AES Crypt User Guide

Publication Date: 2013-12-26

Original Author: Gary C. Kessler (gck@garykessler.net)

Revision History

Date	Contributor	Changes
2012-01-17	Gary C. Kessler	First version
2013-03-03	Doug Reed	Added Linux-related information
2013-08-13	Paul E. Jones	Re-formatted text and added warnings about accidental file deletion
2013-12-26	Paul E. Jones	General improvements, added more Linux documentation

Contents

1 What is AES Crypt?

AES Crypt is a program that will encrypt files using the Advanced Encryption Standard (AES). AES has been adopted by the National Institute of Standards and Technology (NIST) as U.S. Federal Information Processing Standard (FIPS) 197. Please contact the author if you would like additional information about the background and operation of AES.

AES Crypt runs on Windows, Mac OSX, and Linux operating systems. There are versions of AES Crypt in C, C++, C#, and Java. Files encrypted on one platform are compatible with – and can be decrypted on – the other platforms. AES Crypt employs a graphical user interface (GUI) for ease of use and, in fact, has a similar look-and-feel on both Windows and Mac OSX systems. This user guide will describe program installation and use on Windows, Mac, and Linux platforms with the C++ and C implementations.

2 Have Questions?

If you have any questions about AES Crypt or get errors, feel free to ask about it on the discussion forum:

http://forums.packetizer.com/viewforum.php?f=72

Many questions have already been asked and answered, but feel free to post your question if you can't find the answer or you're still unsure of the answer to any question you have.

3 Downloading and Installation

3.1 Downloading the right package

AES Crypt can be downloaded from https://www.aescrypt.com/download/ (secure) or http://www.aescrypt.com/download/ (non-secure). Choose the preferred package for your system; Windows or Linux users will want either the 32-bit or 64-bit GUI or command-line version, while Mac OSX users will probably want the Mac GUI (x86). Note that both the GUI versions for Windows and Mac include the "aescrypt" command-line utility.

3.2 Installing on Windows (GUI)

Download the program ZIP file, unZIP the archive. Inside, the ZIP file you will find setup.exe and aescrypt.msi. On newer systems, you only need to run aescrypt.msi. However, if some of the required Microsoft libraries are not present, you will encounter an error. In that case, run setup.exe to install the required libraries.

If you are interest in using the console version of AES Crypt, it will be installed as "aescrypt.exe" in the installation directory with the other AES Crypt files.

NOTE: If you attempt to run setup.exe and the required Microsoft libraries are already installed, you will get an error message indicating that the run-time libraries on the machine are already installed or are newer. That is normal; just run aescrypt.msi.

3.3 Installing on Windows (console, non-GUI)

No installation is required. Just unzip the downloaded file and you will see aescrypt.exe. You can execute this program from the command prompt. Since no installation is required, you can use this binary on flash drives or other external media.

3.4 Installing on Mac

Download the program ZIP file, unZIP the archive, and install as you would any other Mac program. The *AESCrypt.app* file can be found in the *Applications* directory. You can also drag it to the dock for quicker access, as noted below.

3.5 Installing on Linux (GUI)

The following describes the procedures for Ubuntu. Other Linux variants would be similar to this.

- Download the current Linux GUI version for your operating system (32-bit or 64-bit) and place that in the "Downloads" folder (or somewhere where you can find it).
- Extract the .gz file to get the install file (using Nautilus, just right-click on the file and select "Extract Here")
- Right-click on the -install file and select "Properties". Under the "Permissions" tab, check the "Allow executing file as program"
- Now we need to run the program, but you must be root to do that. Here's one way:
    - Click on the "Ubuntu" logo and type "terminal" in the search box to find the terminal application; open it (or, just type CTRL+ALT+T to open it directly)
    - At the $ prompt, change directories to where the AESCrypt install package is located. If you downloaded it to the Downloads folder, type "cd Downloads".
    - Type "./AESCrypt-GUI-1.0-Linux-x86_64-Install" (or whatever the name of the install package is; usually typing ./AES" and hitting the tab key will cause the shell to expand complete the command for you).
    - You will be prompted to enter the root password to install.
    - From here, you just follow the instructions, which is mostly just clicking "Next".

See the usage instructions below to make it easy to use AES Crypt with your file manager.

NOTE: If you are fairly familiar with working in the shell, then it's much easier to just use the shell to extract the file and install it than trying to do part of it in the GUI and part at the command-line. You can choose whichever approach you prefer.

3.6 Installing on Linux (non-GUI)

To install the command-line version, you will need the GNU C compiler and the “make” utility.

Extract the source archive using a command like this:

```
tar -xzf aescrypt-x.y.z.tgz
```

Replace x.y.z with the version information that is a part of the filename. This should create a directory with the same name, but without .tgz.

Next change directories into aescrypt-x.y.z/src (or whatever the name of the directory is that is created).

Type "make". If this succeeds, you should have the executable files compiled in the directory. To install them, you can type "make install" or manually copy the executable files wherever you want them. The two executable names are "aescrypt" and "aescrypt_keygen".

NOTE: in a subsequent release, “aescrypt_keygen” will be integrated with “aescrypt”. So, do not be surprised if your release is newer than this document.)

4 Using AES Crypt

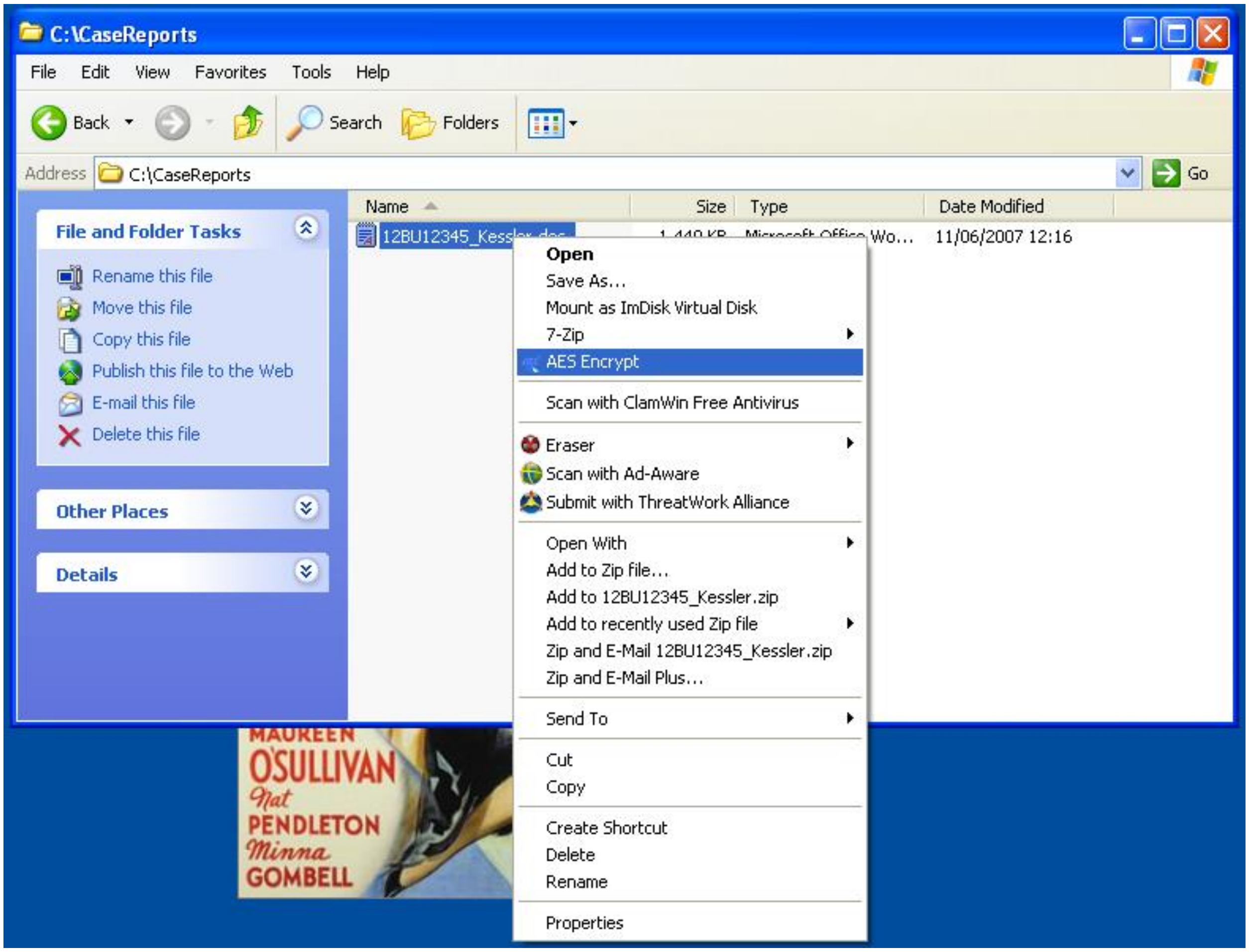
4.1 Using Windows (GUI)

