INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Homework 4 *October 7th, 2016*

1. SUBBYTES

The S-box of AES can be constructed in the following fashion:

1. Initialize the S-box with the byte values in ascending sequence row by row. The first row contains $00, 01, 02, \ldots, 0F$; the second row contains $10, 11, \ldots\ldots, 1F$, and so on.
2. Map each byte in the S-box to its multiplicative inverse in the finite field $GF(2^8)$; the value 00 is mapped to itself.
3. Consider that each byte in the S-box consists of 8 bits labeled $(b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0)$. Apply the following transformation to each bit of each byte in the S-box:

$$b_i' = b_i \oplus b_{(i+4) \text{ mód } 8} \oplus b_{(i+5) \text{ mód } 8} \oplus b_{(i+6) \text{ mód } 8} \oplus b_{(i+7) \text{ mód } 8} \oplus c_i$$

where c_i is the i-th bit of byte c with the value 63; that is, $(c_7c_6c_5c_4c_3c_2c_1c_0) = (01100011)$. The prime (') indicates that the variable is to be updated by the value on the right. The AES standard depicts this transformation in matrix form as follows:

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Explain why this method is equivalent to make the calculations studied in class. You must work and write a brief report. For this purpose you must work with your team. **The report must be sent before October 17th (Monday) before midday** in a pdf named starting with the name of your team, followed by the suffix subbytes.

2. Exercises

Solve the following exercises as a part of your training, please do not send solutions to me. However if you have any question about them, please come to see me during office hours.

2.1. Irreducible polynomials

1. Determine which of the following polynomials are reducible over GF(2).

   a) $x^3 + 1$

   b) $x^3 + x^2 + 1$

   c) $x^4 + 1$

2. Given the irreducible polynomial $1+x+x^7$, which finite field we can construct using it? How many elements does this field have?

3. Using the polynomial $1 + x + x^2$, construct a finite field. How many elements does this field have? Give the table to add and to multiply in this field.

2.2. Multiplicative Inverses

Find the multiplicative inverse for each of the following elements, considering the irreducible polynomial in each case.

1. $m(x) = x^5 + x^2 + 1$

   a) $x + 1$

   b) $x^2 + x + 1$

   c) $x^3 + x^2 + 1$

   d) x^4

   e) $x^3 + 1$

2. $m(x) = x^8 + x^4 + x^3 + x + 1$

   a) $x + 1$

   b) x^7

c) $x^5 + x^4 + 1$

d) $x^6 + x + 1$

e) $x^5 + x^4 + x^3 + x^2 + x + 1$

3. $m(x) = x^4 + x + 1$

a) x

b) x^2

c) $x^3 + 1$

d) $x^4 + x^2 + 1$

e) $x^4 + x^4 + x^3 + x^2 + x + 1$