TECHCRUSH CAPSTONE PROJECT

CAPSTONE PROJECT TOPIC 3 APPYING CRYPTOGRAPHY IN REAL-WORLD SCENARIOS

CAPSTONE PROJECT

Group 9

Team Members

1. ONONOGBU DANIELLA IHEOMA
2. .OGOOLUWA DARASIMI OLUWALOSEYIFUMI
3. CHIMEZIE FEDINARD LIVINUS
4. AKUJOBI FORTUNE CHIWUIKEM
5. TOWOLAWI DANIEL OLAMIDE
6. OJO DAMILARE
7. AGUBOR CLINTON
8. COLLINS KWADWO SENA SABLAH
9. CHUKWUEBUKA CHIKA

Outline

- Aim and Objective
- Methodology
  - Concept of project
  - Tools Used
- Conclusion
- References

Aim and Objective

The aim of this project is to demonstrate the practical application of cryptography in securing data and communication in real world cybersecurity scenarios.

Objectives

To apply symmetric encryption (AES) to protect data confidentiality
To use cryptographic hashing to verify data integrity
To implement asymmetric encryption (RSA) for secure communication
To understand how cryptographic tools are used in real-world systems

Concept of the Project

- Cryptography is a core component of cybersecurity used to protect information from unauthorized access, alteration, or impersonation. This project explores three major cryptographic concepts:
- Symmetric Encryption for protecting data using a shared secret
- Hashing for verifying data integrity and detecting tampering
- Asymmetric Encryption for secure communication using public and private keys
- These techniques collectively ensure the confidentiality, integrity, and authenticity of information in modern digital systems.

METHODOLOGY

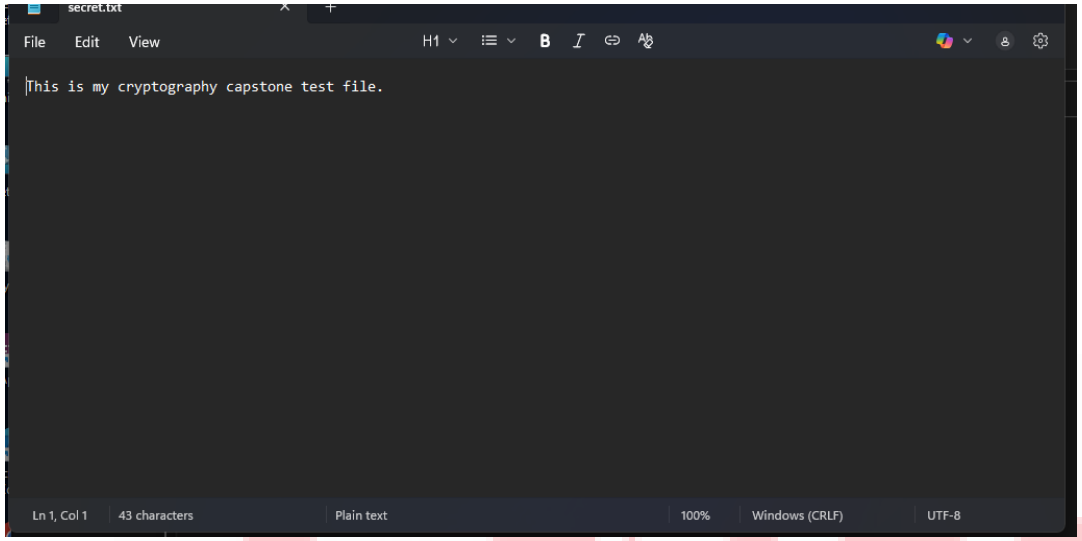
- The project was carried out using a hands on, command line based approach with OpenSSL. The following steps were **f**ollowed**:**

- **Step 1: Symmetric Encryption (AES**)
- A plaintext file (secret.txt) was created.
- The file was encrypted using AES-256-CBC.
- The encrypted file was decrypted using the same password.
- Commands Used:

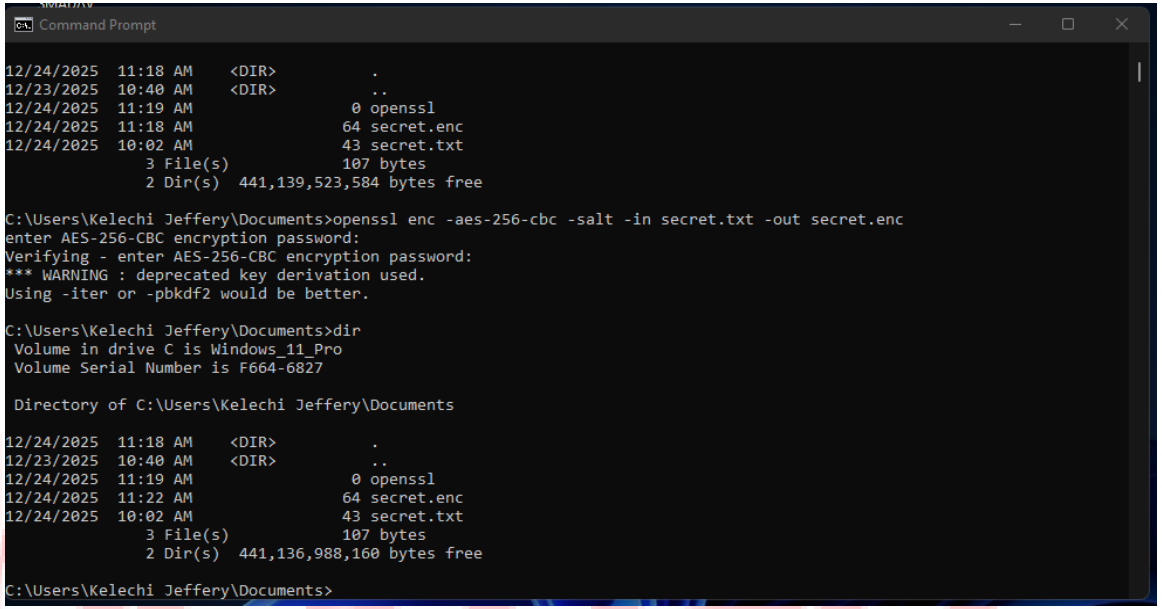
For Encryption; **openssl enc-aes-256-salt-in secret.txt-out secret.enc**