4.1.1 Encrypting Files

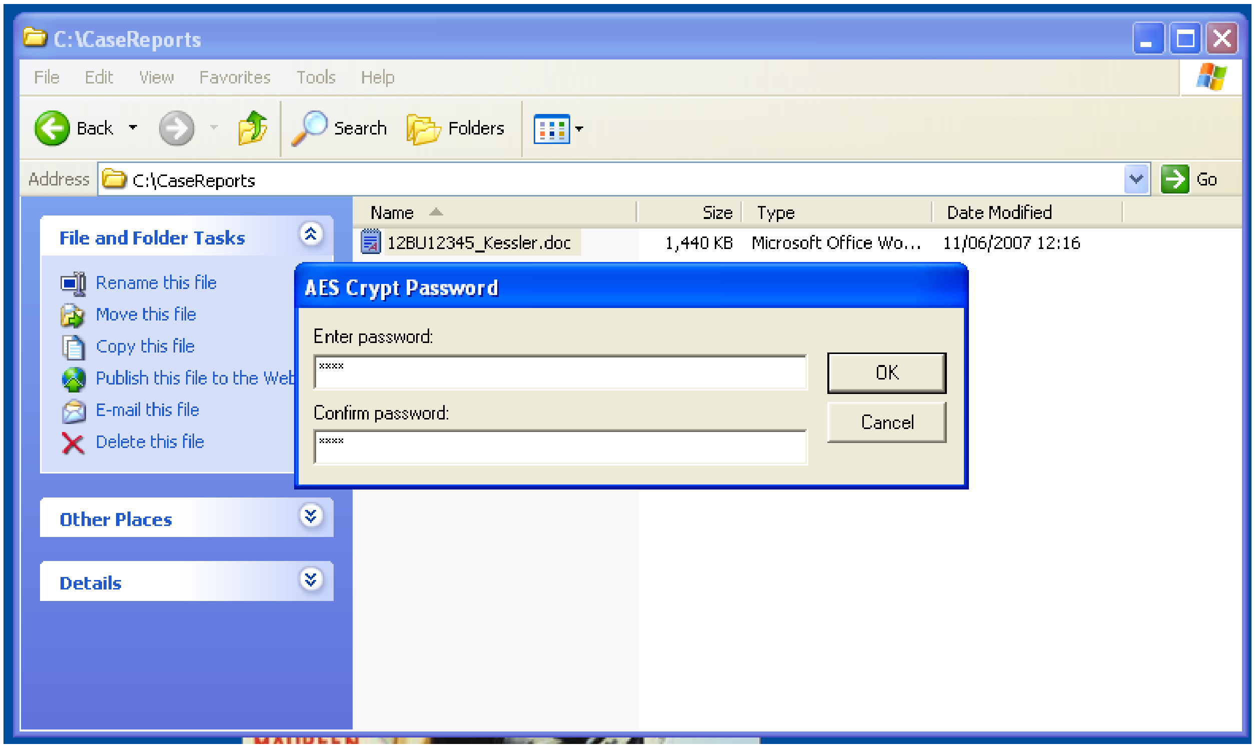
Use the following steps to encrypt a file with AES Crypt:

1. Right-click on the file in Windows Explorer and select “AES Crypt”
2. Enter the password in the dialogue box and click “OK”.
3. The encrypted file will appear with the same name as the original file, but with an “.aes” extension.

The screen shots below detail these steps. First, find the file you wish to encrypt in Windows Explorer. When you right-click, the context menu will appear and click on “AES Crypt”.



You will be asked to enter the file password twice in a dialogue box; do so and click “OK”.



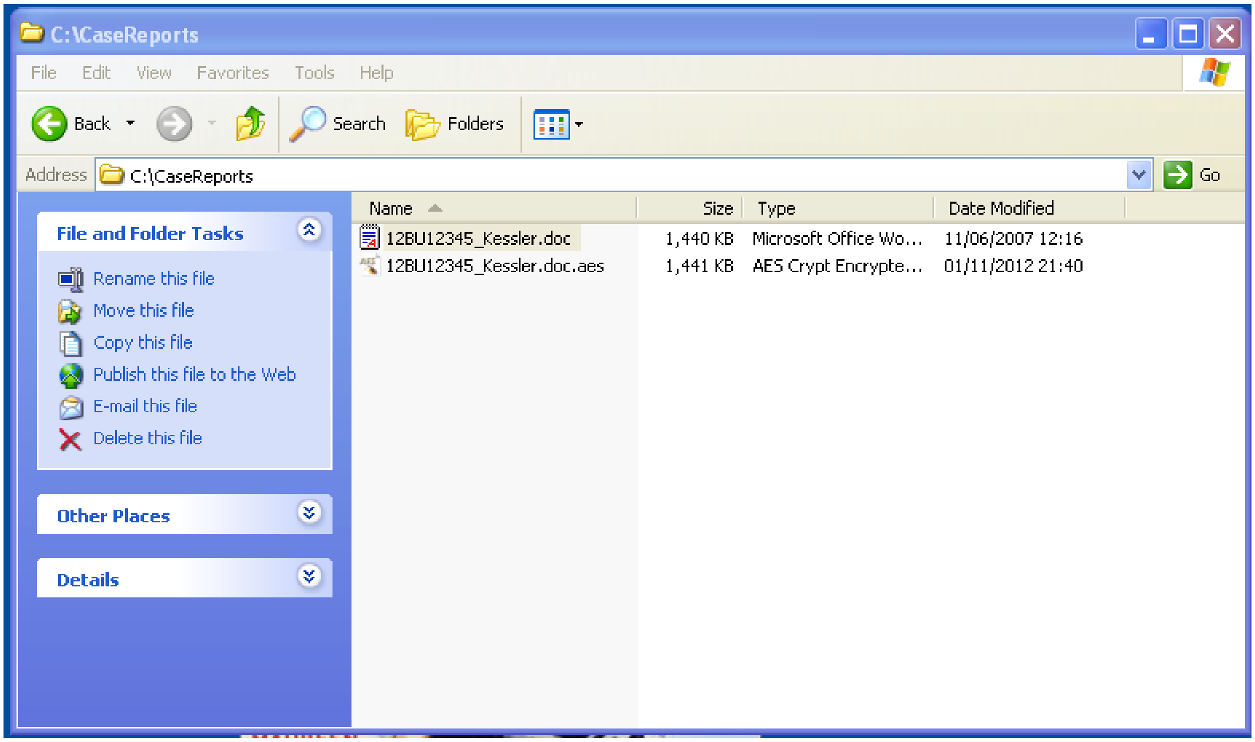
Address: C:\CaseReports

Name	Size	Type	Date Modified
12BU12345_Kessler.doc	1,440 KB	Microsoft Office Wo...	11/06/2007 12:16

Enter password: ****

Confirm password: ****

The encrypted file will appears in the same directory using the original file name with an “.aes” file extension.



