Spring 2023 - ICSI 526
Homework 2

Jacob Clouse

March 10, 2023

1 Running CBC and OFB modes, Calculating the IOC

There are two separate AES files included: One contains my code for CBC mode and the other contains my code for OFB mode. I couldn't get them to work together inside of the same file so I had to split them out into different programs. NOTE: This program was mainly coded on a Linux Mint machine using BASH to compile and Git/Github to host my code (using a private git repo).

How to Compile and Run CBC Mode:

1. Make sure you have a working copy of the Java JDK and a text editor on your machine (I use VS Code because of the built in terminal).
2. Make a copy of the **CBC** folder I have provided and cd into it with your terminal. The ONLY two items you should have inside are the **AES.java** and **AES_Demo.java** files (the demo is required to run this program).
3. You can compile the program by using the syntax:

   ```
   javac AES_Demo.java AES.java
   ```

   This should create a several class files within the **CBC** folder, including a AES_Demo.class file.
4.

Mode	% Dup	IOC
ECB	0%	0.01995247623811906
	25%	0.024443221610805404
	50%	0.03179889944972486
CBC	0%	0.003902951475737869
	25%	0.003873936968484242
	50%	0.003944972486243122
OFB	0%	0.00392896448224112
	25%	0.00386443221610805 4
	50%	0.00392196098049 0245

Problem 1 can be efficiently solved by ...