AES Crypt User Guide

Publication Date: 2013-08-13

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

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 both the Windows and Mac OSX operating systems; files encrypted on one platform are completely compatible with – and can be decrypted on – the other platform. 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 both platforms.

2 Program Installation

AES Crypt can be downloaded from http://www.aescrypt.com/download/. Choose the preferred package for your system; Windows users will want either the 32-bit or 64-bit GUI while Mac OSX users will probably want the Mac GUI (x86).

Download the program ZIP file, unZIP the archive, and install as you would any other Windows or Mac program. The Linux version uses a typical installer similar to those found on Windows machines instead of RPM or APT.

NOTE for Mac users: 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 Program Usage

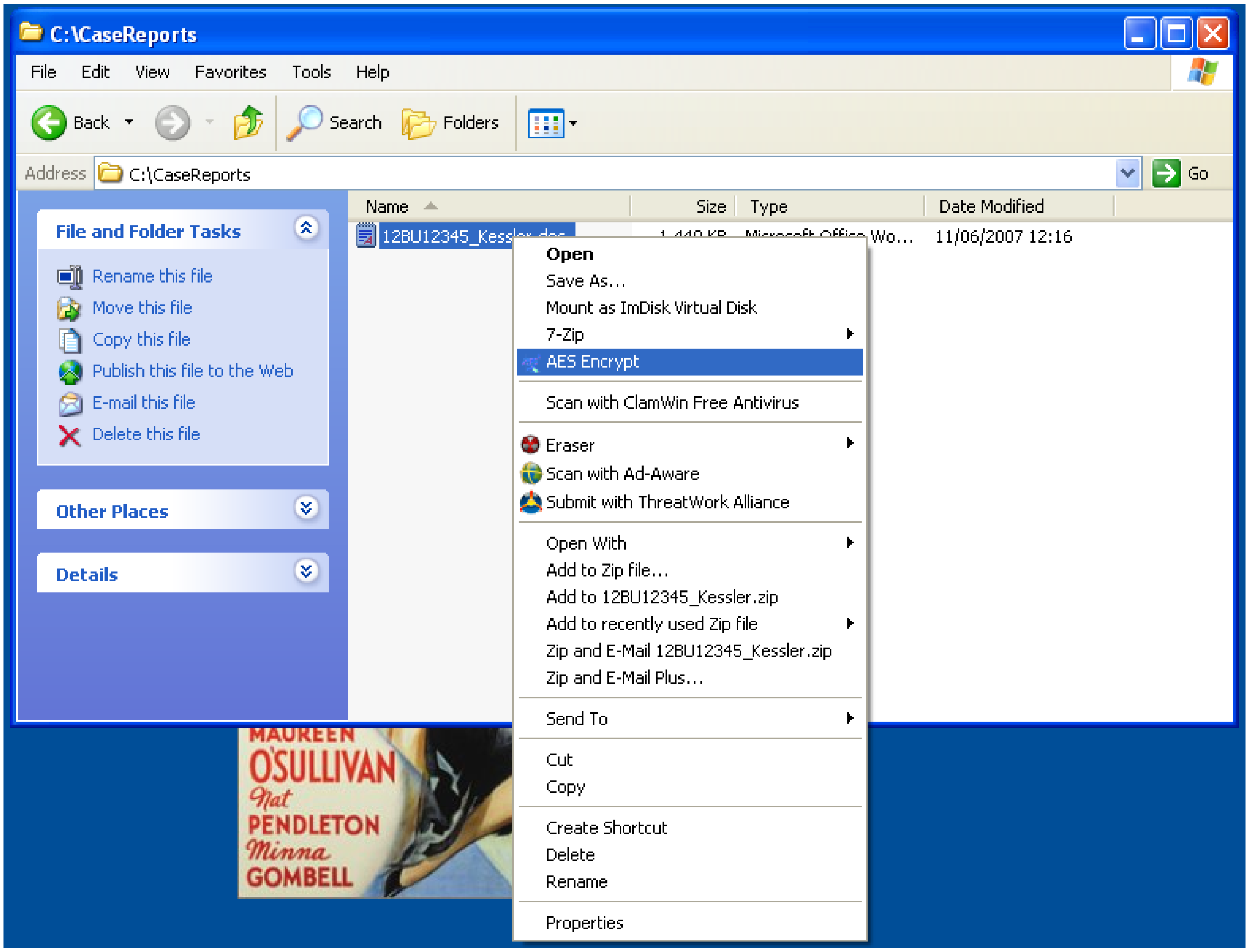
3.1 Using Windows

3.1.1 Encrypting Files

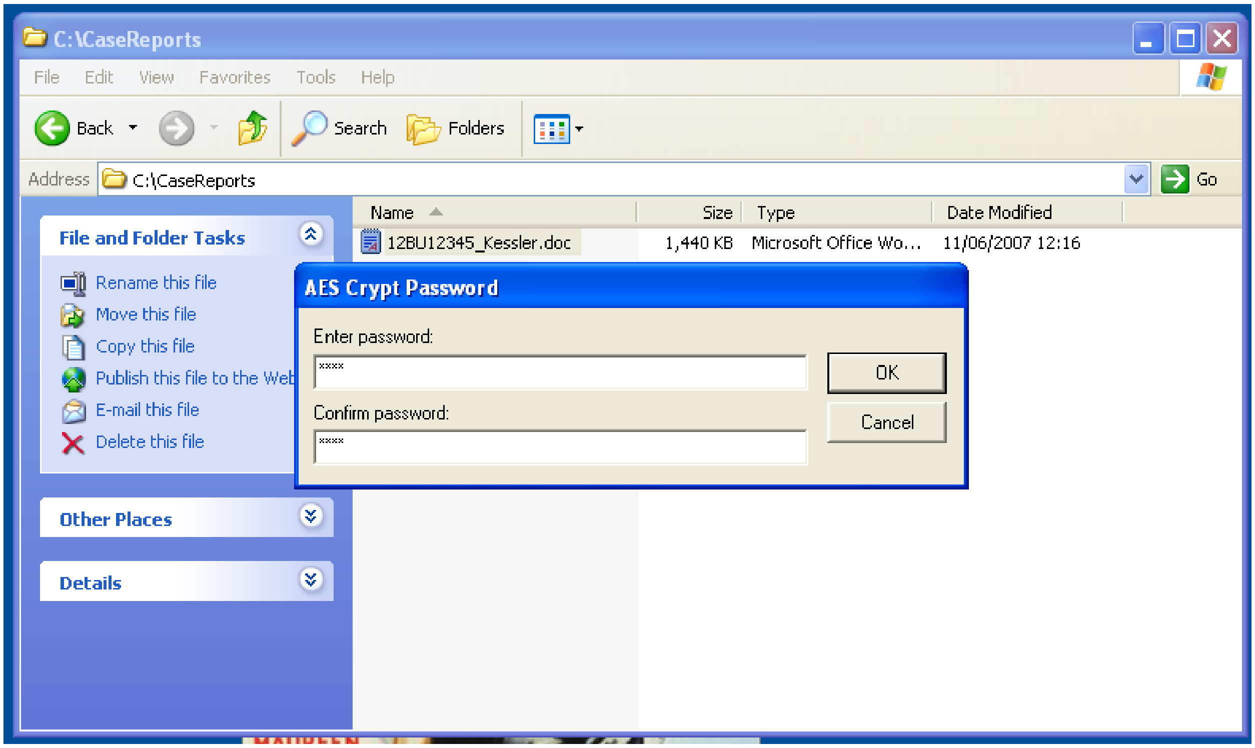
Use the following steps to encrypt a file with AES Crypt:

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”.