Address: C:\CaseReports

Name	Size	Type	Date Modified
12BU12345_Kessler.doc	1,440 KB	Microsoft Office Wo...	11/06/2007 12:16
12BU12345_Kessler.doc.aes	1,441 KB	AES Crypt Encrypte...	01/11/2012 21:40

NOTE: Some email clients will refuse to send or receive files with a double extension (e.g., report.doc.aes). ZIPping and renaming the file prior to sending it will fix this problem, but be sure to let the receiving party know how to get the original file back.

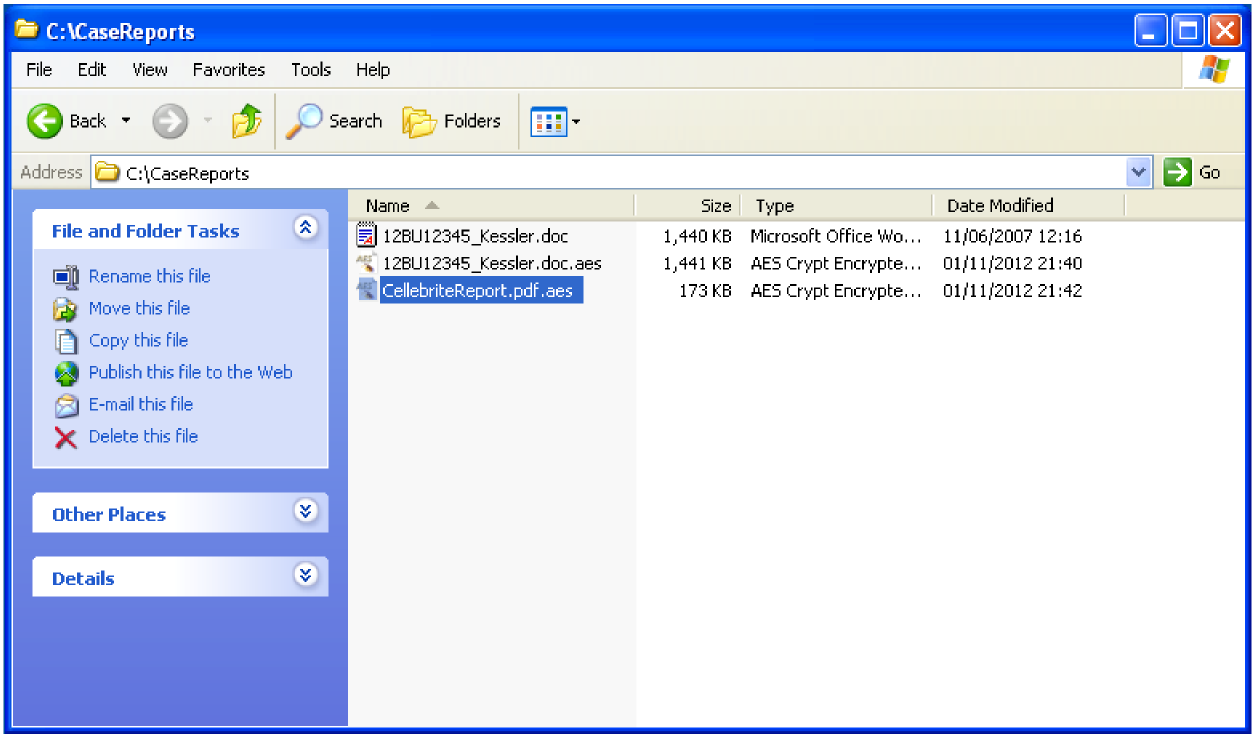
4.1.2 Decrypting Files

Use the following steps to decrypt a file with AES Crypt:

1. Double-click on the file in Windows Explorer
2. Enter the password in the dialogue box and click “OK”.
3. The decrypted file will appear with the same name as the encrypted file, but without the “.aes” file extension.

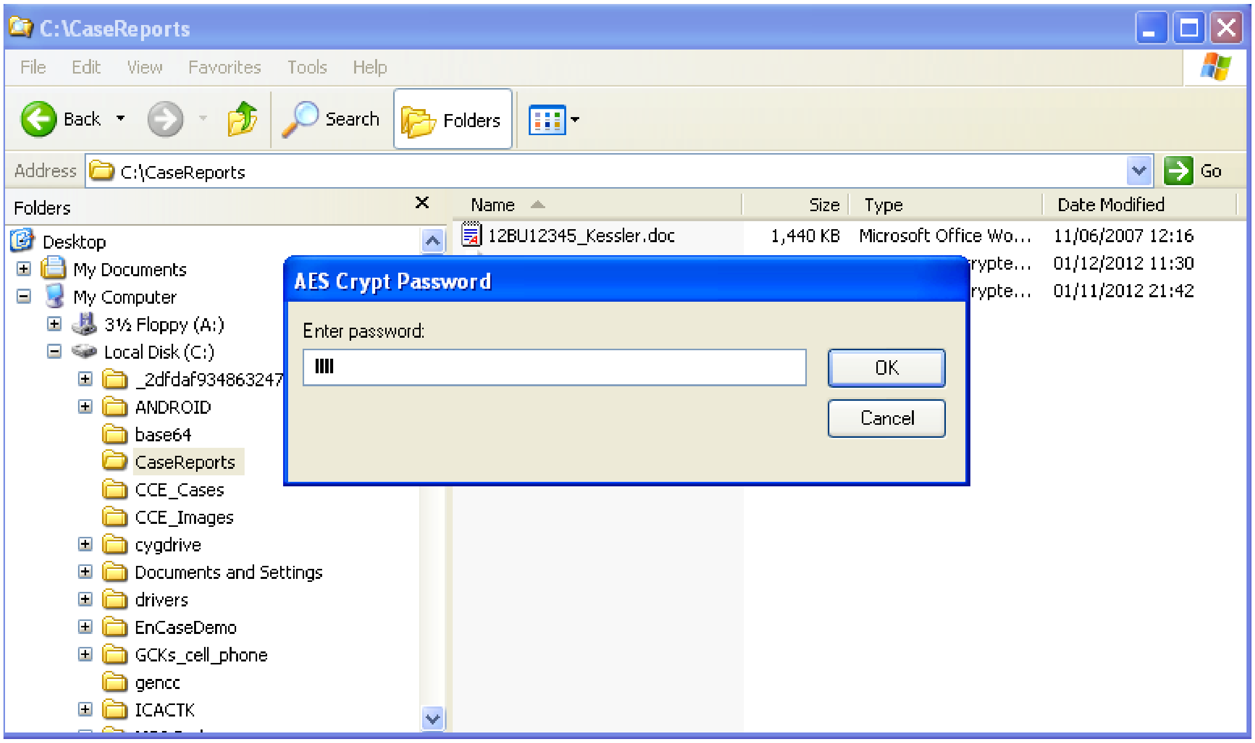
As an alternative to step 1, you may also right-click on the file in the same way as you would to encrypt the file. In that case, AES Crypt will offer a menu option of “AES Decrypt” that you may select to decrypt the file.

The screenshots below detail these steps. First, find the file you wish to decrypt in Windows Explorer.



Name	Size	Type	Date Modified
12BU12345_Kessler.doc	1,440 KB	Microsoft Office Wo...	11/06/2007 12:16
12BU12345_Kessler.doc.aes	1,441 KB	AES Crypt Encrypte...	01/11/2012 21:40
CellebriteReport.pdf.aes	173 KB	AES Crypt Encrypte...	01/11/2012 21:42

Double-click on the filename, enter the password in the dialogue box, and click “OK”.

