DECRYPT AN ENCRYPTED MESSAGE

Pedro Osorio Lopez.

1. High-Level Project Description:

*In this project, we'll complete a series of tasks to obtain instructions for decrypting an encrypted file. Encryption of data in use, at rest, and in transit is critical to security functions. We'll use the Linux skills we have learned to uncover the clues needed to decode a classical cipher, restore a file, and reveal a hidden message.

2. Project Setup and Required Tools:

*A Linux setup was provided to us to perform the required tasks. Some basic knowledge of the Linux CLI is required.

3. Step by Step Project Walkthrough

We will now proceed to perform the following tasks: List the contents of a directory, read the contents of files, use Linux commands to revert a classical cipher back to plaintext, and decrypt an encrypted file and restore the file to its original state.

*As usual, we will simply begin by listing the contents of the directory by using the ls command:

```
analyst@8a0e85102311:~$ ls
Q1.encrypted  README.txt  caesar
```

*We see that there is a README.txt file, so we will proceed to read it with the cat command. This file gives us some instructions on how to proceed, so the next few commands are simply showing how change directories (cd), list hidden files (ls -a), and read the hidden file (cat).

```
analyst@8a0e85102311:~$ 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@8a0e85102311:~$ cd caesar
analyst@8a0e85102311:~/caesar$ ls -a
.  ..  .leftShift3
analyst@8a0e85102311:~/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 hwwxeuxwh
analyst@8a0e85102311:~/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
```

*The last line of the hidden file gives us a pretty long command which will shift the characters from this file three characters to the left to decrypt and give us the actual message. After executing it, a new file appears, so we will finish by simply reading its contents.

```
analyst@8a0e85102311:~/caesar$ cd ~
analyst@8a0e85102311:~$ openssl aes-256-cbc -pbkdf2 -a -d -in Q1.encrypted -out Q1
.recovered -k ettubrute
analyst@8a0e85102311:~$ ls
Q1.encrypted  Q1.recovered  README.txt  caesar
analyst@8a0e85102311:~$ cat Q1.recovered
If you are able to read this, then you have successfully decrypted the classic cip
her text. You recovered the encryption key that was used to encrypt this file. Gre
at work!
analyst@8a0e85102311:~$
```

4. Summary and/or Recommendations:

*After completing this project, now we have practical experience in using Linux Bash commands to list hidden files, decrypt a Ceasar cipher, and decrypt an encrypted file.