

Assignment 6 – Coding A Device Driver

Description:

This project aims to develop a device driver for Linux that enables users to encrypt messages using a Caesar cipher algorithm. The driver will be accompanied by a user-space program that facilitates interactions with the device. Device drivers are important for hardware communication, and this assignment will involve designing a driver with an application for loading and unloading. The driver will provide write and read encrypted message functionalities, making it a valuable addition to any security-conscious user's toolkit.

Approach:

1. I implemented a character device driver for Linux using the kernel's Device Model. The driver registers itself as a character device and provides file operations for opening, reading, writing, releasing, and handling ioctl commands.
2. I implemented a Caesar cipher encryption algorithm within the driver. This algorithm shifts characters in the message by a fixed amount to perform encryption.
3. I created a user-space program that interacts with the driver. This program opens the device file, writes a message to be encrypted, calls ioctl to encrypt the message, reads the encrypted message, and then manually decrypts it.
4. I tested the driver and user-space program by loading the driver into the kernel, interacting with the device, and verifying that messages were encrypted and decrypted correctly.
5. I provided comments throughout the code to explain its functionality and usage.

Additionally, I wrote a brief description of the project to provide context for the code.

Issues and Resolutions:

Issue: My first issue was encrypted message Same as decrypted message. After encrypting a message, the decrypted message was the same as the original message, indicating that encryption and decryption were not functioning correctly.

Resolution: I identified that the decryption algorithm was incorrectly implemented. Instead of using a fixed shift value of 23 for decryption, I modified the algorithm to use the opposite shift value of the encryption (in this case, 3) to correctly decrypt the message. After making this change, the encryption and decryption processes produced the expected results.

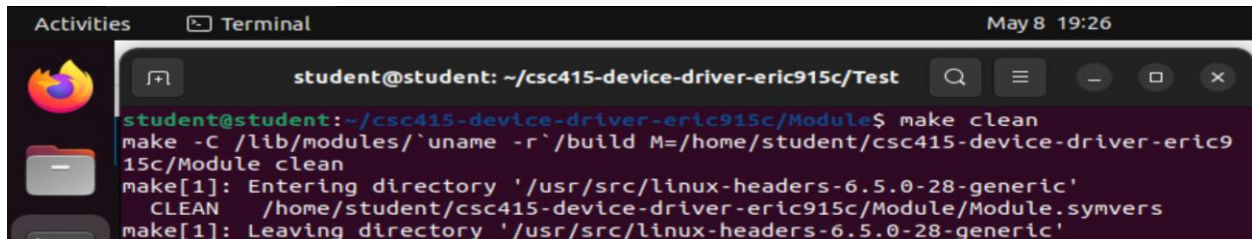
```
//handle ioctl commands function
static long deviceIoctl(struct file *file, unsigned int ioctl_num, unsigned long ioctl_param) {
    int shift = 3; //caesar cipher shift key

    switch (ioctl_num) {
        case 0: //Encrypt
            caesarEnCr(message, shift); //call encryption function
            break;
        case 1: //Decrypt
            caesarDecr(message, shift); //call decryption function
            break;
        default:
            printk(KERN_ALERT "Encryption driver: Invalid ioctl command\n");
            return -EINVAL; //return error for invalid command
    }

    printk(KERN_INFO "Encryption driver: Message processed\n"); // Log message processed
    return 0; //return success
}
```

