Johns Hopkins ■ CS600.424: Network Security ■ Spring 2012

Homework 5 – Assignment

Due Date – April 25, 5 PM (Drop off in Room NEB 219)

Instructions: Please do not submit handwritten assignment.

1. Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101} in hex.

   (a) Show the original contents of the State, displayed as a 4 × 4 matrix.

   (b) Show the value of State after Initial AddRoundKey as a 4 × 4 matrix.

   (c) Show the value of State after SubBytes as a 4 × 4 matrix.

   (d) Show the value of State after ShiftRows as a 4 × 4 matrix.

   (e) Show the value of State after MixColumns as a 4 × 4 matrix.

2. Compute the output of the MixColumns transformation for the following sequence of input bytes 67 89 AB CD. Apply the InvMixColumns transformation to the obtained result to verify your calculations. Change the first byte of the input from 67 to 77, perform the MixColumns transformations for the new input, and determine how many bits have changed in the output. Please do this problem by hand and show all the results in matrix form.

4.28 3. (a) Develop a table similar to Table shown on lecture notes slide 54 (Table 4.9 of Textbook) for GF(2^4) with m(x) = x^4+x+1

4.25 4. Determine the gcd of the following pair of polynomials.

$$(a)\, x^3 + x + 1 \text{ and } x^2 + x + 1 \text{ over } GF(2)$$

$$(b)\, x^3 - x + 1 \text{ and } x^2 + 1 \text{ over } GF(3)$$

$$(c)\, x^5 + x^4 + x^3 - x^2 - x + 1 \text{ and } x^3 + x^2 + x + 1 \text{ over } GF(3)$$

4.15/4.19 5. (a) Find gcd for x= 408 and y = 595 and show the results in a tabular form.

   (b) Find the multiplicative inverse of 797 mod 1047 using Extended Euclidean Algorithm. Show results in a tabular form.