

# TECHCRUSH CAPSTONE PROJECT

## CAPSTONE PROJECT TOPIC 3

### APPYING CRYPTOGRAPHY IN REAL- WORLD SCENARIOS

## 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.

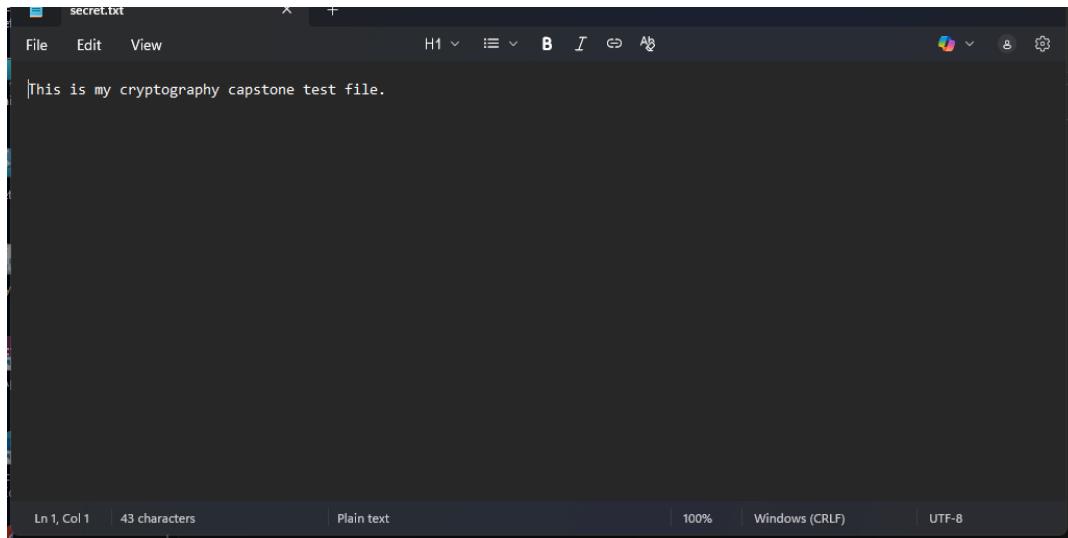
## METHODOLOGY

- The project was carried out using a hands on, command line based approach with OpenSSL. The following steps were followed:
  - **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;**openssl-enc-aes-256-cbc-d-in-secret.enc-out decrypted.txt**

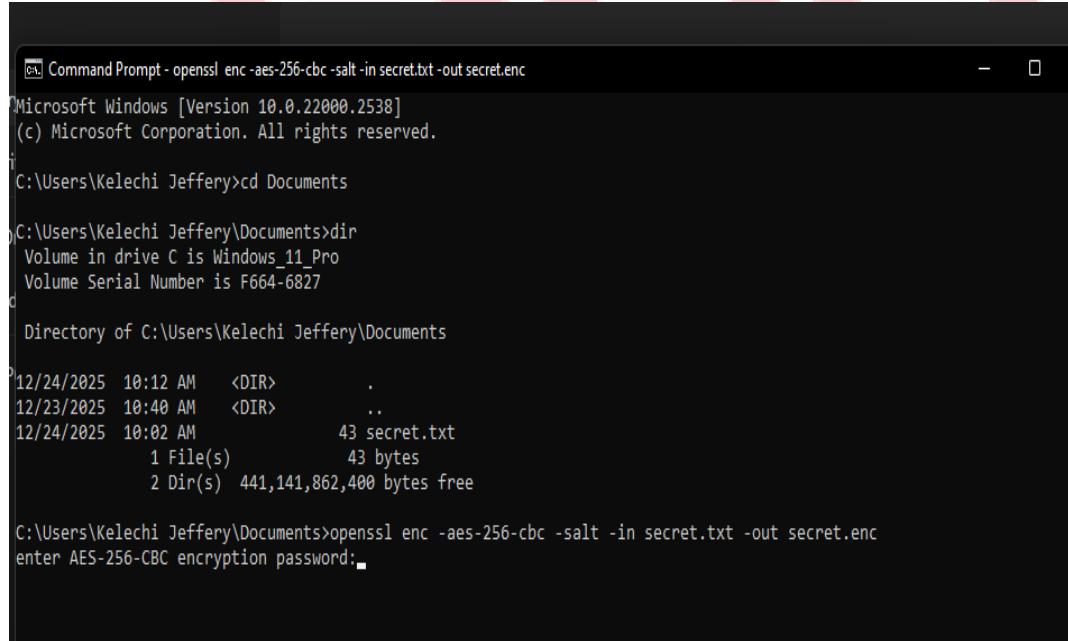
## Plaintext file before encryption



This is my cryptography capstone test file.

