**Handling Encryption Keys with Cloud KMS (Lab-1)**

**Problem:**

Your organization has recently been awarded a federal contract to store sensitive records. You have been asked to familiarize yourself with Cloud KMS to comprehend better the process of encrypting and decrypting files.

**Solution:**

***You must first complete the following steps to complete your lab.***

1. ***Make a keyring***
2. ***Get files from the repository***
3. ***Make the plain text document secure by encrypting it***
4. ***Decrypt the encrypted file***
5. Once you first log in, your screen should look similar to this.



1. Click on the project selector drop-down menu at the top of the screen.



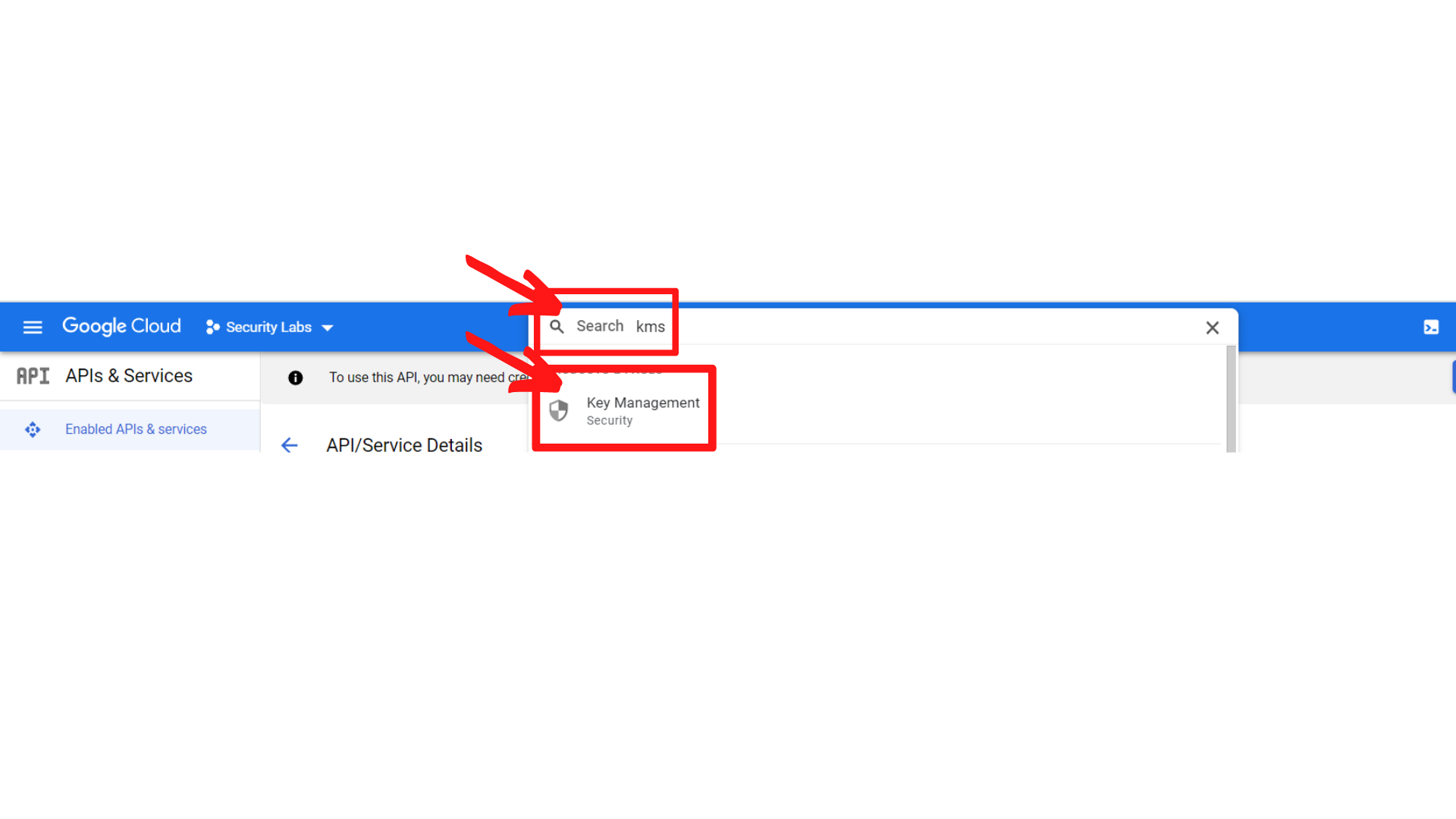
1. Since, we are doing labs on a Security Labs project, Click on *“Security Labs”*.