For Decryption;**openssssl-enc-aes-256-cbc-d-in-secret.enc-out decrypted.txt**

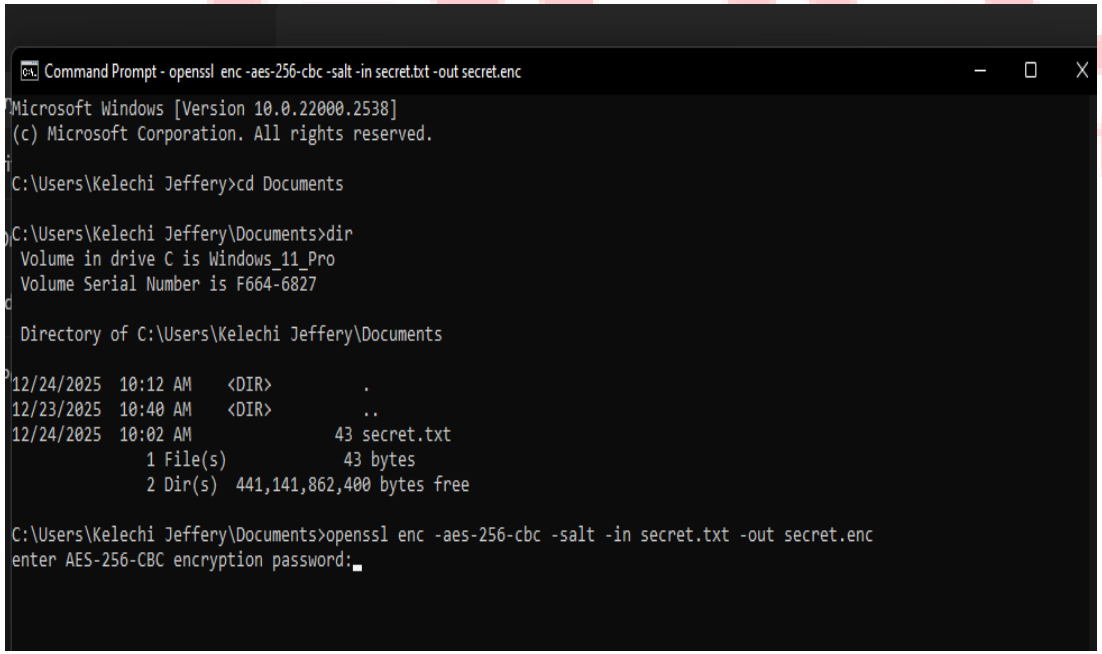
Plaintext file before encryption



Encrypted file (secret.enc)

