INTRODUCTION TO CRYPTOGRAPHY – LAB 6

B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of performance: 23/02/2022

Aim: To code the AES algorithm (ECB and CBC Modes)

Code:

Language: C

Editor: Atom

Compiler: clang/ZSH

Package/Libraries used - https://github.com/kokke/tiny-AES-c

Codes – driver & library will be attached externally

Complete Output:

gcc -c -g aes.c => compiling the library to create object

gcc -c -g aes_driver.c => compiling the driver code to create object

gcc -o aes_driver aes_driver.o aes.o => linking the objects

./aes_driver => executing the code