Ln 1, Col 1 | 43 characters | Plain text | 100% | Windows (CRLF) | UTF-8

## AES encryption command execution



```
openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kelechi Jeffery>cd Documents

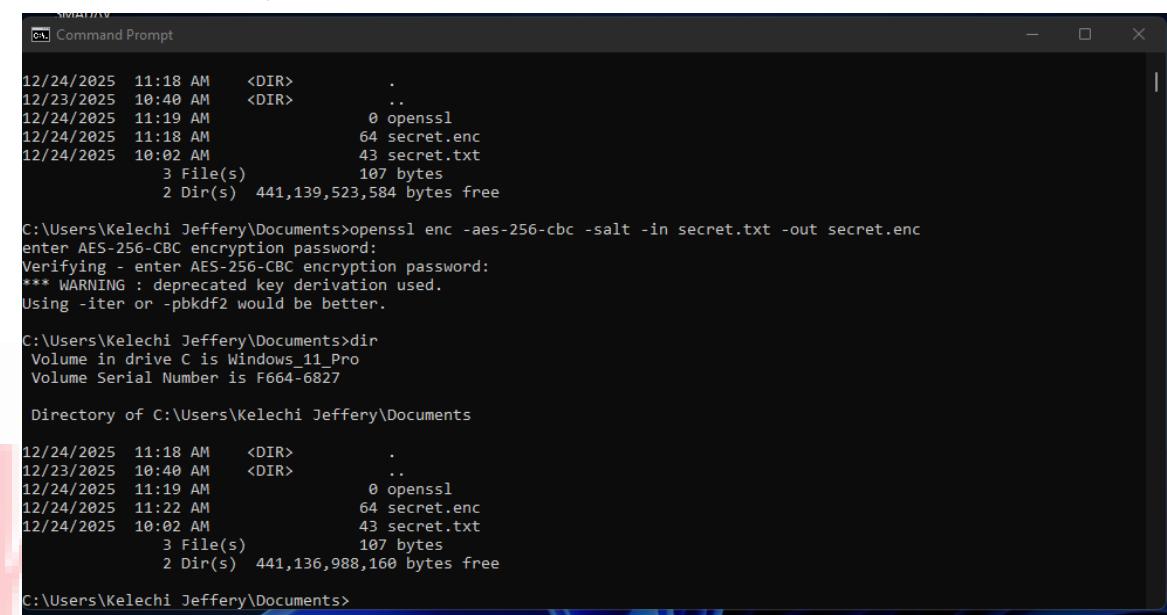
C:\Users\Kelechi Jeffery\Documents>dir
Volume in drive C is Windows_11_Pro
Volume Serial Number is F664-6827

Directory of C:\Users\Kelechi Jeffery\Documents

12/24/2025 10:12 AM <DIR> .
12/23/2025 10:40 AM <DIR> ..
12/24/2025 10:02 AM 43 secret.txt
1 File(s) 43 bytes
2 Dir(s) 441,141,862,400 bytes free

C:\Users\Kelechi Jeffery\Documents>openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc
enter AES-256-CBC encryption password:
```

## Encrypted file (secret.enc)



```
openssl
.
..
0 openssl
64 secret.enc
43 secret.txt
3 File(s) 107 bytes
2 Dir(s) 441,139,523,584 bytes free

C:\Users\Kelechi Jeffery\Documents>openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

C:\Users\Kelechi Jeffery\Documents>dir
Volume in drive C is Windows_11_Pro
Volume Serial Number is F664-6827

Directory of C:\Users\Kelechi Jeffery\Documents

12/24/2025 11:18 AM <DIR> .
12/23/2025 10:40 AM <DIR> ..
12/24/2025 11:19 AM 0 openssl
12/24/2025 11:18 AM 64 secret.enc
12/24/2025 10:02 AM 43 secret.txt
3 File(s) 107 bytes
2 Dir(s) 441,136,988,160 bytes free

C:\Users\Kelechi Jeffery\Documents>
```