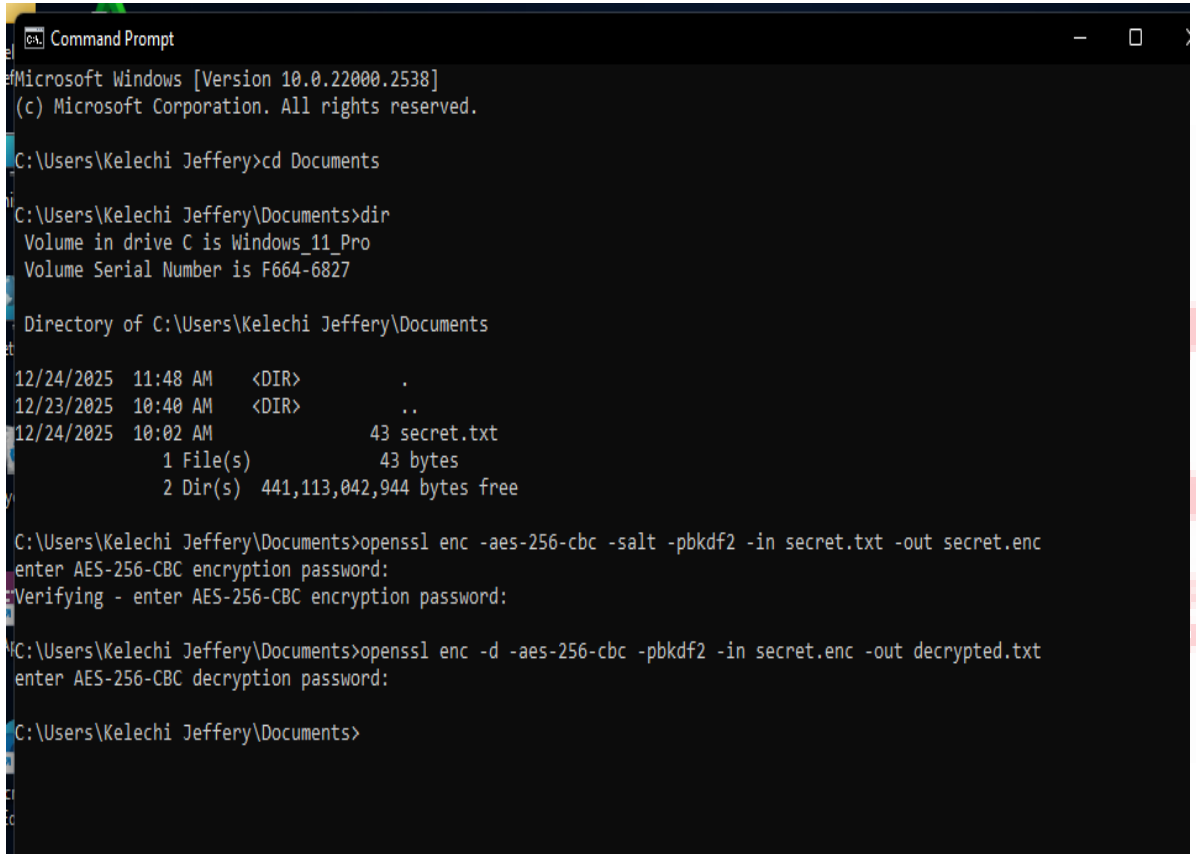


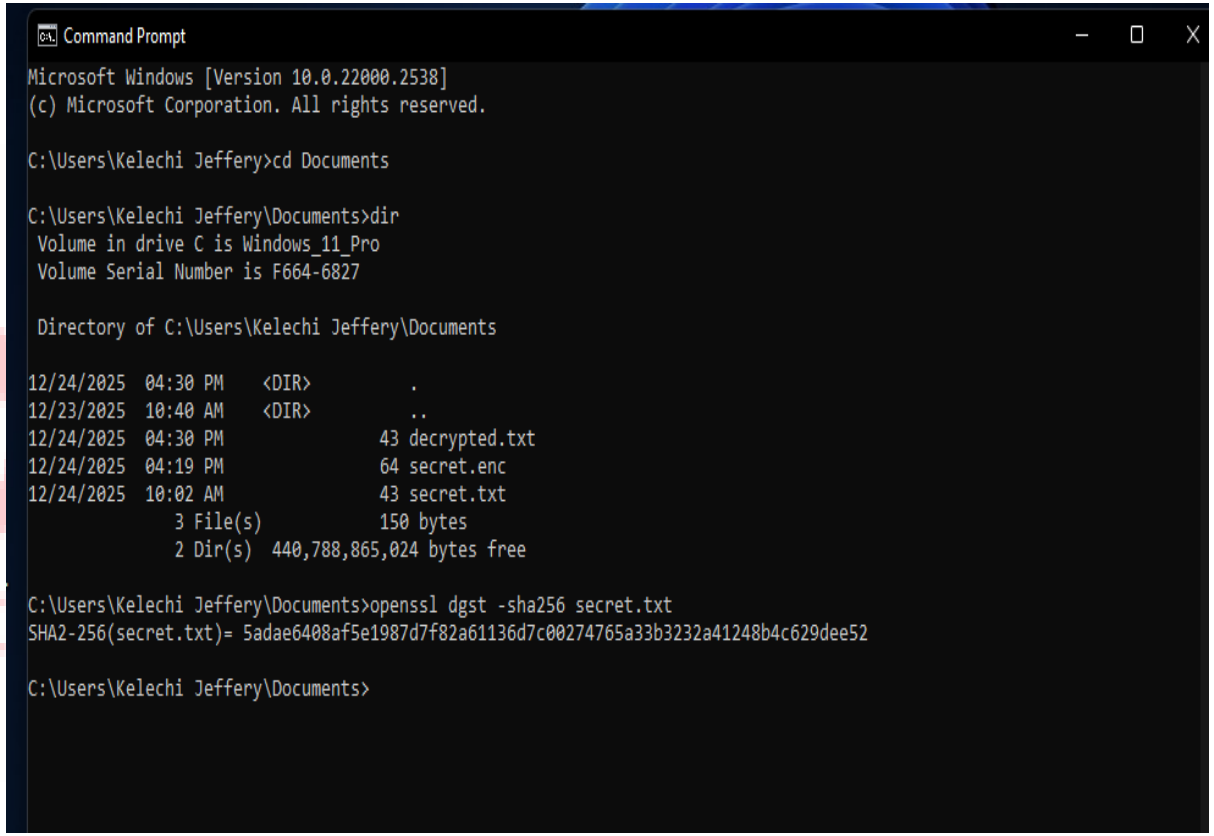
AES encryption command execution



CAPSTONE PROJECT

TechCrush
turning tech dreams into reality

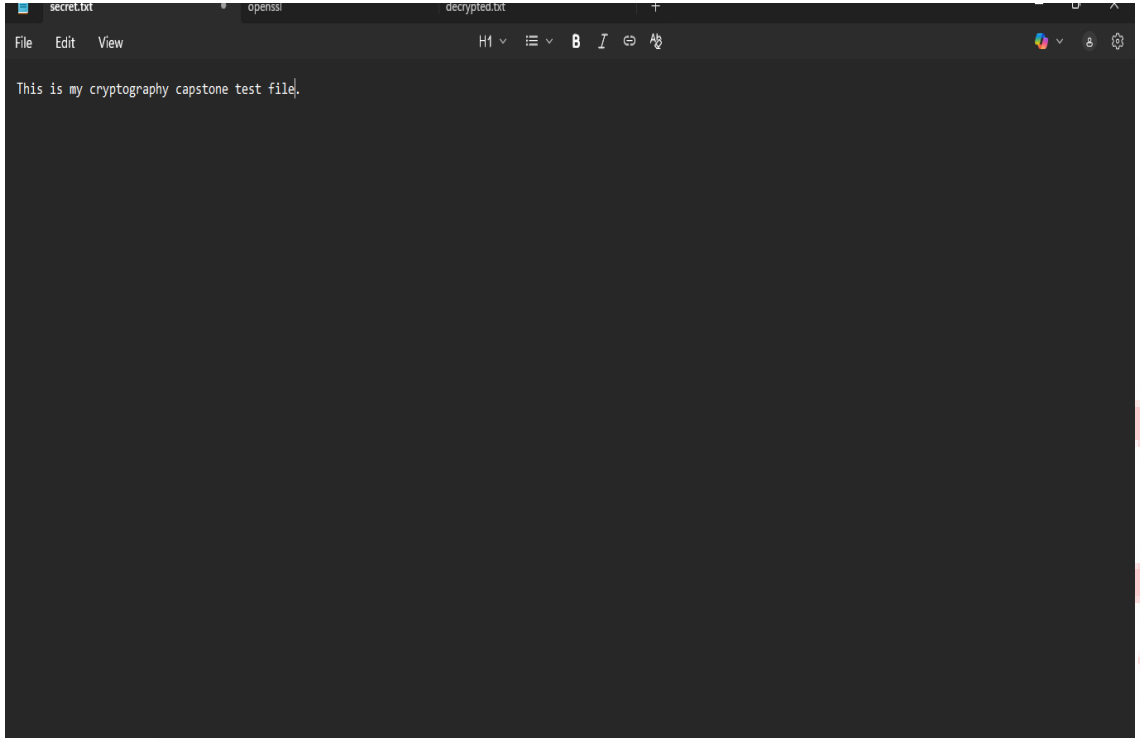


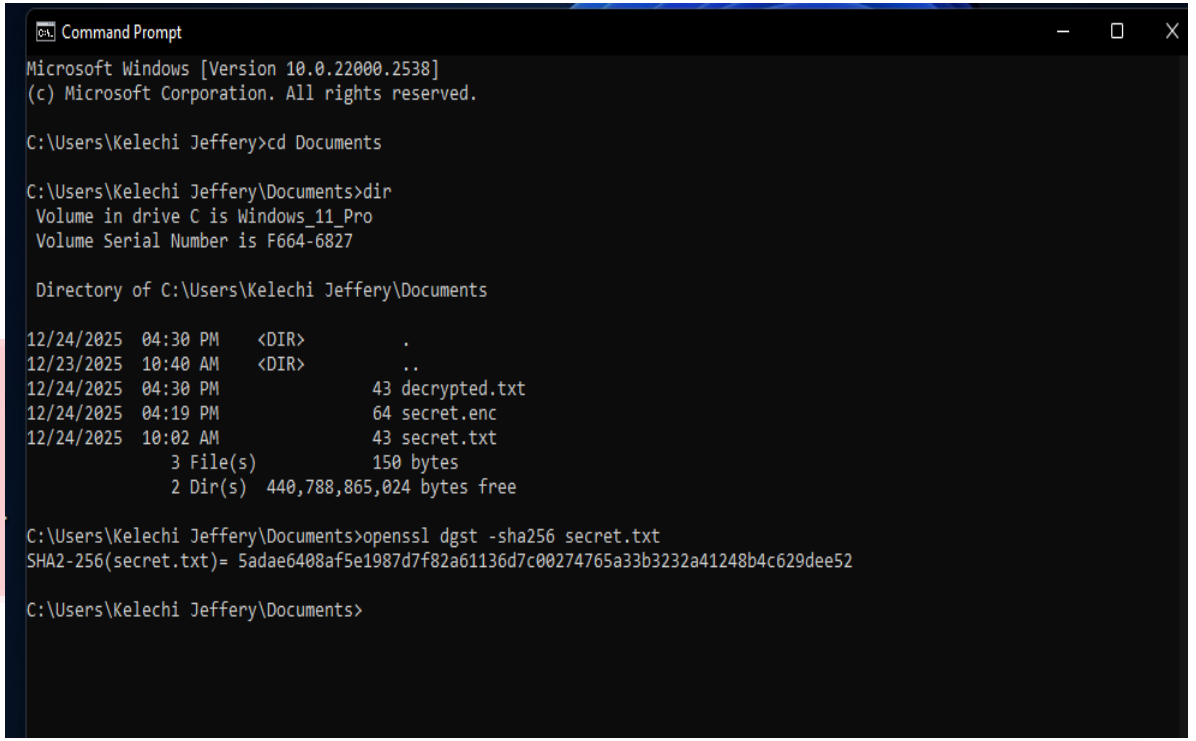


Decrypted output file

- **Step 2: Hashing and Integrity Checking**
- **A SHA-256 hash was generated for the original file.**
- **The file was modified slightly.**
- **A new hash was generated to show how the hash value changes.**
- **Command Used:**
- ***openssl dgst -sha256 secret.txt***

