Cipher - Command Prompt Encryption

The cipher command can be used to encrypt files in Windows from the Command Prompt.

The following parameters can be used with the cipher command:

Parameters	Description
/b	Aborts if an error is encountered. By default, cipher continues to run even if errors are encountered.
/c	Displays information on the encrypted file.
/d	Decrypts the specified files or directories.
/e	Encrypts the specified files or directories. Directories are marked so that files that are added afterward will be encrypted.
/h	Displays files with hidden or system attributes. By default, these files are not encrypted or decrypted.
/k	Creates a new certificate and key for use with Encrypting File System (EFS) files. If the **/k** parameter is specified, all other parameters are ignored.
/r:<filename> [/smartcard]	Generates an EFS recovery agent key and certificate, then writes them to a .pfx file (containing certificate and private key) and a .cer file (containing only the certificate). If /smartcard is specified, it writes the recovery key and certificate to a smart card, and no .pfx file is generated.
/s:<directory>	Performs the specified operation on all subdirectories in the specified directory.
/u [/n]	Finds all encrypted files on the local drive(s). If used with the /n parameter, no updates are made. If used without /n, /u compares the user's file encryption key or the recovery agent's key to the current ones, and updates them if they have changed. This parameter works only with /n.

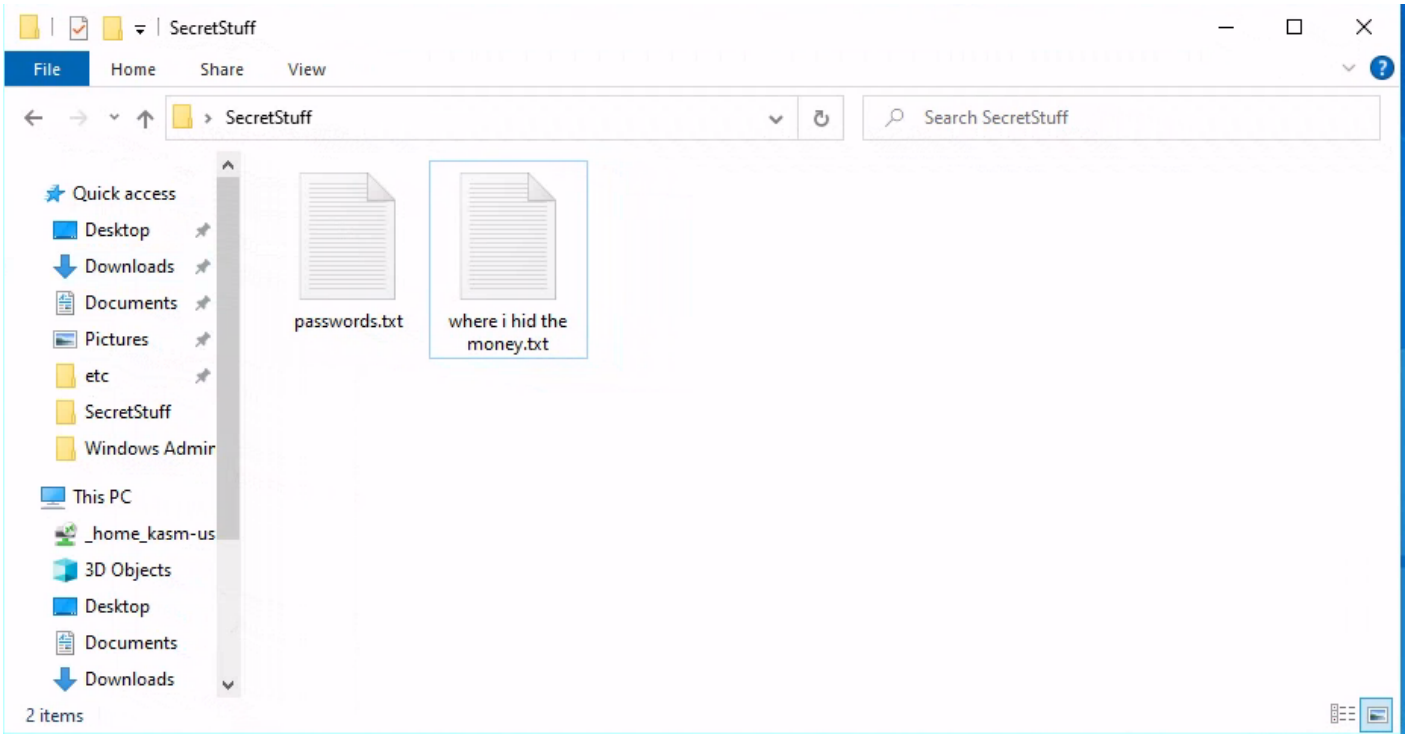
/w:<directory>	Removes data from available unused disk space on the entire volume. If you use the /w parameter, all other parameters are ignored. The directory specified can be located anywhere in a local volume. If it is a mount point or points to a directory in another volume, the data on that volume is removed.
/x[:efsfile] [<FileName>]	Backs up the EFS certificate and keys to the specified file name. If used with :efsfile, /x backs up the user's certificate(s) that were used to encrypt the file. Otherwise, the user's current EFS certificate and keys are backed up.
/y	Displays your current EFS certificate thumbnail on the local computer.
/adduser [/certhash:<hash>]	/certfile:<filename>]
/rekey	Updates the specified encrypted file(s) to use the currently configured EFS key.
/removeuser /certhash:<hash>	Removes a user from the specified file(s). The Hash provided for /certhash must be the SHA1 hash of the certificate to remove.
/?	Displays help at the command prompt.

