BLG 413E – System Programming Project 2

Due **06.12.2021 23:59**

Preliminary

In monoalphabetic substitution ciphers, each letter is replaced by another letter. In the simplest form (the Caesar cipher), each letter is shifted by a certain amount . For example, if the letters are shifted by 3 (the encryption *key*) “A” becomes “D”, “B” becomes “E”, “Y” becomes “B” and “Z” becomes “C”. If the letters are numbered as in:

```
A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
```

this operation can be expressed as:

```
encrypted_letter[i] = (plain_letter[i] + key) mod 26
```

In polyalphabetic substitution ciphers, there are multiple keys where each letter is encrypted using a different key. In the Vigenere cipher, the key is represented by a string and the encryption operation is expressed as:

```
encrypted_letter[i] = (plain_letter[i] + keys[i mod length_of_key]) mod 26
```

For example if the plain text is “SYSTEMS PROGRAMMING” and the key is “LINUX”,
the encrypted text would be “DGFNBXACLLRZNGJTVT” as explained below:

```
 S  Y  S  T  E  M  S  P  R  O  G  R  A  M  M  I  N  G
18 24 18 19  4 12 18 15 17 14  6 17  0 12 12  8 13  6
 L  I  N  U  X  L  I  N  U  X  L  I  N  U  X  L  I  N
11  8 13 20 23 11  8 13 20 23 11  8 13 20 23 11  8 13
-------------------------------------------------
 D  G  F  N  B  X  A  C  L  L  R  Z  N  G  J  T  V  T
 3  6  5 13  1 23  0  2 11 11 17 25 13  6  9 19 21 19
```

Project Description

Develop a Linux character device driver that will implement the Vigenere cipher. The device node will be named “/dev/vigenere” and it will operate as follows:

1. The driver will manage an internal kernel buffer that will be persistent during the module's lifetime. Read and write operations will operate on this buffer. The buffer will have a fixed size which will be a module parameter (with the default value 4KB).
2. The device will be a single-open device, i.e. only one process will be able to access it at a time. You can refer to the *Linux Device Drivers* book for an example on how to do this.
3. The driver will keep a key (also a module parameter with the default value “A”).

4. Any text written to the device will be encrypted using the current key. You can assume that the input text consists of only English uppercase letters.
5. For read operations, the driver will be in one of two modes: decrypting or non-decrypting. In non-decrypting mode (the default) read operations will fill the user space buffer with encrypted text. In decrypting mode, the user space buffer will be filled with the plain text.
6. There will be two “ioctl” commands for setting the mode of the driver:
    - “VIGENERE_MODE_DECRYPT”: This command will take a key value as argument and if it does match with the current key, the driver will be set to decrypting mode for subsequent read operations.
    - “VIGENERE_MODE_SIMPLE”: This command will take a key value as argument and if it does match with the current key, the driver will be set to non-decrypting mode for subsequent read operations.

A simple user-space program for this device can be outlined as follows:

```
fd = open("/dev/vigenere", ...);
write(fd, buffer1, ...);               /* data will be encrypted */
read(fd, buffer2, ...);                /* read encrypted data */
ioctl(fd, VIGENERE_MODE_DECRYPT, key); /* set decrypting mode */
read(fd, buffer2, ...);                /* read decrypted data */
ioctl(fd, VIGENERE_MODE_SIMPLE, key);  /* set non-decrypting mode */
close(fd);
```

Submission Details

- Upload your solutions through Ninova. Homework files sent via e-mail and late submissions will not be accepted.
- Every group member is required to submit source code file(s) through the Ninova system as a zip file.
- Any form of cheating or plagiarism will not be tolerated. This includes actions such as, but not limited to, submitting the work of others as one's own (even if in part and even with modifications) and copy/pasting from other resources (even when attributed). Serious offenses will be reported to the administration for disciplinary measures.
- If you have any questions, please use the message board.