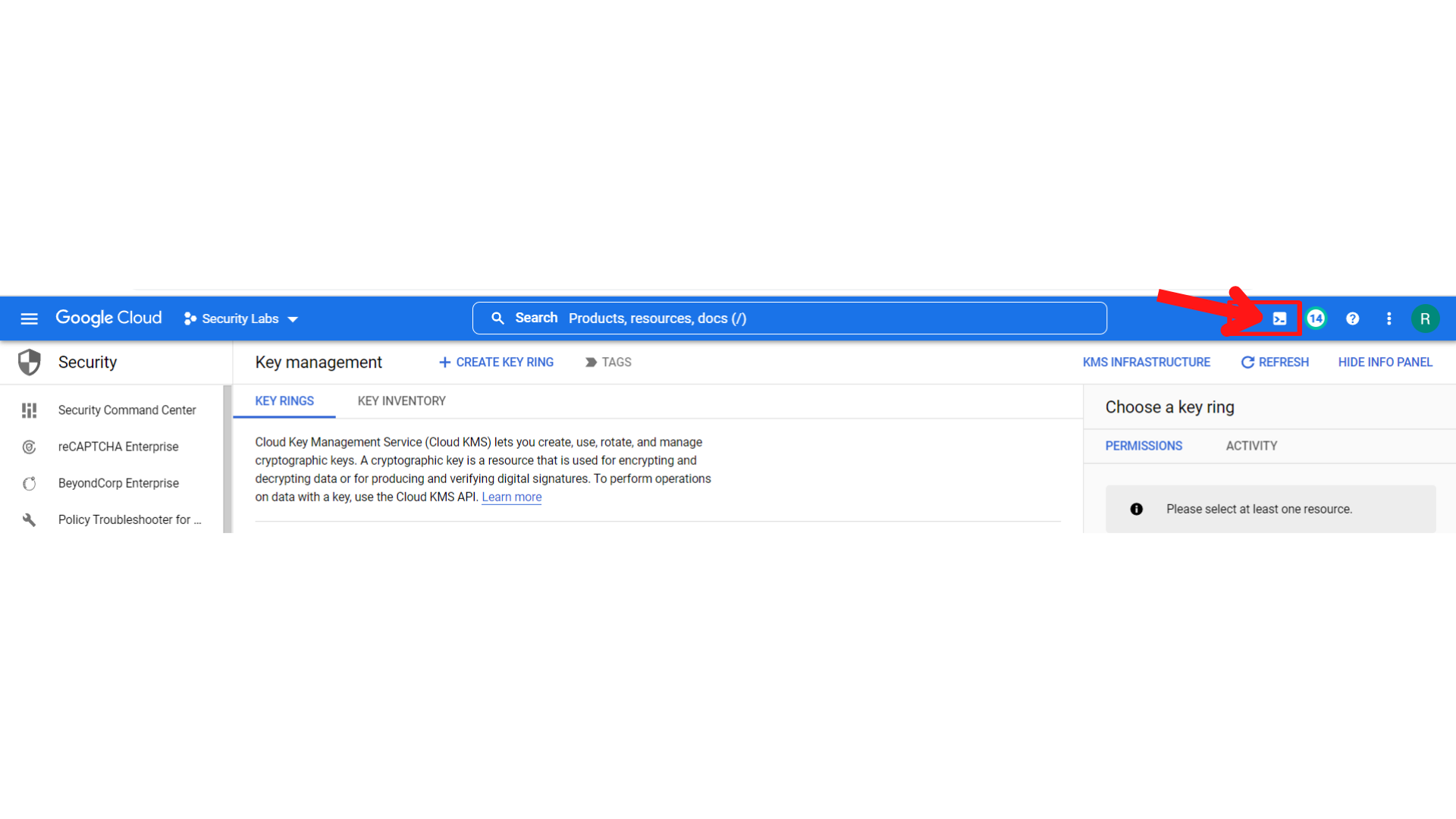
1. Your screen should look similar to this with project info changed to “*Security Labs”* project.



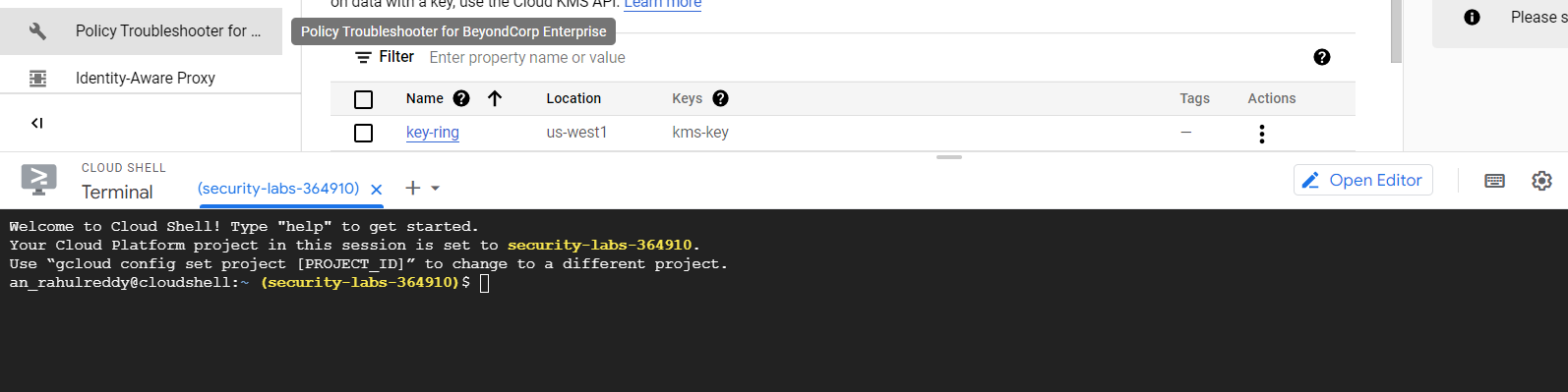
1. Look at the upper part of the GCP console to reach the search bar. **“Enter *kms* and click on Key Management.”**



1. Your screen should look similar to this and ***“click → Cloud shell”*** Icon.

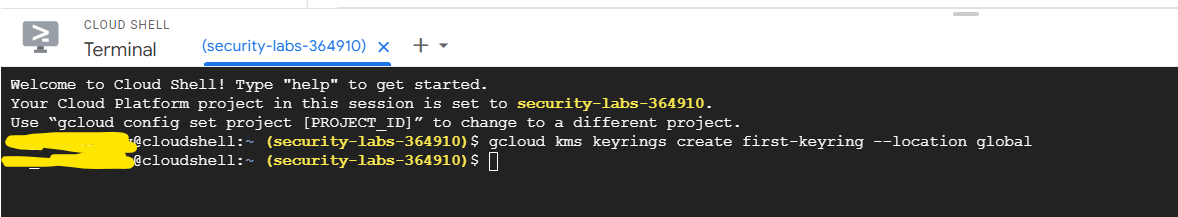


1. Your screen should look similar to this with a cloud shell terminal.



1. Create a first keyring in the Cloud Shell by running the following command:

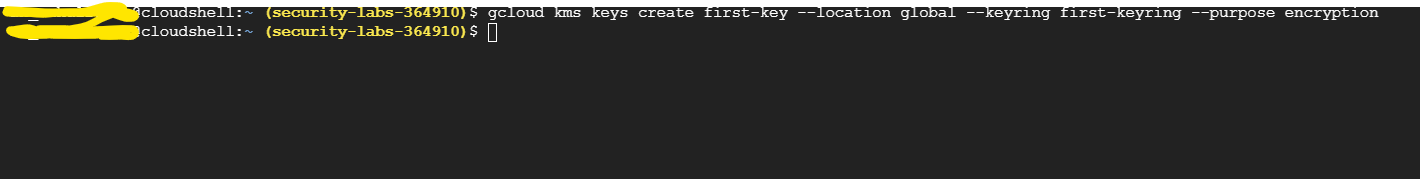
**gcloud kms keyrings create first-keyring --location global**



