CIIC5018 / ICOM5018
Network Security and Cryptography

Project 5 – AES Implementation

Overview

In this project, you will design and implement Python codes to illustrate different aspects of AES, including the four functions in AES (SubByte, ShiftRows, MixColumns, AddRoundKey), and the key expansion function.

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), the polynomial modulo is $m(x)=x^8+x^4+x^3+x+1$.
- AES key size is 128 bits.

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 AES functions
        i. A function to convert a sequence of 16 bytes to a 4x4 square
        ii. A function to convert a 4x4 square to a sequence of 16 bytes
        iii. A function to print the current state
        iv. SubByte
            1. Input: state
            2. Return: state
        v. InvSubByte
            1. Input: state
            2. Return: state
        vi. ShiftRows
            1. Input: state
            2. Return: state
        vii. InvShiftRows
            1. Input: state
            2. Return: state
        viii. MixColumns
            1. Input: state

2. Return: state
ix. InvMixColumns
1. Input: state
2. Return: state
x. AddRoundKey
1. Input: state, expansion key
2. Return: state
d. Section 2: The design of AES key expansion
i. Input: 16 bytes key
ii. Output: an array of 11 expand keys
e. Section 3: The design of AES encryption
i. Input: 16 bytes plaintext, 16 bytes key
ii. Output: 16 bytes cyphertext
f. Section 4: The design of AES decryption
i. Input: 16 bytes cyphertext, 16 bytes key
ii. Output: 16 bytes plaintext
g. References
i. 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 Key expansion
1. Given the input key on page 26, your code must generate the same expansion keys
ii. AES encryption and decryption
1. Given the input and key on page 27, your code must generate the same states
2. Given the cyphertext and key on page 27, your code must generate the same states
iii. The avalanche effects
1. Do the experiments on page 28, and the results shall be the same as those on page 28
2. Do the experiments on page 29, and the results shall be the same as those on page 29
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

You shall submit a zip file that includes the design document, and the Jupyter notebook.

Evaluation

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