CS 5158/6058 Data Security and Privacy, Fall 2019

Name: Anish Ghantasala M#13518394

Step 1: Directory Strcuture: AES,RemoteSystemTempFiles

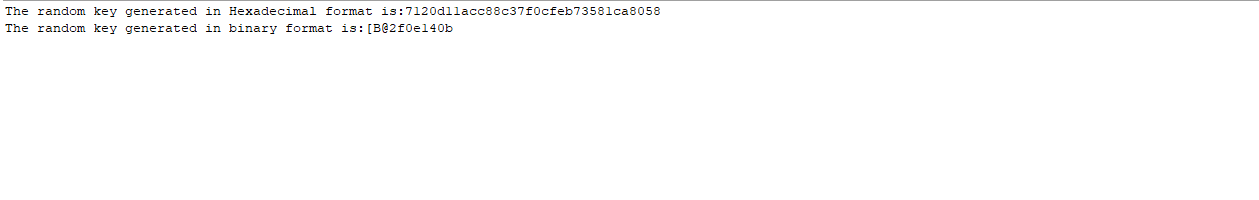
In AES, the directory strcture is src,bin and classpath.

The operating system used is Windows 10 and the IDE used is Eclipse Kepler.

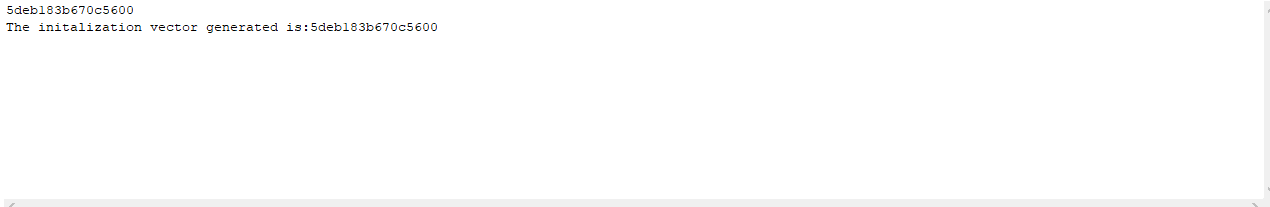
Step 2: There are three class files: **EncryptDecrypt.java**, **RandomIV.java**, **RandomKeyGen.java**

Step 3: Since I need to import various Executable JAR files from bouncy castle, I added them into the eclipse project.

Step 4: Generate a random Key and store it in the file **randombytes.txt** using the class RandomKeyGen.java

