

# 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

```
Lab6 - -zsh - 80x29
((base) anish@PotatoBook lab6 % gcc -c -g aes_driver.c
(base) anish@PotatoBook lab6 % gcc -o aes_driver aes_driver.o aes.o

((base) anish@PotatoBook lab6 % ./aes_driver

Testing AES128 - Anish Sudhan Nair

CBC encrypt: SUCCESS!
CBC decrypt: SUCCESS!
ECB decrypt: SUCCESS!
ECB encrypt: SUCCESS!
ECB encrypt verbose:

plain text:
6bc1bee22e409f96e93d7e117393172a
ae2d8a571e03ac9c9eb76fac45af8e51
30c81c46a35ce411e5fbc1191a0a52ef
f69f2445df4f9b17ad2b417be66c3710

key:
2b7e151628aed2a6abf7158809cf4f3c

ciphertext:
3ad77bb40d7a3660a89ecaf32466ef97
f5d3d58503b9699de785895a96fdbaa
43b1cd7f598ece23881b00e3ed030688
7b0c785e27e8ad3f8223207104725dd4

(base) anish@PotatoBook lab6 %
```