

PGP Encryption using Python

Sushank Saini
July 9, 2024

GitHub Link: https://github.com/Sushank13/BMO-SE-Work/tree/main/python_scripts

Overview

This Python script encrypts and decrypts a file using **PGP encryption-decryption** implemented through **GNU Privacy Guard wrapper** for Python. Once the file is encrypted, it is uploaded to an FTP server. Then, the file is decrypted after being downloaded from the FTP server. The FTP protocol is implemented in the script through **ftplib module**. Finally, the script uploads the file and its decrypted contents to a **MySQL database**.

Best Practices Used

The following best practices have been used to create a **flexible and maintainable code**.

1. **Single Responsibility Principle:** Each method of this script does one and only one thing to have **less coupling and high cohesion**.
2. **Logging:** Logging has been implemented using the **logging module** (see **Figure 1**). This would help with easy troubleshooting of the issues in the code.
3. **Usage of Environment Variables:** To avoid hardcoding of variables directly into the code **.env file** has been used to store the variables and their values (see **Figure 2**).
4. **Usage of Stored Procedures:** All the SQL code has been executed using the stored procedure instead of hard coding the SQL statements in the code itself (see **Figure 3**).

```
PS E:\BMO-SE-Work> & C:/Users/Sushank/AppData/Local/Microsoft/WindowsApps/python3.11.exe e:/BMO-SE-Work/python_scripts/file_encrypt_decrypt.py
INFO:root:Loading .env File
INFO:root:dotenv File Loading Status:
INFO:root:True
INFO:root:GNU PG object initialized successfully
INFO:root:File Path OK
INFO:root:Generating key pair.
INFO:root:Initializing Input Data for Key Generation.
INFO:root:Key Pair Generated successfully.
INFO:root:Encrypting the File.
INFO:root:Encrypting file: E:\BMO-SE-Work\python_scripts\original_file.txt
INFO:root:Absolute Path of the file: E:\BMO-SE-Work\python_scripts\original_file.txt
INFO:root:Reading original file.
INFO:root:File Encrypted Successfully.
INFO:root:Uploading Encrypted file to FTP Server
INFO:root:Connecting to the FTP Server
INFO:root:Successfully Connected to the FTP Server
INFO:root:Accessing Encrypted File
INFO:root:List of files on FTP Server:
```

Figure 1: Implementation of Logging

```
GPG_BINARY_PATH=os.getenv("GPG_BINARY_PATH")
RECIPIENT_EMAIL=os.getenv("RECIPIENT_EMAIL")
PASSPHRASE=os.getenv("PASSPHRASE")
ENCRYPTED_FILE_PATH=os.getenv("ENCRYPTED_FILE_PATH")
DECRYPTED_FILE_PATH=os.getenv("DECRYPTED_FILE_PATH")
FTP_HOSTNAME=os.getenv("FTP_HOSTNAME")
FTP_USERNAME=os.getenv("FTP_USERNAME")
FTP_PASSWORD=os.getenv("FTP_PASSWORD")
DB_HOSTNAME=os.getenv("DB_HOSTNAME")
DB_USERNAME=os.getenv("DB_USERNAME")
DB_PASSWORD=os.getenv("DB_PASSWORD")
DB_DATABASE=os.getenv("DB_DATABASE")

1 GPG_BINARY_PATH="C:\Program Files (x86)\GNU\GnuPG\gpg.exe"
2 RECIPIENT_EMAIL="sushank.saini@abc.com"
3 PASSPHRASE="passphrase"
4 ENCRYPTED_FILE_PATH="E:\BMO-SE-Work\python_scripts\encrypted_file.gpg"
5 DECRYPTED_FILE_PATH="E:\BMO-SE-Work\python_scripts\decrypted_file.txt"
6 FTP_HOSTNAME="ftp.dlptest.com"
7 FTP_USERNAME="dlpuser"
8 FTP_PASSWORD="rNrKYTX9g7z3RgJrmxwuGHbeu"
9 DB_HOSTNAME="localhost"
10 DB_USERNAME="root"
11 DB_PASSWORD="password"
12 DB_DATABASE="decrypted_files"
```

