INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 3: Finite fields *March 23, 2020*

In this session we will work with finite fields. Please do the following programming exercises on your own. Use only one programming language (C/C++, Java, Python). It is recommended that you try to solve the exercises on your own. You can discuss the solution to the exercises with your colleagues but you should not copy source code. If copying is detected, that may immediately lead to a grade less than 6.

1. Programming Exercises

1. Design a function that receives $3 \leq n \leq 8$, for $GF(2^n)$ and as outputs the multiplication table. Consider the following requirements.
   a) The user can choose to represent each element in $GF(2^n)$ as a polynomial or as an hexadecimal number.
   b) The output must be stored in a file.
2. Implement the key schedule for AES, considering a key size of 128 bits. Your program must receive the key in hexadecimal and must store the 10 subkeys (derived from the key) in a file.
3. Repeat the previous point, but now for a key size of 192 bits.

2. Products

The deadline to do the following is March 30.

- 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 most important parts of your source code, explaining what they do.

3. Include screen capture of your programs showing how they work.
4. For the key schedule, include a pseudocode (you can get it from a book) and your source code.
5. **Please write a small user manual to know how to run your programs.**

You must submit your report to classroom.

- To evaluate your programs, you must upload to the folder in google drive (previously created) a zip file with the source code of your programs. The name of the file must be your last name and the suffix lab03_Crypto . For example if Laura Escobar Tellez, must name her file as EscobarTellez_lab03_Crypto.zip