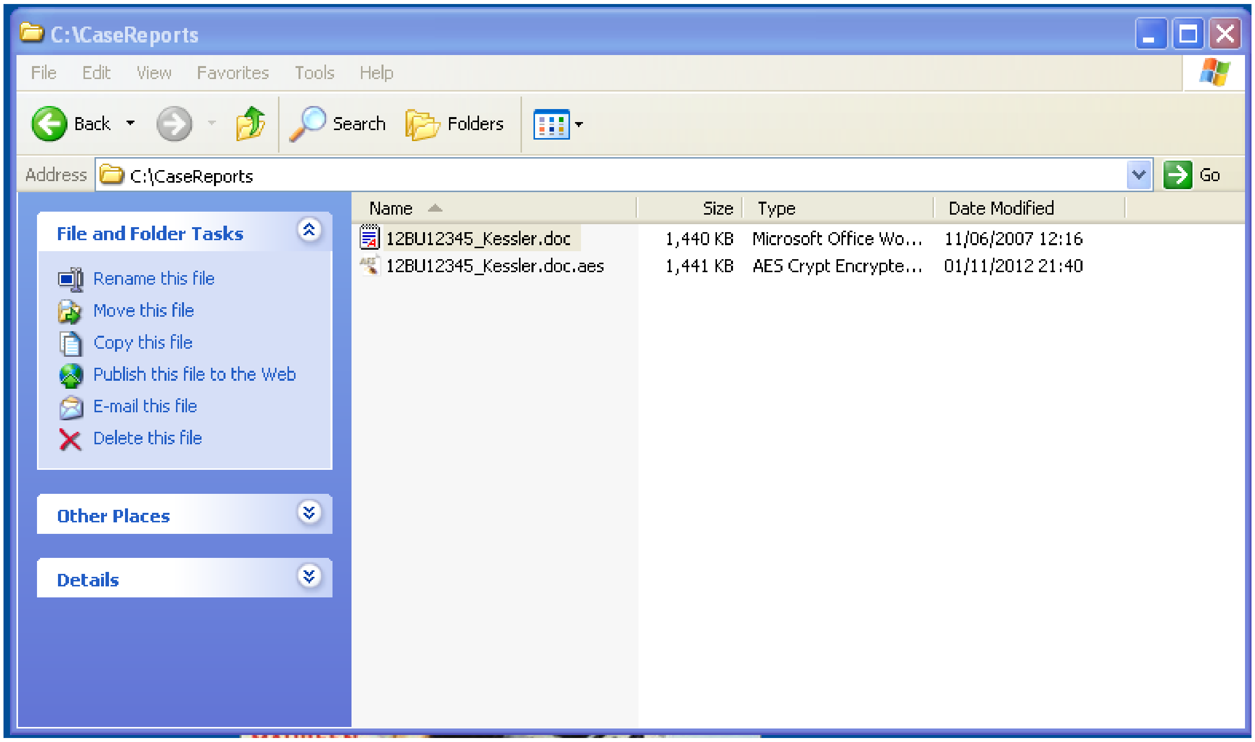


Name	Size	Type	Date Modified
12BU12345_Kessler.doc	1,440 KB	Microsoft Office Wo...	11/06/2007 12:16

Enter password: ****

Confirm password: ****

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



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.

