

# Crypto Lab

The development of this document is funded by the National Science Foundation's Course, Curriculum, and Laboratory Improvement (CCLI) program under Award No. 0618680 and 0231122. Permission is granted to copy, distribute and/or modify this document.

## 1 Overview

The learning objective of this lab is for students to get familiar with encryption, one-way hash function, and Message Authentication Code (MAC).

## 2 Lab Tasks

### 2.1 AES Tool

You need to implement an encryption and decryption tool using the provided AES algorithm (a 128-bit block cipher). AES's key size can be 128 bits, 192 bits, or 256 bits. Your tool should be able to support all these three options. The code given in `aes.c` is for encrypting/decrypting one block (i.e. 128 bits); if we need to encrypt/decrypt data that are more than one block, we need to use a specific AES mode, such as ECB (Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher Feedback), etc. In this lab, you need to implement both CBC and CFB for AES (i.e. AES-CBC and AES-CFB). Since both modes require an Initial Vector (IV), you need to store IV at the beginning of the ciphertext.

AES-CBC requires that data must be encrypted as data chunk with 16 bytes unit. If the data is not multiple of 16, we need to pad the data, and save how many octets we have padded. Decryption needs this length to restore the original data after decryption. Does AES-CFB need padding too? Can AES-CFB be used as a stream cipher?

### 2.2 HMAC Tool

You need to implement a tool to generate Message Authentication Code (MAC) for a file. A family of MAC algorithms is called HMAC (Hashed MAC), which is built on one-way hash functions. A specific HMAC algorithm is called HMAC-XYZ if the underlying hash function is XYZ. In this lab, your tool should use HMAC-SHA-256. The implementation of hash algorithm SHA-256 is given to you; you need to use it to implement HMAC-SHA-256. To help you, we provide an implementation of HMAC-MD5, which is quite similar to HMAC-SHA-256.

## 3 Submission and Demonstration

Please submit a hardcopy of your code, along with the outcome of the followings:

- Use the string "1234567890123456" as the key to encrypt this pdf file, and print out the hexadecimal values of the first 200 bytes of the ciphertext. Please use all 0s as your IV. You should do this with both AES-CBC and AES-CFB.
- Use the string "1234567890123456" as the key to generate a MAC for this pdf file.
- Corrupt any bit in the cipher text, and observe how many blocks can be correctly decrypted.