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

Handout 4
February 5, 2014

Assignment 2 – Due Wednesday, February 12

Chapters 4

This assignment is more straightforward than usual, covers only one chapter, and you only have one week. It will count only half as much as your normal assignments (it will be graded out of 50 points).

1. Compute the following GCD's using the Euclidean algorithm presented in Section 4.2. Show each step and intermediate result.
   (a) gcd(21703, 44850)
   (b) gcd(215258, 71512)
2. Compute gcd(612, 4931) using the *Extended* Euclidean algorithm given in Section 4.3. Show each step and intermediate result. Note that for inputs a and b, the Extended Euclidean algorithm finds not only gcd(a, b) but also values x and y so that $ax + by = gcd(a, b)$ — make sure you clearly mark x and y in your final answer.
3. Prove that for any positive values a, b, c, and n,
   (a) $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$
   (b) $(a \times b \times c) \bmod n = [(a \times b) \bmod n] \times c \bmod n$
4. For each of the following equations, find an integer x that satisfies the equation.
   (a) $3x \equiv 4 \pmod 5$
   (b) $3x \equiv 4 \pmod 7$
   (c) $9x \equiv 1 \pmod{11}$
5. For the following questions, use polynomial arithmetic over GF(2):
   (a) What is the product of $x^7 + x^6 + 1$ and $x^4 + x^3 + x^2$?
   (b) What are the quotient and remainder when $x^{11} + x^8 + x^4 + x^3 + x^2$ is divided by $x^8 + x^4 + x^3 + x + 1$?
   (c) What is the product of $x^7 + x^6 + 1$ and $x^4 + x^3 + x^2$ modulo $x^8 + x^4 + x^3 + x + 1$?
6. Part (c) in the previous question can be viewed as a field operation over GF(2^8) — rewrite that operation and product using the hexadecimal notation described in Section 4.7 (you do *not* need to rework the calculation — just re-write the result using hexadecimal notation).
7. Calculate $\{16\}\times\{64\}$, where these values are hexadecimal notation for elements of GF(2^8) — use the AES modulus ($x^8 + x^4 + x^3 + x + 1$).