

---

## PROJECT 2: FILE ENCRYPTION & DECRYPTION (OpenSSL + Caesar Cipher)

### Screenshot:

```
analyst@4a09ab896c2d:~$ pwd
/home/analyst
analyst@4a09ab896c2d:~$ ls
Q1.encrypted  README.txt  caesar
analyst@4a09ab896c2d:~$ cat README.txt
cat: README.txt: No such file or directory
analyst@4a09ab896c2d:~$ cat README.txt
Hello,
All of your data has been encrypted. To recover your data, you will need to solve a cipher. To get started look for a hidden file in the caesar subdirectory
.
analyst@4a09ab896c2d:~$ cd caesar
analyst@4a09ab896c2d:~/caesar$ ls -a
.  ..  .leftShift3
analyst@4a09ab896c2d:~/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 ettubroute
analyst@4a09ab896c2d:~/caesar$ cd ~
analyst@4a09ab896c2d:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubroute
analyst@4a09ab896c2d:~$ ls
Q1.encrypted  Q1.recovered  README.txt  caesar
analyst@4a09ab896c2d:~$ cat Q1.recovered
If you are able to read this, then you have successfully decrypted the classic cipher text. You recovered the encryption key that was used to encrypt this file. Great work!
analyst@4a09ab896c2d:~$ □
```

## Screenshot

The screenshot shows a web browser window with the address bar at 'cloudskillsboost.google'. The page title is 'Activity: Decrypt an encrypted message'. The main content area is split into two panels. The left panel is a terminal window with a black background and white text, showing a series of commands and their outputs. The right panel has a white background and contains the activity title, a star rating, and a list of tasks. A small orange box in the top right corner of the right panel indicates '3/3'.

```
analyst@4a09ab896c2d:~$ pwd
/home/analyst
analyst@4a09ab896c2d:~$ ls
Q1.encrypted README.txt caesar
analyst@4a09ab896c2d:~$ cat README.txt
cat: README.txt: No such file or directory
analyst@4a09ab896c2d:~$ cat README.txt
Hello,
All of your data has been encrypted. To recover your data, you will need to solve a cipher. To get started look for a hidden file in the caesar subdirectory
analyst@4a09ab896c2d:~$ cd caesar
analyst@4a09ab896c2d:~/caesar$ ls -la
.  .. .leftShift3
analyst@4a09ab896c2d:~/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
analyst@4a09ab896c2d:~/caesar$ cd -
analyst@4a09ab896c2d:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1.recovered -k ettubrute
analyst@4a09ab896c2d:~$ ls
Q1.encrypted Q1.recovered README.txt caesar
analyst@4a09ab896c2d:~$ cat Q1.recovered
If you are able to read this, then you have successfully decrypted the classic cipher text. You recovered the encryption key that was used to encrypt this file. Great work!
analyst@4a09ab896c2d:~$
```

### Activity: Decrypt an encrypted message

Lab 1 hour No cost Introductory

★★★★★

This lab may incorporate AI tools to support your learning.

#### Lab instructions and tasks

- Activity overview
- Scenario
- Start your lab
- Task 1. Read the contents of a file
- Task 2. Find a hidden file
- Task 3. Decrypt a file
- Conclusion
- End your lab

**Description: Hybrid Challenge — Symmetric AES-256 encryption + Caesar cipher decoding**

## What I Did

This project simulates a real-world decryption task using:

- A hidden Caesar cipher to reveal a key.
- AES-256-CBC encryption with OpenSSL for secure file handling.

### Step-by-Step Process:

#### 1. Read the warning from README.txt:

I saw a message stating that files had been encrypted and that I'd need to "solve a cipher" to decrypt them.

#### 2. Navigated to the caesar folder:

Listed files and discovered .leftShift3, a text file used for Caesar cipher decoding.

### 3. Used tr to decode the cipher:

Command used:

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

3. This translated the Caesar cipher back into readable instructions. It revealed the decryption key (ettubrrute) and how to use it.

### 4. Ran OpenSSL AES-256 decryption command:

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

### 4. Recovered the file:

I opened Q1.recovered, which confirmed successful decryption of a file containing instructions or validation of the key used.

---

#### Skills Applied

Area	Description
Cipher Analysis	Practiced Caesar cipher decryption using Linux tools (tr)
OpenSSL Decryption	Ran a real-world symmetric encryption decryption using AES-256
File Forensics	Understood how attackers may encrypt data and how defenders can recover it if the key is leaked
CLI Navigation	Used bash commands to inspect, analyze, and decrypt files

---

#### Real-World Benefits

- **Cryptography Awareness:** I now understand how both symmetric and classical encryption techniques work, especially in ransomware scenarios.
  - **Blue Team Relevance:** If attackers encrypt files and leave ransom notes, I can investigate folders, decode ciphers, and try brute-force or leaked key decryption.
  - **Tool Usage:** openssl is widely used in file encryption and SSL/TLS, so knowing how it works is essential in cyber defense.
-