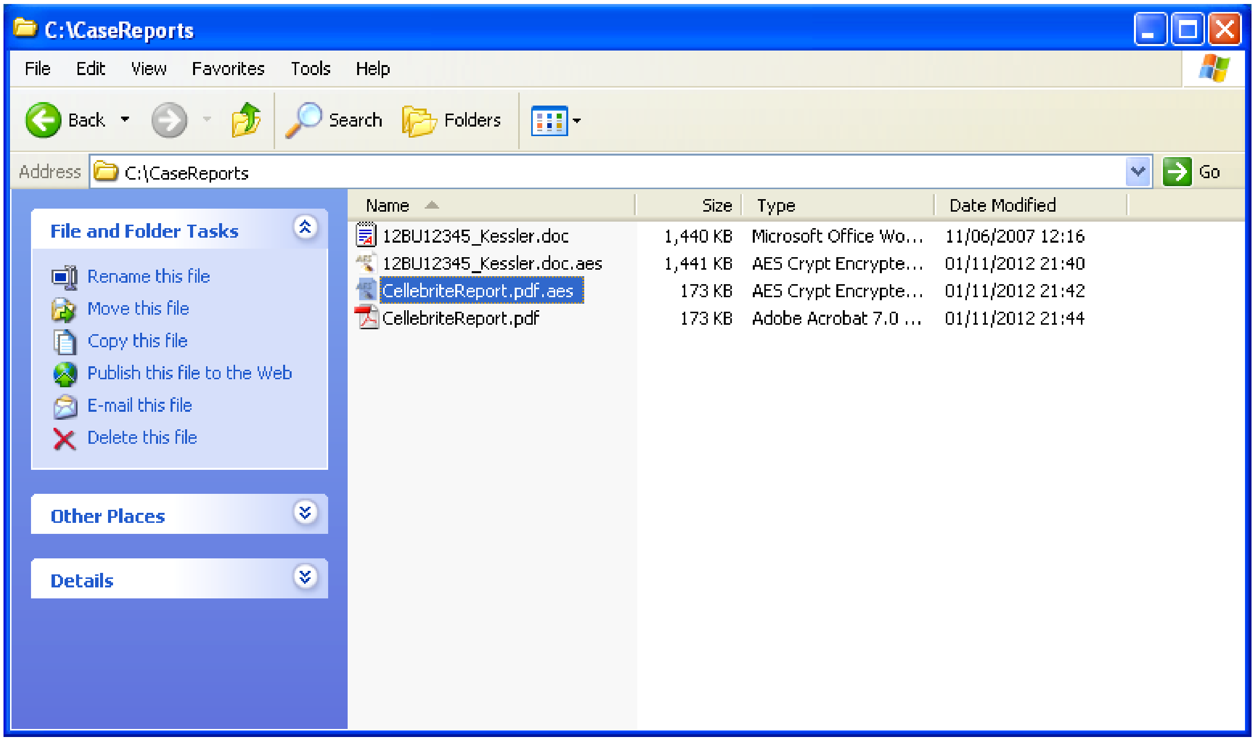


Name	Size	Type	Date Modified
12BU12345_Kessler.doc	1,440 KB	Microsoft Office Wo...	11/06/2007 12:16
		rypte...	01/12/2012 11:30
		rypte...	01/11/2012 21:42

AES Crypt Password

Enter password: ||||

The unencrypted file will appears with the same name as the encrypted file, but without the “.aes” file extension.



Name	Size	Type	Date Modified
12BU12345_Kessler.doc	1,440 KB	Microsoft Office Wo...	11/06/2007 12:16
12BU12345_Kessler.doc.aes	1,441 KB	AES Crypt Encrypte...	01/11/2012 21:40
CellebriteReport.pdf.aes	173 KB	AES Crypt Encrypte...	01/11/2012 21:42
CellebriteReport.pdf	173 KB	Adobe Acrobat 7.0 ...	01/11/2012 21:44

4.2 Using Windows (console, non-GUI)

If you prefer working at the command-line (console) on Windows, you can use the “aescrypt” utility from there. If you downloaded the GUI version and installed that, the command-line utility will be in the same directory as the GUI binaries; it is named “aescrypt.exe”. If you downloaded the command-line version, there is no installation procedure and you place it wherever you wish.

Using the windows command-line version is exactly like the Linux version. Rather than replicate those instructions, please refer to the instructions for the Linux command-line version.

NOTE: the Windows command-line version does not support the -k switch, nor does it have the “aescrypt_keygen” utility. This is planned, but has not been implemented as of the date this document was published.

4.3 Using Mac OS X

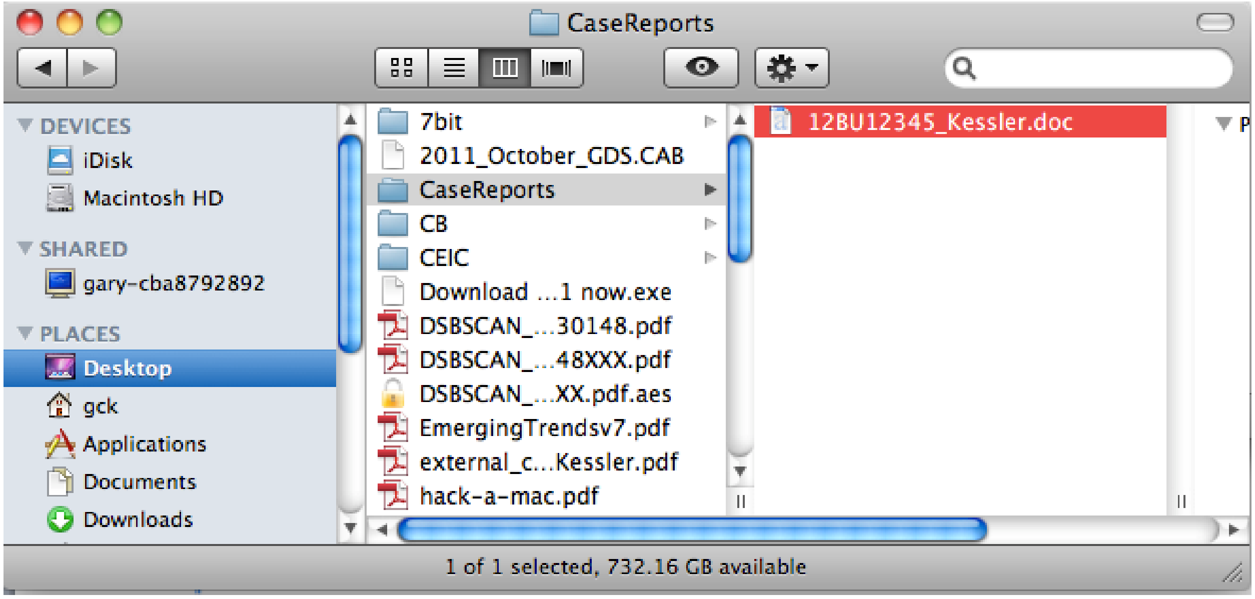
4.3.1 Encrypting Files

Use the following steps to encrypt a file with AES Crypt:

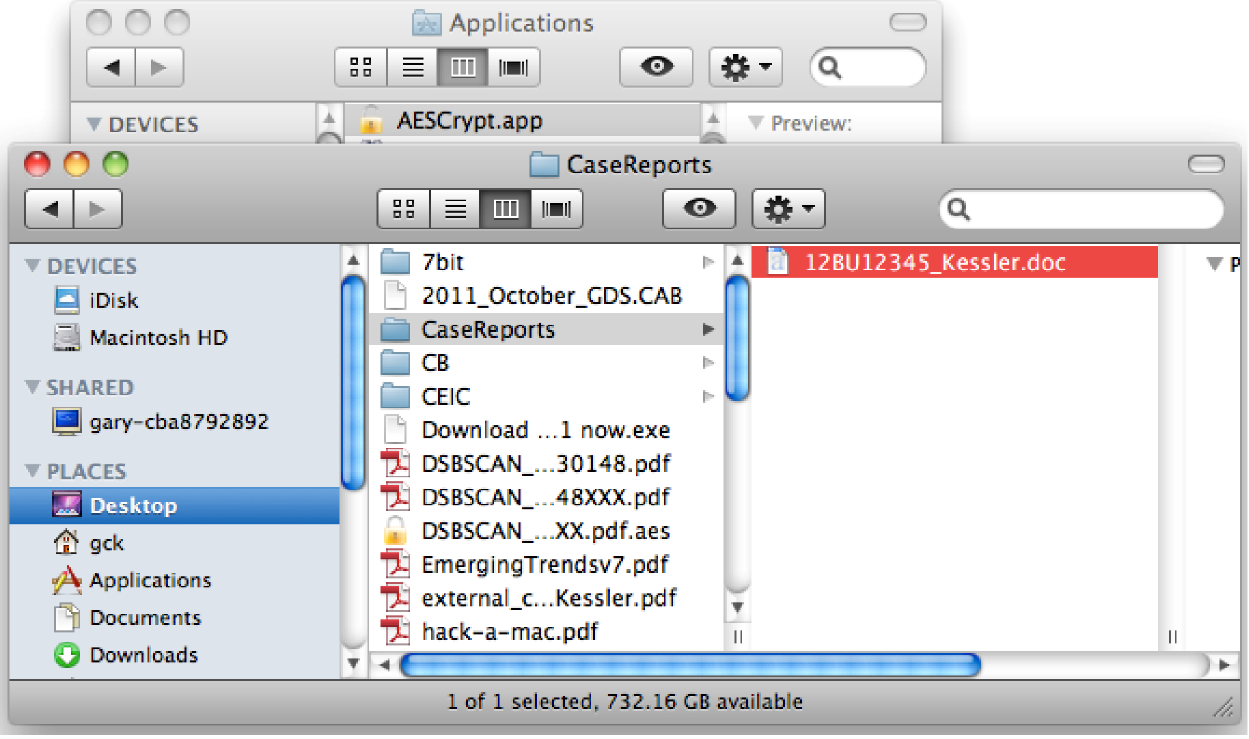
1. Find the file in Finder and drag it to the *AESCrypt.app* file or the AES Crypt icon on the dock.
2. Enter the password in the dialogue box and click “Continue”.
3. The encrypted file will appear with the same name as the original file a “.aes” file extension.

WARNING: If you already have a file with the same name and “.aes” extension, this process will over-write the existing “.aes” file!

The screenshots below detail these steps. First, find the file you wish to encrypt in Finder.

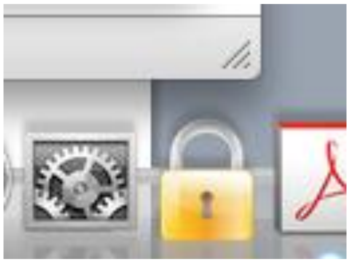


Drag the file to encrypt onto the *AESCrypt.app* file in the Applications directory ***or***…

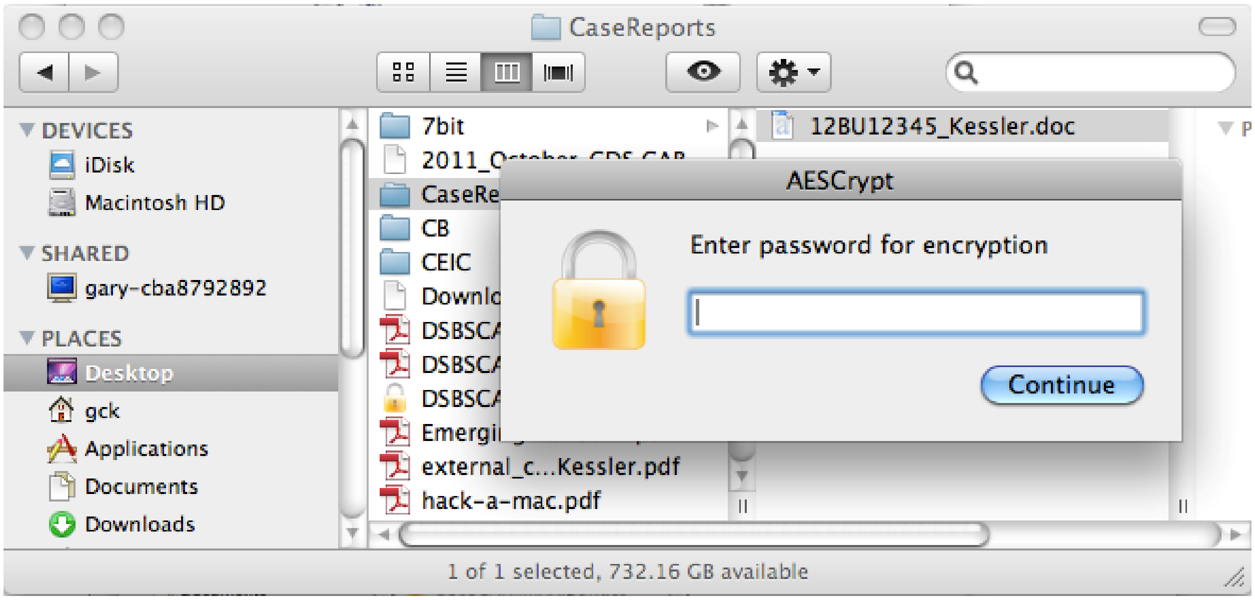


1 of 1 selected, 732.16 GB available

… drag the file onto the AES Crypt "lock" icon on the dock.



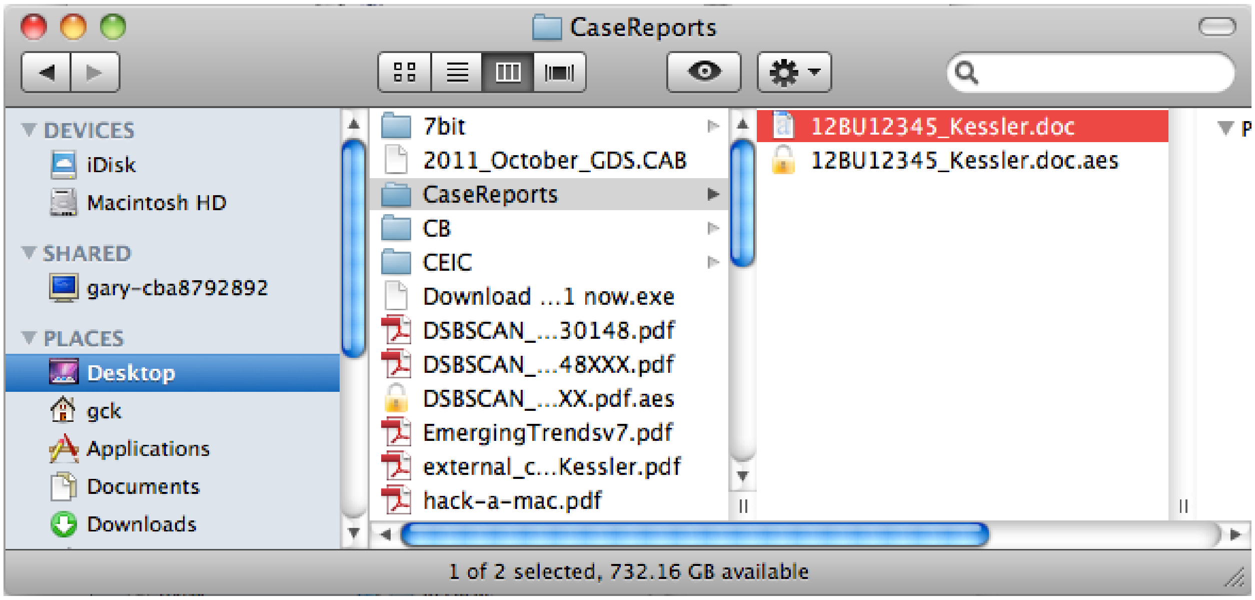
Enter the password into the dialogue box and click “Continue”.