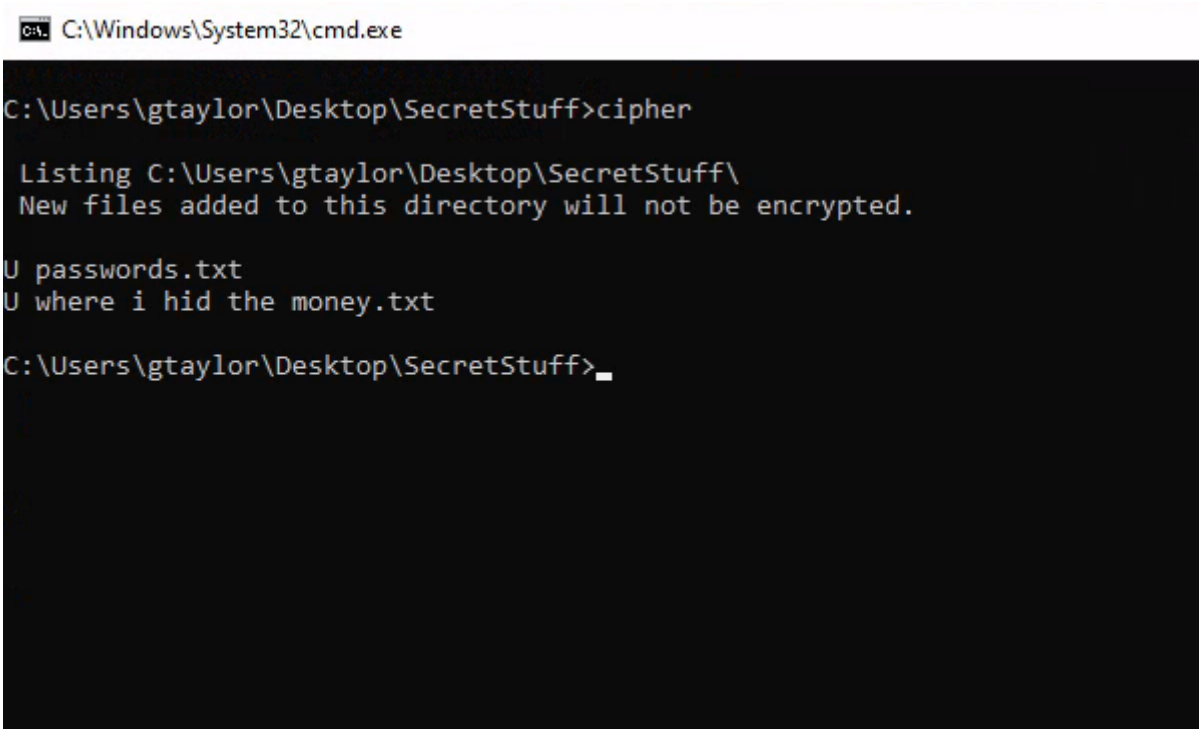
**Source

Example of Encrypting and Decrypting a Folder in Windows 10

Below is an example folder (SecretStuff) that has two files in it. If I want to encrypt the folder and the two files in it I can use the cipher command from an administrator privilege command prompt to see the status of encryptioncls

