Marc Lapira
Assignment 5

Abstract

This assignment delves into the development of a Bash shell script to facilitate basic encryption functionalities using ROT13 and Caesar's cipher. Executed within an Ubuntu virtual machine's command prompt, the task entails creating an intuitive menu-driven interface for users. The script allows users to input plaintext or ciphertext, either through direct typing or file reading. It grants flexibility by enabling users to choose between ROT13 and Caesar's cipher encryption methods, with the latter allowing dynamic shifts determined by the user.

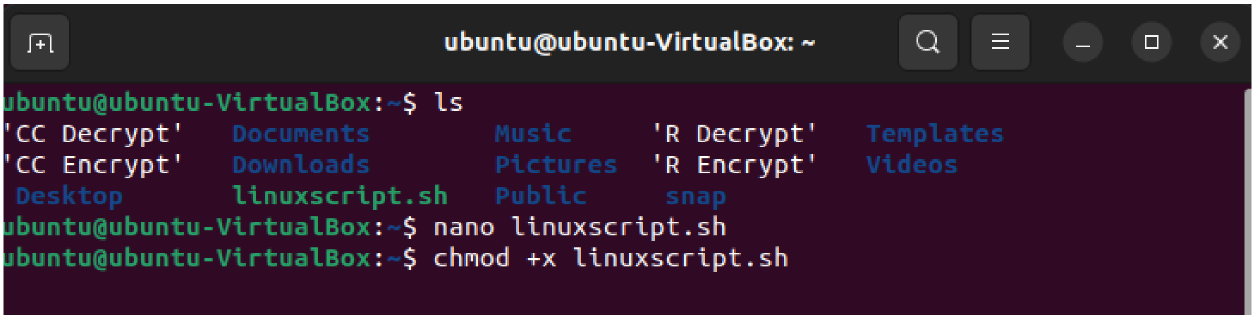
Introduction

Ubuntu will be used in a VirtualBox Virtual machine.

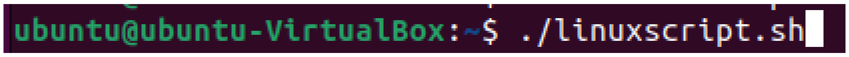
Changing File permissions to run as an executable
chmod +x encrypt.sh

Running a file as a script
./encrypt.sh

Summary of Results

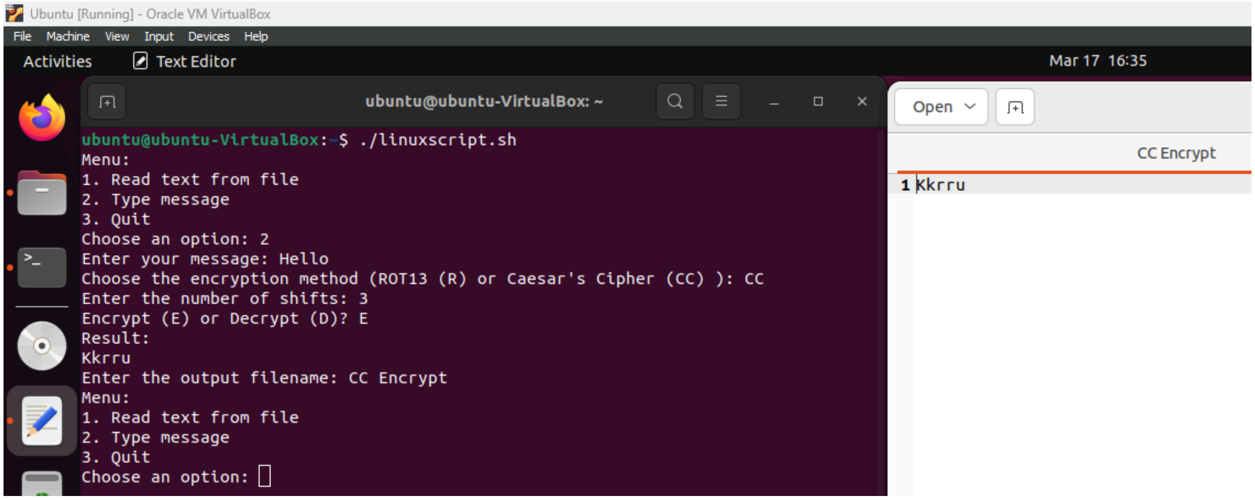


```
ubuntu@ubuntu-VirtualBox:~$ ls
'CC Decrypt'   Documents        Music      'R Decrypt'   Templates
'CC Encrypt'   Downloads        Pictures   'R Encrypt'   Videos
 Desktop       linuxscript.sh   Public      snap
ubuntu@ubuntu-VirtualBox:~$ nano linuxscript.sh
ubuntu@ubuntu-VirtualBox:~$ chmod +x linuxscript.sh
```



