INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Introduction to Cryptography

Lab 05. AES key expansion *May 3, 2024*

1. Understanding the algorithm for key expansion

Please do the following exercise in groups of 2 or 3 students. Write down the solution in your notebook or tablet and upload to Teams before this session ends

The following algorithm takes a key K of 128 bits for AES and expands it to obtain 10 key rounds. It incorporates the following operations: ROTWORD(B_0, B_1, B_2, B_3) performs a cyclic shift of the four bytes B_0, B_1, B_2, B_3, i.e.

$$\text{ROTWORD}(B_0, B_1, B_2, B_3) = B_1, B_2, B_3, B_0,$$

SUBWORD(B_0, B_1, B_2, B_3) applies S-box to each of the four bytes B_0, B_1, B_2, B_3, i.e.

$$\text{SUBWORD}(B_0, B_1, B_2, B_3) = B'_0, B'_1, B'_2, B'_3$$

Rcon is an array of 10 words. These are constants in hexadecimal notation

Algorithm 3.6: KEYEXPANSION(key)

external ROTWORD, SUBWORD
$RCon[1] \leftarrow$ 01000000
$RCon[2] \leftarrow$ 02000000
$RCon[3] \leftarrow$ 04000000
$RCon[4] \leftarrow$ 08000000
$RCon[5] \leftarrow$ 10000000
$RCon[6] \leftarrow$ 20000000
$RCon[7] \leftarrow$ 40000000
$RCon[8] \leftarrow$ 80000000
$RCon[9] \leftarrow$ 1B000000
$RCon[10] \leftarrow$ 36000000
for $i \leftarrow 0$ **to** 3
  do $w[i] \leftarrow (key[4i], key[4i+1], key[4i+2], key[4i+3])$
for $i \leftarrow 4$ **to** 43
  do
  $temp \leftarrow w[i-1]$
  if $i \equiv 0 \pmod 4$
    then $temp \leftarrow$ SUBWORD(ROTWORD($temp$)) $\oplus$ $RCon[i/4]$
  $w[i] \leftarrow w[i-4] \oplus temp$
return $(w[0], \ldots, w[43])$

Using Algorithm 3.6 (shown above), generate the subkey for the first round if the key in hexadecimal notation is 00000000 $F0F0F0F0$ $0F0F0F0F$ 01010101.

2. Programming exercises

Please do the following exercises by your own. Choose ONLY ONE of the following programming languages TO DO ALL THE EXERCISES: C, C++ or Python.

1. Design a program that implements the algorithm 3.6. Your program must receive a key with 32 hexadecimal digits, and must store in text file the array w. Please print in each row four values of w. For example in the first row you must write $w[0], w[1], \ldots w[3]$ in the second row $w[4], w[5], \ldots w[7]$ and so on. The values of w must be write in the file in hexadecimal notation.

2. Test your program with at least 10 different AES keys of 128 bits.

3. Report

Every student must write her/his own document to present the programming exercise. **It is mandatory** that your document fulfill the following:

- You can use English or Spanish to write it, but pay attention to spelling.
- Include your full name, number and title of the lab session, date.
- The source code you wrote to implement algorithm 3.6 and a brief explanation of the changes that you did to the algorithm
- Screen shots of your program running.
- Content of the output file for one key.