AESCrypt

Enter password for encryption

The encrypted file will appear in the same directory using the original file name with an “.aes” file extension.



NOTE: Some email clients will refuse to send or receive files with a double extension (e.g., report.doc.aes). ZIPping and renaming the file prior to sending it will fix this problem, but be sure to let the receiving party know how to get the original file back.

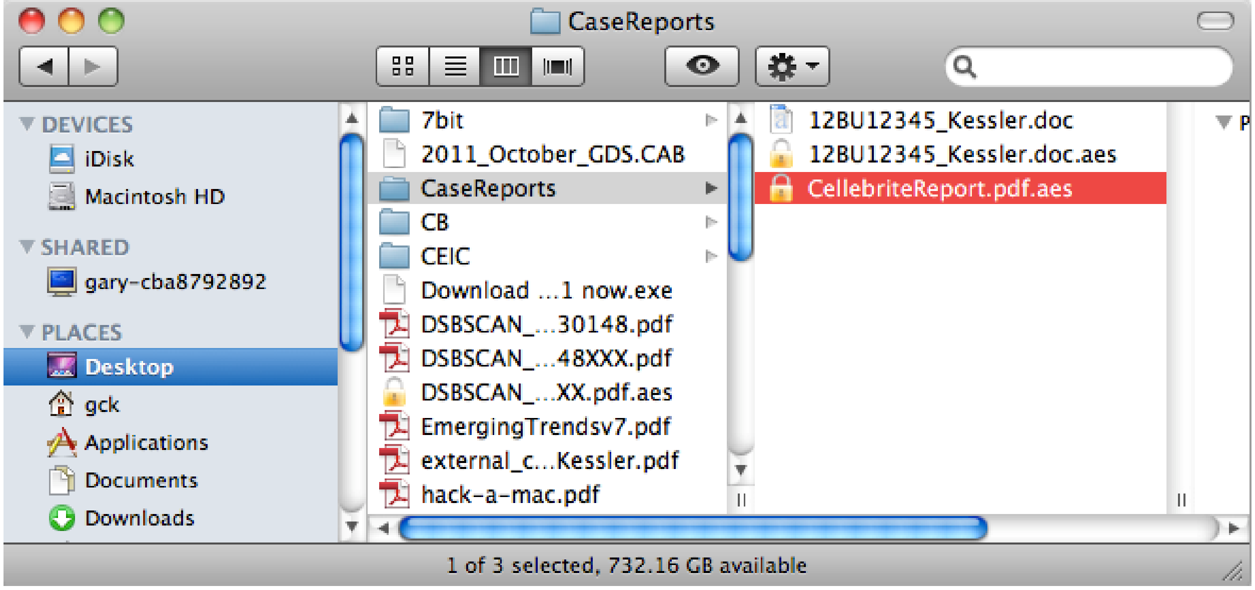
4.3.2 Decrypting Files

Use the following steps to decrypt a file with AES Crypt:

1. Double-click on the file in Finder.
2. Enter the password in the dialogue box and click "Continue".
3. The decrypted file will appear with the same name as the encrypted file, but without the ".aes" file extension.

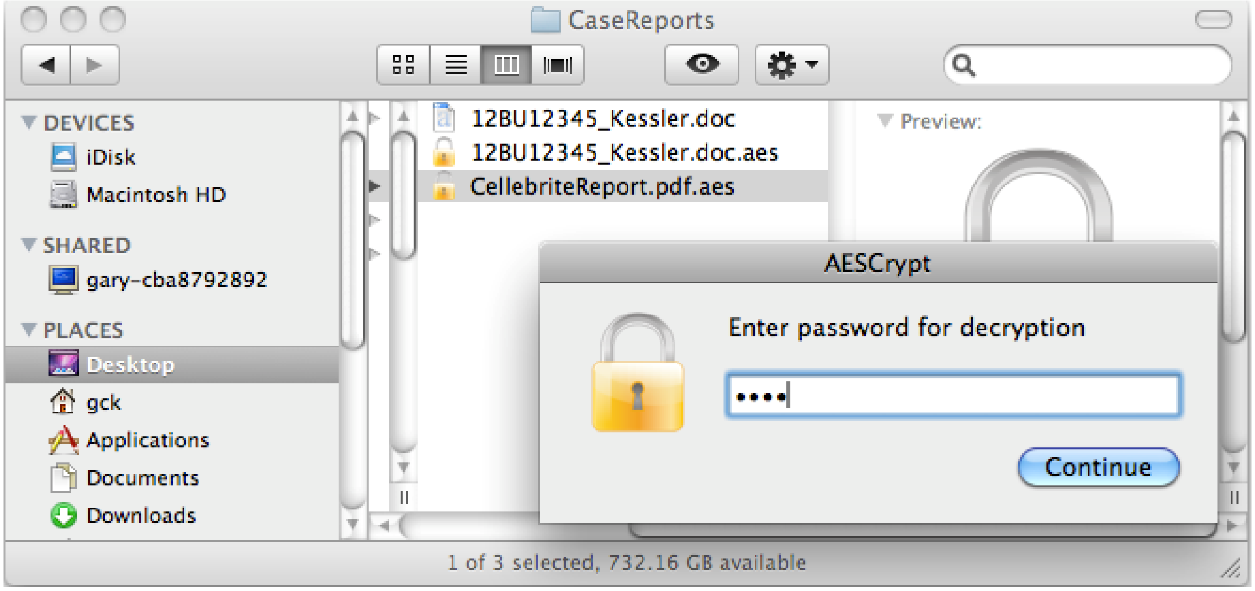
WARNING: If you already have a file with the same name as the encrypted file, but without the ".aes" extension, this process will over-write the existing file!

The screenshots below detail these steps. First, find the file you wish to decrypt in Finder.



1 of 3 selected, 732.16 GB available

Double-click on the filename, enter the password in the dialogue box, and click “Continue”.