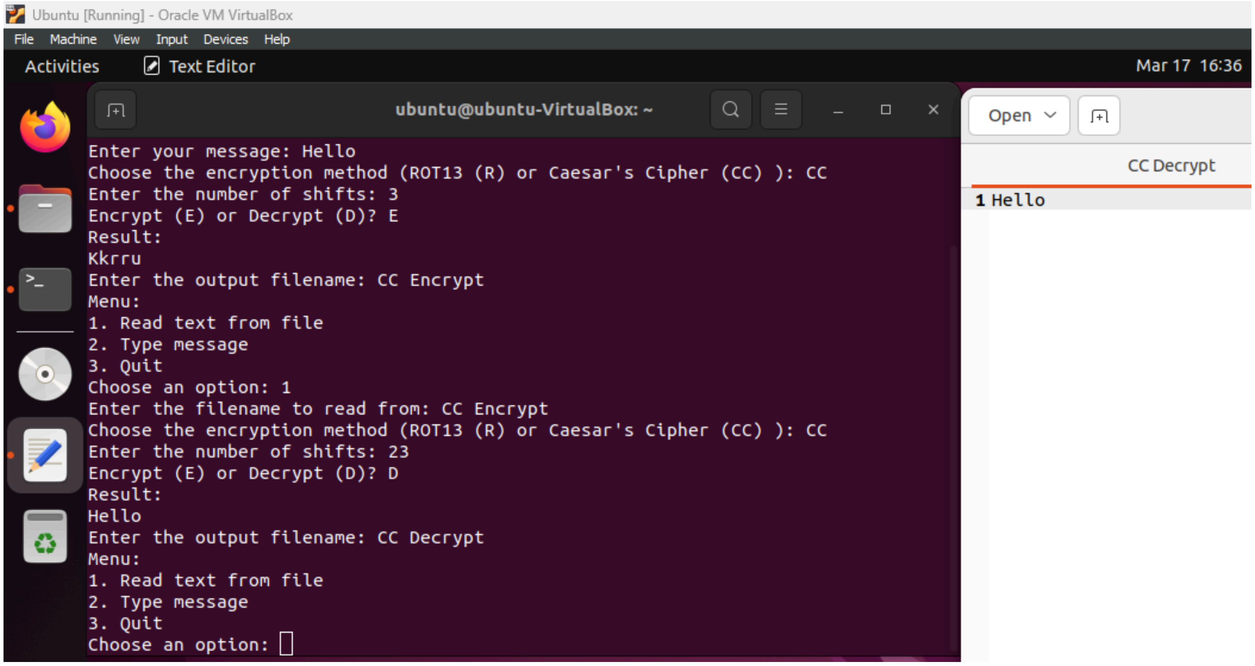
```
ubuntu@ubuntu-VirtualBox:~$ ./linuxscript.sh
```

Here we start with creating a file to begin our shells script. Once we have created the code and are satisfied with it, we change the permissions on the file to be able to run it as an executable, hence the chmod command. Also, make sure to name the file properly with '.sh' as it may or may not run properly or be recognized by the system as a shell script as well as putting the shabang to specify that the proper shell is being used. Once we have verified that the file permissions include an executable, we simply run the script and see if it works.


