011

1011 0101 (B5)

Thus, our final answer will be F7 + 3D + 16 + B5. Separating out the hex chars, we must calculate

F + 3 + 1 + B = C + A = 6
7 + D + 6 + 5 = A + 3 = 9

Thus, the final output is **69 = 0110 1001.** (Note: Either form is acceptable since the question didn't specify.)

Grading: 6 pts 03 product, 4 pts 02 product, 4 pts final XOR. If wrong entry calculated give max 3 pts out of 14. Take off 1 pt per error otherwise.

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
2F 63 DE 9C	**15 FB 1D DE**	**36 00 00 00**	**23 FB 1D DE**	**92 72 D9 D9**

Grading: 1 pt RotWord, 4 pts SubWord (1 pt per byte), 1 pt Rcon, 1 pt XOR, 3 pts final answer

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

Saturday (Grading: Give to All)