CIIC5018 / ICOM5018
Network Security and Cryptography

Project 4 – GF(2^8) operations for AES

Overview

In this project, you will design and implement python codes to illustrate different aspects of AES, including the basic operations on GF(2^8) and the generation of S-Box and Inverse S-Box.

Design Requirements

- You **must** implement all functions by using pure Python. That is, you cannot use GF operations and AES functions defined in existing packages.
- In the GF(2^8) for AES, the polynomial modulo is $m(x)=x^8+x^4+x^3+x+1$.

Document requirements

To work on the project, you will need to prepare **three** documents following the guidelines below.

1. A design document
    a. Cover page
        i. It shall include the title of the document, student name, student ID, department and university information, etc.
    b. Table of content
    c. Section 1: The design of operations on GF(2^8)
        i. Addition of two numbers
            1. Input: two 8-bit integers
            2. Return: one 8-bit integers
        ii. Multiplication of two numbers
            1. Input: two 8-bit integers
            2. Return: one 8-bit integers
        iii. Inverse of a number
            1. Input: one 8-bit integers
            2. Return: one 8-bit integers
        iv. Tester for demonstration
    d. Section 2: The Generation of S-Box and InvS-Box
        i. A function to generate S-Box
        ii. A function to generate InvS-Box
    e. References
        i. Cite at least 5 references
        ii. Including a link to your YouTube video.
2. A Python notebook
    a. Implements of all functions mentioned above

   b. Some testing procedures
      i. Testing the GF(2^8) operations
         1. Adding every number and itself shall be 0
         2. Multiplying every number and its inverse shall be 1
         3. The inverse's inverse of every non-zero number shall be itself
      ii. Testing the S-Box and InvS-Box generation
         1. Your code must generate the same boxes on page 13 and page 14 in the slides
3. A YouTube video
   a. You shall record a video and upload it to YouTube
      i. Set the video to private
      ii. Share the video to me at Kejie.lu@upr.edu
   b. In the video, you shall explain all functions you implemented and verify the correctness of your code.

Submission

Submit a single zip file that includes:
1. the design document
2. the Jupyter notebook

Evaluation

1. Rubrics are used in the evaluation.
2. You must carefully review all rubrics before preparing for the documents.