**This will create a new keyring with name first-keyring**

1. Now to make a key for a first-keyring, use the following command:

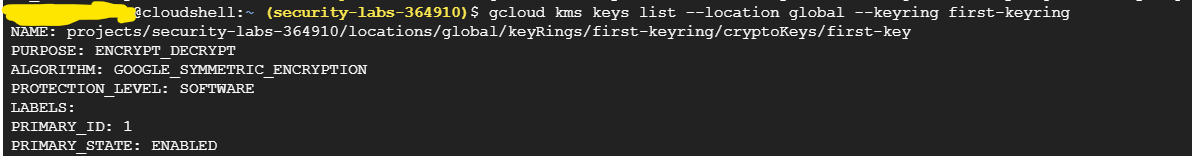
**gcloud kms keys create first-key --location global --keyring first-keyring --purpose encryption**



**This will create a key for the first-keyring**

1. Now to see the list of existing keys, use the following command:

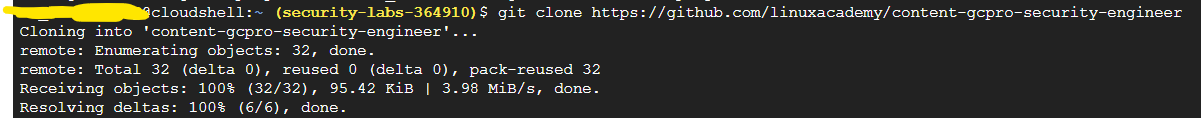
**gcloud kms keys list --location global --keyring first-keyring**



This will show the list of keys.

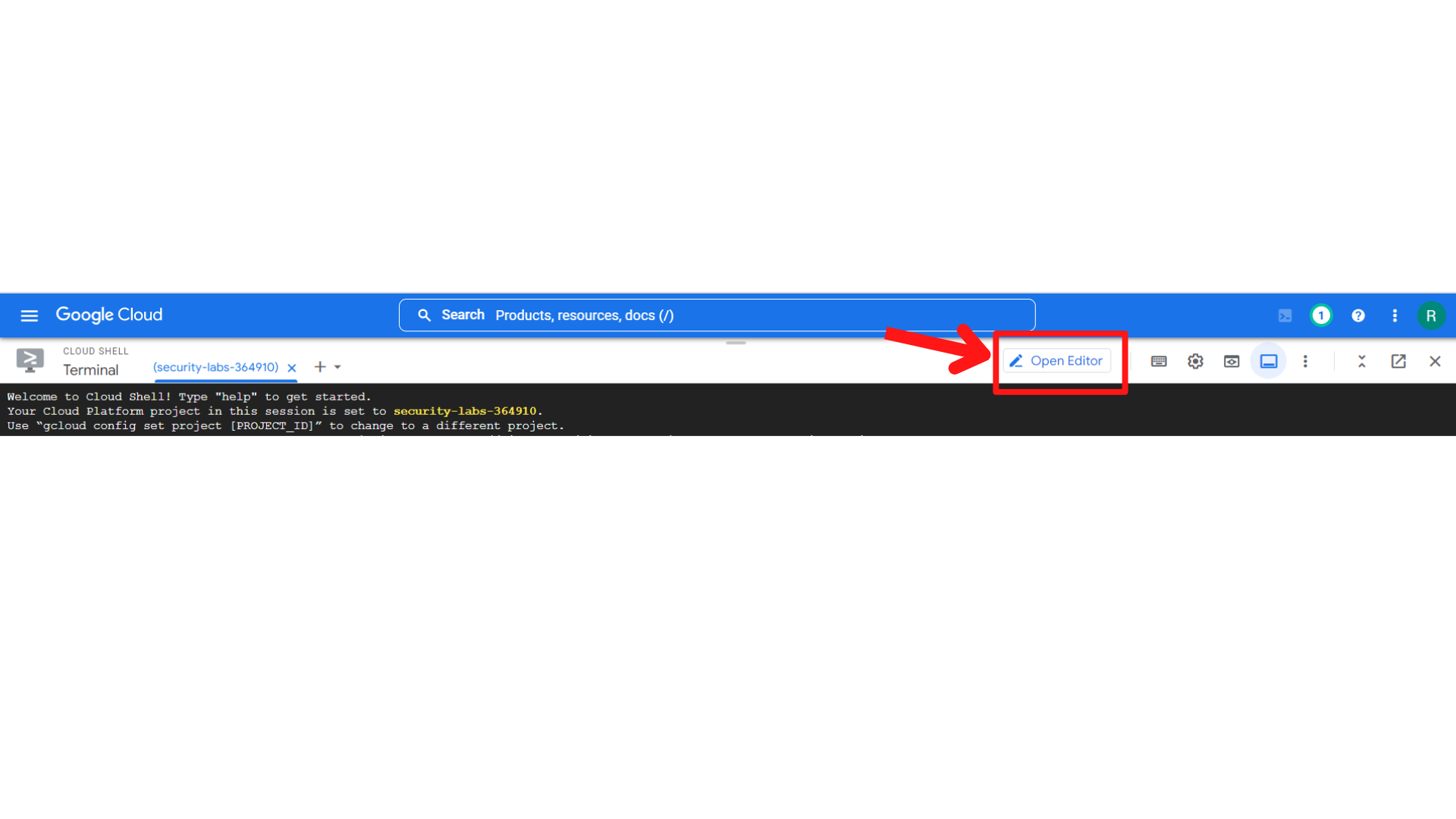
1. Now Github repository should be cloned: Use the following command:

**git clone https://github.com/linuxacademy/content-gcpro-security-engineer**

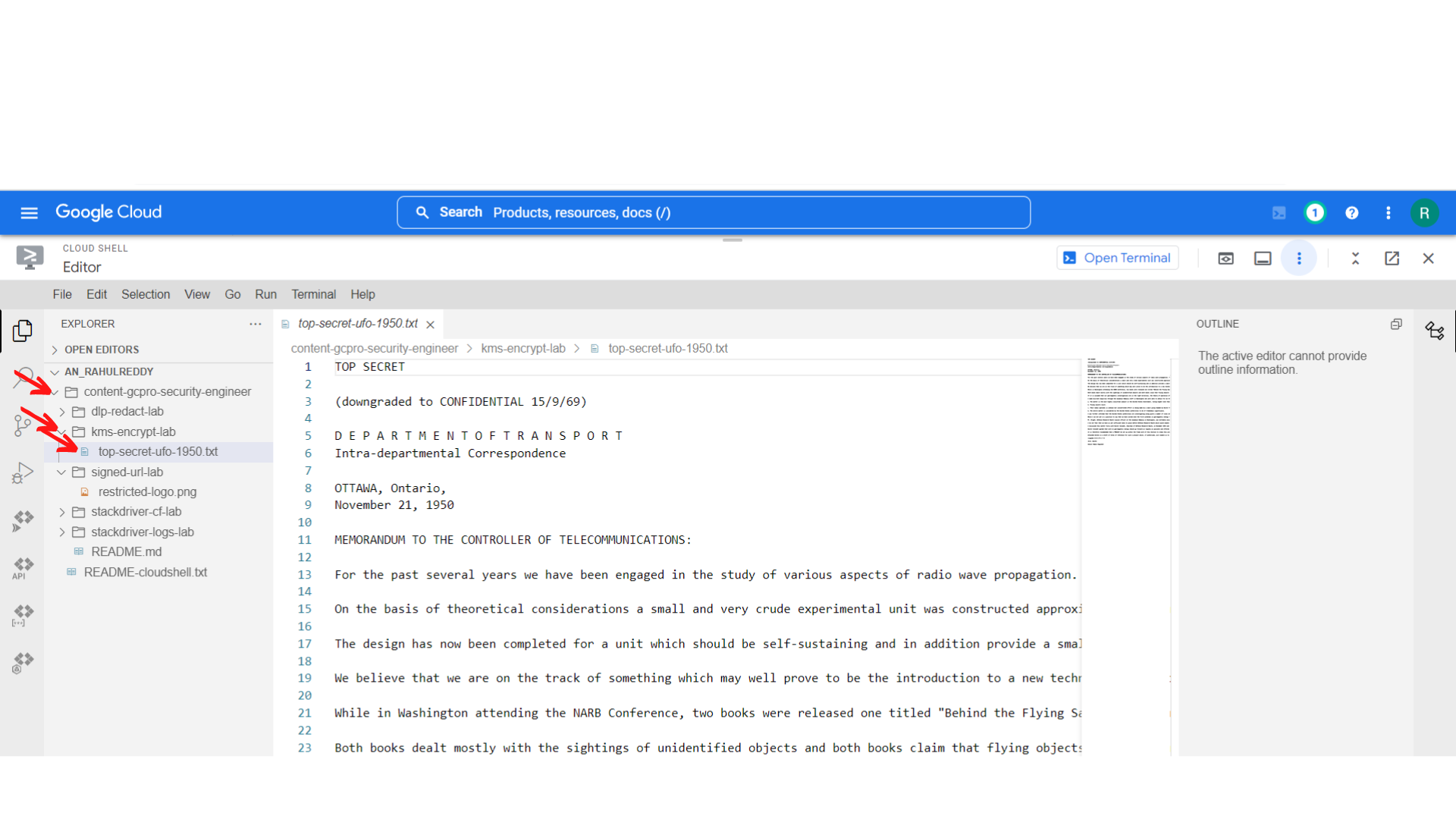


This command will clone git into your VM.

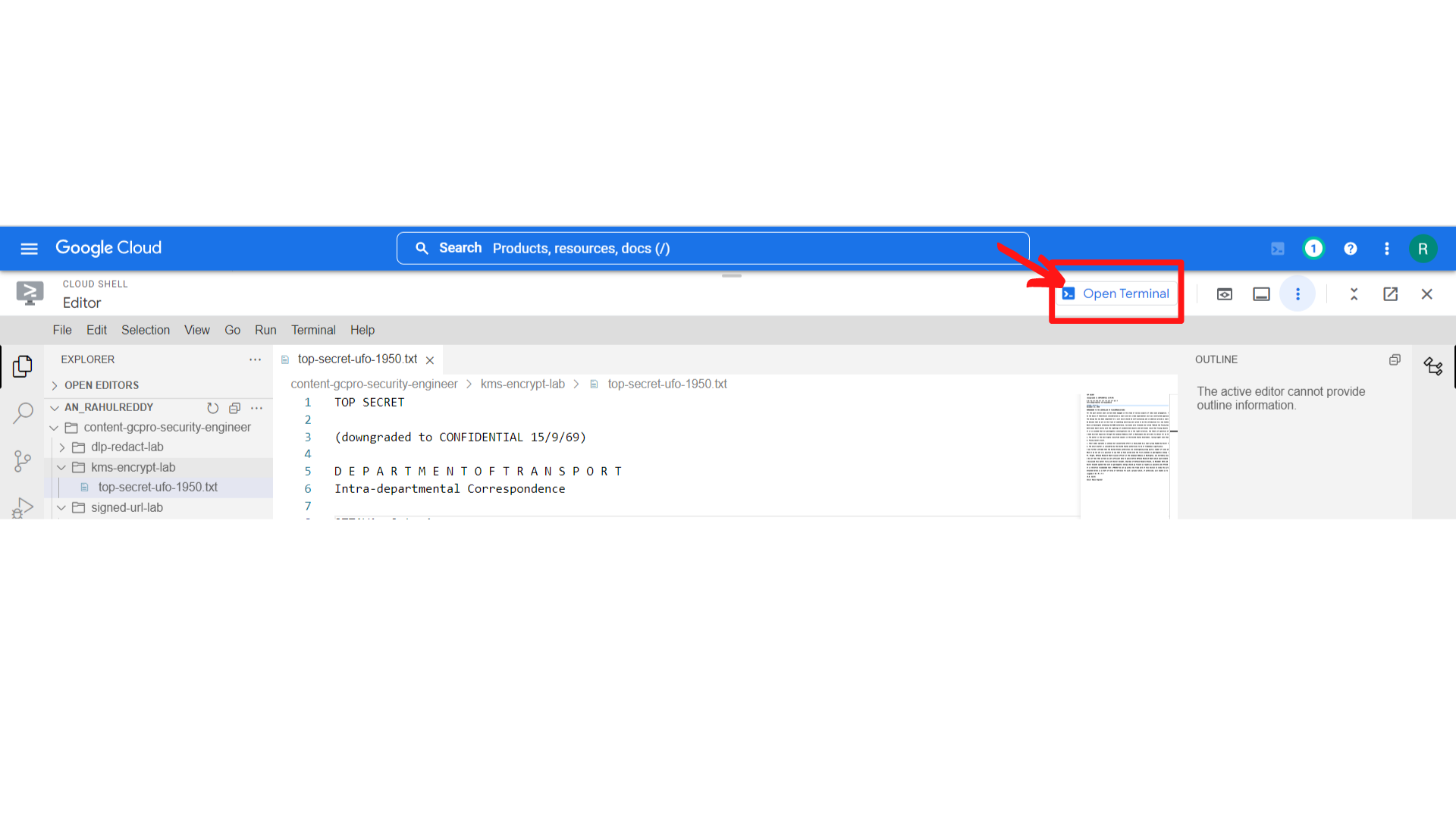
1. Now by clicking on the pencil symbol, you can access the cloud shell editor where you can see the cloned files.



