Delivery for Data Engineering 2, Assignment 1

Myitzu: ID 2300350

David: ID 2302806

1. **Key Generation Command:**

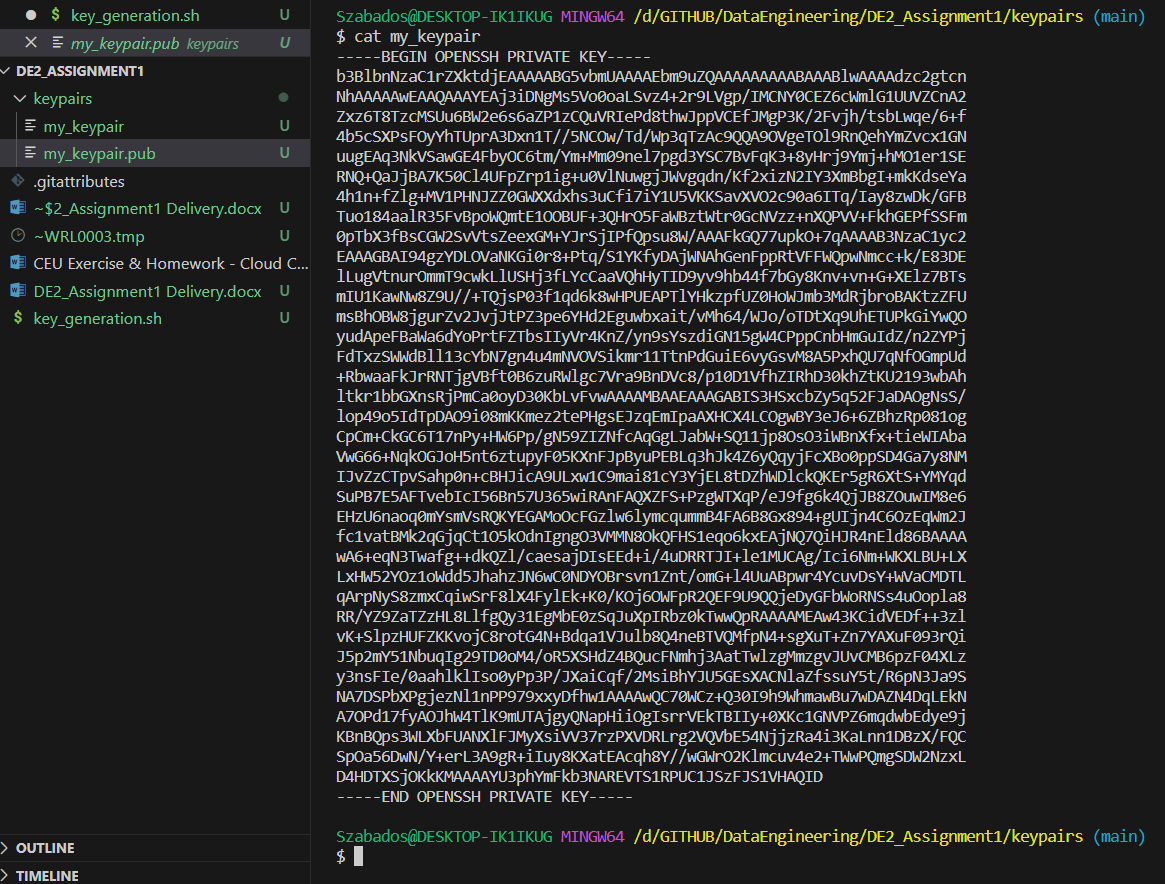
****

ssh-keygen -t rsa -f ./keypairs/my\_keypair -N ''

1. **Contents of the private and public keys:**

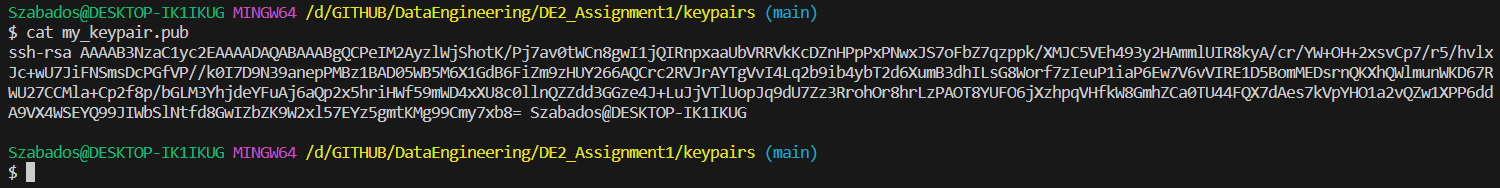
*Private:*

**



*Public:*

**



1. **Visitor Encryption (Made in Linux)**

****

import os

from pathlib import Path

from Cryptodome.Cipher import PKCS1\_OAEP

from Cryptodome.PublicKey import RSA

PROJECTFOLDER = os.getcwd()

print(PROJECTFOLDER)

PUBLIC\_KEY\_FILE = PROJECTFOLDER + "/my\_keypair.pub"

print(PUBLIC\_KEY\_FILE)

assert os.path.isfile(PUBLIC\_KEY\_FILE)

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)

1. **CEU Decryption (Made in Windows)**

****

# %%

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:**