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Text Editor
Mar 17 16:35
ubuntu@ubuntu-VirtualBox: ~
Open
CC Encrypt

```
ubuntu@ubuntu-VirtualBox:~$ ./linuxscript.sh
Menu:
1. Read text from file
2. Type message
3. Quit
Choose an option: 2
Enter your message: Hello
Choose the encryption method (ROT13 (R) or Caesar's Cipher (CC) ): CC
Enter the number of shifts: 3
Encrypt (E) or Decrypt (D)? E
Result:
Kkrru
Enter the output filename: CC Encrypt
Menu:
1. Read text from file
2. Type message
3. Quit
Choose an option: 
```

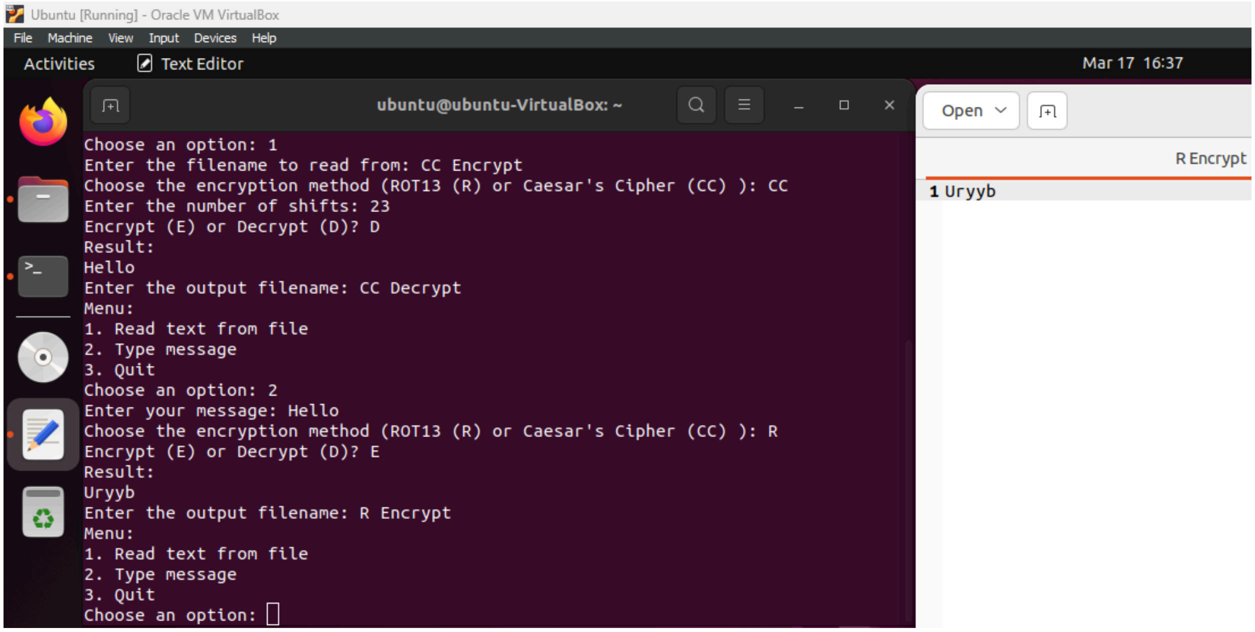
```
Kkrru
```


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Text Editor
Mar 17 16:36
ubuntu@ubuntu-VirtualBox: ~
Open
CC Decrypt

```
Enter your message: Hello
Choose the encryption method (ROT13 (R) or Caesar's Cipher (CC) ): CC
Enter the number of shifts: 3
Encrypt (E) or Decrypt (D)? E
Result:
Kkrru
Enter the output filename: CC Encrypt
Menu:
1. Read text from file
2. Type message
3. Quit
Choose an option: 1
Enter the filename to read from: CC Encrypt
Choose the encryption method (ROT13 (R) or Caesar's Cipher (CC) ): CC
Enter the number of shifts: 23
Encrypt (E) or Decrypt (D)? D
Result:
Hello
Enter the output filename: CC Decrypt
Menu:
1. Read text from file
2. Type message
3. Quit
Choose an option: 
```