Figure 2: Snapshot of .env file

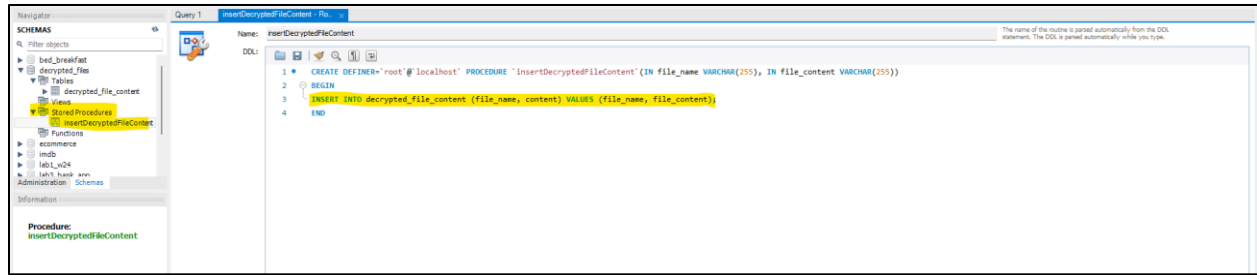


Figure 3: Stored Procedure

Program Execution

The script first reads the original file (**Figure 4**) that is to be encrypted.

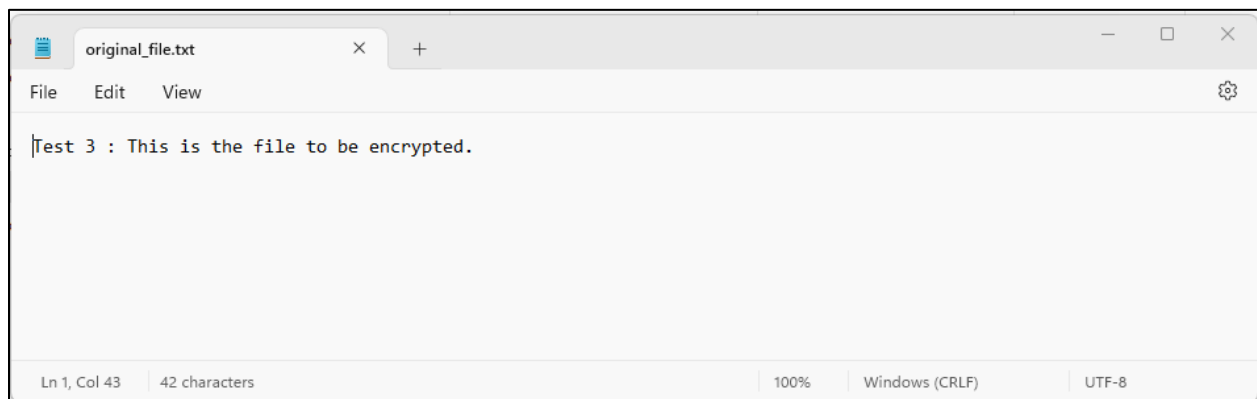


Figure 4: Original text file

After this the file is encrypted (**Figure 5**) and uploaded to the FTP server (**Figure 6**).