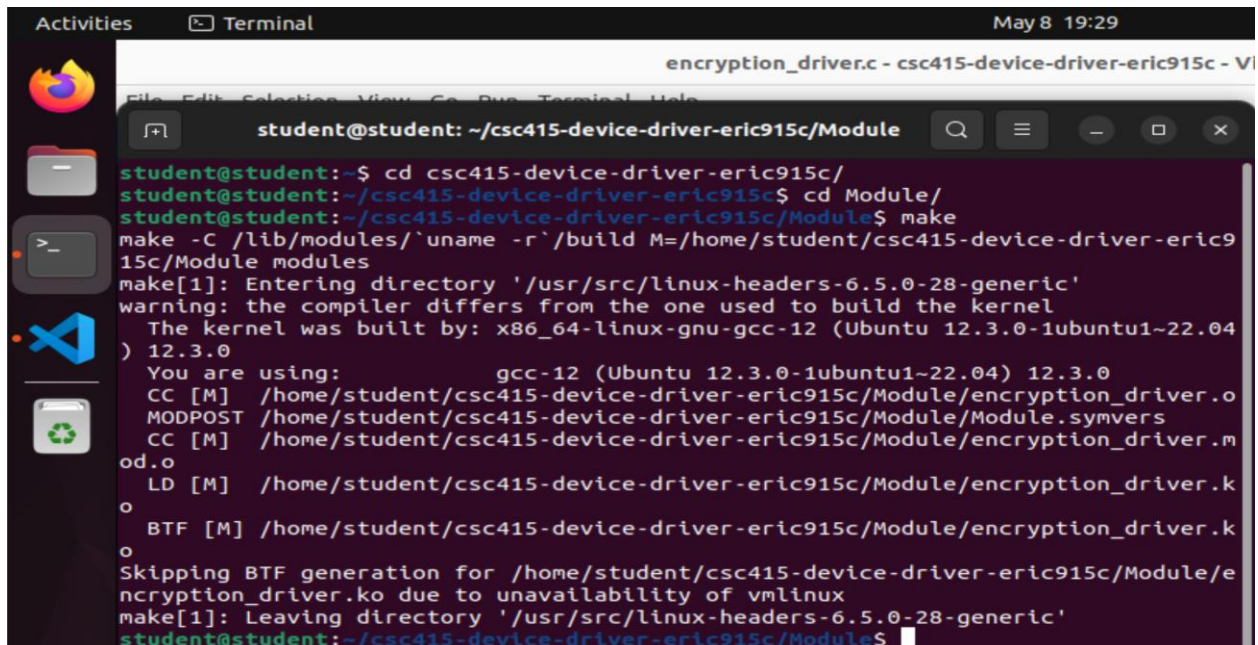
Building the Kernel Module:

Make clean



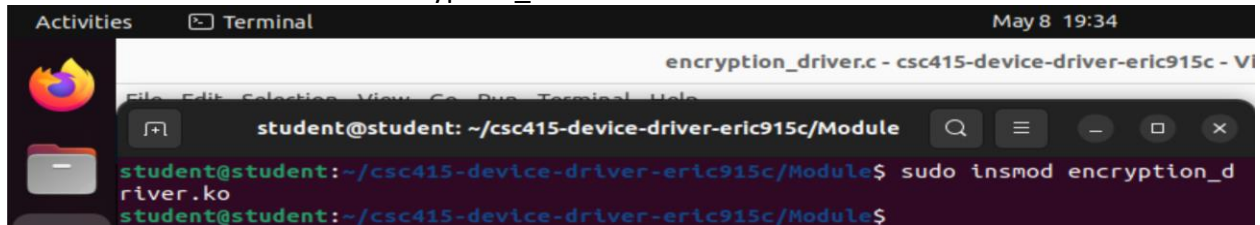
A terminal window titled 'student@student: ~/csc415-device-driver-eric915c/Test' showing the execution of 'make clean'. The output shows the command being run in the directory '/lib/modules/`uname -r`/build M=/home/student/csc415-device-driver-eric915c/Module', followed by 'make[1]: Entering directory \'/usr/src/linux-headers-6.5.0-28-generic\'', 'CLEAN /home/student/csc415-device-driver-eric915c/Module/Module.symvers', and 'make[1]: Leaving directory \'/usr/src/linux-headers-6.5.0-28-generic\''.