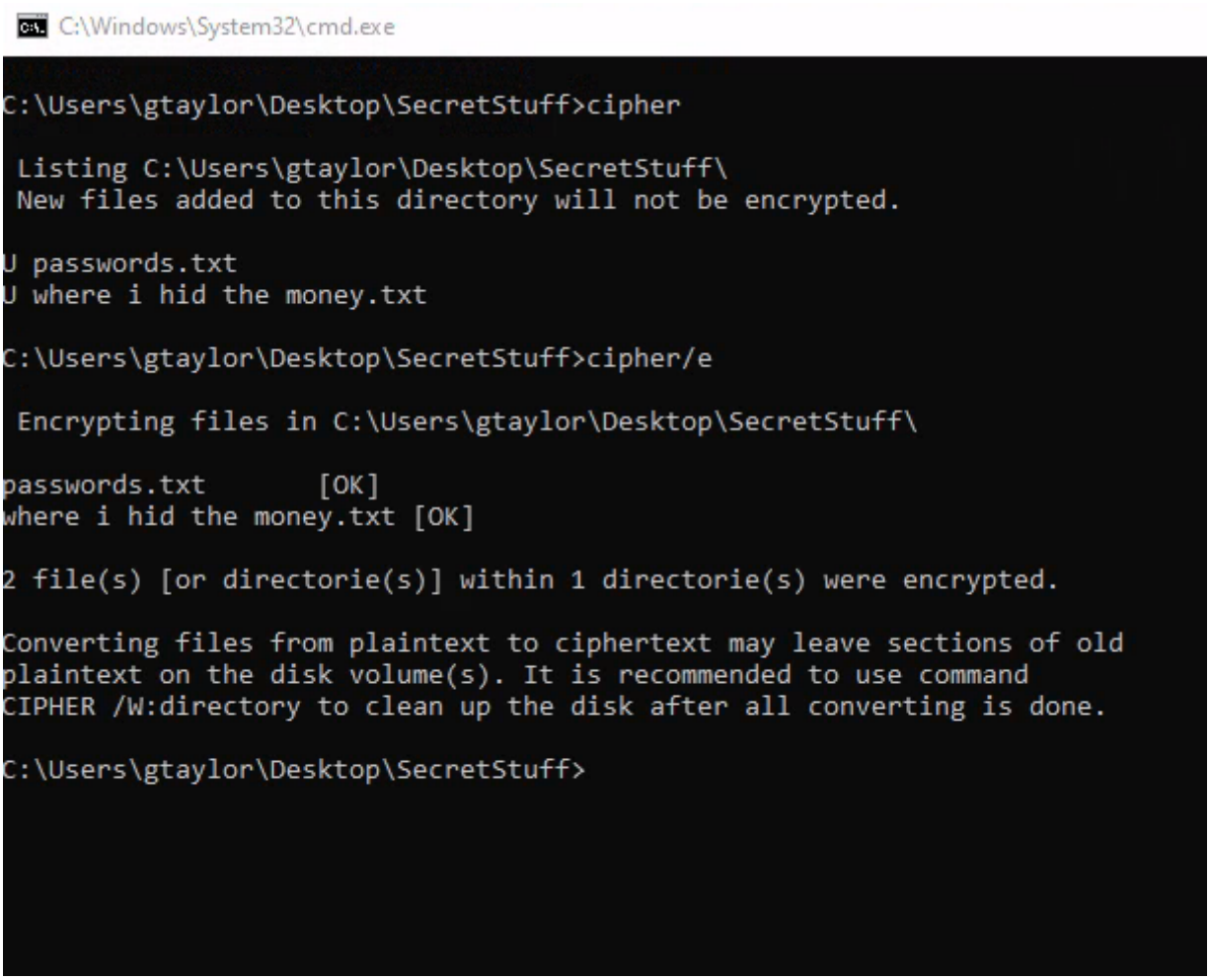
.





The 'U' next to the two files indicates that the files are not encrypted.

