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

$$\begin{pmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{pmatrix}$$

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

$$\begin{pmatrix} 00 & 04 & 08 & 0C \\ 01 & 05 & 09 & 0D \\ 02 & 06 & 0A & 0E \\ 03 & 07 & 0B & 0F \end{pmatrix} \oplus \begin{pmatrix} 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \\ 01 & 01 & 01 & 01 \end{pmatrix} = \begin{pmatrix} 01 & 05 & 09 & 0D \\ 00 & 04 & 08 & 0C \\ 03 & 07 & 0B & 0F \\ 02 & 06 & 0A & 0E \end{pmatrix}$$

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

$$\begin{pmatrix} 01 & 05 & 09 & 0D \\ 00 & 04 & 08 & 0C \\ 03 & 07 & 0B & 0F \\ 02 & 06 & 0A & 0E \end{pmatrix} \rightarrow \begin{pmatrix} 7C & 6B & 01 & D7 \\ 63 & F2 & 30 & FE \\ 7B & C5 & 2B & 76 \\ 77 & 6F & 67 & AB \end{pmatrix}$$

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

$$\begin{pmatrix} 7C & 6B & 01 & D7 \\ 63 & F2 & 30 & FE \\ 7B & C5 & 2B & 76 \\ 77 & 6F & 67 & AB \end{pmatrix} \rightarrow \begin{pmatrix} 7C & 6B & 01 & D7 \\ F2 & 30 & FE & 63 \\ 2B & 76 & 7B & C5 \\ AB & 77 & 6F & 67 \end{pmatrix}$$

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

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \otimes \begin{pmatrix} 7C & 6B & 01 & D7 \\ F2 & 30 & FE & 63 \\ 2B & 76 & 7B & C5 \\ AB & 77 & 6F & 67 \end{pmatrix} = \begin{pmatrix} 75 & 87 & 0F & A2 \\ 55 & E6 & 04 & 22 \\ 3E & 2E & B8 & 8C \\ 10 & 15 & 58 & 0A \end{pmatrix}$$

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:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}\begin{pmatrix} 67 \\ 89 \\ AB \\ CD \end{pmatrix}=\begin{pmatrix} 02\cdot 67\oplus 03\cdot 89\oplus 01\cdot AB\oplus 01\cdot CD \\ 01\cdot 67\oplus 02\cdot 89\oplus 03\cdot AB\oplus 01\cdot CD \\ 01\cdot 67\oplus 01\cdot 89\oplus 02\cdot AB\oplus 03\cdot CD \\ 03\cdot 67\oplus 01\cdot 89\oplus 01\cdot AB\oplus 02\cdot CD \end{pmatrix}=\begin{pmatrix} CE\oplus 80\oplus AB\oplus CD \\ 67\oplus 09\oplus E6\oplus CD \\ 67\oplus 89\oplus 4D\oplus 4C \\ A9\oplus 89\oplus AB\oplus 81 \end{pmatrix}$$

$$=\begin{pmatrix} 28 \\ 45 \\ EF \\ 0A \end{pmatrix}$$

InvMixCOlumns:

$$\begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix}\begin{pmatrix} 28 \\ 45 \\ EF \\ 0A \end{pmatrix}=\begin{pmatrix} 0E\cdot 28\oplus 0B\cdot 45\oplus 0D\cdot EF\oplus 09\cdot 0A \\ 09\cdot 28\oplus 0E\cdot 45\oplus 0B\cdot EF\oplus 0D\cdot 0A \\ 0D\cdot 28\oplus 09\cdot 45\oplus 0E\cdot EF\oplus 0B\cdot 0A \\ 0C\cdot 28\oplus 0D\cdot 45\oplus 09\cdot EF\oplus 0E\cdot 0A \end{pmatrix}=\begin{pmatrix} AB\oplus D1\oplus 47\oplus 5A \\ 73\oplus 9B\oplus 13\oplus 72 \\ D3\oplus 5B\oplus 6D\oplus 4E \\ 23\oplus 54\oplus D6\oplus 6C \end{pmatrix}$$

