INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 5: AES *October 11th, 2016*

In this session we will work with the block cipher, that actually is the standard: Advanced Encryption Standard (AES).

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 lab5_section1. For example DiazSantiago_lab5_section1.zip

1. Extract from the code that implements AES, the key schedule algorithm. Generate random keys of different sizes (128, 192, 256 bits), k and using the key schedule algorithm, generate the 10,12,14 subkeys, The key k and the subkeys $k_1, \ldots k_{16}$ must be stored in a file, represented in hexadecimal (**not as a binary string**). The filename must be given by the user.

2. Binary fields

2.1. Theory

1. Write down the most important biographical data about Evariste Galois.
2. Write down in your own words a summary about the history of Rijndael and AES.

Please include your source of information for this section.

2.2. Programming Exercises

1. Analize the following algorithm, where m is an irreducible polyonomial of degree t, and $a \in GF(2^t)$. $\deg(u)$ indicates de degree of the polynomial u. Explain how it works and what is the output of this algorithm.

Algorithm(a, m)

1. $u \leftarrow a; v \leftarrow m$
2. $g_1 \leftarrow 1, g_2 \leftarrow 0;$
3. **while** $u \neq 1$ **do**

3.1. $j \leftarrow \deg(u)\text{-}\deg(v)$

3.2. if $j < 0$ then $u \leftrightarrow v, g_1 \leftrightarrow g_2, j \leftarrow -j;$

3.3 $u \leftarrow u + x^j v;$

3.4 $g_1 \leftarrow g_1 + x^j g_2;$

3. return (g_1)

2. Implement the previous algorithm, assume that the inputs are given as hexadecimal values. Prove your program with different binary fields.

3. Implement modes of operation CBC and CTR using the code that implements AES. Your program must offer 3 options:

   a) Key generation: In this case you will need 3 keys, store these keys in a file. The filename must be chosen by the user.

   b) Selection of operation mode.

   c) Encryption: Here the user must choose the key file, the file containing the plaintext and the filename that will store the ciphertext.

   d) Decryption: Here the user must choose the key file, the file containing the ciphertext and the filename that will store the plaintext.

   e) Selection of operation mode.

2.3. 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. The answers for Section 2.1. Here give your source of information (webpage, book, or paper).

3. **Only the most important functions** of your source code, explaining what they do. Here you must include code for **Section 1 and Section 2.2**.

4. Print screens showing how your programs work for **Section 1 and Section 2.2**.

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: _lab5_report. For example: DiazSantiago_lab5_report. The deadline for sending this is **October 17th (Monday) at midday**.
In this ocassion we will check your programs, in our next session: October 18th