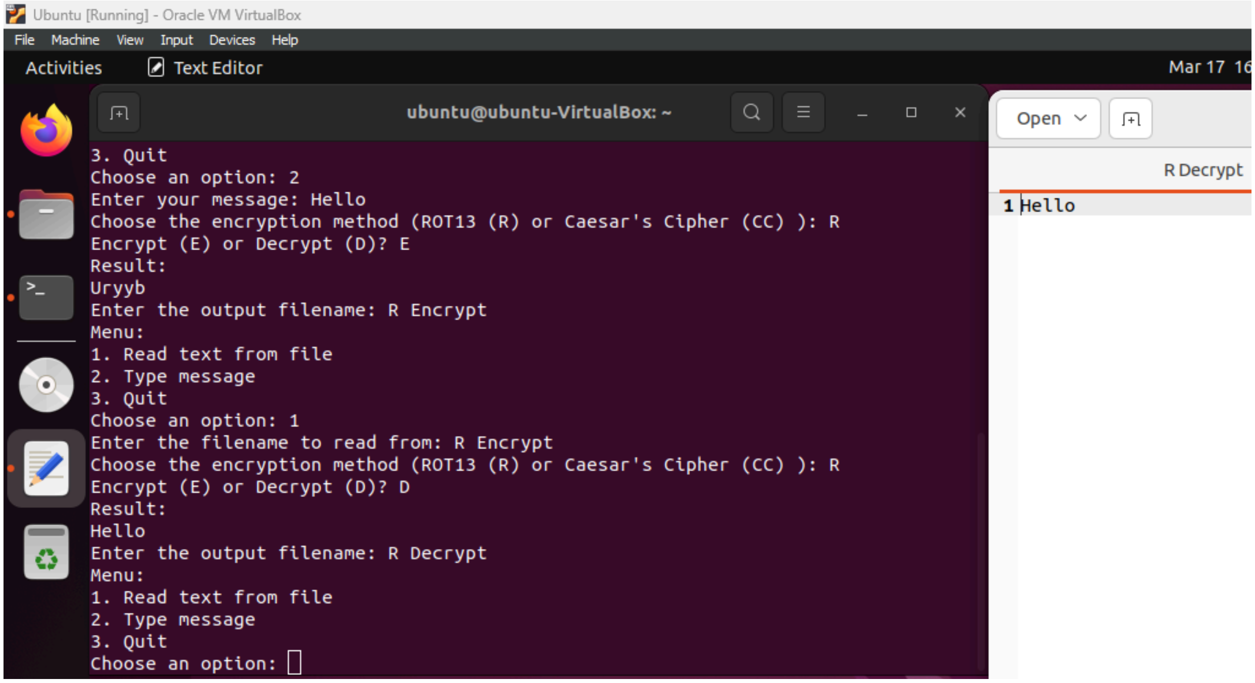
```
Hello
```

Here, we show an example by encrypting and decrypting using the Caesar's Cipher option taking a message and reading from a text file. This step is what I had the most amount of trouble and time with as it would encrypt properly but not decrypt to its original message. I initially tried encrypting forward and then decrypting backward instead of doing the difference over 26 letters but to no avail due to my curiosity, so I decided to just encrypt and decrypt the normal way. After spending some time looking at the code, I realized that I was not properly shifting the message after the user inputs the number of shifts and translating the characters. I also happened upon a 'tr: extra operand 'xyz\n' error which seemed to be that I was improperly passing in an argument into the tr command. I saw that I was telling the tr command that the newline character was being interpreted into the range specification, which explained the difference in encrypted and decrypted messages after passing it along in the Caesar Cipher. As I was trying to adjust these errors, I also got the error ‘tr: range-endpoints of 'A-2' are in reverse collating sequence order’ which told me that I was not shifting the lowercase letters properly either but it was no problem as it was simply the same problems that I solved with the uppercase letters.


