Decrypt an encrypted message

First I used the ls command to identify the files in the current directory. There is a Q1.encrypted file that needs to be decrypted as part of the exercise as indicated if I use the cat command to read it.

```
analyst@3df127ee461d:~$ ls
Q1.encrypted  README.txt  caesar
```

```
analyst@3df127ee461d:~$ cat README.txt
Hello,
All of your data has been encrypted. To recover your data, you will need to solve a cipher. To get start
ed look for a hidden file in the caesar subdirectory.
```

I changed directories to caesar which contains a hidden file known as .leftShift3 which may indicate that the cipher has shifted the alphabet by three spaces.

```
analyst@3df127ee461d:~$ cd caesar
analyst@3df127ee461d:~/caesar$ ls -a
.  ..  .leftShift3
```

I used the cat command on the file followed by piping the tr “d-za-cD-ZA-C” “a-zA-Z” command to shift the alphabet by three spaces from d-z back to a-c and D-Z back to A-C. Doing this, will give me the deciphered message in the file which instructs me to use the following command in the Q1.encrypted file of the previous directory.

```
analyst@3df127ee461d:~/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 ettubrute
```

Plugging the command in the previous directory will then output a Q1.recovered file which, when used with the cat command, will indicate that the exercise has been completed.

```
analyst@3df127ee461d:~/caesar$ cd
analyst@3df127ee461d:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrut
e
analyst@3df127ee461d:~$ ls
Q1.encrypted  Q1.recovered  README.txt  caesar
```

```
analyst@3df127ee461d:~$ cat Q1.recovered
If you are able to read this, then you have successfully decrypted the classic cipher text. You recovere
d the encryption key that was used to encrypt this file. Great work!
```