1. Your screen should now look similar to this, then ***“click → content-gcpro-security-engineer → kms-encrypt-lab → top-secret-ufo-1950.txt”***

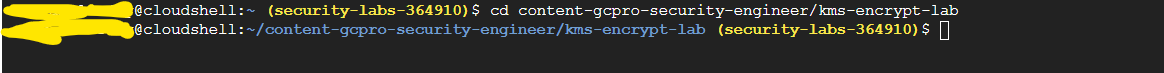


1. Now we have to encrypt that file “top-secret-ufo-1950.txt” and **“click → Open terminal”**



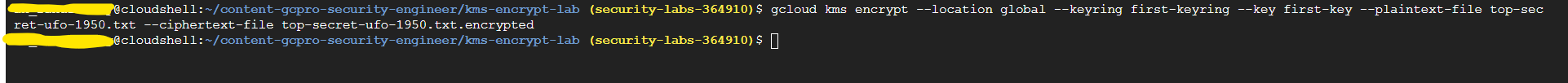
1. Now you will see the terminal screen, Now navigate to the content-gcpro-security-engineer/kms-encrypt-lab directory:

**cd content-gcpro-security-engineer/kms-encrypt-lab**



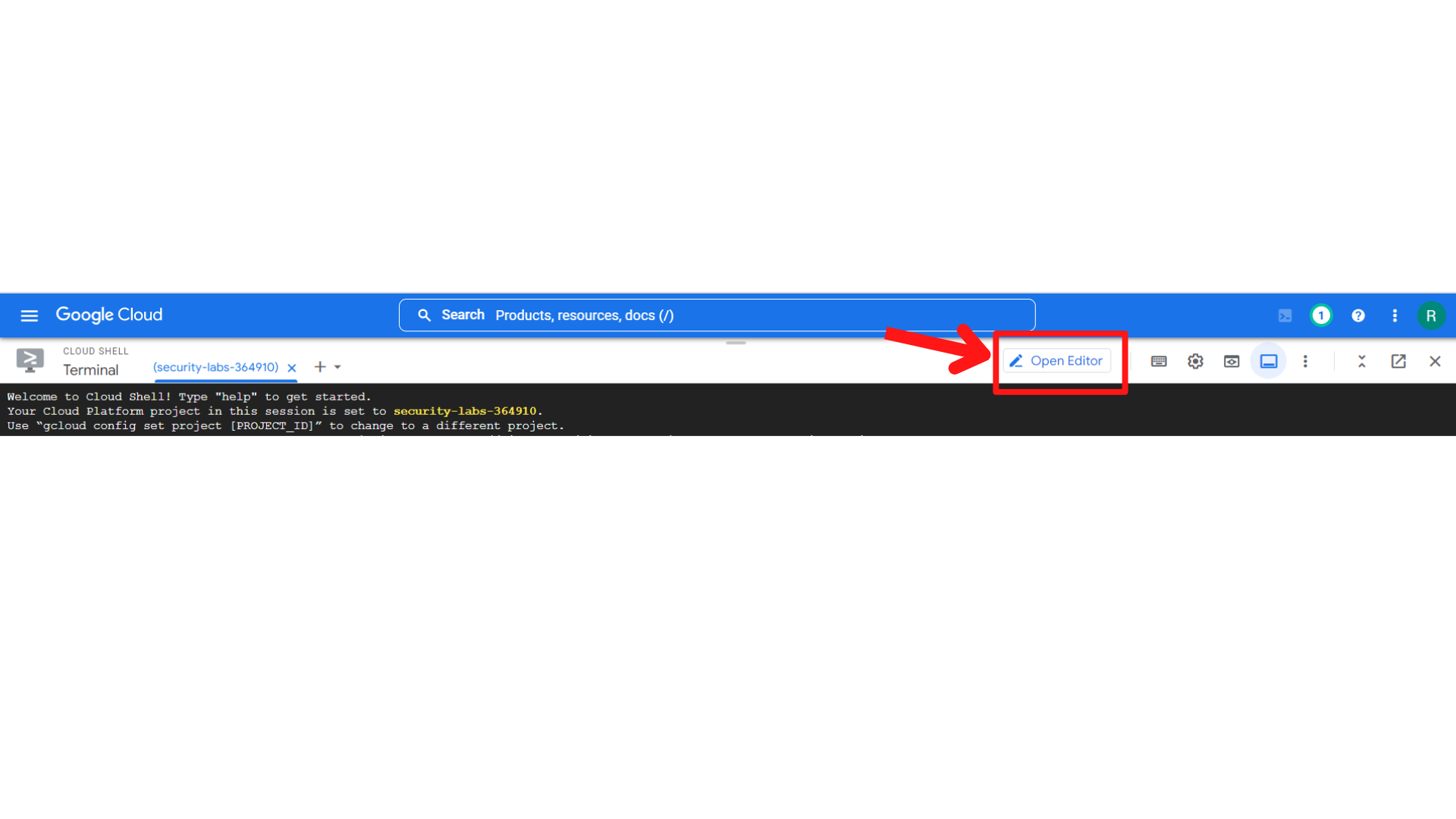
1. Now to encrypt the file, use the following command:

**gcloud kms encrypt --location global --keyring first-keyring --key first-key --plaintext-file top-serect-ufo-1950.txt --ciphertext-file top-secret-ufo-1950.txt.encrypted**

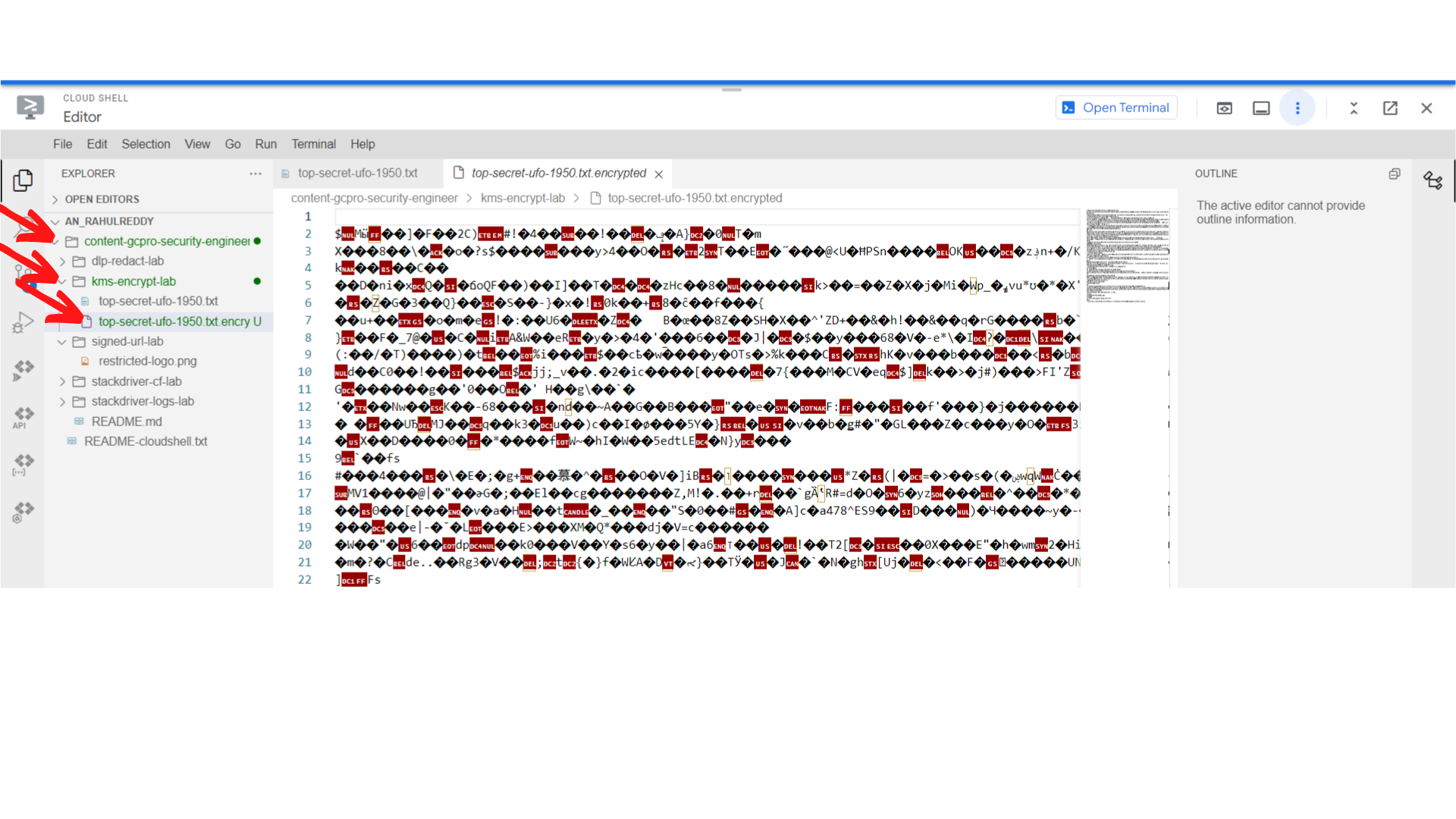


Now the file is encrypted with name **“top-secret-ufo-1950.txt.encrypted”**

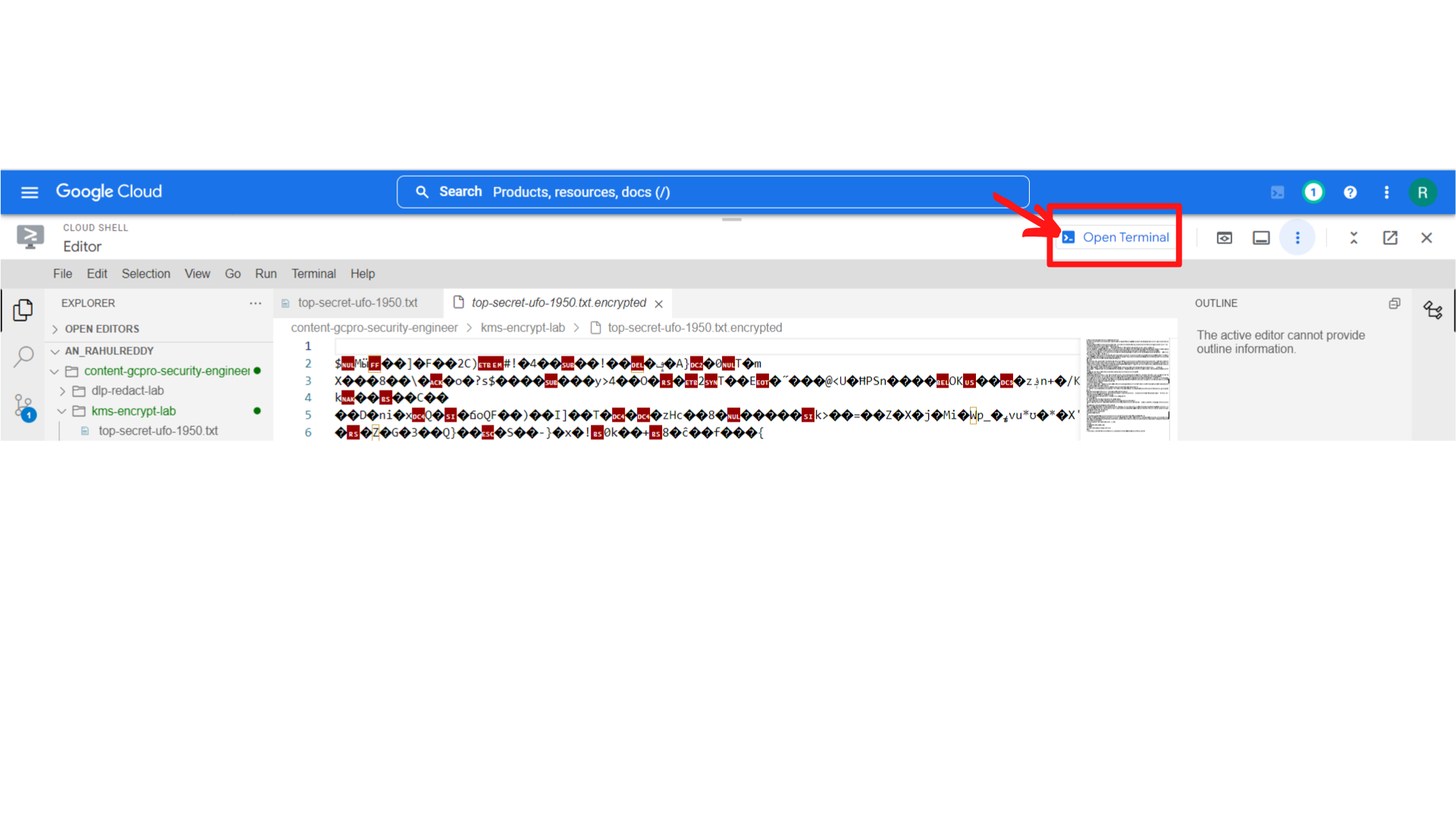
1. Now you examine the **“top-secret-ufo-1950.txt.encrypted”** by *“****clicking on pencil symbol”***



1. Your screen should now look similar to this, then ***“click →content-gcpro-security-engineer → kms-encrypt-lab → top-secret-ufo-1950.txt.encrypted”*** *and you will see the encrypted text file.*