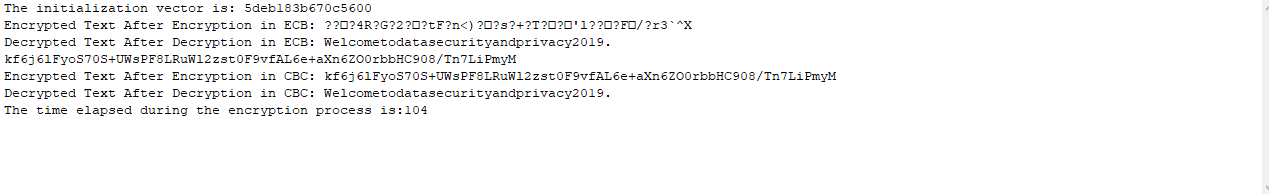
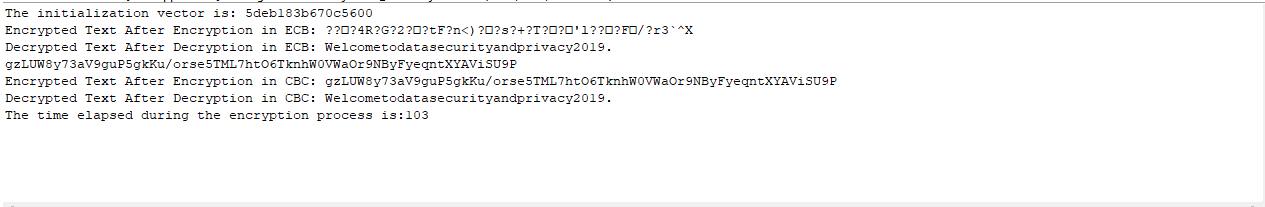
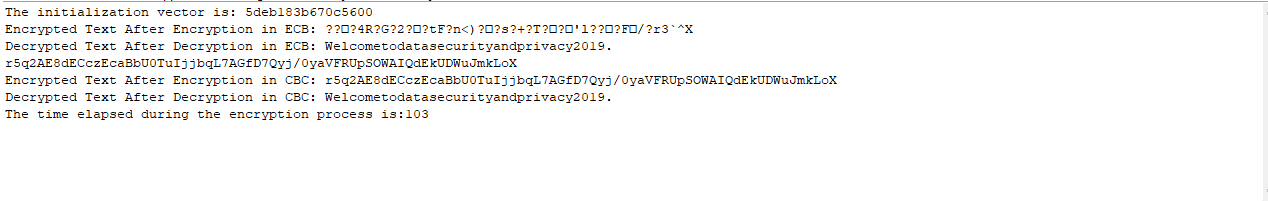
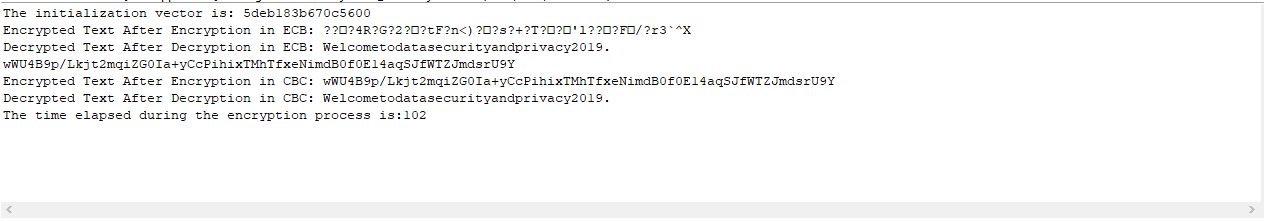
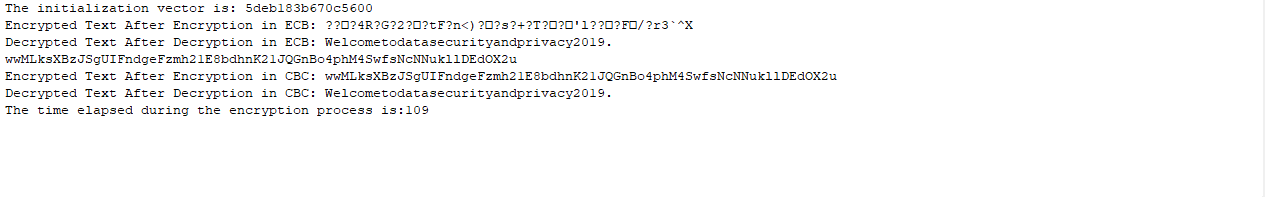


Step 5: Generate a initial vector and store it in the file randomiv1.txt using the class **randomIV.java** (optional)



Step 6: Execute the class **EncryptDecrypt.java** and using the Random Key and Initialization vector the cipher text is generated. The plaintext is loaded from the file named myfile.txt.

Run the program for 5 times.



Step 7: In the above examples, we can see that the cipher generated in CBC changes from one execution to another and in ECB, the cipher text does not change. The average running time of encryption is also given above.

Step 8: The average time is calculated using a function in milliseconds.

Step 8: The average running time of total encryption is an average of all the time elapsed can be calculated by taking the sum of all and dividing them by 5.

The **average running time**= (109+102+103+103+104)/5

= 104.2