# Network Security

# Homework 5

## CHANG LIU

## chang.liu@jhu.edu

# April. 22, 2012

**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.**

**FIRST OUTPUT: 67 89 AB CD**

MixColumns:



InvMixCOlumns:



**SECOND OUTPUT: 77 89 AB CD**

MixColumns:

 **The number of bits changed in the output:** 5

**3. (a) Develop a table similar to Table shown on lecture notes slide 54 (Table 4.9 of Textbook) for GF(24) with m(x) = x4+x+1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Power**  **Representation** | **Polynomial**  **Representation** | **Binary**  **Representation** | **Decimal (Hex)**  **Representation** |
| 0 | 0 | 0000 | 0 |
| g0(=g15) | 1 | 0001 | 1 |
| g1 | g | 0010 | 2 |
| g2 | g2 | 0100 | 4 |
| g3 | g3 | 1000 | 8 |
| g4 | g+1 | 0011 | 3 |
| g5 | g2+g | 0110 | 6 |
| g6 | g3+ g2 | 1100 | 12 |
| g7 | g3+g+1 | 1011 | 11 |
| g8 | g2+1 | 0101 | 5 |
| g9 | g3+g | 1010 | 10 |
| g10 | g2+g+1 | 0111 | 7 |
| g11 | g3+ g2+g | 1110 | 14 |
| g12 | g3+ g2+g+1 | 1111 | 15 |
| g13 | g3 +g2+1 | 1101 | 13 |
| g14 | g3+1 | 1001 | 9 |

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

**(a) x3+x+1 and x2+x+1 over GF(2)**

   

Thus the GCD is 1.

**(b) x3-x+1 and x2+1 over GF(3)**

  

Thus the GCD is 1.

**(c) x5+x4+x3-x+1 and x2+x+1 over GF(2)**

 

Thus the GCD is x+1.

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

|  |  |  |  |
| --- | --- | --- | --- |
| Dividend | Divisor | Quotient | Remainder |
| y = 595 | X = 408 | Q1 = 1 | R1 = 187 |
| X = 408 | R1 = 187 | Q2 = 2 | R2 = 34 |
| R1 = 187 | R2 = 34 | Q3 = 5 | R3 = 17 |
| R2 = 34 | R3 = 17 | Q4 = 2 | R4 = 0 |

Thus the GCD = 17

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Quotient** | **Remainder** | **Substitute** | **Combine terms** |
| 1 |  | 1047 |  | 1047 = 1047x1 + 797x0 |
| 2 |  | 797 |  | 797 = 1047x0 + 797x1 |
| 3 | 1 | 250=1047-797 | 250=(1047x1+797x0)-(1047x0+797x1)x1 | 250=1047x1+797x(-1) |
| 4 | 3 | 47=797-250x3 | 47=(1047x0+797x1)-(1047x1+797x(-1))x3 | 47=1047x(-3)+797x(4) |
| 5 | 5 | 15=250-47x5 | 15=(1047x1+797x(-1))- (1047x(-3)+797x(4))x5 | 15=1047x16+797x(-21) |
| 6 | 3 | 2=47-15x3 | 2=(1047x(-3)+797x(4))-( 1047x16+797x(-21))x3 | 2=1047x(-51)+797x(67) |
| 7 | 7 | 1=15-7x2 | 1=(1047x16+797x(-21))-( 1047x(-51)+797x(67))x7 | 1=1047x373-797x490 |

Thus the multiplicative inverse is 1047x373-797x490 = 1.