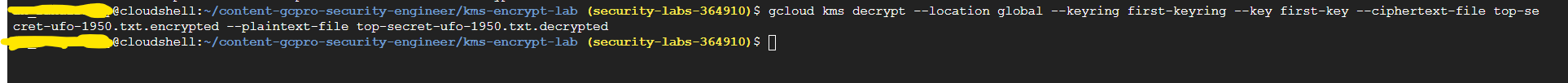


1. Now we have to **decrypt that file “top-secret-ufo-1950.txt.encrypted”** and ***“click → Open terminal”***

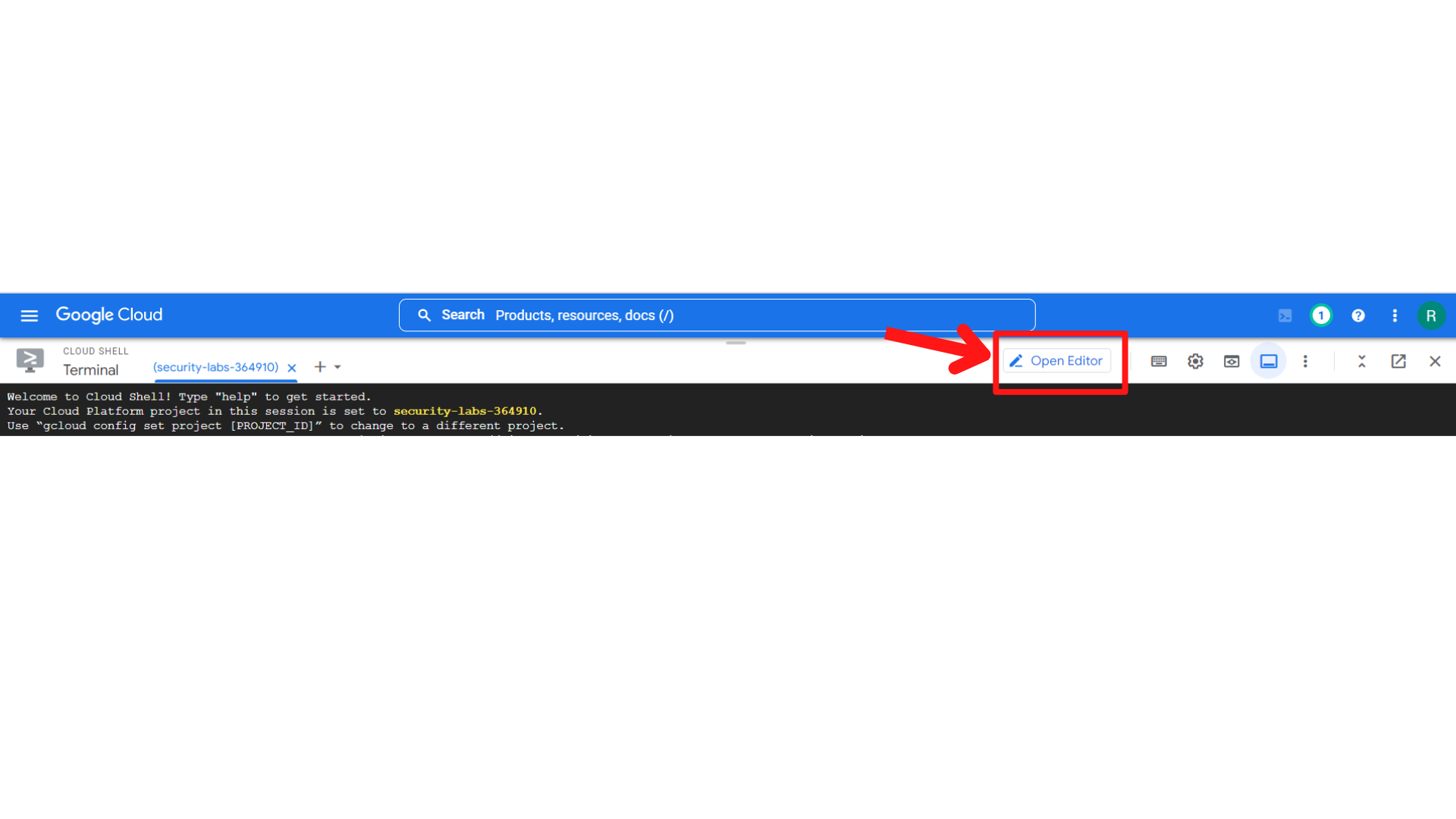


1. Now you will see the terminal; To decode the encrypted file, use the following command:

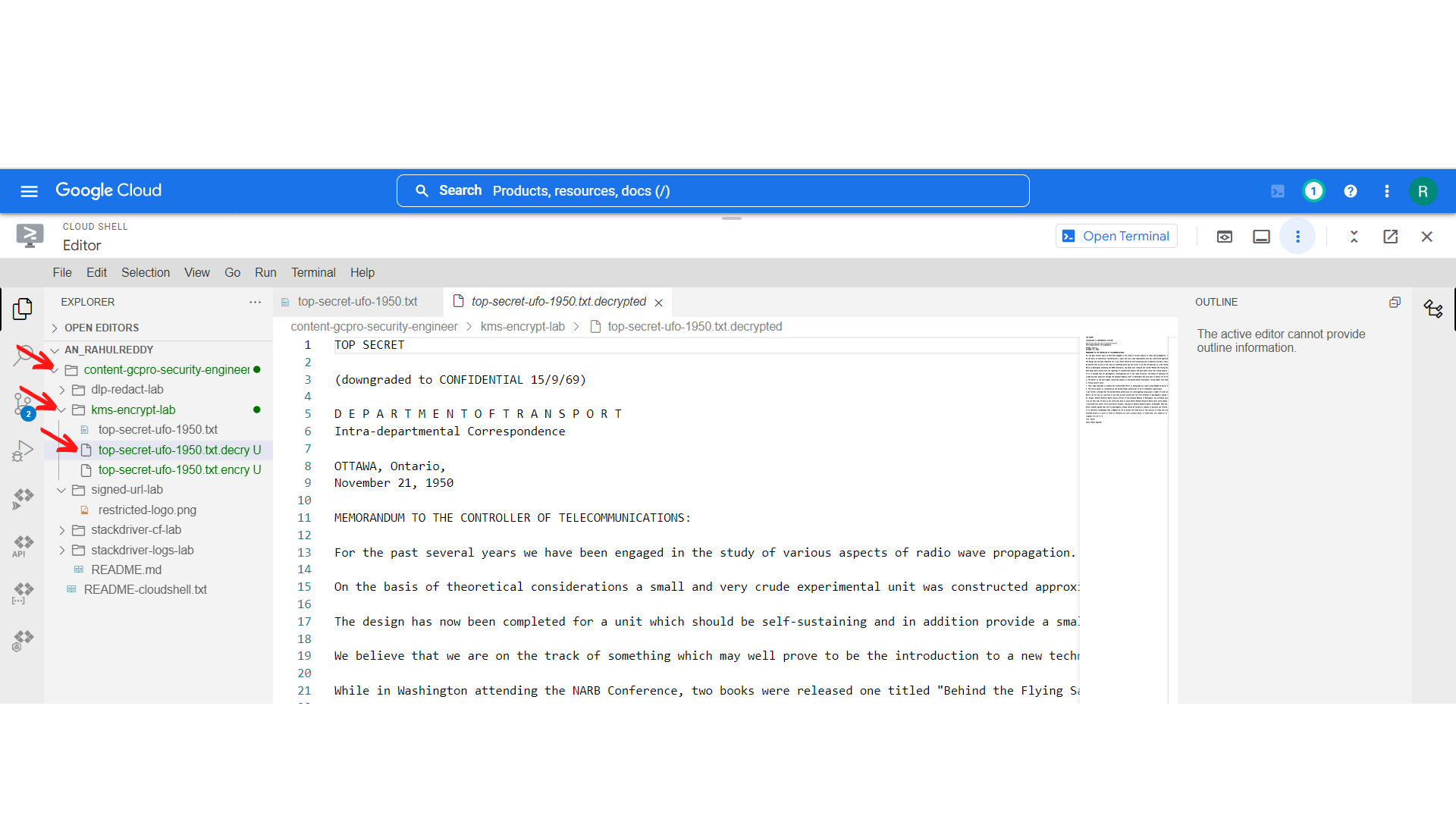
**gcloud kms decrypt --location global --keyring first-keyring --key first-key --ciphertext-file top-secret-ufo-1950.txt.encrypted --plaintext-file top-secret-ufo-1950.txt.decrypted**



1. Now you examine the **“top-secret-ufo-1950.txt.decrypted”** by *“****clicking on pencil symbol”***



1. Your screen should now look similar to this, then ***“click →content-gcpro-security-engineer → kms-encrypt-lab → top-secret-ufo-1950.txt.decrypted”*** *and you will see the decrypted text file.*



Now the file has been decrypted to the original file.

1. That’s it you have successfully completed the lab.