**FUNDAMENTALS OF CRYPTOGRAPHY – CAPSTONE PROJECT**

**Generating SHA256 Checksum of a File Using CMD**

**1) Text File and Command Prompt**

The objective of this project is to demonstrate a practical application of cryptographic hashing by computing the SHA256 checksum of a file.

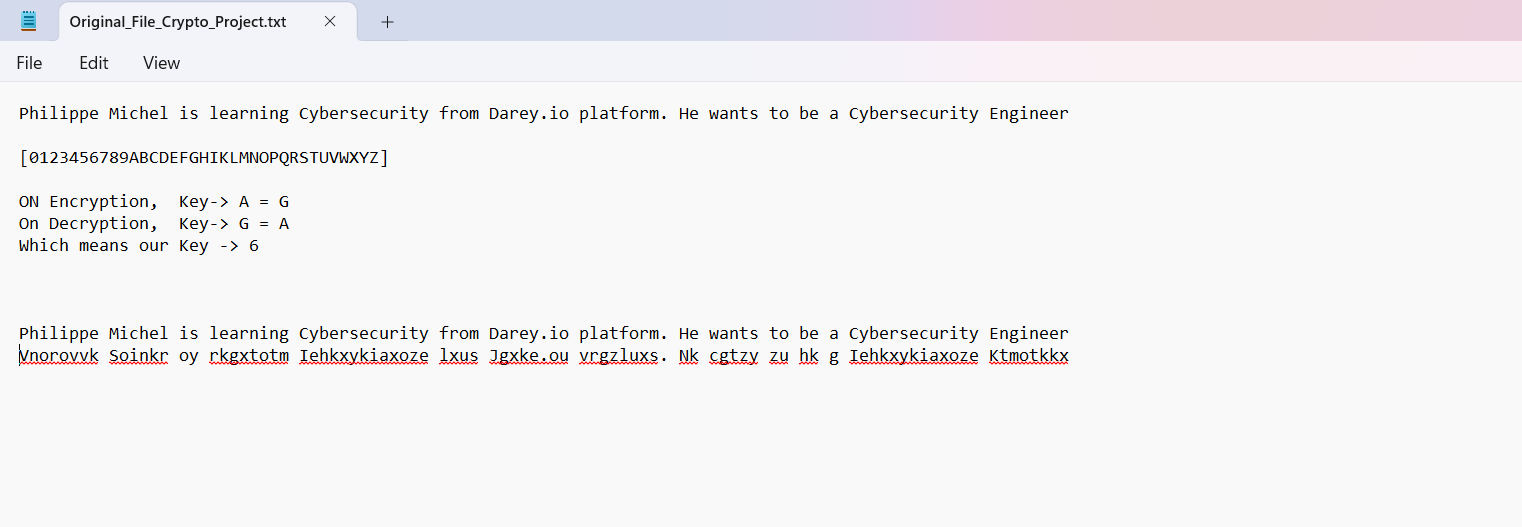
On Encryption, Key - > A = G

On Decryption, Key -> G = A

From the Alphanumeric above G is 6 shifts from A which means our Key -> 6 for this project.

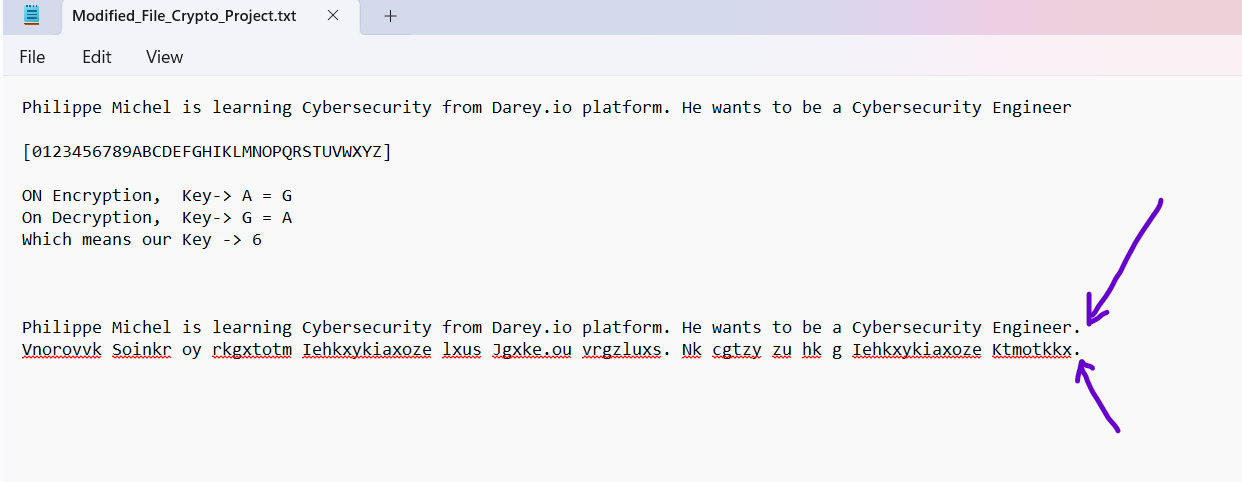
The original text of my choice is the following:  
Philippe Michel is learning Cybersecurity from Darey.io platform. He wants to be a Cybersecurity Engineer

