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 sure you have x3 test files of 2000 characters each (with 0%, 25% and 50% duplication respectively).
3. 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).
4. 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.
5. Now you can run this file using the syntax:

   ```
   java AES_Demo
   ```

   If successful, a window should pop up titled **Jacob Clouse CBC Demo:** that will allow you to select your sample data files.
6. You can use the *Browse Files* button and navigate to the first test file on your computer. **DO NOT** select either 'Preserve Image Header' or 'Reduced AES - 4 rounds'.
7. You can select where you want the encrypted output file to go using the **Choose Save Directory** button. **NOTE:** On linux, I have noticed that the output file sometimes will be stored in the parent directory of the folder you initially selected.
8. Finally, you can click Begin AES and it will encrypt your file (there is no decryption in this file, so the 'Encryption Time' and 'Decryption Time' fields may be blank). You now have your encrypted output and you repeat the process to encrypt other files as you please.

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 ...