CAPSTONE PROJECT

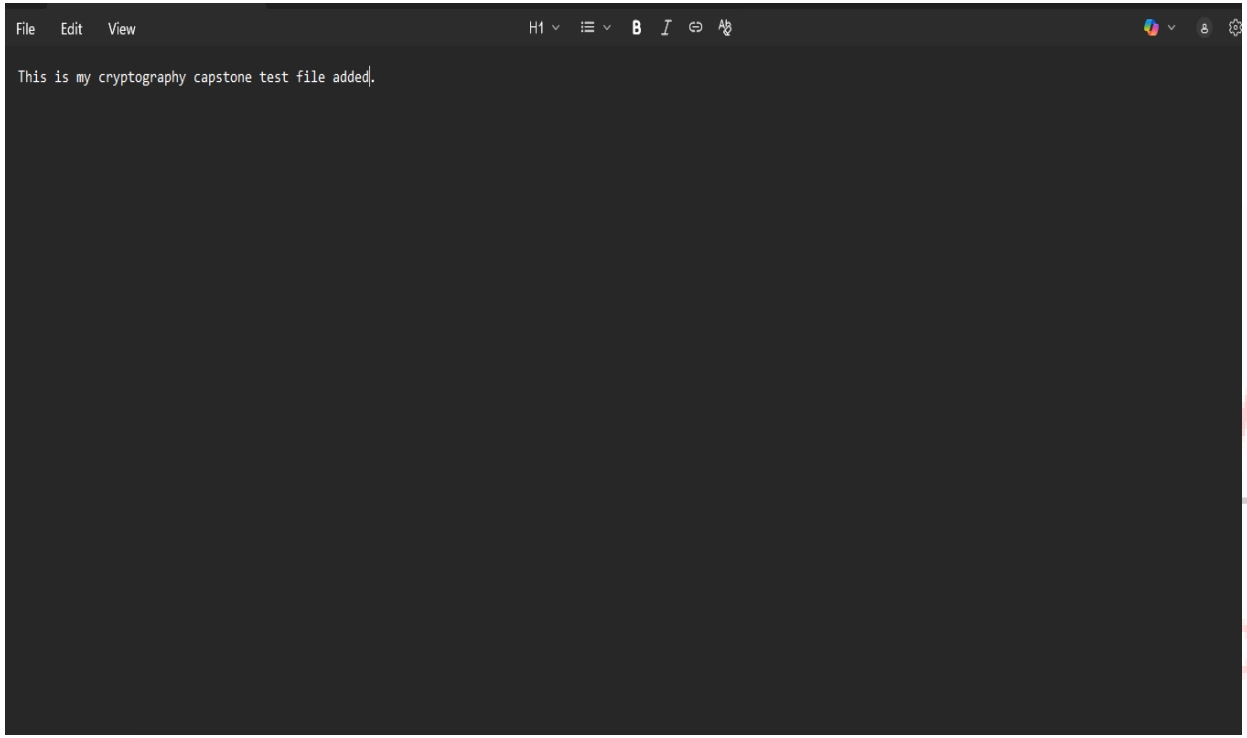




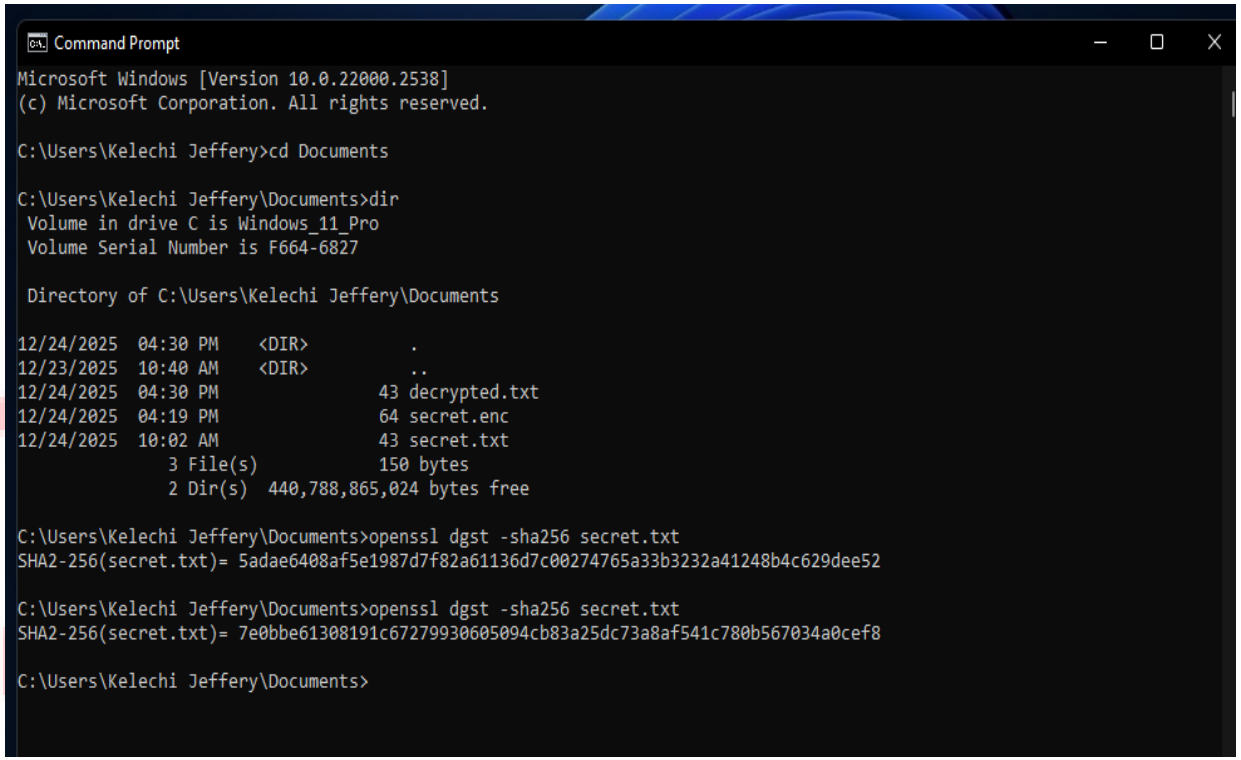
The hash value of the file secret.txt

CAPSTONE PROJECT

TechCrush
turning tech dreams into reality



Modified file



Hash value of the modified file

Step 3: Asymmetric Encryption (RSA – Public and Private Keys)
A private key was generated.
A public key was extracted from the private key.
A message was encrypted using the public key.
The encrypted message was decrypted using the private key.
Commands Used:

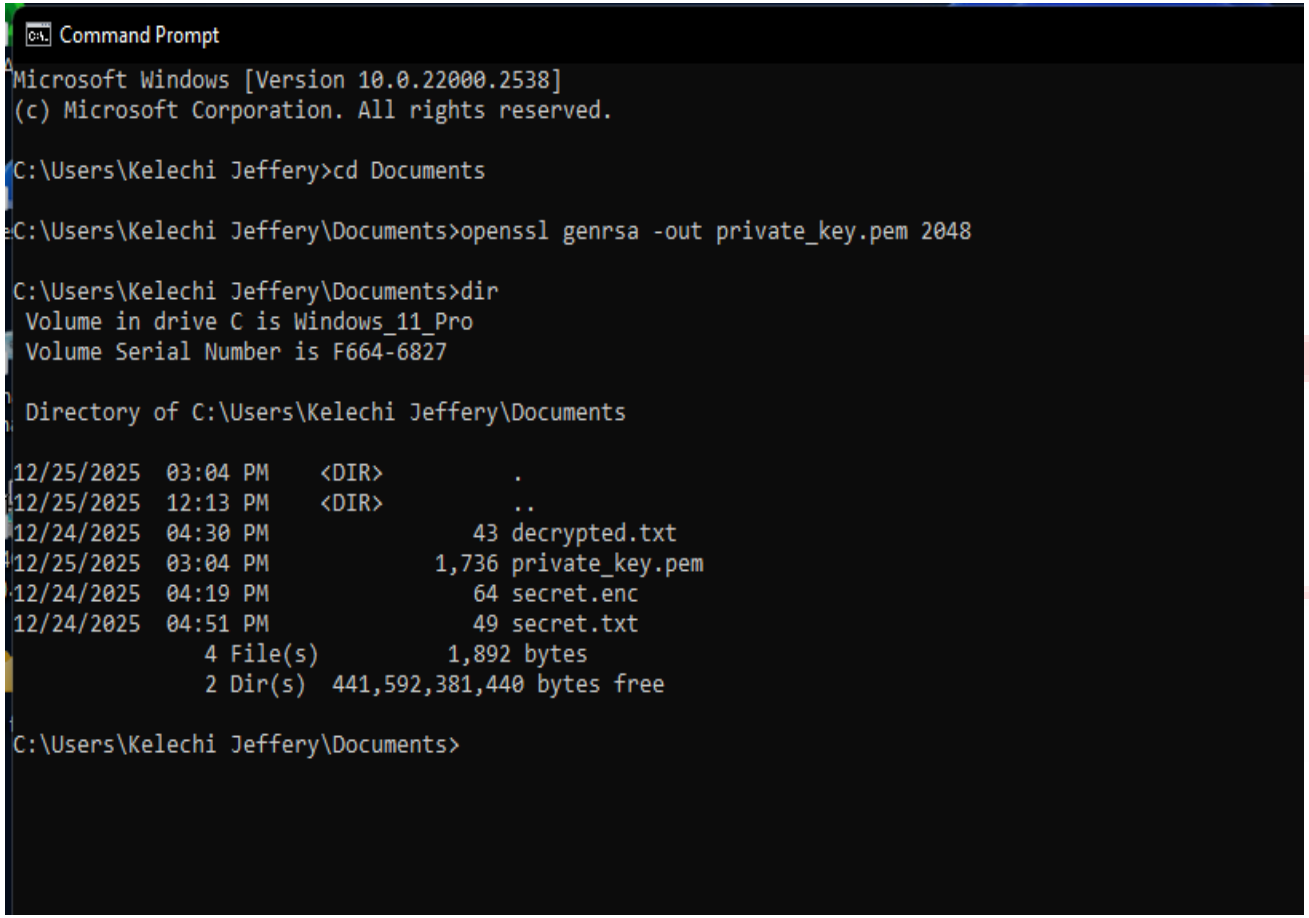
To create private key - *openssl genrsa -out private_key.pem 2048*
To create public key - *openssl rsa -in private_key.pem -pubout -out public_key.pem*