# CAPSTONE PROJECT

```
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kelechi Jeffery>cd Documents

C:\Users\Kelechi Jeffery\Documents>dir
Volume in drive C is Windows_11_Pro
Volume Serial Number is F664-6827

Directory of C:\Users\Kelechi Jeffery\Documents

12/24/2025  11:48 AM    <DIR>      .
12/23/2025  10:40 AM    <DIR>      ..
12/24/2025  10:02 AM           43 secret.txt
                           1 File(s)   43 bytes
                           2 Dir(s)  441,113,042,944 bytes free

C:\Users\Kelechi Jeffery\Documents>openssl enc -aes-256-cbc -salt -pbkdf2 -in secret.txt -out secret.enc
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:

C:\Users\Kelechi Jeffery\Documents>openssl enc -d -aes-256-cbc -pbkdf2 -in secret.enc -out decrypted.txt
enter AES-256-CBC decryption password:

C:\Users\Kelechi Jeffery\Documents>
```

```
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kelechi Jeffery>cd Documents

C:\Users\Kelechi Jeffery\Documents>dir
Volume in drive C is Windows_11_Pro
Volume Serial Number is F664-6827

Directory of C:\Users\Kelechi Jeffery\Documents

12/24/2025  04:30 PM    <DIR>      .
12/23/2025  10:40 AM    <DIR>      ..
12/24/2025  04:30 PM           43 decrypted.txt
12/24/2025  04:19 PM           64 secret.enc
12/24/2025  10:02 AM           43 secret.txt
                           3 File(s)   150 bytes
                           2 Dir(s)  440,788,865,024 bytes free

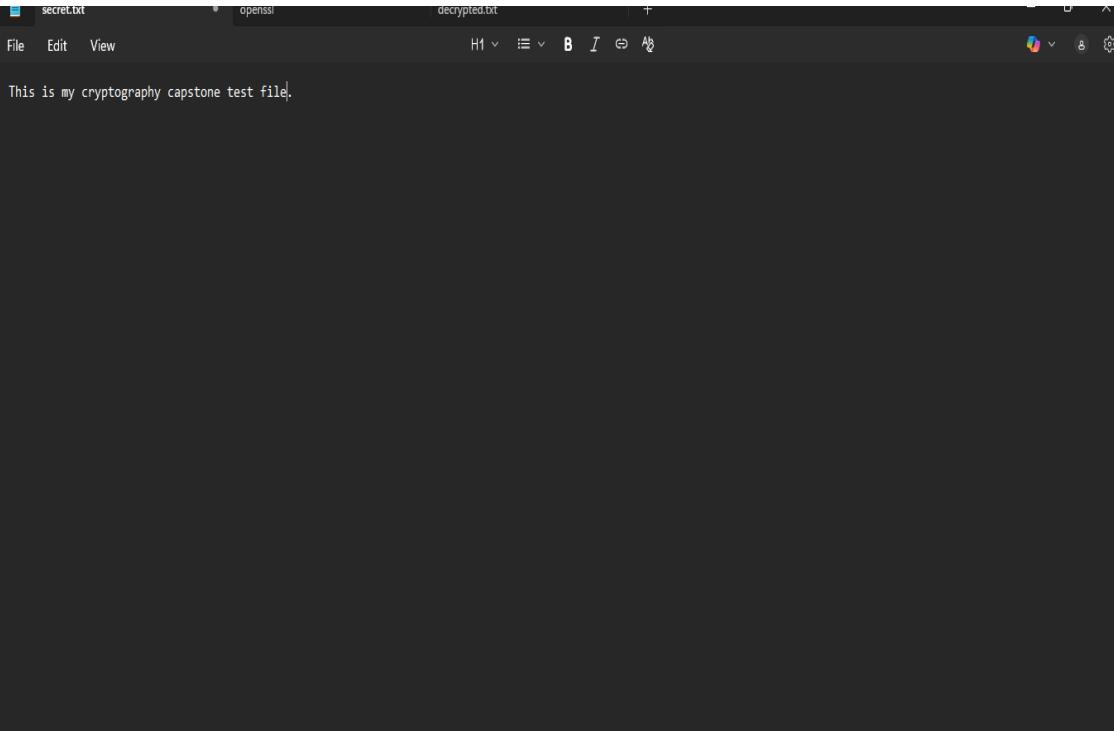
C:\Users\Kelechi Jeffery\Documents>openssl dgst -sha256 secret.txt
SHA2-256(secret.txt)= 5adae6408af5e1987d7f82a61136d7c00274765a33b3232a41248b4c629dee52

C:\Users\Kelechi Jeffery\Documents>
```