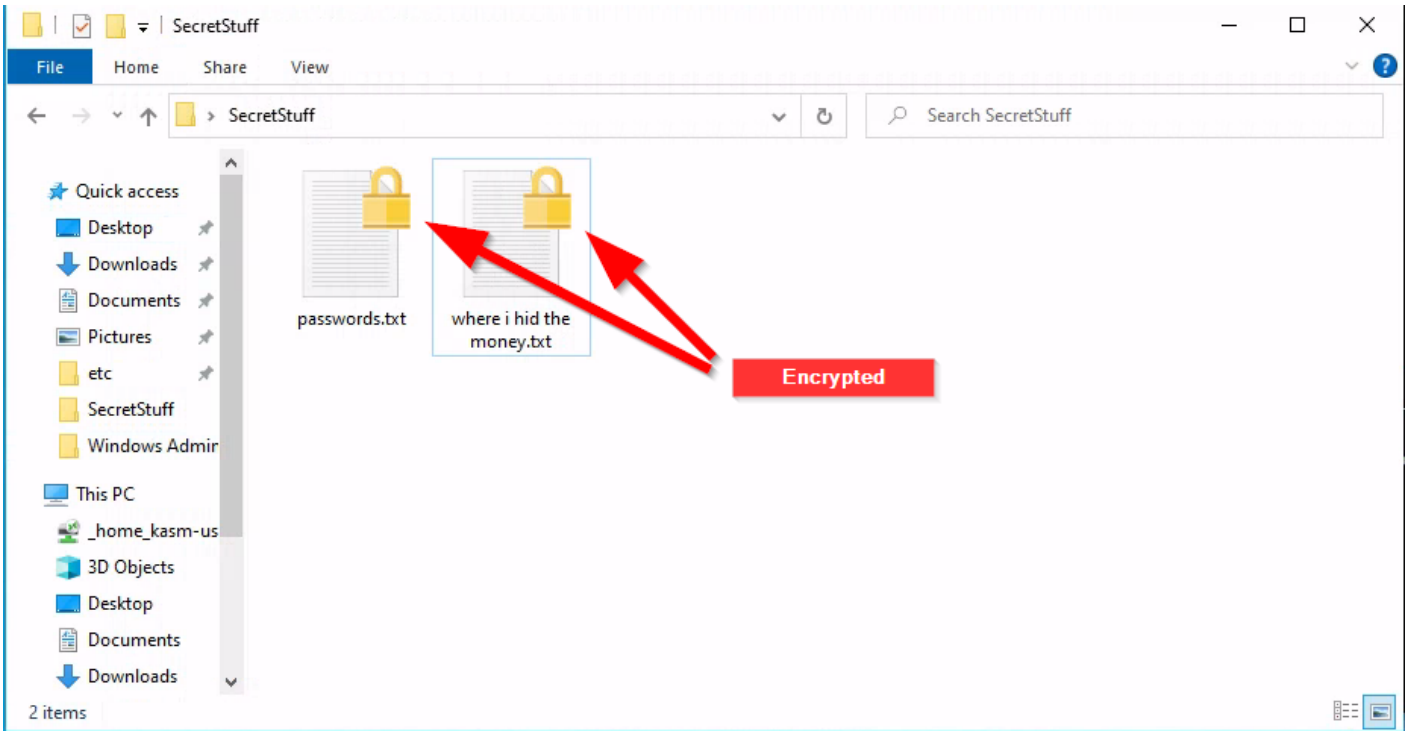
To encrypt the files use the cipher /e parameter to encrypt everything in the SecretStuff folder and the folder itself.

