

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

```
• $ key_generation.sh U
X my_keypair.pub keypairs U
DE2_ASSIGNMENT1
  keypairs
    my_keypair U
    my_keypair.pub U
  .gitattributes
  ~$2_Assignment1 Delivery.docx U
  ~WRL0003.tmp U
  CEU Exercise & Homework - Cloud C...
  DE2_Assignment1 Delivery.docx U
  $ key_generation.sh U

Szabados@DESKTOP-1K1IKUG MINGW64 /d/GITHUB/DataEngineering/DE2_Assignment1/keypairs (main)
$ cat my_keypair
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAAAwAAAdzc2gtcn
NhAAAAAwEAAQAAAEAj3iDNgMs5Vo0aLSvz4+2r9LVgp/IMCNY0CEZ6cWmLG1UUVZCnA2
Zxz6T8TzcMSUu6BW2e6s6aZP1zCQUVRIePd8thwJppVCEfJMGp3K/2Fvjh/tSbLwqe/6+f
4b5cSXPsfOyYhTUPrA3Dxn1T//5NCOW/Td/Wp3qTzAc9QQA9OVgeT019RnQehYmZvcx1GN
uugEAq3NkVSawGE4FbyOC6tm/Ym+Mm09ne17pgd3YSC7BvFqK3+8yHr-j9YmjhM01er1SE
RNQ+QaJjBA7K50C14UFpZrp1ig+u0VlNuwgjJwvgqdn/Kf2xiZn2IY3XmbBgI+mkkdseYa
4h1n+fZlg+MV1PHNJZZ0GwXXdxhs3uCFi7iY1U5VKKsAvXV02c90a6ITq/Iay8zWdK/GFB
Tuo184aa1R35FvBpokmTE100BUF+3QHR05FawBztWtr0GcNVzz+nXQPVW+FkhGEPfSSFM
0pTbX3fBsCGw2SvVtsZeexGM+YJrSjIPFQpsu8W/AAAFKQ77upk0+7qAAAAAB3NzaC1yc2
EAAAQBAI94gzYDLOvaNKGi0r8+Ptq/S1YKfyDAjwNAHGenFppRtVFFWQpwNmcc+k/E83DE
1LugVtnurOmmT9cwkL1LUSHj3fLYcCaaVQhHyTID9yv9hb44f7bgY8Knn+vn+G+XELZ7BTs
mIU1KawNw8Z9U//+TQjsP03f1qd6k8wHPUEAPTLVHkzpfUz0H0wJmb3MdrjbroBAKtZFU
msBhOBW8jgurZv2JvjJtPZ3peYHd2Eguwbxait/vmH64/WJo/oTDtXq9UhtEUPKgiYwQ0
yudApeFBaWad6YoPrTFZTbsIiYvR4KnZ/yn9sYszdIGN15gw4CPppcnbHmguIdZ/n2ZYPj
FdTxzSWwdbL113cYbN7gn4u4mMV0VSikmr11TtnPdGuiE6vyGsvM8A5PxbQU7qNfOGmpUd
+RbwaaFkjrRNTjgVBft0B6zuRwlgc7Vra9BndVc8/p10D1VfhZIRhd30khZtkU2193wbaH
ltkr1bbGXnsRjPmCa0oyD30KbLVfVwAAAAABAAEAAAGABIS3HSxcbyZy5q52FJaDA0Gns/
lop49o5ITdPDA0i08mKKmez2tePHgsEJzqEmIpaAXHC4LC0gwBY3eJ6+6ZBhzRp081og
CpCm+CkGC6T17nPy+Hw6Pp/gN59ZIZNfCAqGgJabW+SQ11jp80s03iWbNxfx+tiEWIAba
VwG66+NqKOGJoH5nt6ztupyF05KXnFjPbyuPEBLq3hJk4Z6yQyqjFcXBo0ppSD4Ga7y8NM
IJVZCTpvSahp0n+cBHJicA9ULxw1C9mai81cY3YjEL8tdZhwD1ckQKEr5gR6Xts+YMYqd
SuPB7E5AFTvebIcI56Bn57U365wiRANFAQXZFS+PzgwTXqP/eJ9fg6k4QjJB8Z0uWIM8e6
EHZU6naoq0mYsmVSQKYEGAMoCfGzlw6lymcquumB4FA6B8Gx894+gUJjn4C60zEqWm2J
fc1vatBMk2qGjQCT105K0dnIIng03VMMN80kQFHS1eqo6kxkEAjNQ7QIHJR4nElD86BAAAA
wA6+eqN3TwaFg++dkQZ1/caesajDIseEd+i/4uDRRTJI+1e1MUCAG/Ici6Nm+WXKLBU+LX
LxHw52Y0z1owdd5JhahzJN6wC0NDYOBrsvn1Znt/omG+14UuABpwr4YcuvDsY+HwACMDTL
qArpMyS8zmxCqiWsrF8LX4Fy1Ek+K0/KOj6OMFpR2QEF9U9QqjeDyGfBwRnSS4u0opla8
RR/YZ9ZaTzZHL8LlfgQy31EgmbE0zsqJuXpIRbz0kTwwQpRAAAAMEAw43KciDVEDf++3zL
vK+S1pzHUFZKKvoJc8rotG4N+Bdqa1VJulb8Q4neBTVMQfPM4+sgXuT+Zn7YAXuF093RQi
J5p2mY51NbuqIg29TD0oM4/or5XSHdZ4BQucFnmhj3AatTwlZgmMzgVJuvCM86pzF04XLz
y3nsFIe/0aah1klIso0yPp3P/JXaiCqf/2MsiBhYJU5GESXACN1azfssuY5t/R6pN3Ja9S
NA7DSPbXPgjezN1nPP979xyDfhw1AAAAwQC70WCz+Q30I9h9WhmawBu7WDAZN4DqLEKN
A7OPd17fyAOJhW4TlK9mUTajgyQNapHiiogIsrrVEKBTiTy+0XKc1GNVPZ6mqdwbEdye9j
KBnBQps3WLXbFUANXLFJMyXs1Vv37rZPXVDRlrg2VQVbE54NjjzRa4i3KaLnn1DBZx/FQC
Sp0a56DwN/Y+erL3A9gr+iuy8KXatEAcqh8Y//wGwR02Klmcuv4e2+TwWpQmgSDW2NzXL
D4HDTXSjOKKMAAAAYU3phYmFkb3NAREVTS1RPUc1J5zFJ51VHAQID
-----END OPENSSH PRIVATE KEY-----

Szabados@DESKTOP-1K1IKUG MINGW64 /d/GITHUB/DataEngineering/DE2_Assignment1/keypairs (main)
$
```

