Operating System
Assignment 4
Encryption-Decryption Drivers

Kaustav Vats 2016048
Saksham Vohra 2016085

In the given problem statement, we need to implement an Encryption-Decryption modules, in which we need to take the input from the text file defined by the user and Encrypt the data by writing the data to the /dev/enc_dev/ folder, which is the driver module for Encryption. We first generate a unique random 16-byte string from <dev/urandom> header file and write it to the driver folder. We then read the key in the driver and then in the second read call, we read the encrypted message. We encrypt the message using the key provided, and the modify the key as the encrypted key and then use the new key to encrypt the message. At the end, we write an EOF character at the end of the file. We then write the encrypted message to the driver folder and read it in the user space. We then pass the key and the encrypted message to the decrypter where we use the key first to decode the first 128 bits and then use the encrypted message as the key for further decryption. We do so in block of 16 bytes.

Compilation:

For module compilation:

Make all

For installing:

Make install

For creating drivers:

Make mknod

INPUTS TO BE PROVIDED:

Input .txt file.

Expected output:

-Encrypted data

-Decrypted data

Error Values Handled:

- Data no sent to the user.
- Data not received from the user
- Cannot open device
- Cannot write to device
- Failed to read data from device