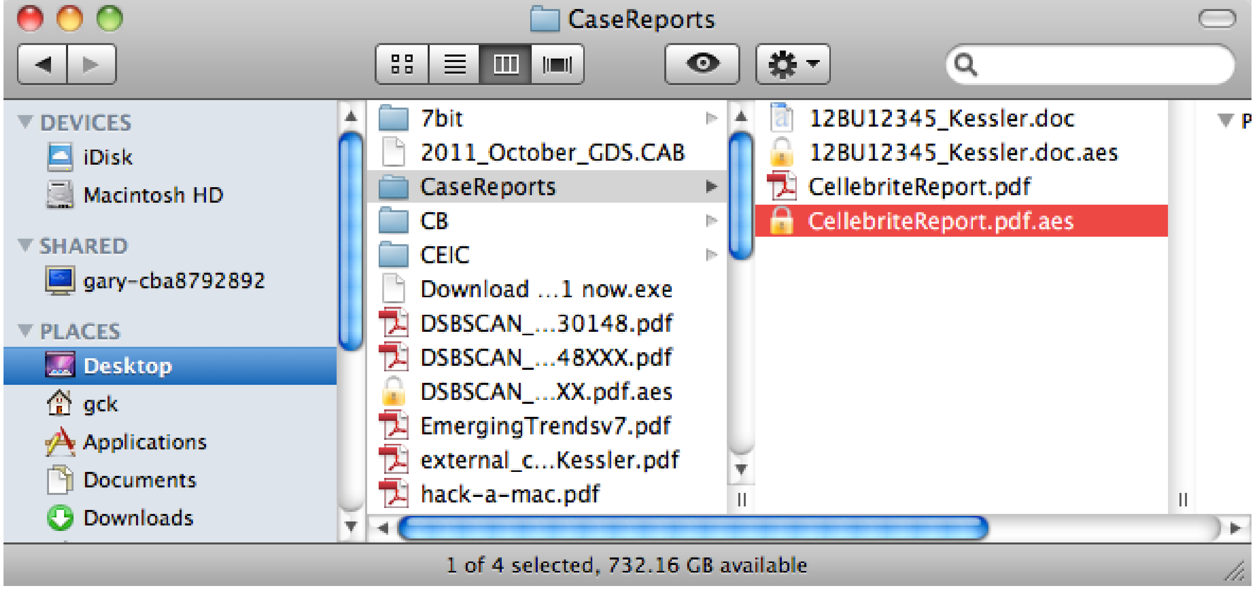


Enter password for decryption

••••

1 of 3 selected, 732.16 GB available

The unencrypted file will appear with the same name as the encrypted file, but without the “.aes” file extension.



1 of 4 selected, 732.16 GB available

4.4 Using Linux (GUI)

4.4.1 Encrypting Files

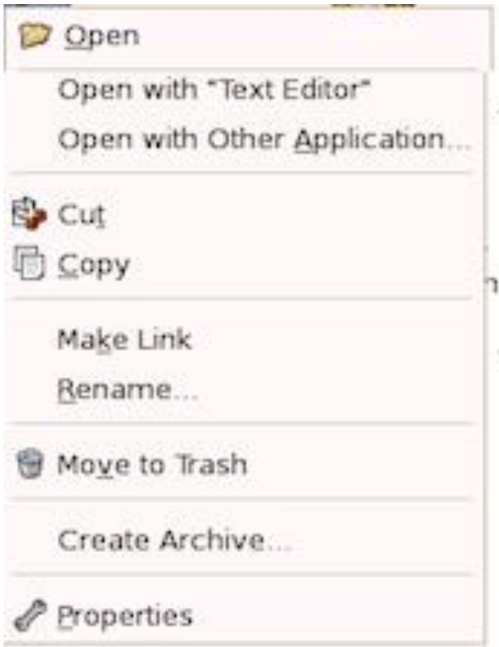
Use the following steps to encrypt a file with AES Crypt:

1. Find the file in your file browser (usually “Dolphin” in KDE or “Nautilus” in Gnome) and right-click in the file.

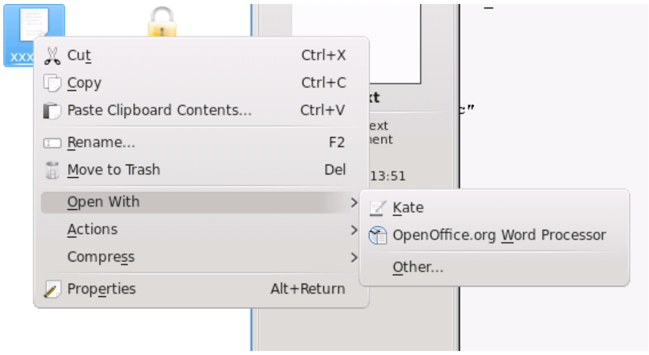
2. Select “AESCrypt” (you may have to select “Open with…” and locate the AES Crypt application the first time).
3. Enter the password in the dialogue box and click “OK”.
4. The encrypted file will appear with the same name as the original, but with an “.aes” file extension.

WARNING: If you already have a file with the same name and “.aes” extension, this process will over-write the existing “.aes” file!

The screenshots below detail these steps. First, find the file you wish to encrypt in your file browser. Gnome is on the left and KDE is on the right.



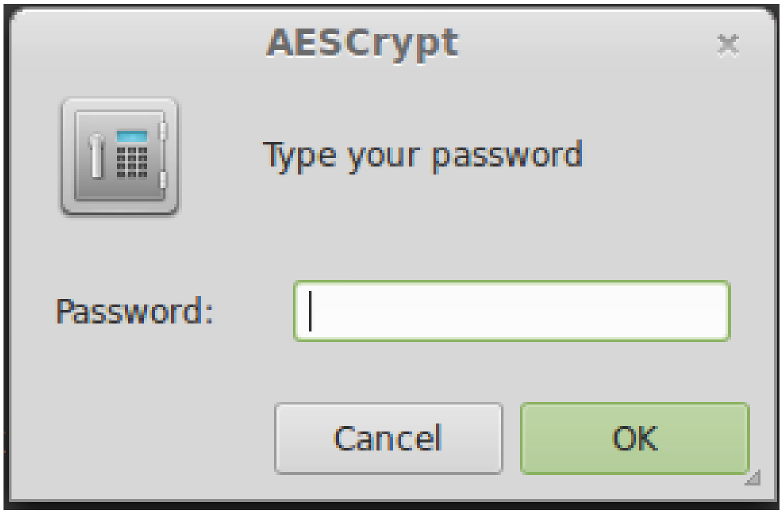
For Gnome, choose “**Open with Other Application…**”



For KDE, choose “**Other…**”

Once you have done this step once, AES Crypt should be offered to you as a choice in the secondary menu when you wish to encrypt a file of the same type.

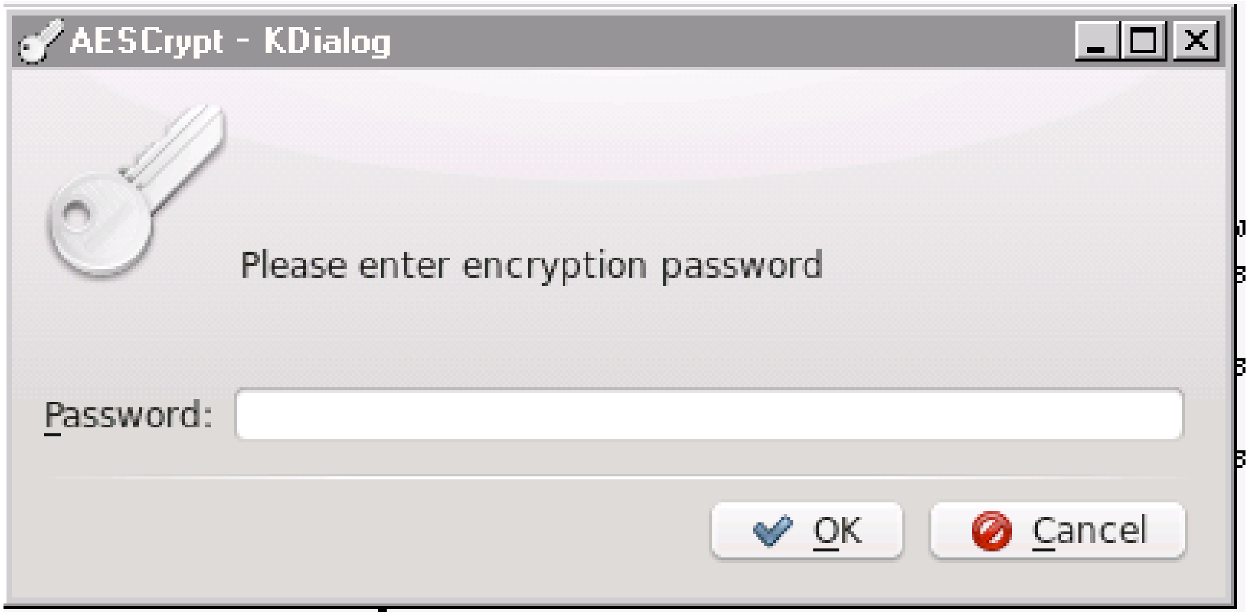
You will get a dialogue asking for your password twice:



Type your password

Password:

Gnome Password Prompt

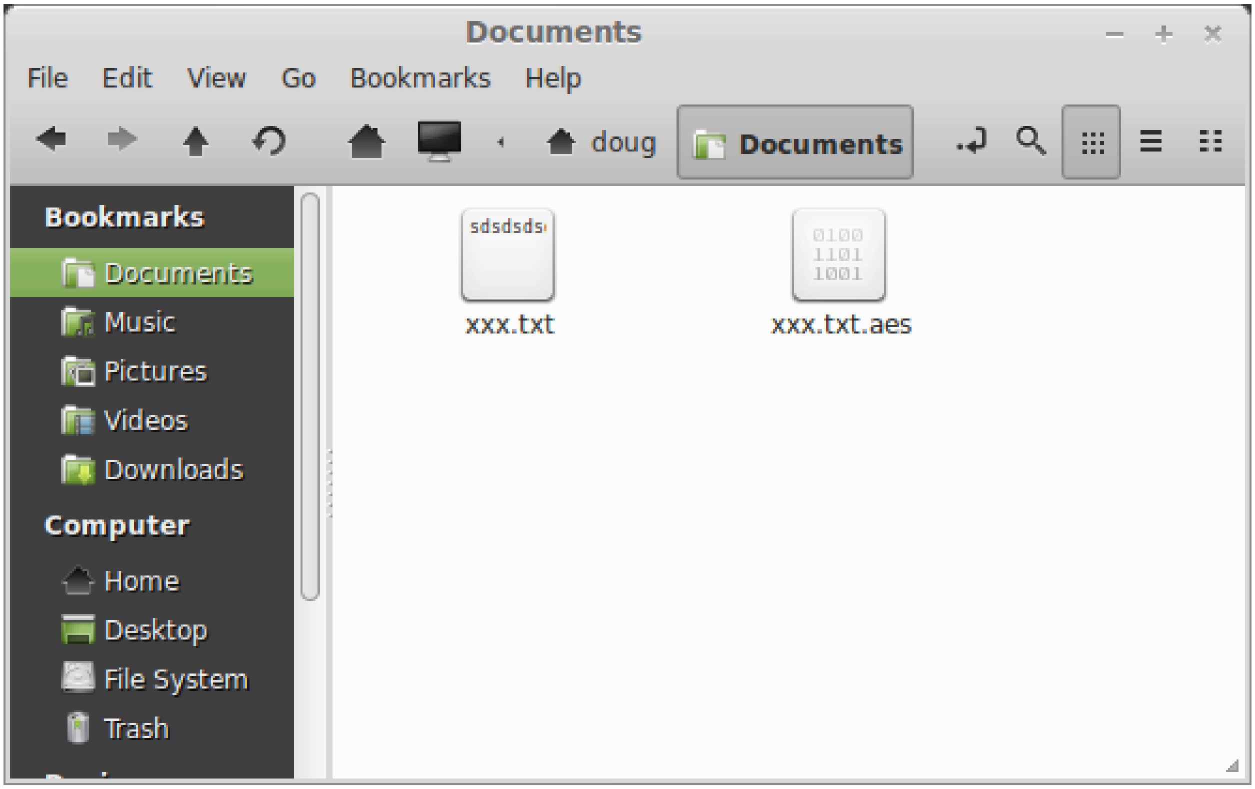


Please enter encryption password

Password:

KDE Password Prompt

The encrypted file will appear in the same directory as the original file, but with a ".aes" file extension.



(Linux Mint shown above)

NOTE: Some email clients will refuse to send or receive files with a double extension (e.g., report.doc.aes). ZIPping and renaming the file prior to sending it will fix this problem, but be sure to let the receiving party know how to get the original file back.

4.4.2 Decrypting Files

Use the following steps to decrypt a file with AES Crypt:

1. Initially you will need to follow step 2 in the previous section to establish AES Crypt as the default handler for the ".aes" file extension. Once this has been done, you can simply double-click on the file in the file manager.
2. Enter the password in the dialogue box and click "OK".
3. The decrypted file will appear with the same name as the encrypted file, but without the ".aes" file extension.

WARNING: If you already have a file with the same name as the encrypted file, but without the ".aes" extension, this process will over-write the existing file!

4.5 Using Linux (command-line)

If you prefer to use AES Crypt from the command-line, can do so by either installing the source code version of AES Crypt or the GUI version. With either, the tool for encrypting files is called “aescrypt”. With the current Linux source code package, there is another tool called “aescrypt_keygen” which can be used to generate random keys in key files that may be used with aescrypt using the -k flag.

Typing “aescrypt -?” will show usage information for aescrypt:

```
aescrypt {-e|-d} [ { -p <password> | -k <keyfile> } ] { [-o <output
filename>] <file> | <file> [<file> ...] }
```

You do not need to be an expert to use AES Crypt for Linux to securely encrypt your data files. To encrypt a file, you simply enter the "aescrypt" command with the appropriate command-line arguments.

Suppose you have a file called "picture.jpg" that you would like to encrypt using the password "apples". You would enter the following command:

```
aescrypt -e -p apples picture.jpg
```

That's it! The program will create a file with the name "picture.jpg.aes".

When you want to later decrypt the file "picture.jpg.aes", you would enter the following command:

```
aescrypt -d -p apples picture.jpg.aes
```

The program will create the file "picture.jpg", containing the contents of the original file before it was encrypted.

Of course, many Linux users create sophisticated scripts that pipe input from one program into another, and AES Crypt fully supports such usage. For example, you could backup files and encrypt them with a command like this:

```
tar -cvf - /home | aescrypt -e -p apples - >backup_files.tar.aes
```

In all of the examples above, the password is provided on the command line. Since there are certain risks associated with that kind of usage, it may be preferred to let aescrypt prompt you to enter the password. This can be accomplished simply by not including the -p parameter, like this:

```
aescrypt -d picture.jpg.aes
```

AES Crypt will prompt you for the password, but what you enter will not be displayed on the screen.

What if you want to decrypt a file, but just want to have it displayed on the screen and not stored in a plaintext file? That's possible. To do that, just use this syntax:

```
aescrypt -d -o - passwords.txt.aes
```

AES Crypt for Linux has the ability to use an encryption key file. This more securely allows for automated backups or other system administration tasks where one needs to provide a password, but would prefer to not have it appear on the command-line and clearly cannot be there to enter it. To use a key file, first create a key file using the aescrypt_keygen utility. This program works like "aescrypt", allowing you to enter a password via the -p option or to be prompted for a password. The specified file it the key file. You use it like this:

```
aescrypt_keygen -p apples secret.key
```

Place the file "secret.key" somewhere secure. If you prefer to let the utility generate a random password for you of a specific length, then enter something like this:

```
aescrypt_keygen -g 64 secret.key
```

This will create a key file containing 64 random octets. Given the algorithm employed, this is roughly 381 random bits. For more information on the random number generation, see https://secure.packetizer.com/pwgen/.

Now when you wish to encrypt a file, you call AES Crypt like this:

```
tar -cvf - /home | aescrypt -e -k secret.key - >backup_files.tar.aes
```

Be sure to provide the full pathname to the key file.

NOTE: For those who are curious, the key file is nothing more than a UTF-16LE encoded file containing the password. One can use Notepad on Windows to create a key file. Just save the file using the "Unicode" format when saving. AES Crypt will actually accept either a UTF-16BE or UTF-16LE file as the parameter to -k as long as the byte order mark is preserved. See the Readme.txt in the source files for more details about the key file.