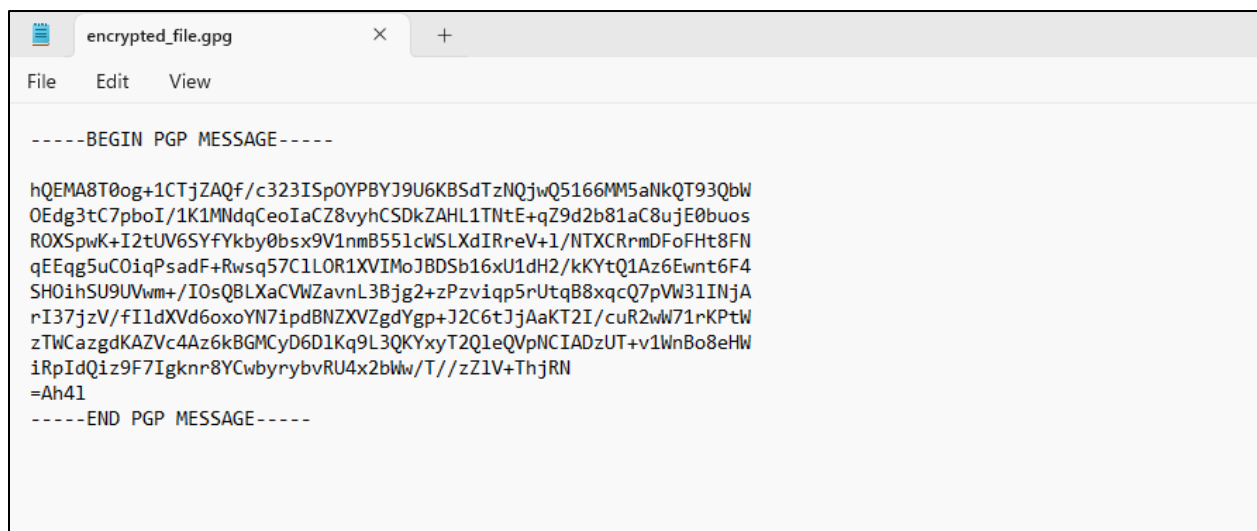


Figure 5: Encrypted File

```

-rw-r--r-- 1 1001 1001 117650 Jul 10 19:38 10.101.1.2_20240710-15380610_IVA.jpg
-rw-r--r-- 1 1001 1001 136859 Jul 10 19:38 10.101.1.2_20240710-15380750_IVA.jpg
-rw-r--r-- 1 1001 1001 135394 Jul 10 19:38 10.101.1.2_20240710-15380770_IVA.jpg
-rw-r--r-- 1 1001 1001 141218 Jul 10 19:38 10.101.1.2_20240710-15380990_IVA.jpg
-rw-r--r-- 1 1001 1001 127270 Jul 10 19:38 10.101.1.2_20240710-15381190_IVA.jpg
-rw-r--r-- 1 1001 1001 157627 Jul 10 19:38 10.101.1.2_20240710-15381510_IVA.jpg
-rw-r--r-- 1 1001 1001 118640 Jul 10 19:38 10.101.1.2_20240710-15381751_IVA.jpg
-rw-r--r-- 1 1001 1001 139400 Jul 10 19:38 10.101.1.2_20240710-15381890_IVA.jpg
-rw-r--r-- 1 1001 1001 135701 Jul 10 19:38 10.101.1.2_20240710-15382370_IVA.jpg
-rw-r--r-- 1 1001 1001 149722 Jul 10 19:38 10.101.1.2_20240710-15382531_IVA.jpg
-rw-r--r-- 1 1001 1001 143825 Jul 10 19:38 10.101.1.2_20240710-15382630_IVA.jpg
-rw-r--r-- 1 1001 1001 134864 Jul 10 19:38 10.101.1.2_20240710-15382889_IVA.jpg
-rw-r--r-- 1 1001 1001 93982 Jul 10 19:38 10.101.1.2_20240710-15383190_IVA.jpg
-rw-r--r-- 1 1001 1001 143814 Jul 10 19:39 10.101.1.2_20240710-15383370_IVA.jpg
-rw-r--r-- 1 1001 1001 138705 Jul 10 19:39 10.101.1.2_20240710-15384170_IVA.jpg
-rw-r--r-- 1 1001 1001 119860 Jul 10 19:39 10.101.1.2_20240710-15384349_IVA.jpg
-rw-r--r-- 1 1001 1001 132098 Jul 10 19:39 10.101.1.2_20240710-15384569_IVA.jpg
-rw-r--r-- 1 1001 1001 124287 Jul 10 19:39 10.101.1.2_20240710-15385770_IVA.jpg
-rw-r--r-- 1 1001 1001 122805 Jul 10 19:39 10.101.1.2_20240710-15385789_IVA.jpg
-rw-r--r-- 1 1001 1001 133330 Jul 10 19:39 10.101.1.2_20240710-15385828_IVA.jpg
-rw-r--r-- 1 1001 1001 134812 Jul 10 19:39 10.101.1.2_20240710-15385849_IVA.jpg
-rw-r--r-- 1 1001 1001 57792 Jul 10 19:39 10.101.1.2_20240710-15385908_IVA.jpg
-rw-r--r-- 1 1001 1001 958 Jul 10 19:30 BunkerEastProdProxiesResFile_bebbluecoat6_2024-07-10-15-30-03.txt
-rw-r--r-- 1 1001 1001 958 Jul 10 19:30 BunkerWestProdProxiesResFile_bwbbluecoat6_2024-07-10-13-30-03.txt
-rw-r--r-- 1 1001 1001 7430807 Jul 10 19:37 Margenes_2024-07-10T19:37:12.csv
-rw-r--r-- 1 1001 1001 100000 Jul 10 19:38 _11471632
-rw-r--r-- 1 1001 1001 100000 Jul 10 19:38 _11471749
-rw-r--r-- 1 1001 1001 100000 Jul 10 19:38 _11471965
-rw-r--r-- 1 1001 1001 100000 Jul 10 19:37 _11472817
-rw-r--r-- 1 1001 1001 100000 Jul 10 19:37 _11474446
-rw-r--r-- 1 1001 1001 577 Jul 10 19:39 encrypted_file.gpg
-rw-r--r-- 1 1001 1001 144 Jul 10 19:35 test.zip
-rw-r--r-- 1 1001 1001 102400 Jul 10 19:38 upload.txt
INFO:root:Encrypted File Uploaded to FTP Server Successfully

