PROJECT BASED TASK

ASSIGNMENT

NAME : ***Ch.Vyshnavi***

BRANCH : **CSE**

REGD NO: **22PA1A0524**

SECTION : **A**

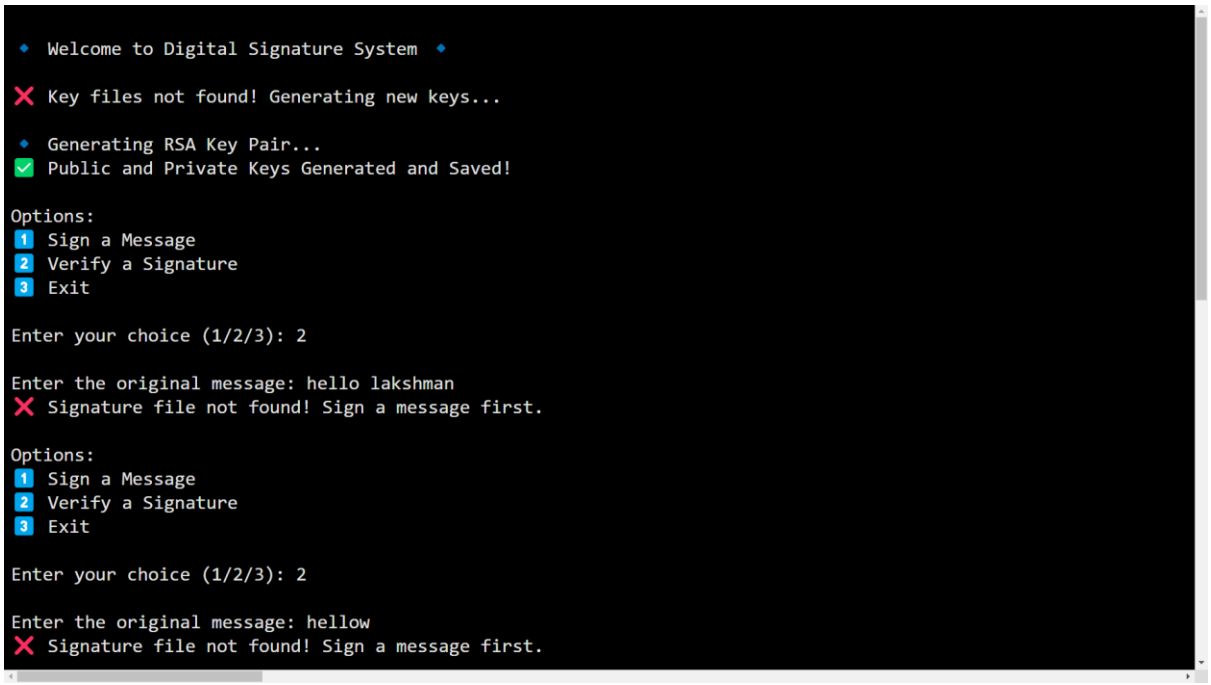
SUBJECT : **CNS**

GITHUB LINK:

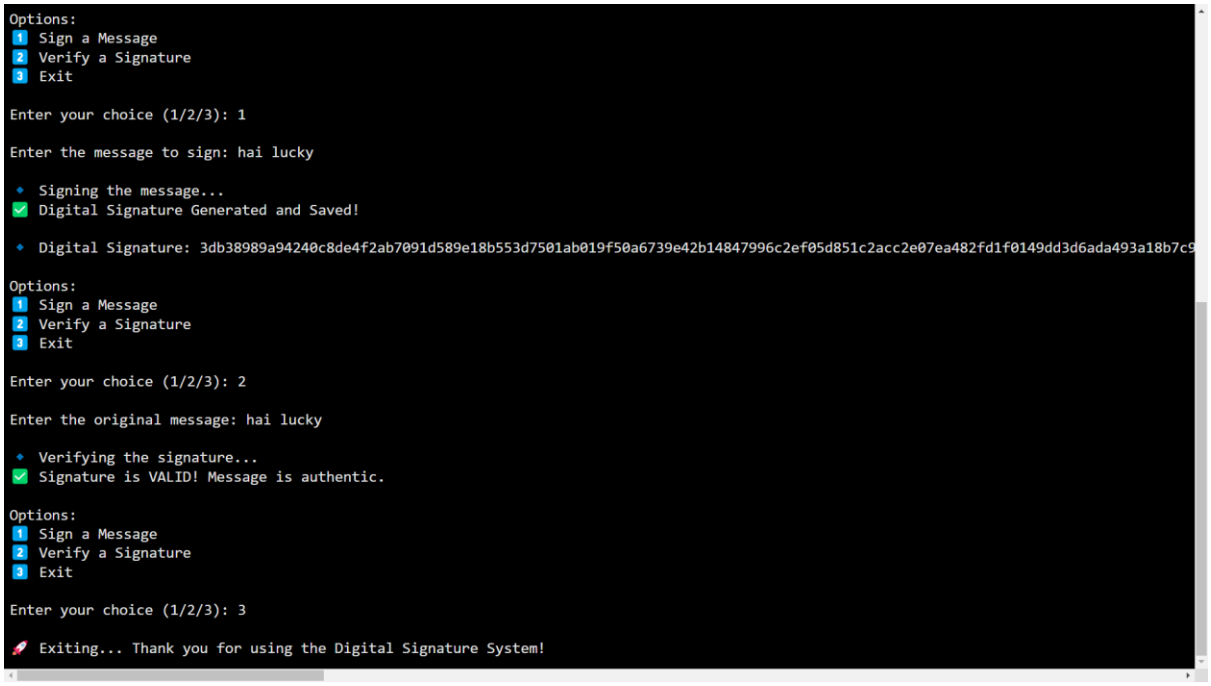
https://github.com/vyshu0111/CNS-Digital-signature-system

SCREENSHOTS OF OUTPUT:

SCREENSHOT -1



SCREENSHOT-2



📂 File Structure

```
$bash
$Copy
$Edit
📁 Digital-Signature-System/
|——Digital_signature_system.ipynb #Jupyter Notebook containing the digital signature system
|—— 📄 README.md
```

Usage

Generating RSA Keys

Upon the first execution of the program, it will automatically generate and save both the public and private RSA keys in PEM format.

Signing a Message

To sign a message, follow these steps:

1. Run the digital_signature.py script.
2. Select the option "1️⃣ Sign a Message" from the menu.
3. Enter the message you wish to sign (e.g., "Hello, Secure World!").
4. The program will generate a digital signature for the entered message and save it to signature.txt.

Verifying a Signature

To verify a signature, follow these steps:

1. Run the digital_signature.py script.
2. Select the option "2️⃣ Verify a Signature" from the menu.
3. Enter the original message that was signed.
4. The program will check if the signature stored in signature.txt is valid for the entered message.