The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 3
February 12, 2013

Assignment 2 – Due Tuesday, February 26

1. Textbook, page 144, Problem 4.26 (you may either do this by hand or write a program to do it).

2. Textbook, page 145, Problem 4.27.

3. Pick two random 8-bit values, x and y, write them in hexadecimal, with the only condition being that the number of “1 bits” in each of x and y must be between 3 and 6 bits (inclusive). Next, treating these as elements from $GF(2^8)$ (using the “AES modulus” of $m(x) = x^8 + x^4 + x^3 + x + 1$), calculate the product of x and y — show your work! [*This problem and the next are “create your own unique problem” problems. If you pick random values, then your values and your problem/solution will be different from everyone else’s in the class.*]

4. Select a random 8-bit value (with at least 2 bits set to 1), and show the work required to find the AES S-box mapping for this value. Your final result should agree with the look-up table given in Table 5.2.

5. Do some on-line research and find information on the AES acceleration instructions introduced by Intel in its latest processors (these are called the AES-NI instructions). Briefly describe the new instructions and what they do in terms of the AES algorithm. Be sure to cite whatever source you use for this information.

6. Textbook, page 216, Problem 6.4.

7. Textbook, page 216, Problem 6.10.

8. Textbook, page 216, Problem 6.11 — to this problem, add a part c:

   c. Write out mathematical formulas for the last two blocks in CTS mode.

9. Textbook, page 240, Problem 7.4.

10. Textbook, page 240, Problem 7.6.

11. (**Extra Credit.**) There are 14 students in this class — if each student picks a truly random value that meets the criteria for problem 4, what is the probability that two students will pick the same value? What’s the probability that two students will pick the same two values in problem 3?