Run: make



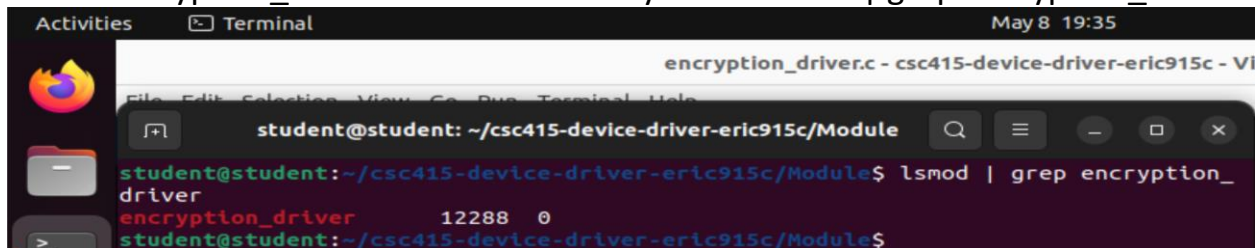
A terminal window titled 'student@student: ~/csc415-device-driver-eric915c/Module' showing the execution of 'make'. The output shows the command being run in the directory '/lib/modules/`uname -r`/build M=/home/student/csc415-device-driver-eric915c/Module', followed by 'make[1]: Entering directory \'/usr/src/linux-headers-6.5.0-28-generic\'', a warning about the compiler difference, the kernel version 'x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0', the compiler 'gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0', and the compilation of 'encryption_driver.o' and 'encryption_driver.ko'. The output also shows 'MODPOST /home/student/csc415-device-driver-eric915c/Module/Module.symvers', 'CC [M] /home/student/csc415-device-driver-eric915c/Module/encryption_driver.o', 'LD [M] /home/student/csc415-device-driver-eric915c/Module/encryption_driver.ko', 'BTF [M] /home/student/csc415-device-driver-eric915c/Module/encryption_driver.ko', 'Skipping BTF generation for /home/student/csc415-device-driver-eric915c/Module/encryption_driver.ko due to unavailability of vmlinux', and 'make[1]: Leaving directory \'/usr/src/linux-headers-6.5.0-28-generic\''.

Load Module : `sudo insmod encryption_driver.ko`



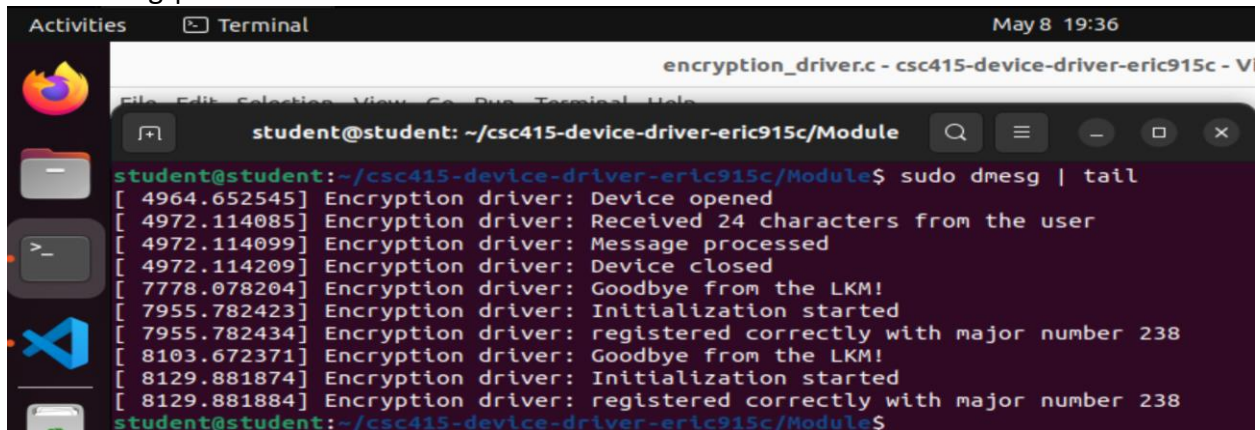
```
student@student: ~/csc415-device-driver-eric915c/Module
student@student:~/csc415-device-driver-eric915c/Module$ sudo insmod encryption_driver.ko
student@student:~/csc415-device-driver-eric915c/Module$
```

Check encryption_driver is loaded in the system : `lsmod | grep encryption_driver`



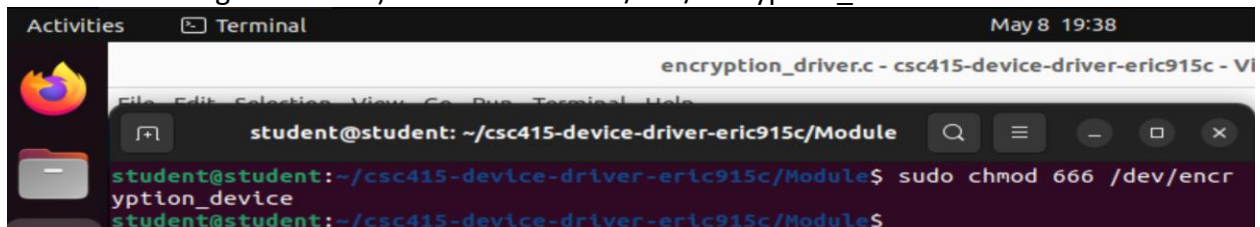
```
student@student:~/csc415-device-driver-eric915c/Module$ lsmod | grep encryption_driver
encryption_driver      12288  0
student@student:~/csc415-device-driver-eric915c/Module$
```

