Project

In this project, I find myself in a challenging scenario: all the files in my home directory have been encrypted using a Caesar cipher. My mission is to use Linux commands to break this encryption and decrypt the files, revealing the hidden messages they contain.

First I used the ls command to list the contents of the working directory

```
analyst@38eb9459d32d:~$ pwd
/home/analyst
analyst@38eb9459d32d:~$ ls
Q1.encrypted  README.txt  caesar
```

Then I checked the contents of the readme file using cat command

```
analyst@38eb9459d32d:~$ cat README.txt
Hello,
All of your data has been encrypted. To recover your data, you will need to solv
e a cipher. To get started look for a hidden file in the caesar subdirectory.
```

The README.txt file indicates that the caesar subdirectory contains a hidden file, which I accessed using the ls -a command to view hidden files.

```
analyst@38eb9459d32d:~$ cd caesar
analyst@38eb9459d32d:~/caesar$ ls -a
.  ..  .leftShift3
```

I then used the cat .leftShift3 command to view the contents of the file.

```
analyst@38eb9459d32d:~/caesar$ cat .leftShift3
Lq rughu wr uhfryhu brxu ilohv brx zloo qhhg wr hqwhu wkh iroorzlqj frppdqg:

rshqvvo dhv-256-fef -sengi2 -d -g -lq T1.hqfubswhg -rxw T1.uhfryhuhg -n hwwxeuxw
h
```

The message in the .leftShift3 file is scrambled due to encryption with a Caesar cipher, which I decrypted using the command cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z".

```
analyst@38eb9459d32d:~/caesar$ cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z"
In order to recover your files you will need to enter the following command:

openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrut
e
```

The command returned the following message: "In order to recover your files, you will need to enter the following command:
`openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute`."
I then returned to the home directory with `cd ~` and executed the command:
`openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute`.

```
analyst@38eb9459d32d:~/caesar$ cd ~
analyst@38eb9459d32d:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out
Q1.recovered -k ettubrute
```

In this step, I relisted the contents of the working directory using the `ls` command and then used the `cat` command to display the contents of the `Q1.recovered` file.

```
analyst@38eb9459d32d:~$ ls
Q1.encrypted  Q1.recovered  README.txt  caesar
analyst@38eb9459d32d:~$ cat Q1.recovered
If you are able to read this, then you have successfully decrypted the classic c
ipher text. You recovered the encryption key that was used to encrypt this file.
 Great work!
analyst@38eb9459d32d:~$
```