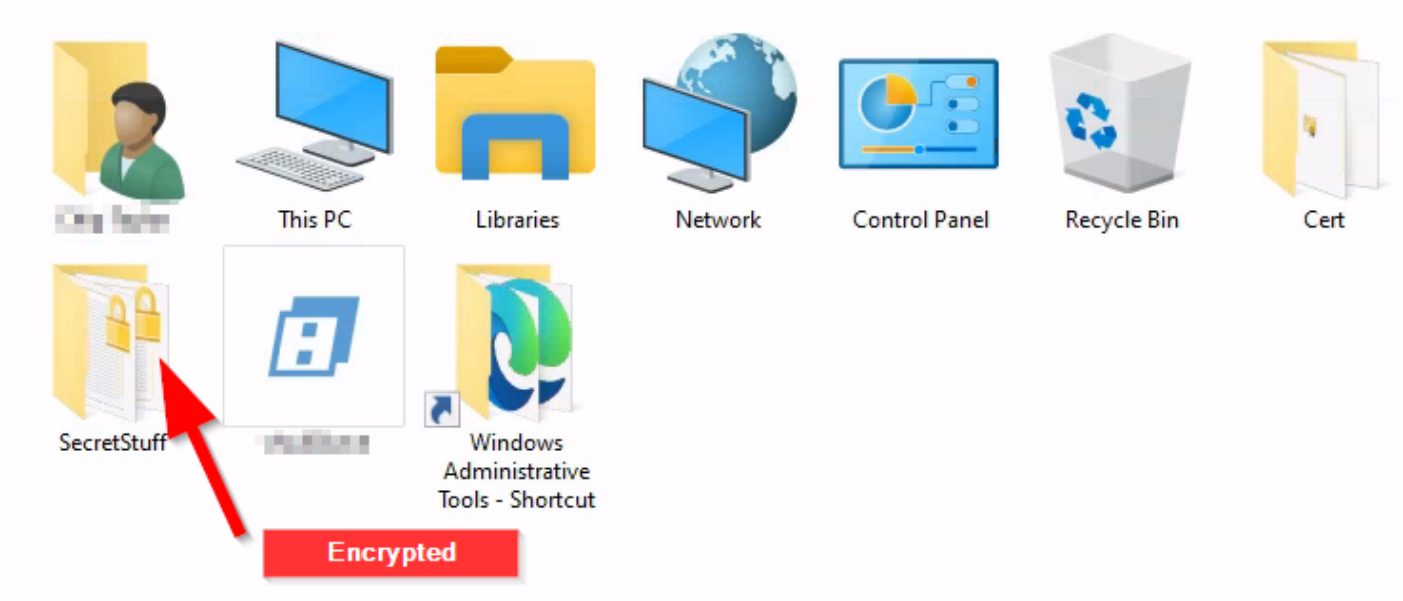


Now, if we check again using the cipher command without any parameters we see that the files are encrypted. The 'E' denotes that the files are now encrypted. There is also a visual queue in Windows Explorer that shows that the files are encrypted. A padlock icon is added to the icons for both files.

C:\Windows\System32\cmd.exe

```
C:\Users\gtaylor\Desktop\SecretStuff>cipher

 Listing C:\Users\gtaylor\Desktop\SecretStuff\
 New files added to this directory will not be encrypted.

U passwords.txt
U where i hid the money.txt

C:\Users\gtaylor\Desktop\SecretStuff>cipher/e

 Encrypting files in C:\Users\gtaylor\Desktop\SecretStuff\

passwords.txt       [OK]
where i hid the money.txt [OK]

2 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

C:\Users\gtaylor\Desktop\SecretStuff>cipher

 Listing C:\Users\gtaylor\Desktop\SecretStuff\
 New files added to this directory will not be encrypted.

E passwords.txt
E where i hid the money.txt

C:\Users\gtaylor\Desktop\SecretStuff>_
```





Last, if you want to decrypt everything the SecretStuff folder and the folder itself just use the command cipher /d

```
C:\Windows\System32\cmd.exe
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

C:\Users\gtaylor\Desktop\SecretStuff>cipher

 Listing C:\Users\gtaylor\Desktop\SecretStuff\
 New files added to this directory will not be encrypted.

E passwords.txt
E where i hid the money.txt

C:\Users\gtaylor\Desktop\SecretStuff>cipher /d

 Decrypting files in C:\Users\gtaylor\Desktop\SecretStuff\

passwords.txt       [OK]
where i hid the money.txt [OK]

2 file(s) [or directorie(s)] within 1 directorie(s) were decrypted.


C:\Users\gtaylor\Desktop\SecretStuff>cipher

 Listing C:\Users\gtaylor\Desktop\SecretStuff\
 New files added to this directory will not be encrypted.

U passwords.txt
U where i hid the money.txt

C:\Users\gtaylor\Desktop\SecretStuff>_
```

And the files and folder are now decrypted again.

Revision #3
Created 29 March 2023 19:47:23 by Glen Taylor
Updated 29 March 2023 20:59:11 by Glen Taylor