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Text Editor
Mar 17 16:37
ubuntu@ubuntu-VirtualBox: ~
Open
R Encrypt

```
Choose an option: 1
Enter the filename to read from: CC Encrypt
Choose the encryption method (ROT13 (R) or Caesar's Cipher (CC) ): CC
Enter the number of shifts: 23
Encrypt (E) or Decrypt (D)? D
Result:
Hello
Enter the output filename: CC Decrypt
Menu:
1. Read text from file
2. Type message
3. Quit
Choose an option: 2
Enter your message: Hello
Choose the encryption method (ROT13 (R) or Caesar's Cipher (CC) ): R
Encrypt (E) or Decrypt (D)? E
Result:
Uryyb
Enter the output filename: R Encrypt
Menu:
1. Read text from file
2. Type message
3. Quit
Choose an option: 
```

```
1 Uryyb
```


Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Text Editor
Mar 17 16
ubuntu@ubuntu-VirtualBox: ~
Open
R Decrypt

```
3. Quit
Choose an option: 2
Enter your message: Hello
Choose the encryption method (ROT13 (R) or Caesar's Cipher (CC) ): R
Encrypt (E) or Decrypt (D)? E
Result:
Uryyb
Enter the output filename: R Encrypt
Menu:
1. Read text from file
2. Type message
3. Quit
Choose an option: 1
Enter the filename to read from: R Encrypt
Choose the encryption method (ROT13 (R) or Caesar's Cipher (CC) ): R
Encrypt (E) or Decrypt (D)? D
Result:
Hello
Enter the output filename: R Decrypt
Menu:
1. Read text from file
2. Type message
3. Quit
Choose an option: 
```

```
1 Hello
```

Here, we show the other method, doing the same as Caesar’s Cipher, taking an input or reading from a text file. ROT13 is a simple letter substitution cipher that replaces a letter with the 13th letter after it in the Latin alphabet and is a special case of the Caesar cipher which was developed in ancient Rome. Personally, using ROT13 from a security and encryption standpoint, it would be a horrible decision to use it as its method to encrypt to hide sensitive information or data would be easily cracked if given time to be looked at. Working on the ROT13 method, was not as much trouble as it did not factor in a specific or special amount of steps or shifts that needed to be accounted for as with Caesar’s Cipher. Overall, for both methods, I had trouble making it output the correct result whether its encrypted or decrypted into the output file until I realized that I was telling it to echo only the encrypted text into the file, which explained why it only worked when the user would pick the encrypt option in the looping menu. I realized this mistake that outside the cases for the methods of encryption, it would only echo the output of the encrypted text. I fixed this by making a specified echo command into an output file inside each case method instead of outside them to make it easier.

Conclusion

In conclusion, this assignment has shown Bash shell scripting and file manipulation techniques within Ubuntu. Through the development of a naive encryption utility using ROT13 and Caesar's cipher, we have created menu interfaces, handling user inputs from both files and direct input, and implementing encryption operations using native Linux utilities. Each step of the process, from handling user inputs to executing encryption operations, helped show the importance of robust cryptographic techniques in controlling risks associated with unauthorized access and data breaches. Also, with the user inputs and file manipulation within the Linux environment, a need for strong security measures to maintain the integrity of digital assets became more apparent, especially for applications that use or require encryption in some capacity. The implementation of encryption methods using ROT13 and Caesar's cipher, with a focus on the 'tr' command for letter shifting, asks for an understanding of cryptography concepts and their practical application in shell scripting. This assignment helped in my Bash shell scripting and Linux command-line utilities but has also deepened our understanding of encryption techniques and their integration into practical applications to hide or censor sensitive information, data, or media.