AES and Encryption Modes

CIS-4040 Homework #3

Peter C. Chapin, Vermont Technical College

Copyright © 2017 Peter C. Chapin

Due: Monday, June 19, 2017

This assignment covers AES and encryption modes. In the text Chapter 6 covers AES. There is a fair amount of mathematical material in the chapter, and also in Chapter 5, that we are going to skip. However, that material is worth looking over if you feel inclined (we may talk about some of it later). Chapter 6 has a section on Double-DES and Triple-DES that are worth looking at also, but I'm mostly concerned with the sections 7.2 through 7.7 on modes of operation.

1. Suppose AES is given a plaintext block of `0x0101020304050607080 90A0B0C0D0E0F` and the key of `0x01010101010101010101010101010100`. Notice that these values different from the sample on the class web site [http://www.pchapin.org/VTC/cis-4040/AES-action.txt] by one bit in the plaintext and one bit in the key. Show the results of each step in the first round of the algorithm. That is, show the state matrix initially, after the first `AddRoundKey`, and then after `SubstituteBytes`, `ShiftRows`, `MixColumns`, and the `AddRoundKey` at the end of Round #1. You will also need to show one step of key expansion.

   Note that a Windows executable of the MixColumns program I demonstrated in class can be found here [http://www.pchapin.org/VTC/cis-4040/MixColumns.exe].

2. Read about Output Feedback Mode (OFB) in the text. Does it allow easy random access to the data? What are its error propagation characteristics? OFB mode has a security concern. What is it? HINT: What can an attacker who can modify the cipher text do?

3. Read about "Tweakable Block Ciphers" in the text on page 192. Describe in your own words what they are and what advantage they have. Note that a hash function outputs a value such that it is computationally infeasible to determine the input given the output.

4. Do Problem 7.11 in the text (on ciphertext stealing). The problem is on page 229.