Midterm Project
Cryptography
ECE:5995 - Spring 2020

Introduction

For this midterm project, you are to implement a subset of the US Government's Advanced Encryption Standard (AES). Specifically, you should implement AES for the 128-bit key size. For your implementation, you may use any language you prefer (python, C(++), C#, Ruby, etc.), but you may not use any high-level functions (APIs, libraries, modules, etc.) that support development of an AES implementation. The spirit of this requirement is that you should implement all of the required structure to build the AES primitive by yourself. Standard libraries are acceptable for use.

AES is formally defined in the FIPS 197 document from NIST available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. Further, there is an excellent discussion of the required implementation details for AES in our text, chapter 4. In your project final report, you should include these two references, as well as any others you used to help you complete the project.

Deliverables

1. In Appendix C, the FIPS 197 document provides several encryption/decryption examples in order to verify a particular implementation of AES is working correctly. For AES-128 specifically, section C.1 gives the complete state of the AES cipher during the encryption and decryption processes. Your final submission should verify that your implementation exhibits the same state.

2. A second decryption should be performed using the following key/ciphertext pair.

```
Key:        30 31 32 33  34 35 36 37  38 39 3A 3B  3C 3D 3E 3F
Ciphertext: F4 35 15 03  AA 78 1C 52  02 67 D6 90  C4 2D 1F 43
```

   Your final submission should contain the cipher state for the decryption process, as well as the plaintext you obtained from the decryption.

3. Your final submission should contain a brief discussion of your implementation, instructions for compiling your source code, the source code itself (links to e.g. github repositories are fine), and items 1 and 2 above. Discussion should be limited to four pages.

Timeline

This midterm project will be distributed in class on February 27, 2020. It will be due Thursday, March 26, 2020. In addition to time outside of class, you will be given the class periods of March 11 and 13 to work on the project. No class attendance is required or expected, nor will any lectures be given, on these two days.

Groups

You may choose to work by yourself or in a group of two people to complete the project. All projects will be graded to the same standard, regardless of whether the group contains one or two people.