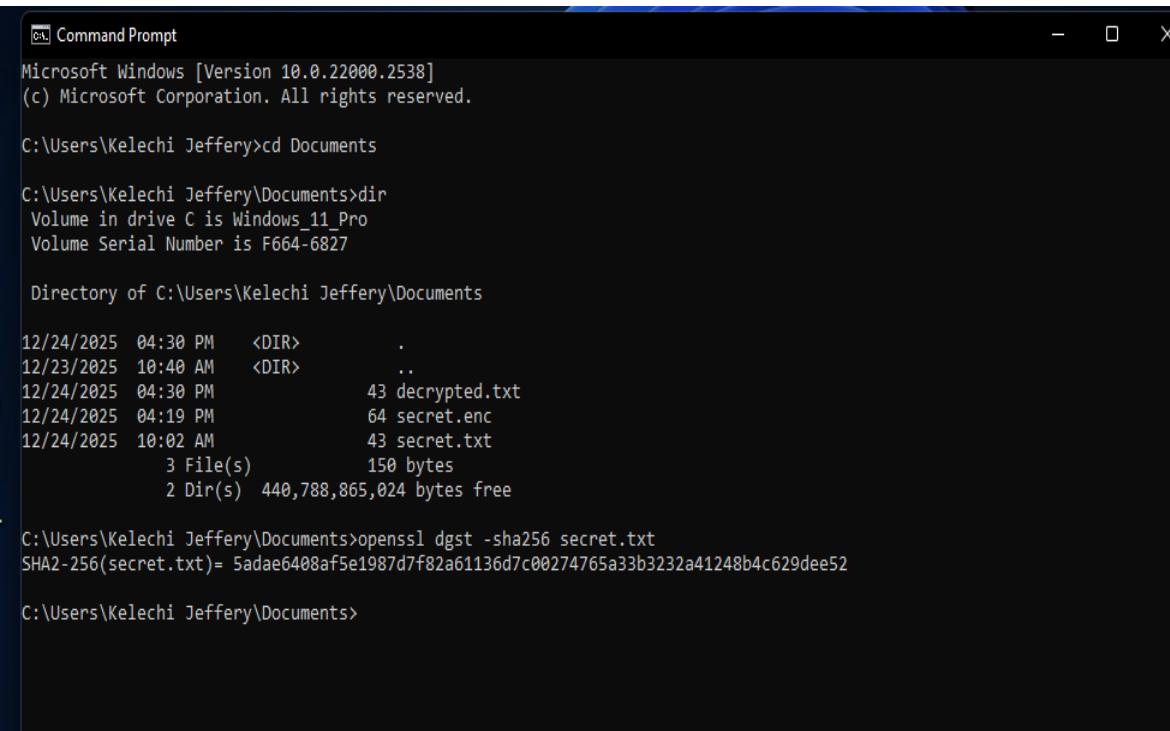
**Decrypted output file**

- 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



This is my cryptography capstone test file.



```
Command Prompt
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kelechi Jeffery>cd Documents

C:\Users\Kelechi Jeffery\Documents>dir
Volume in drive C is Windows_11_Pro
Volume Serial Number is F664-6827

Directory of C:\Users\Kelechi Jeffery\Documents

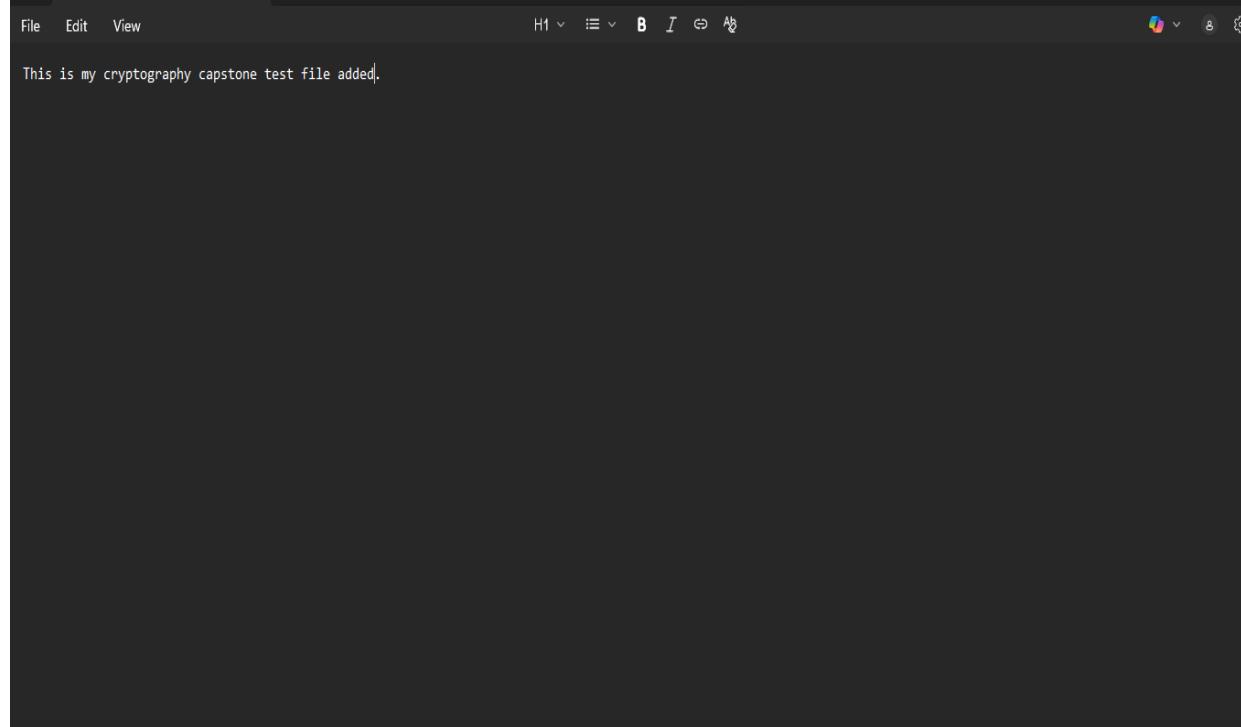
12/24/2025  04:30 PM    <DIR>      .
12/23/2025  10:40 AM    <DIR>      ..
12/24/2025  04:30 PM           43 decrypted.txt
12/24/2025  04:19 PM           64 secret.enc
12/24/2025  10:02 AM           43 secret.txt
                           3 File(s)     150 bytes
                           2 Dir(s)  440,788,865,024 bytes free

C:\Users\Kelechi Jeffery\Documents>openssl dgst -sha256 secret.txt
SHA2-256(secret.txt)= 5adae6408af5e1987d7f82a61136d7c00274765a33b3232a41248b4c629dee52

C:\Users\Kelechi Jeffery\Documents>
```

The hash value of the file secret.txt

# CAPSTONE PROJECT



```
Command Prompt
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kelechi Jeffery>cd Documents

C:\Users\Kelechi Jeffery\Documents>dir
Volume in drive C is Windows_11_Pro
Volume Serial Number is F664-6827

Directory of C:\Users\Kelechi Jeffery\Documents

12/24/2025  04:30 PM    <DIR>      .
12/23/2025  10:40 AM    <DIR>      ..
12/24/2025  04:30 PM            43 decrypted.txt
12/24/2025  04:19 PM            64 secret.enc
12/24/2025  10:02 AM            43 secret.txt
                           3 File(s)   150 bytes
                           2 Dir(s)  440,788,865,024 bytes free

C:\Users\Kelechi Jeffery\Documents>openssl dgst -sha256 secret.txt
SHA2-256(secret.txt)= 5adae6408af5e1987d7f82a61136d7c00274765a33b3232a41248b4c629dee52

C:\Users\Kelechi Jeffery\Documents>openssl dgst -sha256 secret.txt
SHA2-256(secret.txt)= 7e0bbe61308191c67279930605094cb83a25dc73a8af541c780b567034a0cef8

C:\Users\Kelechi Jeffery\Documents>
```

