INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 6: Mixcolumn *October 18th, 2016*

In this session we will continue working with the block cipher AES, in particular with the operation MixColumn.

1. Programming exercises for here

The exercises of this section must be done in teams of 2 students. At the end of this session, you must send your code in a single compressed file, the name of this file will begin with the last name of one student followed by the sufix lab6_section1. For example DiazSantiago_lab6_section1.zip

1. Implement in your favorite programming language multiplication over finite field $GF(2^8)$, using the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$, as we explained it in class.
2. Use the code of the previous point to generate the Mixcolumn table that we saw in the previous class, by multiplying each element in $GF(2^8)$ by the polynomial used for the operation MixColumn $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.
3. Now generate the table InvMixColumn multiplying each element in the field $GF(2^8)$ by the polynomial $b(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$.
4. Implement a function in your favorite programming language to prove that

$$a(x) * b(x) \bmod (x^4 + 1) = 1$$

1.1. Products

You must write a report, containing:

1. Your personal information, date of the lab session and the topic that we are studying in this lab session.
2. **Only the most important functions** of your source code, explaining what they do.
3. Print screens showing how your programs work.

You must send by email your report and your source code already improved in a compressed file. The filename of this file must have a name that starts with the last name of one of the members of the team, followed by his/her name, and the suffix: _lab6_report. For example: DiazSantiago_lab6_report. The deadline for sending this is **October 24th (Monday) at midday**.