The ciphertext is the following:  
Vnorovvk Soinkr oy rkgxtotm Iehkxykiaxoze lxus Jgxke.ou vrgzluxs. Nk cgtzy zu hk g Iehkxykiaxoze Ktmotkkx



In the Modified file, I added a dot at the end of the text after “Engineer”:

Philippe Michel is learning Cybersecurity from Darey.io platform. He wants to be a Cybersecurity Engineer.

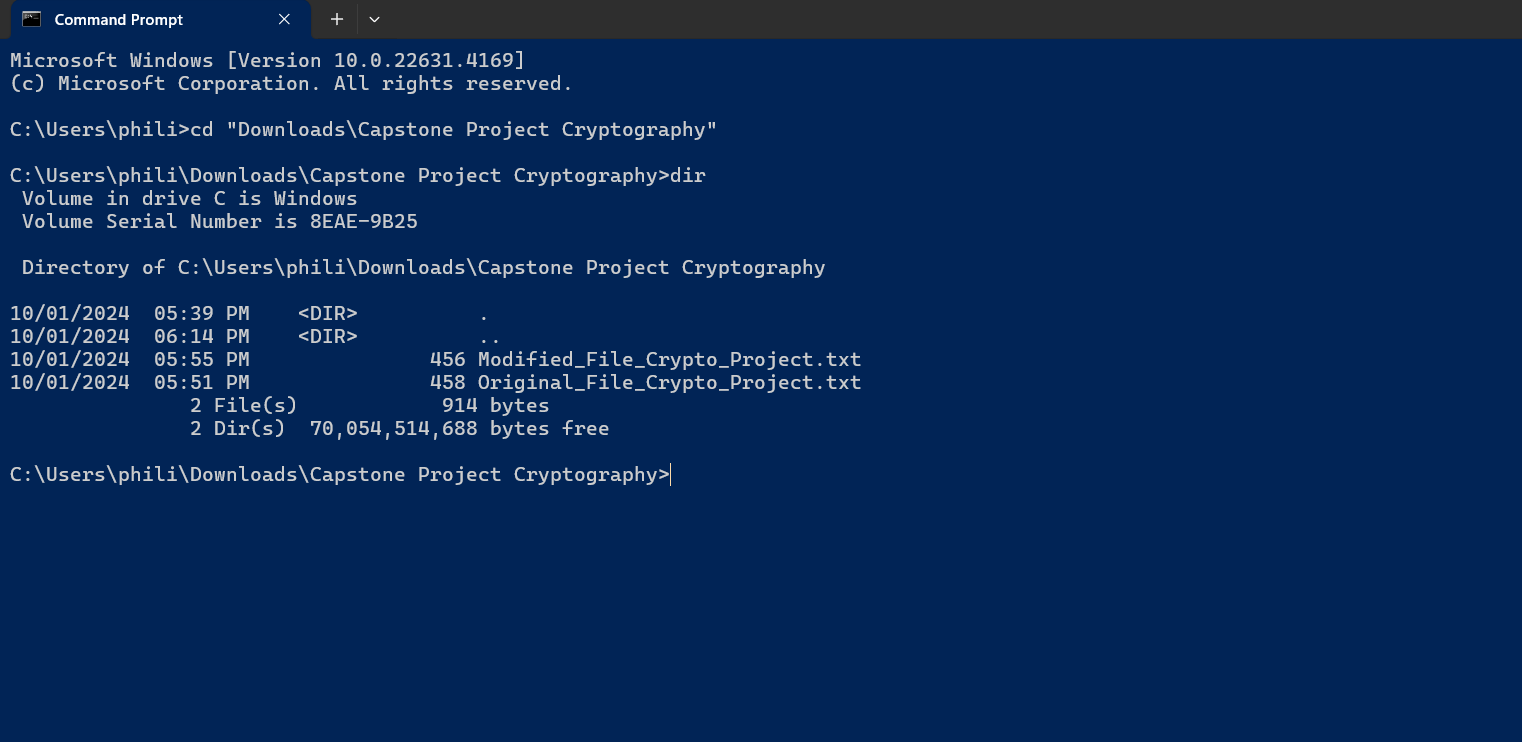


2) **Navigating to the Directory Containing the Files**

Screenshot of the location of both Original and Modified text files:

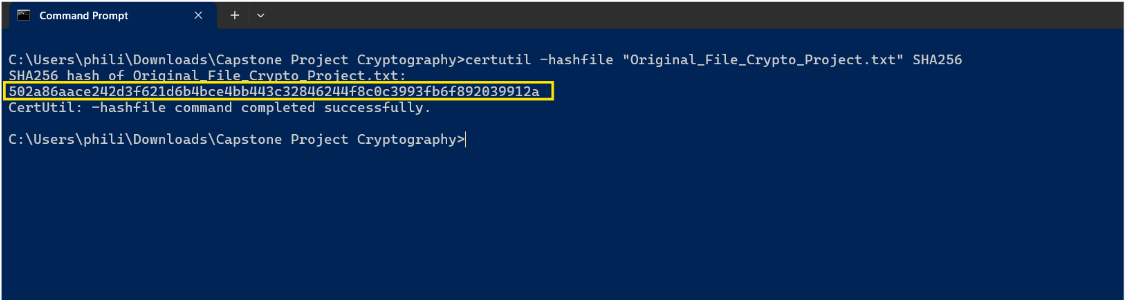
C:\Users\phili\Downloads\Capstone Project Cryptography\Original\_File\_Crypto\_Project.txt

C:\Users\phili\Downloads\Capstone Project Cryptography\ Modifified\_File\_Crypto\_Project.txt

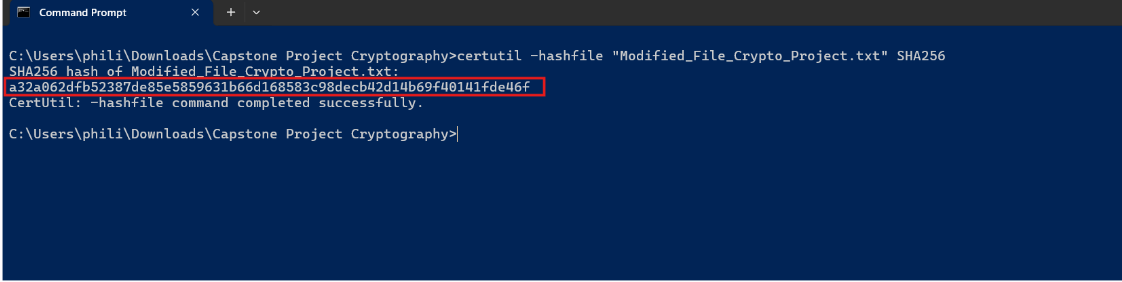


**3) Running the SHA256 Checksum Computation**

C:\Users\phili\Downloads\Capstone Project Cryptography> certutil -hashfile “Original\_File\_Crypto\_Project.txt” SHA256

When running this command, the SHA256 Hash value of the “original” text generates the following value highlighted in yellow:

C:\Users\phili\Downloads\Capstone Project Cryptography> certutil -hashfile “Modified\_File\_Crypto\_Project.txt” SHA256

Running that command, the SHA256 Hash value of the “Modified” text generates the following value highlighted in red:

According to CIA triad standards, we can conclude that a little modification from a text/file does completely change the entire value after running SHA256 command. This proves how cryptography can detect when the integrity of a data has been changed, altered or corrupted.