Public:



my_keypair

```
Szabados@DESKTOP-1K1IKUG MINGW64 /d/GITHUB/DataEngineering/DE2_Assignment1/keypairs (main)
$ cat my_keypair.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCEPIM2AyZlWjShotK/Pj7av0tWcn8gwi1jQIRnpxaaubVRRVkkCDZnHPpPxPmWxJS7oFbZ7qzppk/XMJC5VEh493y2HAmmlUIR8kyA/cr/Yw+OH+2xsvCp7/r5/hvLx
Jc+uU7JiFNSmsDcPGfVP//k0I7D9N39anepPMBz1BAD05MB5M6X1GdB6FiZm9zHUY266AQCrC2RV3rAYTgVvI4Lq2b9ib4ybT2d6XumB3dhILsG8WorF7zIeuP1iaP6Ew7V6VVIRE1D58omMEDsrnQIOhQwLmunwKD67R
WU27CCM1a+Cp2F8p/bGLMB3YhjdeYFuAj6aOp2xShriHwF59mWd4xXU8c01lnQZZdd3GGze4J+Lu3jVT1UopJq9dU7Zz3RrohOr8hrLzPAOT8YUFO6jXzhpqVhFkx8GmhZCa0TU44FQX7dAes7KvpyH01a2vQ2w1XPPGdd
A9VX4MSEYQ99J1WbS1ntfd8GwIZbZK9M2x157EYz5gmtKMg99Cmy7xb8= Szabados@DESKTOP-1K1IKUG

Szabados@DESKTOP-1K1IKUG MINGW64 /d/GITHUB/DataEngineering/DE2_Assignment1/keypairs (main)
$
```

c. Visitor Encryption (Made in Linux)



Visitor Code.ipynb

```
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)
```

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')}")  
1  ✓ 0.0s  
Decrypted message: The pink otter is cheesy
```