How to Use the Encipher-Decipher Tool for Double Encryption

William M. Marcy, PhD, PE

Las Cruces, NM

Updated 10-23-2023

We will assume you have already downloaded and installed Python 3.12 or later from Python.org for your computer's operating system. https://www.python.org

Example of OTP Double Enciphering a File

Start **Python IDLE** and load **OTP-encipher-decipher.py program. Hit F5** or choose **Run Module under Run** to execute the program.

There are 4 example settings files. These should be in the same directory as the source program to load correctly.

Step-1 and Step-2 settings files help you perform a **double encipher** of the file **sunset.jpg** using two different OTP's and 2 different cipher keys.

Step-3 and Step-4 settings files help you perform a **double decipher** starting first with the second encryption to recover the first encryption file followed by another decryption to recover the original file.

Step-3 and Step-4 files must use the corresponding OTP files and cipher keys used in **Step-1 and Step-2 files**.

This allows verification that everything was performed correctly in all four steps so the recipient of the second encryption file (who should already have the two OTP files and know the cipher keys) will be able to decipher the enciphered file received.

Step by Step Instructions

Choose Command 10.

Enter the settings file name: **Step-1.txt Hit Enter.**

You should see **sunset.jpg** as the file to be enciphered. Verify the directory listed to be sure it corresponds to the one you created. If not, choose **Command 1** and find the file. You may need to do this in each step below.

You should see **enciphered-1.bin** as the file to receive the encryption.

You should see **OTP-2MB.bin** as the OTP to be used. After you learn the process, you can choose whatever OTP you wish to use.

You should see **step-1-pass as the pass phrase.** After you learn the process, you can choose whatever cipher key or pass phrase you wish.

Update the settings file for **Step-1.txt Choose Command 9.** You should see **step-1.txt** as the current settings file. If not enter it. After you learn the process, you can choose any name you wish to use. When satisfied hit **Enter** to accept and save all current settings.

We are now ready to perform our first encryption of **sunset.jpg**. **Choose Command 7**. If everything looks OK hit **Enter** and you will get a report.

Choose Command 10

Enter the settings file name: **Step-2.txt**

You should see **enciphered-1.bin** as the file to be enciphered. This will encipher the result of the first step with yet another OTP and cipher key.

You should see **enciphered-2.bin** as the file to receive the encryption.

You should see **OTP-5MB.bin** as the OTP to be used.

You should see **step-2.pass as the pass phrase**.

Update the settings file for **Step-2.txt Choose Command 9**. You should see **step-2.txt** as the current settings file. If not enter it. When satisfied hit **Enter** to accept and save all current settings.

We are now ready to perform an encryption of the encryption of **enciphered-1.bin**. Choose Command 7. If everything looks OK hit **Enter** and you will get a report.

The file **enciphered-2.bin** in the **Enciphered** directory is the **encryption of the encryption** of **sunset.jpg**
enciphered-2.bin is the file you can send to whomever you wish. You can rename it later if needed.

Choose Command 10.

Enter the settings file name: **Step-3.txt**

You should see **enciphered-2-bin** as the file to be deciphered.

You should see **enciphered-1.bin** as the file to receive the decryption.

You should see **OTP-5MB.bin** as the OTP to be used. This must be the same as that used in **Step-2.txt**

You should see **step-2-pass as the pass phrase**. This must be the same as that used in **Step-2.**

Update the settings file for **Step-3.txt Choose Command 9**. You should see S**tep-3.txt** as the current settings file. If not enter it. When satisfied hit **Enter** to accept and save all current settings.

We are now ready to perform a decryption of the second encryption of **sunset.jpg**. **Choose Command 8.** If everything looks OK hit **Enter** and you will get a report.

Choose Command 10

Enter the settings file name: **Step-4.txt**

You should see **enciphered-1.bin** as the file to be deciphered.

You should see **sunset.jpg** as the file to receive the decryption. This can be any name you wish to use.

You should see **OTP-2MB.bin** as the OTP to be used. This must be the same as used in **step-1.txt**

You should see **step-1-pass as the cipher phrase**. This must be the same as used in **step-1.txt**

Update the settings file for **step-4.txt Choose Command 9**. You should see **step-4.txt** as the current settings file. If not enter it. **Enter** to accept and save all current settings.

We are now ready to perform a decryption of the first encryption of **sunset.jpg. Choose Command 8**. If everything looks OK hit **Enter** and you will get a report.

Confirm that everything worked before sending the second enciphered file, **enciphered-2.bin,** to your recipients! Change the file name to anything you wish, including spurious file extensions.

sunset.jpg will be found in the subdirectory **Deciphered.** This file will be byte for byte identical to the original file **sunset.jpg**

The elegance of this **OTP encryption** tool is that you can encipher any 8 bit file no matter how large or what it does.

Surviving a Brute Force Attack

In this example we used a **2e6 OTP** and a **5e6 OTP**. To perform a **brute force** attack on the second enciphered file, assuming the bad actors have obtained the two OTP's will require them to perform trial decryptions equal to the product of these two numbers = **1e13**. A supercomputer can perform about 1e6 trial decryptions per second. To decipher the double encrypted file would require about 1e7 seconds (worst case). There are 86,400 seconds in a 24 hour day. It would take about 116 days (worst case) to break the double enciphered file by brute force. On average it would take about half that time or about 58 days.

The best supercomputers today cost about $2500/hour ($60,000 per day) run. Even if the bad actors were willing to spend 58 days (on average) to "hack" the double enciphered file unless they are a nation state, they could not afford the $3.48 million it would cost per file. Your double enciphered file is extremely safe from all but nation states with unlimited budgets and access to supercomputers. **If they can't get your OTP files it is safe from them as well**.

Need to send multiple files in a directory structure?

Get a subscription to **WinZip**. Zip all of the files/directories into a **single ZIP file**. **Use the OTP-encipher decipher tool to encrypt the Zip file.** The encrypted ZIP file size may be too large to send as an email attachment. If so, put it on the **Cloud** and give your recipients access. If this is too

dangerous then **copy the encrypted file to tiny SDC's** and send them by **FEDX, UPS, or snail mail** to your recipients. ***This is a good way to send OTP files*****. Be sure the SDC is enciphered.**