**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

```
Command Prompt
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Kelechi Jeffery>cd Documents

C:\Users\Kelechi Jeffery\Documents>openssl genrsa -out private_key.pem 2048

C:\Users\Kelechi Jeffery\Documents>dir
 Volume in drive C is Windows_11_Pro
 Volume Serial Number is F664-6827

 Directory of C:\Users\Kelechi Jeffery\Documents

12/25/2025  03:04 PM    <DIR>      .
12/25/2025  12:13 PM    <DIR>      ..
12/24/2025  04:30 PM          43 decrypted.txt
12/25/2025  03:04 PM          1,736 private_key.pem
12/24/2025  04:19 PM          64 secret.enc
12/24/2025  04:51 PM          49 secret.txt
                           4 File(s)       1,892 bytes
                           2 Dir(s)  441,592,381,440 bytes free

C:\Users\Kelechi Jeffery\Documents>
```

```
Command Prompt
12/25/2025  03:04 PM    <DIR>      .
12/25/2025  12:13 PM    <DIR>      ..
12/24/2025  04:30 PM          43 decrypted.txt
12/25/2025  03:04 PM          1,736 private_key.pem
12/24/2025  04:19 PM          64 secret.enc
12/24/2025  04:51 PM          49 secret.txt
                           4 File(s)       1,892 bytes
                           2 Dir(s)  441,592,381,440 bytes free

C:\Users\Kelechi Jeffery\Documents>openssl rsa -in private_key.pem -pubout -out public_key.pem
writing RSA key

C:\Users\Kelechi Jeffery\Documents>dir
 Volume in drive C is Windows_11_Pro
 Volume Serial Number is F664-6827

 Directory of C:\Users\Kelechi Jeffery\Documents

12/25/2025  03:06 PM    <DIR>      .
12/25/2025  12:13 PM    <DIR>      ..
12/24/2025  04:30 PM          43 decrypted.txt
12/25/2025  03:04 PM          1,736 private_key.pem
12/25/2025  03:06 PM          460 public_key.pem
12/24/2025  04:19 PM          64 secret.enc
12/24/2025  04:51 PM          49 secret.txt
                           5 File(s)       2,352 bytes
                           2 Dir(s)  441,591,517,184 bytes free
```

## Creation of Private Key

## Creation of Public Key

*Disclaimer: This training material belongs to techcrush and shouldn't be shared*