$$=\begin{pmatrix} 67 \\ 89 \\ AB \\ CD \end{pmatrix}$$

SECOND OUTPUT: 77 89 AB CD

MixColumns:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}\begin{pmatrix} 77 \\ 89 \\ AB \\ CD \end{pmatrix}=\begin{pmatrix} 02\cdot 77\oplus 03\cdot 89\oplus 01\cdot AB\oplus 01\cdot CD \\ 01\cdot 77\oplus 02\cdot 89\oplus 03\cdot AB\oplus 01\cdot CD \\ 01\cdot 77\oplus 01\cdot 89\oplus 02\cdot AB\oplus 03\cdot CD \\ 03\cdot 77\oplus 01\cdot 89\oplus 01\cdot AB\oplus 02\cdot CD \end{pmatrix}=\begin{pmatrix} EE\oplus 80\oplus AB\oplus CD \\ 77\oplus 09\oplus E6\oplus CD \\ 77\oplus 89\oplus 4D\oplus 4C \\ 99\oplus 89\oplus AB\oplus 81 \end{pmatrix}$$

$$=\begin{pmatrix} 08 \\ 55 \\ FF \\ 3A \end{pmatrix}$$

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(2^4) with m(x) = x^4+x+1

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	0000	0
$g^0(=g^{15})$	1	0001	1
g^1	g	0010	2
g^2	g^2	0100	4
g^3	g^3	1000	8
g^4	g+1	0011	3
g^5	g^2+g	0110	6
g^6	g^3+ g^2	1100	12
g^7	g^3+g+1	1011	11
g^8	g^2+1	0101	5
g^9	g^3+g	1010	10
g^{10}	g^2+g+1	0111	7
g^{11}	g^3+ g^2+g	1110	14
g^{12}	g^3+ g^2+g+1	1111	15
g^{13}	g^3 +g^2+1	1101	13
g^{14}	g^3+1	1001	9

4. Determine the gcd of the following pair of polynomials

(a) x^3+x+1 and x^2+x+1 over GF(2)

$$\begin{array}{r} x+1 \\ x^2+x+1 \overline{)x^3+x+1} \\ \underline{x^3+x^2+x} \\ x^2+1 \\ \underline{x^2+x+1} \\ x \end{array} \qquad \begin{array}{r} x+1 \\ x \overline{)x^2+x+1} \\ \underline{x^2} \\ x+1 \\ \underline{x} \\ 1 \end{array} \qquad \begin{array}{r} x \\ 1 \overline{)x} \\ \underline{x} \\ 0 \end{array} \qquad \begin{array}{r} x \\ 1 \overline{)x} \\ \underline{x} \\ 0 \end{array}$$

Thus the GCD is 1.

(b) x^3-x+1 and x^2+1 over GF(3)

$$\begin{array}{r} x \\ x^2+1 \overline{)x^3-x+1} \\ \underline{x^3+x} \\ 1 \end{array} \qquad \begin{array}{r} x^2 \\ 1 \overline{)x^2+1} \\ \underline{x^2} \\ 1 \end{array} \qquad \begin{array}{r} 1 \\ 1 \overline{)1} \\ \underline{1} \\ 0 \end{array}$$

Thus the GCD is 1.

(c) $x^5+x^4+x^3-x+1$ and x^2+x+1 over GF(2)

$$\begin{array}{r} x^2 \\ x^3+x^2+x+1 \overline{)x^5+x^4+x^3-x^2-x+1} \\ \underline{x^5+x^4+x^3+x^2} \\ x+1 \end{array} \qquad \begin{array}{r} x^2+1 \\ x+1 \overline{)x^3+x^2+x+1} \\ \underline{x^3+x^2} \\ x+1 \\ \underline{x+1} \\ 0 \end{array}$$

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.