To encrypt using public key - *openssl pkeyutl -encrypt -pubin -inkey public_key.pem -in message.txt -out encrypted_message.bin*

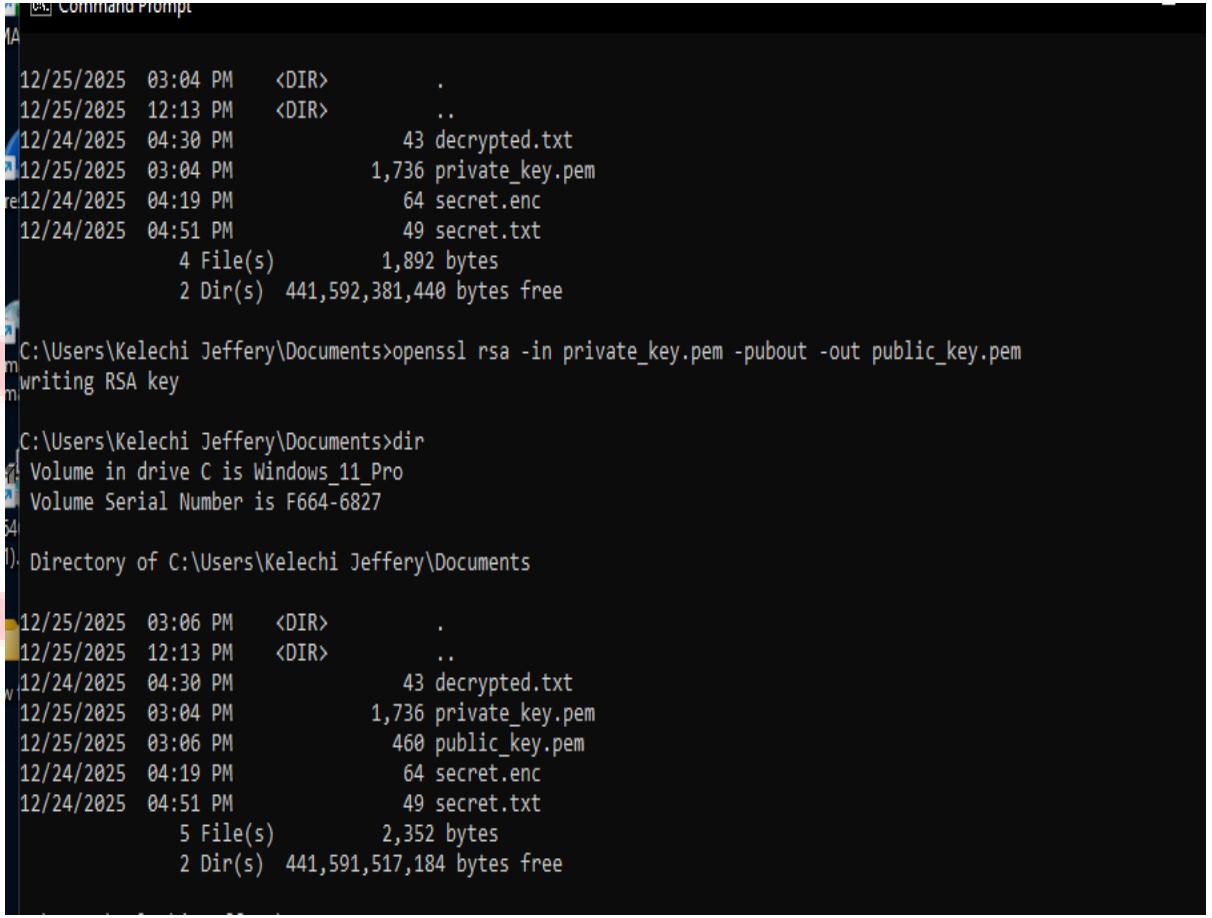
To decrypt using private key - openssl pkeyutl -decrypt -inkey private_key.pem -in encrypted_message.bin -out decrypted_message.txt

