Homework 13, due October 2

(1) Remember that for the smaller version of AES we did in class using $GF(8) = \mathbb{Z}_2[x]/(x^3 + x + 1)$, the S-box is generated by

$$S(x) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} x^6 + \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Write down the S-box. (Go ahead and write three bits as a column vector by writing the first bit on the top, the second in the middle, and the third on the bottom. This isn't the way AES does it, but it's easier.)

(2) Remember that if $4 \nmid i$, then

$$W(i) = W(i-4) \oplus W(i-1),$$

and that if $4|i$, then

$$W(i) = W(i-4) \oplus T(W(i-1)),$$

where T shifts the entries of $W(i-1)$ up one, shifting the first entry to the last, applies the S-box to each entry in the shifted column, and adds $010^{(i-4)/4}$ to the first 3-bit entry in the S-boxed column.

Given the key

$$\begin{pmatrix} 000 & 001 & 001 & 010 \\ 010 & 100 & 100 & 101 \\ 001 & 001 & 001 & 001 \\ 010 & 010 & 010 & 000 \end{pmatrix},$$

make the key schedule for two more rounds.

(3) Encrypt the all-zero matrix using two rounds of the smaller version of AES, using the key above. (The steps should be ARK(0), BS-SR-MC-ARK(1), BS-SR-ARK(2).)