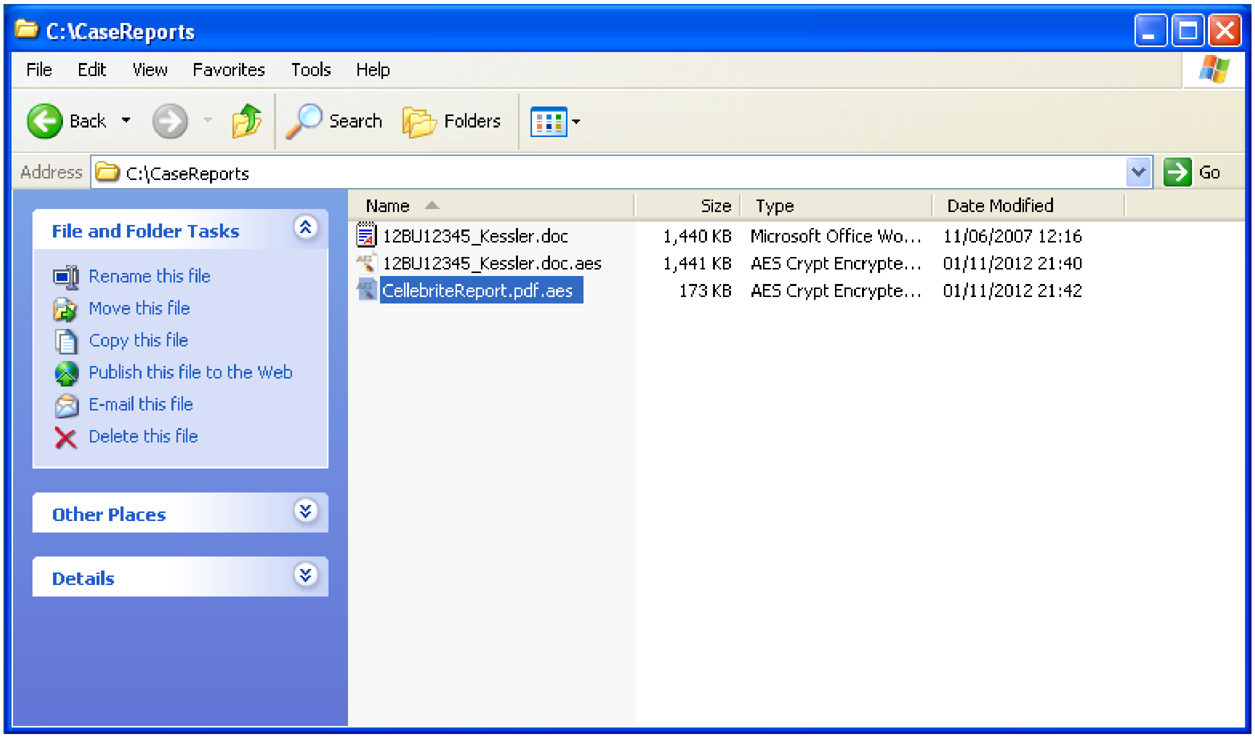
3.1.2 Decrypting Files

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.

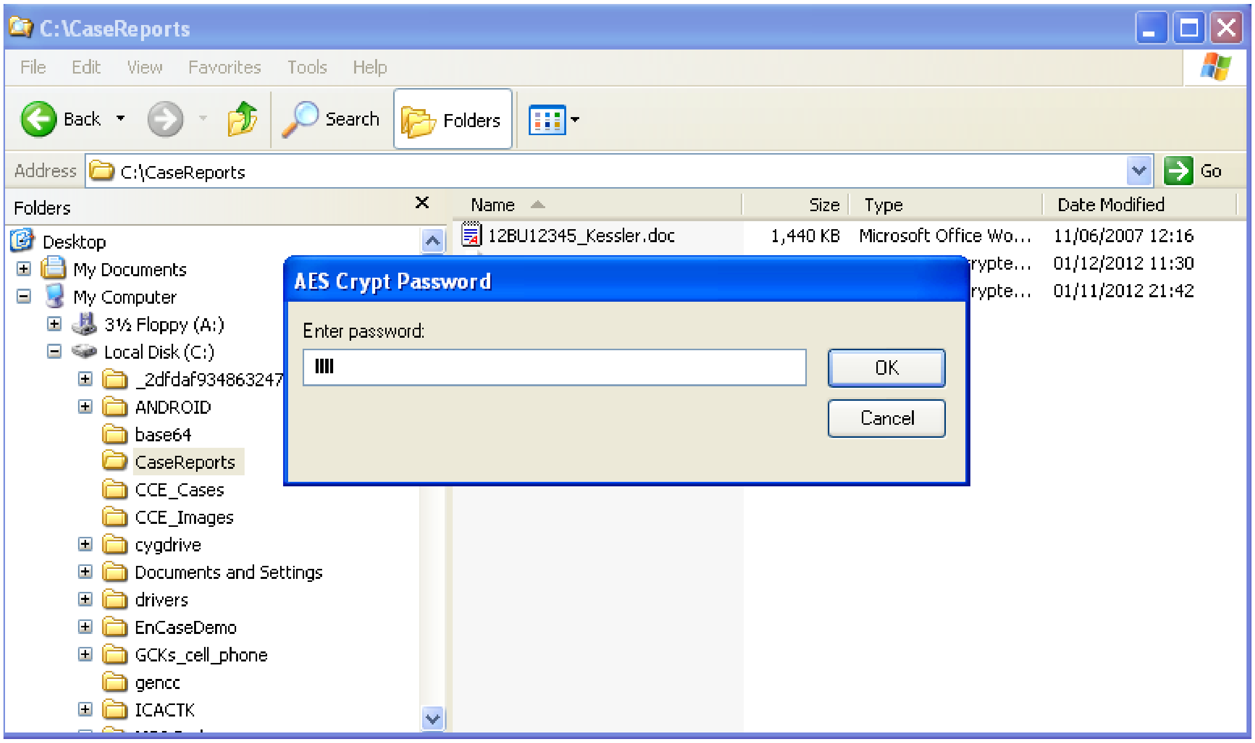
As an alternative to step 1, you may also right-click on the file in the same way as you would to encrypt the file. In that case, AES Crypt will offer a menu option of “AES Decrypt” that you may select to decrypt the file.

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”.