CAPSTONE PROJECT

TechCrush
turning tech dreams into reality



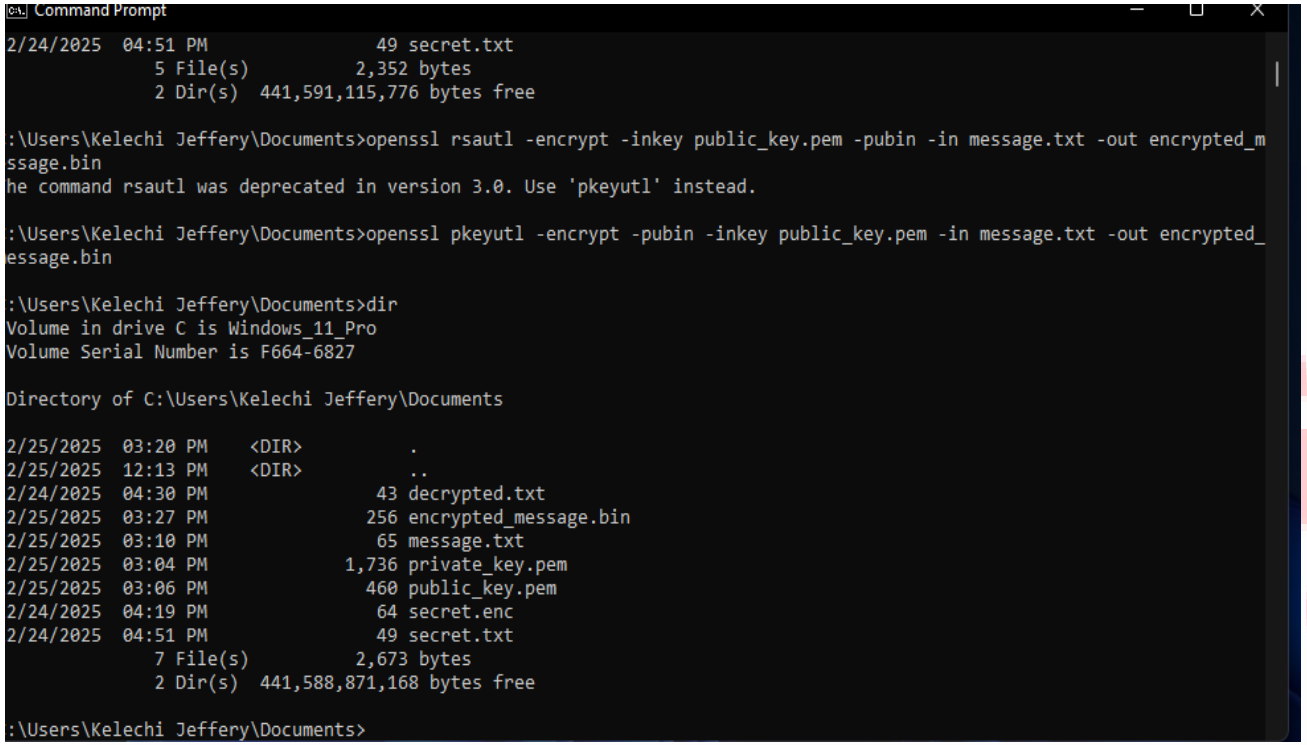
Creation of Private Key

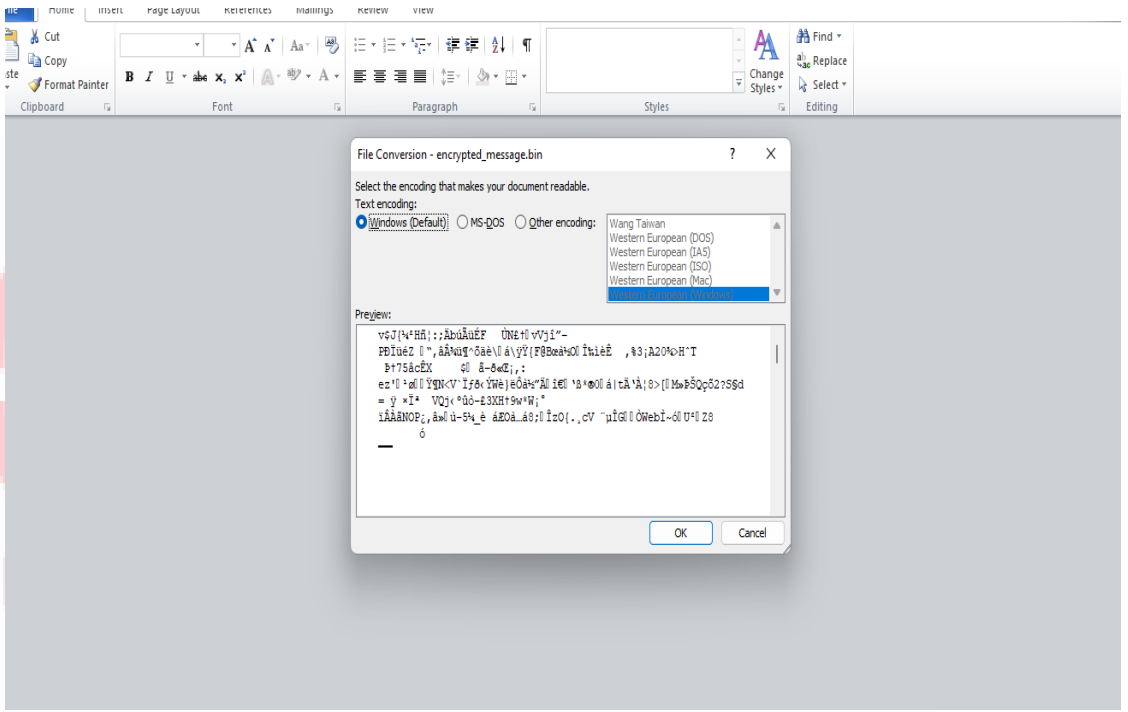


Creation of Public Key

CAPSTONE PROJECT

TechCrush
turning tech dreams into reality

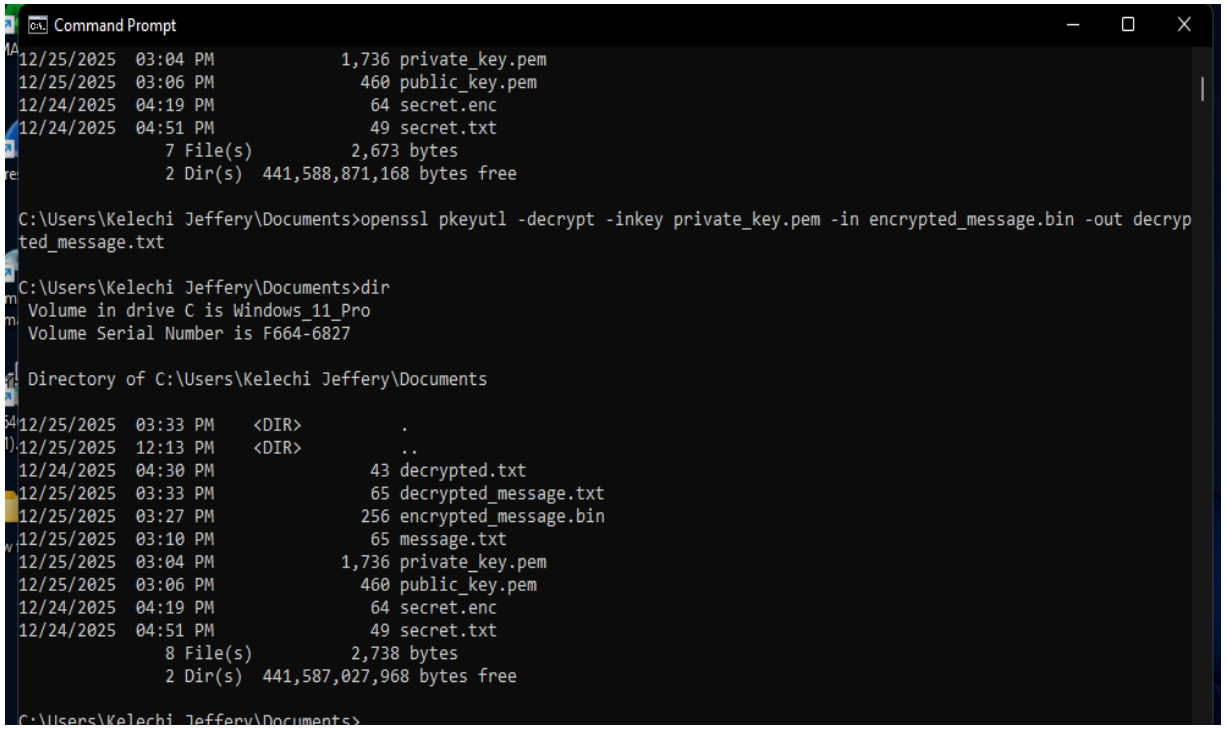


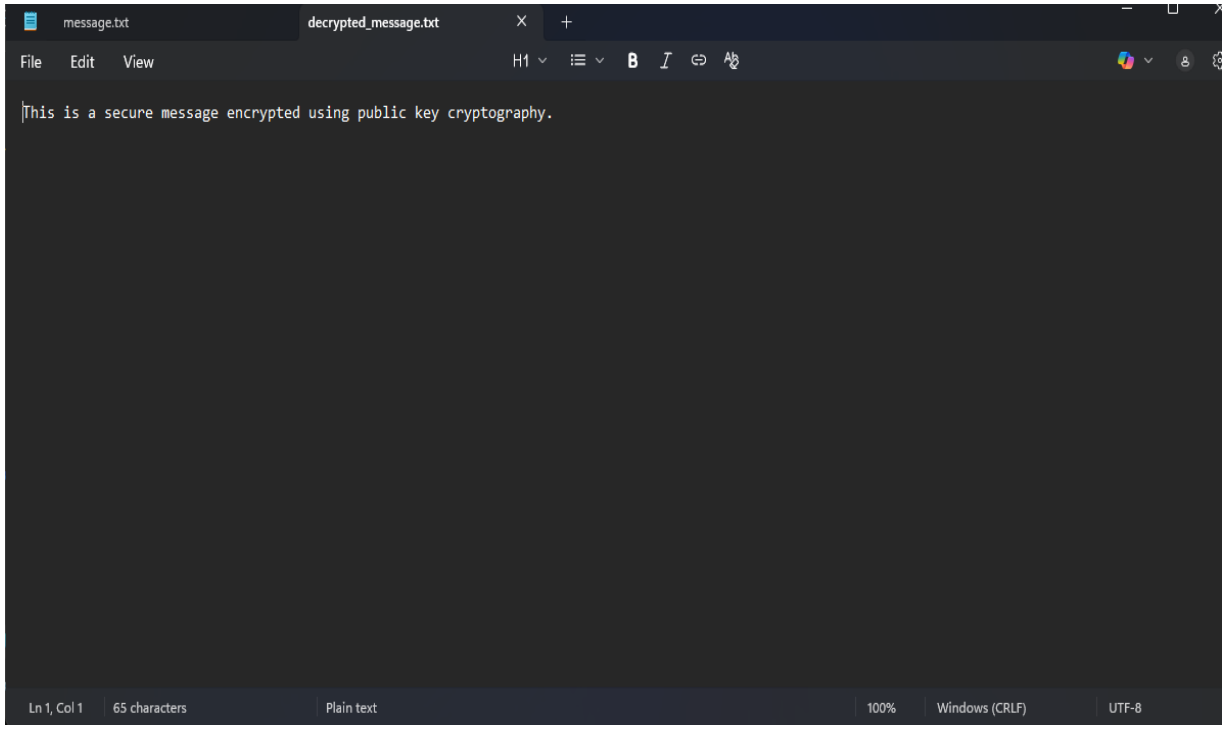


Encryption of the txt. file using public key

CAPSTONE PROJECT

TechCrush
turning tech dreams into reality





Decryption of the .txt file using the private key

Tools Used

- **OpenSSL – For encryption, decryption, hashing, and key generation**
- **Command Prompt (Windows) – To execute cryptographic commands**
- **Text Editor (Notepad / Microsoft Word) – To create and edit text files**

Conclusion

This project provided practical experience in applying cryptographic techniques to real-world cybersecurity problems. Through symmetric encryption, hashing, and asymmetric encryption, the project demonstrated how cryptography protects data confidentiality, ensures integrity, and enables secure communication. The hands-on approach enhanced understanding of how cryptographic tools are used in modern systems.

References

- OpenSSL Documentation – https://www.openssl.org/docs/
- NIST Cryptographic Standards – https://www.nist.gov/cryptography
- TechCrush Cybersecurity Training Materials

THANK YOU