# CAPSTONE PROJECT

```
Command Prompt
2/24/2025 04:51 PM      49 secret.txt
      5 File(s)    2,352 bytes
      2 Dir(s) 441,591,115,776 bytes free

:\Users\Kelechi Jeffery\Documents>openssl rsautil -encrypt -inkey public_key.pem -pubin -in message.txt -out encrypted_message.bin
The command rsautil was deprecated in version 3.0. Use 'pkeyutl' instead.

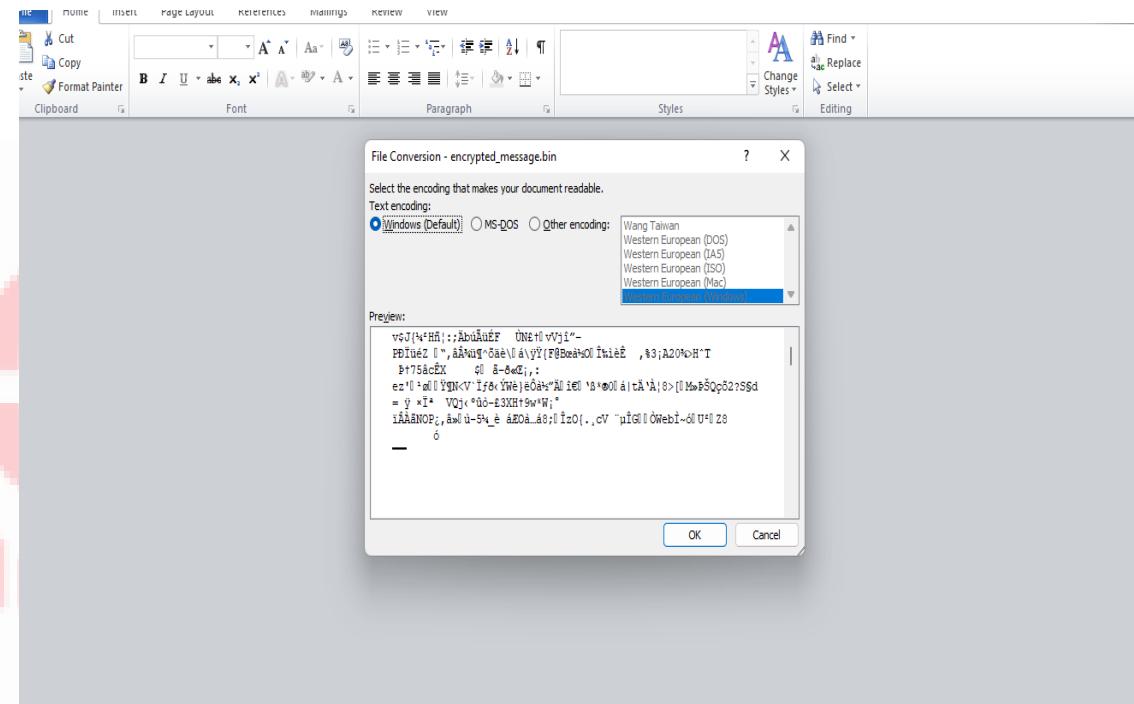
:\Users\Kelechi Jeffery\Documents>openssl pkeyutl -encrypt -pubin -inkey public_key.pem -in message.txt -out encrypted_message.bin

:\Users\Kelechi Jeffery\Documents>dir
Volume in drive C is Windows_11_Pro
Volume Serial Number is F664-6827

Directory of C:\Users\Kelechi Jeffery\Documents

2/25/2025 03:20 PM <DIR> .
2/25/2025 12:13 PM <DIR> ..
2/24/2025 04:30 PM      43 decrypted.txt
2/25/2025 03:27 PM      256 encrypted_message.bin
2/25/2025 03:10 PM      65 message.txt
2/25/2025 03:04 PM     1,736 private_key.pem
2/25/2025 03:06 PM      460 public_key.pem
2/24/2025 04:19 PM      64 secret.enc
2/24/2025 04:51 PM      49 secret.txt
      7 File(s)    2,673 bytes
      2 Dir(s) 441,588,871,168 bytes free

:\Users\Kelechi Jeffery\Documents>
```



## Encryption of the txt. file using public key

# CAPSTONE PROJECT

```
Command Prompt
12/25/2025 03:04 PM      1,736 private_key.pem
12/25/2025 03:06 PM      460 public_key.pem
12/24/2025 04:19 PM      64 secret.enc
12/24/2025 04:51 PM      49 secret.txt
              7 File(s)    2,673 bytes
              2 Dir(s)   441,588,871,168 bytes free

C:\Users\Kelechi Jeffery\Documents>openssl pkcs12 -inkey private_key.pem -in encrypted_message.bin -out decrypted_message.txt

C:\Users\Kelechi Jeffery\Documents>dir
Volume in drive C is Windows 11 Pro
Volume Serial Number is F664-6827

Directory of C:\Users\Kelechi Jeffery\Documents

12/25/2025 03:33 PM    <DIR>      .
12/25/2025 12:13 PM    <DIR>      ..
12/24/2025 04:30 PM      43 decrypted.txt
12/25/2025 03:33 PM      65 decrypted_message.txt
12/25/2025 03:27 PM      256 encrypted_message.bin
12/25/2025 03:10 PM      65 message.txt
12/25/2025 03:04 PM      1,736 private_key.pem
12/25/2025 03:06 PM      460 public_key.pem
12/24/2025 04:19 PM      64 secret.enc
12/24/2025 04:51 PM      49 secret.txt
              8 File(s)    2,738 bytes
              2 Dir(s)   441,587,027,968 bytes free

C:\Users\Kelechi Jeffery\Documents>
```

```
message.txt           decrypted_message.txt
File   Edit   View   H1   I   B   I   A
This is a secure message encrypted using public key cryptography.

Ln 1, Col 1  65 characters  Plain text  100%  Windows (CRLF)  UTF-8
```

**Decryption of the .txt file using the private key**

*Disclaimer: This training material belongs to techcrush and shouldn't be shared*

## 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