CPSC4160 APPLIED CRYPTOGRAPHY Spring 2018  
**Programming Assignment 3**

## Modes of Operation with AES

## Objective

The objective of this lab is to explore the different modes of operation of block ciphers by implementing 5 of the modes.

## Task

Write a program that encrypts a given plaintext file with the given key. The program gets the name of the file that contains the key, name of the file that contains the plaintext, and a prefix for the names of the file containing the ciphertexts from the command line. The program will encrypt the plaintext file in the 5 modes below using 128-bit AES and produce a file for each mode below. You can use the AES implementation that was provided in the previous assignment.

1. EBC
2. CBC
3. OFB
4. CFB (128-bit)
5. CTR (counter starts with 0)

After producing the 5 ciphertext files, the program will decrypt these files and store the decrypted texts in 5 separate files. NoteCBC,OFB, and CFB modes require an initialization vector (IV). Use the [SecureRandom class](https://docs.oracle.com/javase/7/docs/api/java/security/SecureRandom.html) in Java to generate the IVs. Note that you need to keep these IVs for decryptions in modes CBC, CFB, and OFB.

So, if the program is run by

encrypt key.txt plain.txt cipher

then the program will produce 10 files :

cipherECB.txt

cipherCBC.txt

cipherOFB.txt

cipherCFB.txt

cipherCTR.txt

cipherECBdec.txt

cipherCBCdec.txt

cipherOFBdec.txt

cipherCFBdec.txt

cipherCTRdec.txt.

Note that at the end of a successful run, the files cipherECBdec.txt, cipherCBCdec.txt, cipherOFBdec.txt, cipherCFBdec.txt, cipherCTRdec.txt will all contain the same data which will be the pliantext that you started with. The plaintext will be given in hexadecimal one block per line. You can assume that each line will have 32 hex digits (hence you will NOT need to do any padding.)

**What to submit:**

1. Your documented source code. DO NOT include key, plaintext, or ciphertext files, just the source code

|  |
| --- |
| REMINDER ABOUT ACADEMIC INTEGRITY  Any work turned in for individual credit must be entirely the work of the student submitting the work (unless it is a sanctioned pair or group effort). All work must be your own. You may share ideas but submitting identical assignments (for example) will be considered cheating. You may discuss the material in the course and help one another with debugging, however, I expect any work you hand in for a grade to be your own. A simple way to avoid inadvertent plagiarism is to talk about the assignments, but don't read each other's work or write solutions together. Having access to another person’s work on the system or giving access to your work to another person is not allowed. It is your responsibility to keep your work confidential.  No cheating in any form will be tolerated. Please be aware that anyone caught cheating or plagiarizing in this class will receive a “0” for the assignment/exam and may receive a “0” for the course. |