```

Figure 6:File Upload on FTP

Then the file is downloaded from the FTP server so that it can be decrypted. Once decrypted, the file's content is pushed to a MySQL database (**Figure 7**).

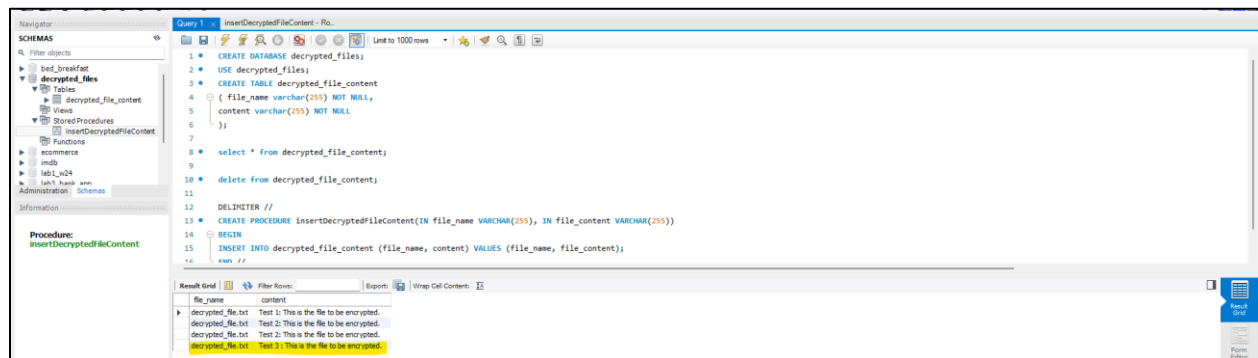


Figure 7: File Upload to Database