Due: October 27, 2008

Trappe and Washington, Chapter 5 – 3, 4, 5.

4. Compute $x^{-1}$ for 10011011 in the Galois Field constructed with the Rijndael minimal polynomial.

5. Calculate the polynomial that represents the 3rd most significant bit of $S_5$ (the fifth S-box). Bits with a lower index value are the more significant bit. Do the same thing for the 3rd most significant bit of Bytesub (the Rijndael substitution).

6. What is the best linear approximation of any (nontrivial) linear combination of the $S_5$? Bytesub?