

Homework 13, due October 6

- (1) Recall the AES key schedule for AES with a 128-bit key, which creates round keys $K_0, K_1, \dots, K_{10}$. 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 $00000010^{(i-4)/4}$ to the first 8-bit entry in the S-boxed column.

Given the AES key which is 128 zero bits, find the round keys K_0, K_1, K_2 (you will need the AES S-box on page 155 of the text).

- (2) (Page 105, problem 10) A group of people are arranging themselves for a parade. If they line up three to a row, one person is left over. If they line up four to a row, two people are left over, and if they line up five to a row, three people are left over. What is the smallest possible number of people?
- (3) Find the smallest nonnegative solution to the system of congruences

$$19x \equiv 103 \pmod{900},$$

$$10x \equiv 511 \pmod{841}.$$