Delivery for Data Engineering 2, Assignment 1

Myitzu: ID 2300350

David: ID 2302806

a. Key Generation Command:

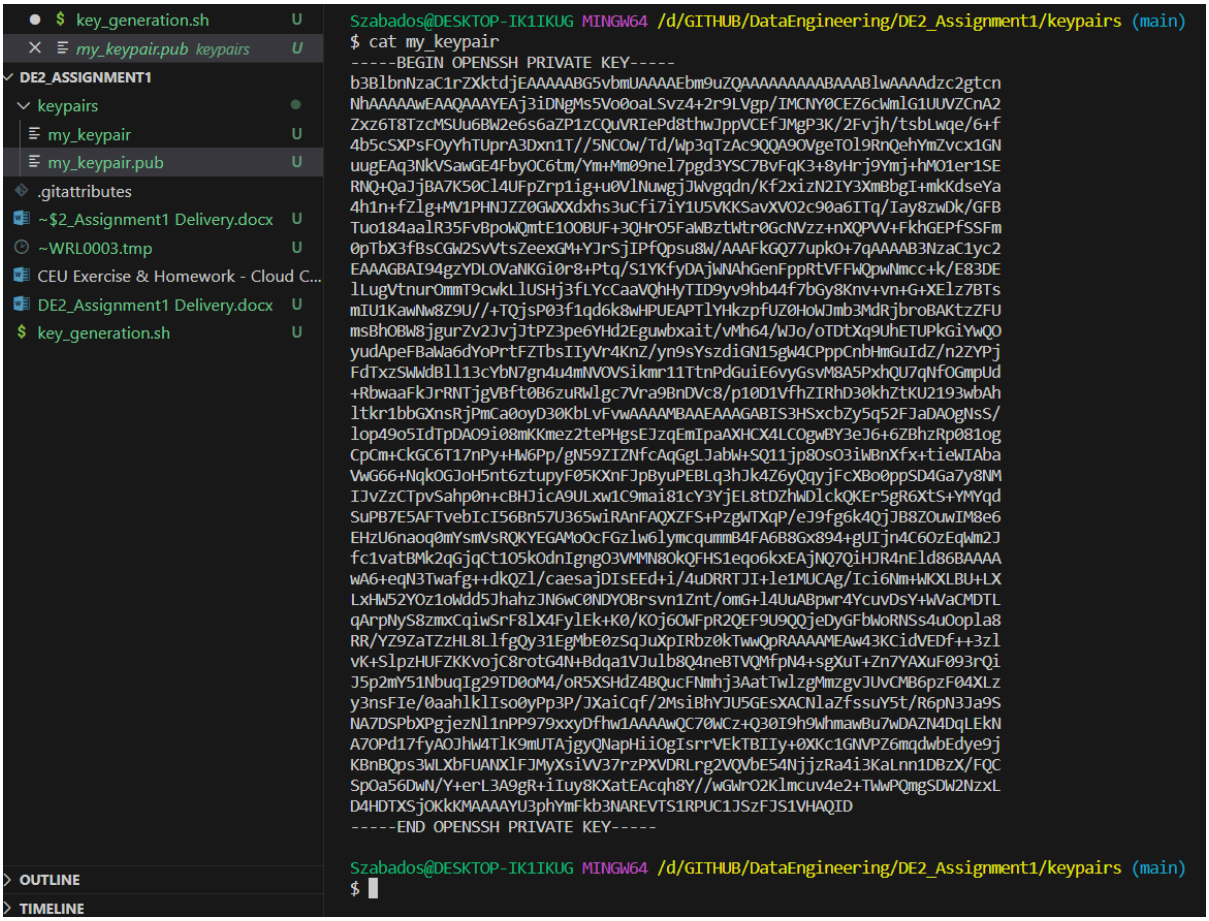
key_generation.sh

```
ssh-keygen -t rsa -f ./keypairs/my_keypair -N ''
```

b. Contents of the private and public keys:

Private:

my_keypair.pub



Public:

my_keypair

```
Szabados@DESKTOP-IK1IKUG MINGW64 /d/GITHUB/DataEngineering/DE2_Assignment1/keypairs (main)
$ cat my_keypair.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCPeIM2AyzlWjShotK/Pj7av0tWCn8gwI1jQIRnpxaaUbVRRVkKcDZnHPpPxPNwxJS7oFbZ7qzppk/XMJC5VEh493y2HAmmlUIR8kyA/cr/YW+OH+2xsvCp7/r5/hvlx
Jc+wU7JiFNSmsDcPGfVP//k0I7D9N39anepPMBz1BAD05WB5M6X1GdB6FiZm9zHUY266AQCrc2RVJrAYTgVvI4Lq2b9ib4ybT2d6XumB3dhILsG8Worf7zIeuP1iaP6Ew7V6vVIRE1D5BomMEDsrnQKXhQwlmunWKD67R
WU27CCMla+Cp2f8p/bGLM3YhjdeYFuAj6aQp2x5hriHWf59mWD4xXU8c0llnQZZdd3GGze4J+LuJjVTlUopJq9dU7Zz3RrohOr8hrLzPAOT8YUFO6jXzhpqVHfkw8GmhZCa0TU44FQX7dAes7kVpYHO1a2vQZw1XPP6dd
A9VX4WSEYQ99JIWbSlNtfd8GwIZbZK9W2xl57EYz5gmtKMg99Cmy7xb8= Szabados@DESKTOP-IK1IKUG

Szabados@DESKTOP-IK1IKUG MINGW64 /d/GITHUB/DataEngineering/DE2_Assignment1/keypairs (main)
$
```

c. Visitor Encryption (Made in Linux)

Visitor Code.ipynb

```python
import os

from pathlib import Path

from Cryptodome.Cipher import PKCS1_OAEP
from Cryptodome.PublicKey import RSA

PROJECTFOLDER = os.getcwd()
print(PROJECTFOLDER)
```

```python
PUBLIC_KEY_FILE = PROJECTFOLDER + "/my_keypair.pub"

print(PUBLIC_KEY_FILE)

assert os.path.isfile(PUBLIC_KEY_FILE)
```

```python
short_secret_message = "The pink otter is cheesy".encode("utf-8")
key = RSA.importKey(open(PUBLIC_KEY_FILE).read())
public_key_cipher = PKCS1_OAEP.new(key)
encrypted_message = public_key_cipher.encrypt(short_secret_message)
print(f"Encrypted message:")
print(encrypted_message)

ENCRYPTED_MESSAGE_FILE = PROJECTFOLDER + "/encrypted_message.bin"
with open(ENCRYPTED_MESSAGE_FILE, "wb") as f:
    f.write(encrypted_message)
```

d. CEU Decryption (Made in Windows)

CEU_Decryption.py

```
# %%

import os

from pathlib import Path

from Cryptodome.Cipher import PKCS1_OAEP
from Cryptodome.PublicKey import RSA

PROJECT_FOLDER = os.getcwd()
print(PROJECT_FOLDER)

PRIVATE_KEY_FILE = PROJECT_FOLDER + "\keypairs\my_keypair"
print(PRIVATE_KEY_FILE)

assert os.path.isfile(PRIVATE_KEY_FILE)
# %%

# Load the private key from file
with open(PRIVATE_KEY_FILE, "r", encoding="utf8") as key_file:
    private_key = RSA.import_key(key_file.read())


# %%
ENCRYPTED_MESSAGE_FILE = PROJECT_FOLDER + "\encrypted_message.bin"
# %%
with open(ENCRYPTED_MESSAGE_FILE, "rb") as f:
    encrypted_message_from_file = f.read()

private_key_cipher = PKCS1_OAEP.new(private_key)
decrypted_message = private_key_cipher.decrypt(encrypted_message_from_file)
print(f"Decrypted message: {decrypted_message.decode('utf-8')}")
# %%
```

Decrypted message:

```
1  with open(ENCRYPTED_MESSAGE_FILE, "rb") as f:
2      encrypted_message_from_file = f.read()
3
4  private_key_cipher = PKCS1_OAEP.new(private_key)
5  decrypted_message = private_key_cipher.decrypt(encrypted_message_from_file)
6  print(f"Decrypted message: {decrypted_message.decode('utf-8')}")
✓ 0.0s
Decrypted message: The pink otter is cheesy
```