`sudo dmesg | tail`



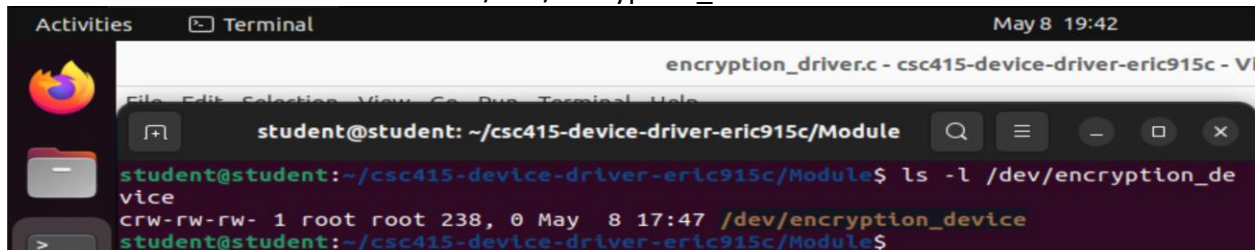
```
student@student:~/csc415-device-driver-eric915c/Module$ sudo dmesg | tail
[ 4964.652545] Encryption driver: Device opened
[ 4972.114085] Encryption driver: Received 24 characters from the user
[ 4972.114099] Encryption driver: Message processed
[ 4972.114209] Encryption driver: Device closed
[ 7778.078204] Encryption driver: Goodbye from the LKM!
[ 7955.782423] Encryption driver: Initialization started
[ 7955.782434] Encryption driver: registered correctly with major number 238
[ 8103.672371] Encryption driver: Goodbye from the LKM!
[ 8129.881874] Encryption driver: Initialization started
[ 8129.881884] Encryption driver: registered correctly with major number 238
student@student:~/csc415-device-driver-eric915c/Module$
```

(To set permissions for the `/dev/encryption_device` device, allowing all users to read and write, use the following command.): `sudo chmod 666 /dev/encryption_device`



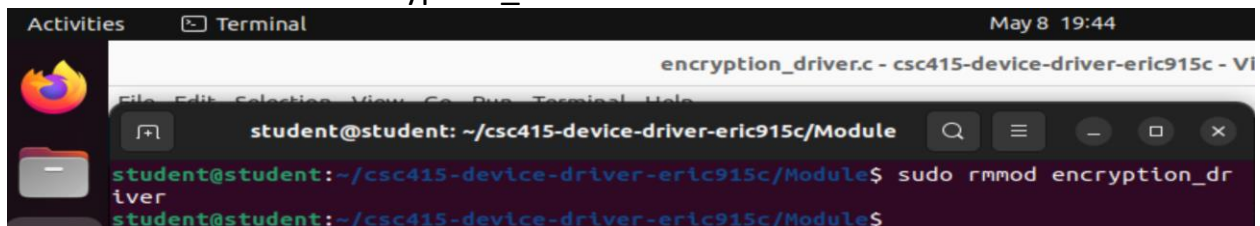
```
student@student:~/csc415-device-driver-eric915c/Module$ sudo chmod 666 /dev/encryption_device
student@student:~/csc415-device-driver-eric915c/Module$
```


