Assignment 2 – Due Tuesday, February 16

Chapters 4–5

1. Compute the following GCD's using the Euclidean algorithm presented in Section 4.2. Show each step and intermediate result.

   (a) gcd(20259, 41962)

   (b) gcd(750588,374851)

2. Compute gcd(472,7107) 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. Textbook page 125, Problem 4.2

4. Textbook page 125, Problem 4.3

5. Textbook page 126, Problem 4.12, adding the additional requirement that a and b are natural numbers, and for part (a) further assume that $a \geq b$ — this way no values will be negative.

6. For the following questions, use polynomial arithmetic over GF(2):

   (a) What is the product of $x^5 + x^4 + 1$ and $x^5 + x^4 + x^3$?

   (b) What are the quotient and remainder when $x^{10} + x^7 + x^5 + x^4 + x^3$ is divided by $x^8 + x^4 + x^3 + x + 1$?

   (c) What is the product of $x^5 + x^4 + 1$ and $x^5 + x^4 + x^3$ modulo $x^8 + x^4 + x^3 + x + 1$?

7. 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, and for full credit do all operations in binary representation (don't write out polynomials)! [*This problem and the next two 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.*]

8. 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. [*Hint: You can select your 8-bit value so that it is "easy to invert," but you should still have some randomness in your selection — don't just pick the easiest value.*]

9. For this question, you are to work through the first four steps of AES encryption (the initial AddRoundKey followed by the first 3 steps in round 1). Show enough work to demonstrate how you calculated the result of each step.

   (a) Pick a 16 byte plaintext and 16 byte key. You can pick some random values, or write down some pattern, but don't use anything obvious — I don't want to see any two students with the same values! Write down your values in the 4×4 state matrix form used in the book.

   (b) Perform the initial AddRoundKey step on the values from (a).

   (c) Perform SubBytes on the result of part (b).

   (d) Perform ShiftRows on the result of part (c).

   (e) Perform MixColumns on the result of part (d).