**Activity: Decrypt an encrypted message**

**Overview:** You were also introduced to the Caesar cipher, one of the earliest cryptographic algorithms used to protect people’s privacy. In this lab activity, you’ll be guided through some basic cryptographic activities using Linux commands to decrypt files and reveal hidden messages.

**Scenario:** In this scenario, all of the files in your home directory have been encrypted. You’ll need to use Linux commands to break the Caesar cipher and decrypt the files so that you can read the hidden messages they contain.

**First**, you’ll explore the contents of the home directory and read the contents of a file. **Next**, you’ll find a hidden file and decrypt the Caesar cipher it contains. **Finally**, you’ll decrypt the encrypted data file to recover your data and reveal the hidden message.

**Start your lab:** click on “start lab” to start the lab.

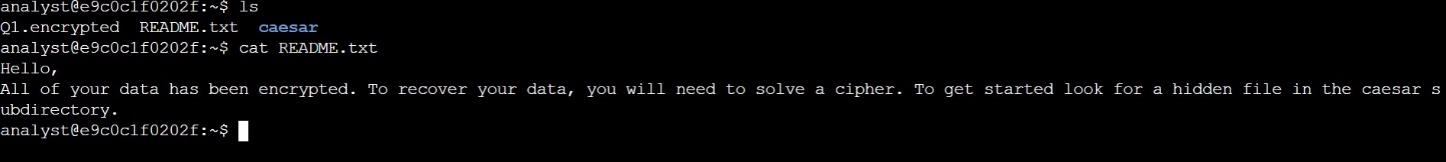
**Task 1. Read the contents of a file**

The lab starts in your home directory, /home/analyst, as the current working directory. In this task, you need to explore the contents of your home directory and read the contents of a file to get further instructions.

1. Use the ls command to list the files in the current working directory.

**$ ls**

1. Use the cat command to list the contents of the README.txt file.

**$ cat README.txt**

**Task 2. Find a hidden file**

In this task, you need to find a hidden file in your home directory and decrypt the Caesar cipher it contains. This task will enable you to complete the next task.

1. First, use the cd command to change to the caesar subdirectory of your home directory:

**$ cd Caesar**

1. Use the ls -a command to list all files, including hidden files, in your home directory.

**$ ls –a**

1. Use the cat command to list the contents of the .leftShift3 file.

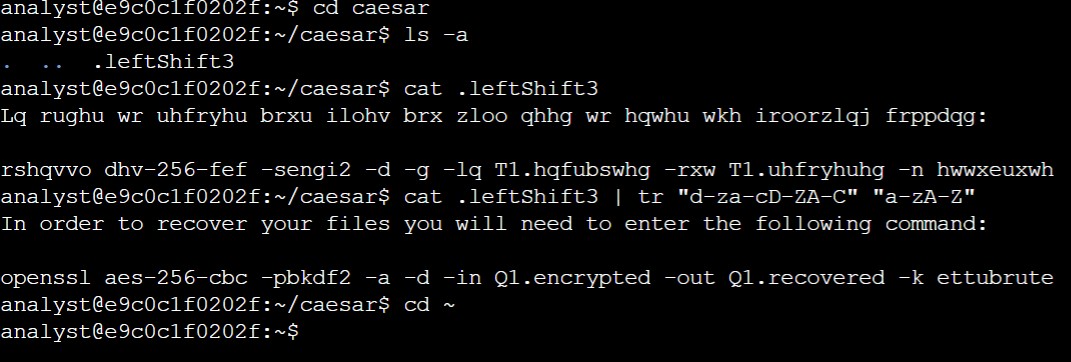
**$ cat .leftshift3**

1. You can decrypt the Caesar cipher in the .leftshift3 file by using the following command:

**$ cat .leftShift3 | tr "d-za-cD-ZA-C" "a-zA-Z"**

1. Now, return to your home directory before completing the next task:

**$ cd ~**



**Task 3. Decrypt a file**

Now that you have solved the Caesar cipher, in this task you need to use the command revealed in .leftshift3 to decrypt a file and recover your data so you can read the message it contains.

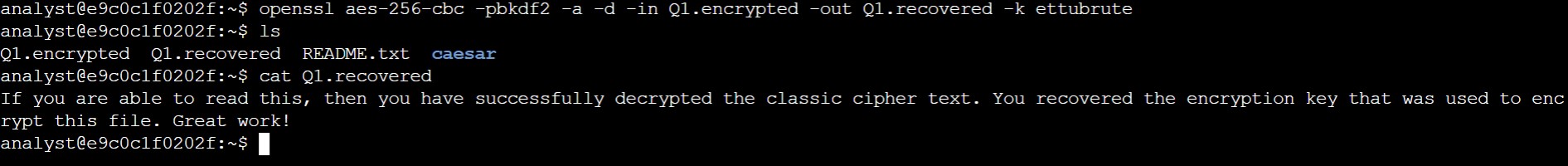
1. Use the exact command revealed in the previous task to decrypt the encrypted file:

**$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute**

1. Use the ls command to list the contents of your current working directory again.

**$ ls**

1. Use the cat command to list the contents of the Q1.recovered file.

**$ cat Q1.recovered**

**Conclusion**

You now have practical experience in using basic Linux Bash shell commands to

* list hidden files,
* decrypt a Caesar cipher, and
* Decrypt an encrypted file.