Shows the detailed information: `ls -l /dev/encryption_device`



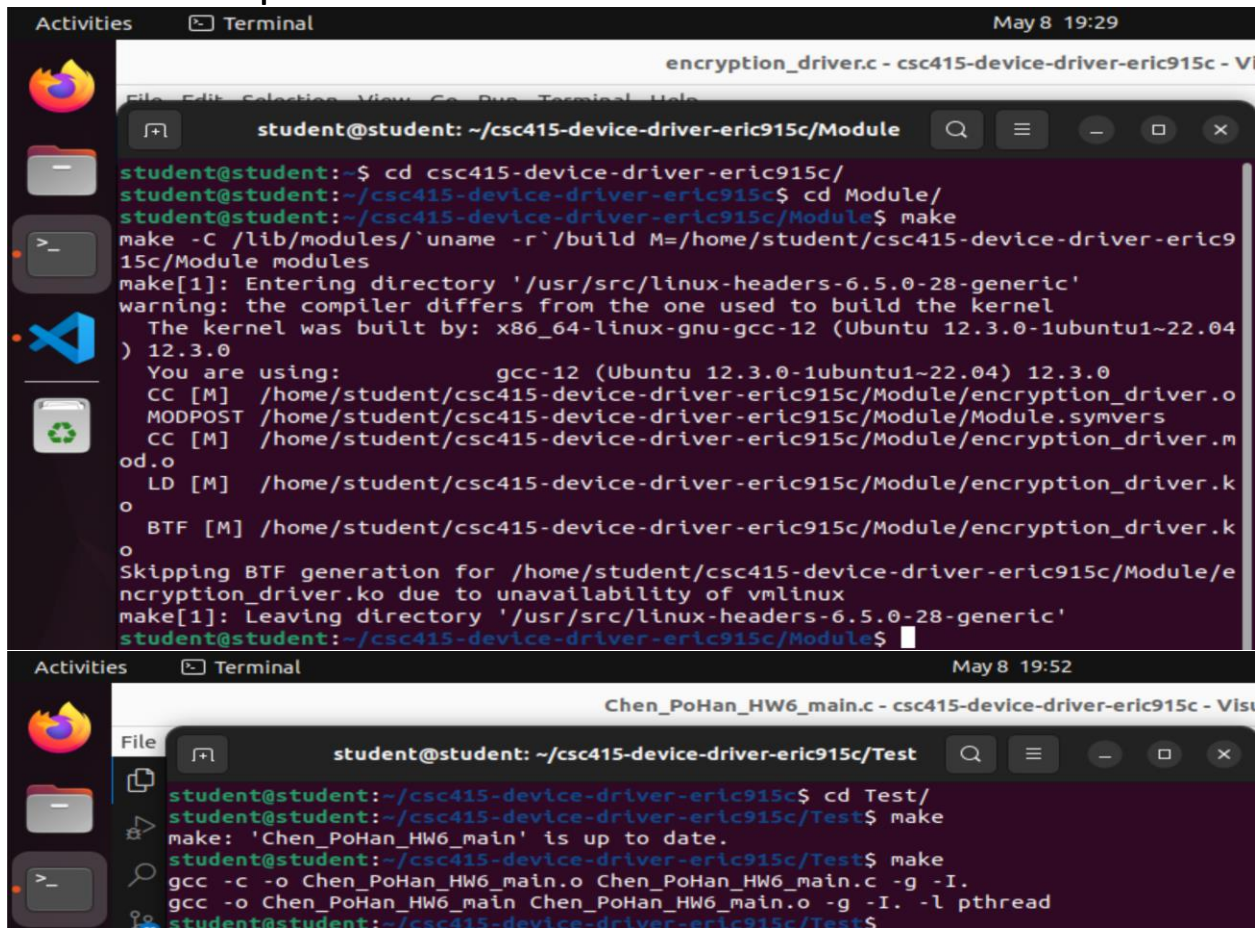
```
student@student: ~/csc415-device-driver-eric915c/Module
student@student:~/csc415-device-driver-eric915c/Module$ ls -l /dev/encryption_device
crw-rw-rw- 1 root root 238, 0 May  8 17:47 /dev/encryption_device
student@student:~/csc415-device-driver-eric915c/Module$
```

Unload: `sudo rmmod encryption_driver`



```
student@student: ~/csc415-device-driver-eric915c/Module
student@student:~/csc415-device-driver-eric915c/Module$ sudo rmmod encryption_driver
student@student:~/csc415-device-driver-eric915c/Module$
```

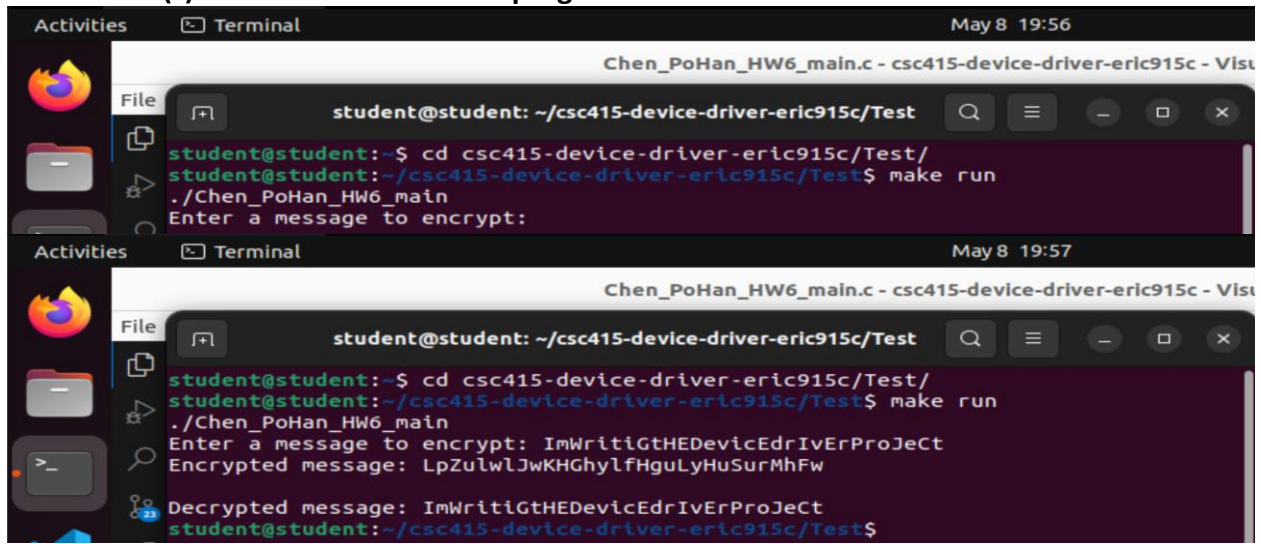
Screen shot of compilation:



```
student@student:~$ cd csc415-device-driver-eric915c/
student@student:~/csc415-device-driver-eric915c$ cd Module/
student@student:~/csc415-device-driver-eric915c/Module$ make
make -C /lib/modules/`uname -r`/build M=/home/student/csc415-device-driver-eric915c/Module modules
make[1]: Entering directory '/usr/src/linux-headers-6.5.0-28-generic'
warning: the compiler differs from the one used to build the kernel
The kernel was built by: x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
You are using: gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
CC [M] /home/student/csc415-device-driver-eric915c/Module/encryption_driver.o
MODPOST /home/student/csc415-device-driver-eric915c/Module/Module.symvers
CC [M] /home/student/csc415-device-driver-eric915c/Module/encryption_driver.mod.o
LD [M] /home/student/csc415-device-driver-eric915c/Module/encryption_driver.ko
BTf [M] /home/student/csc415-device-driver-eric915c/Module/encryption_driver.ko
Skipping BTF generation for /home/student/csc415-device-driver-eric915c/Module/encryption_driver.ko due to unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-6.5.0-28-generic'
student@student:~/csc415-device-driver-eric915c/Module$

student@student:~/csc415-device-driver-eric915c/Test$ cd Test/
student@student:~/csc415-device-driver-eric915c/Test$ make
make: 'Chen_PoHan_HW6_main' is up to date.
student@student:~/csc415-device-driver-eric915c/Test$ make
gcc -c -o Chen_PoHan_HW6_main.o Chen_PoHan_HW6_main.c -g -I.
gcc -o Chen_PoHan_HW6_main Chen_PoHan_HW6_main.o -g -I. -l pthread
student@student:~/csc415-device-driver-eric915c/Test$
```

Screen shot(s) of the execution of the program:



```
student@student: ~/csc415-device-driver-eric915c/Test
student@student:~$ cd csc415-device-driver-eric915c/Test/
student@student:~/csc415-device-driver-eric915c/Test$ make run
./Chen_PoHan_HW6_main
Enter a message to encrypt:

student@student:~/csc415-device-driver-eric915c/Test$
student@student:~/csc415-device-driver-eric915c/Test$ make run
./Chen_PoHan_HW6_main
Enter a message to encrypt: ImWritiGtHEDevicEdrIvErProJeCt
Encrypted message: LpZulwlJwKHGhyLfHgulyHuSurMhFw
Decrypted message: ImWritiGtHEDevicEdrIvErProJeCt
student@student:~/csc415-device-driver-eric915c/Test$
```