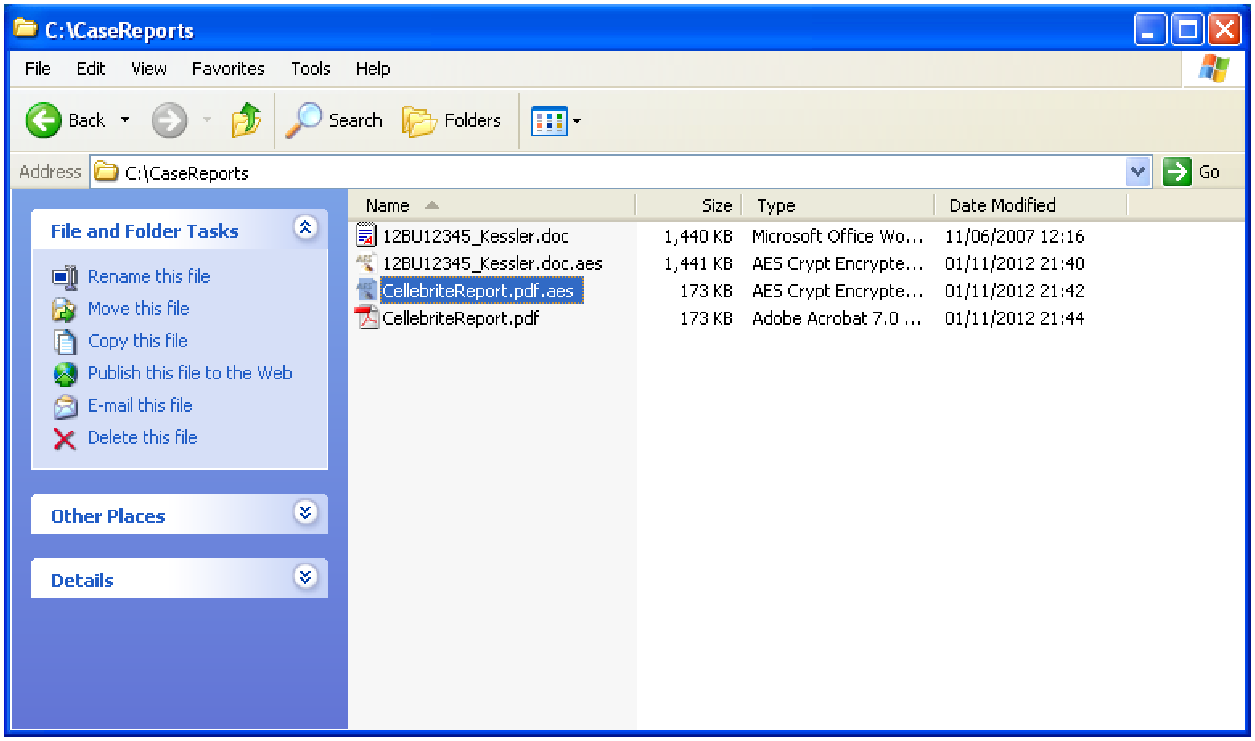


Address: C:\CaseReports

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

Enter password: IIII

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

3.2 Using Mac OS X

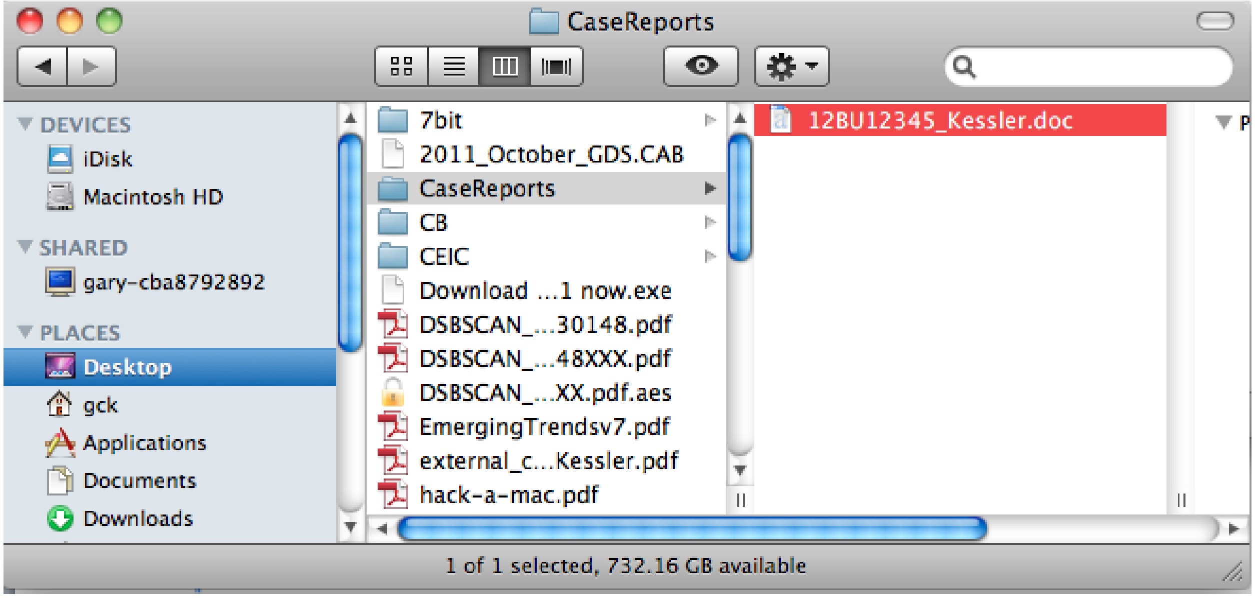
3.2.1 Encrypting Files

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

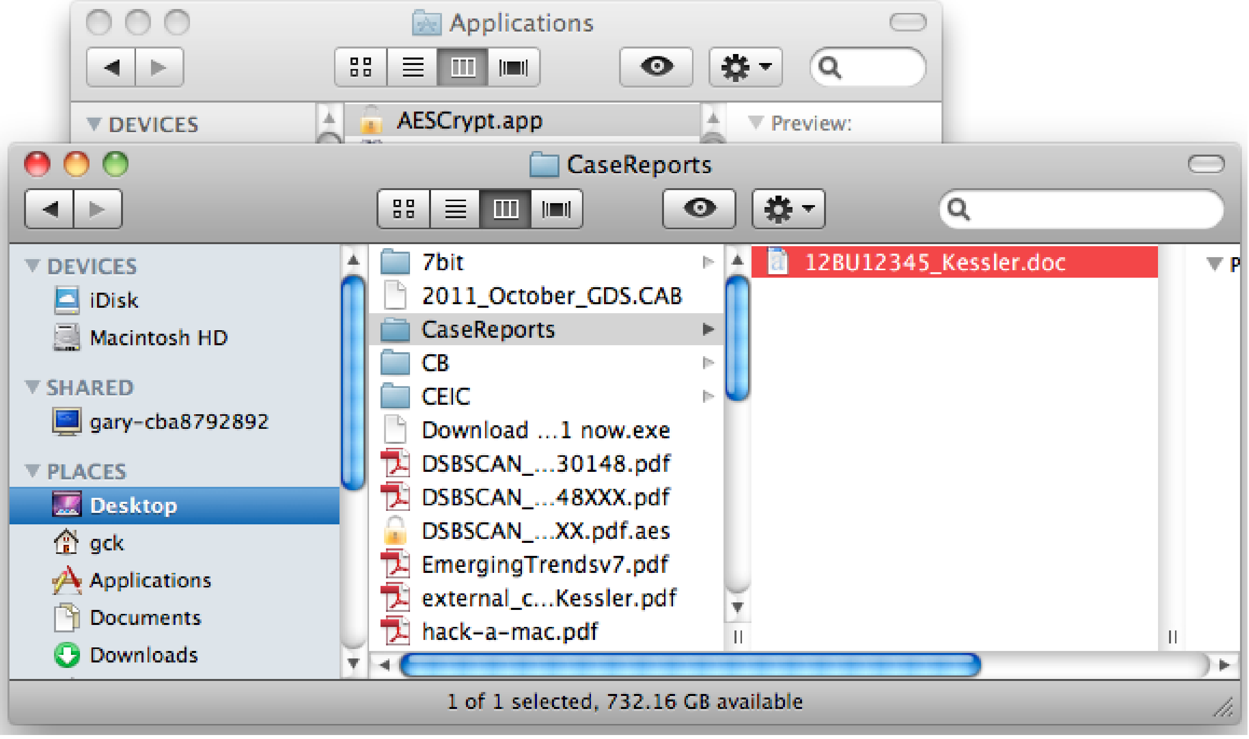
1. Find the file in Finder and drag it to the *AESCrypt.app* file or the AES Crypt icon on the dock.
2. Enter the password in the dialogue box and click “Continue”.
3. The encrypted file will appear with the same name as the original file a “.aes” file extension.

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

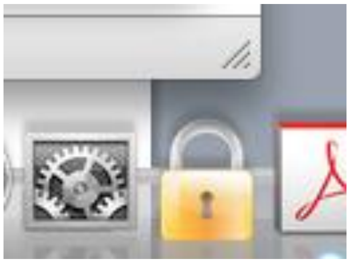
The screenshots below detail these steps. First, find the file you wish to encrypt in Finder.



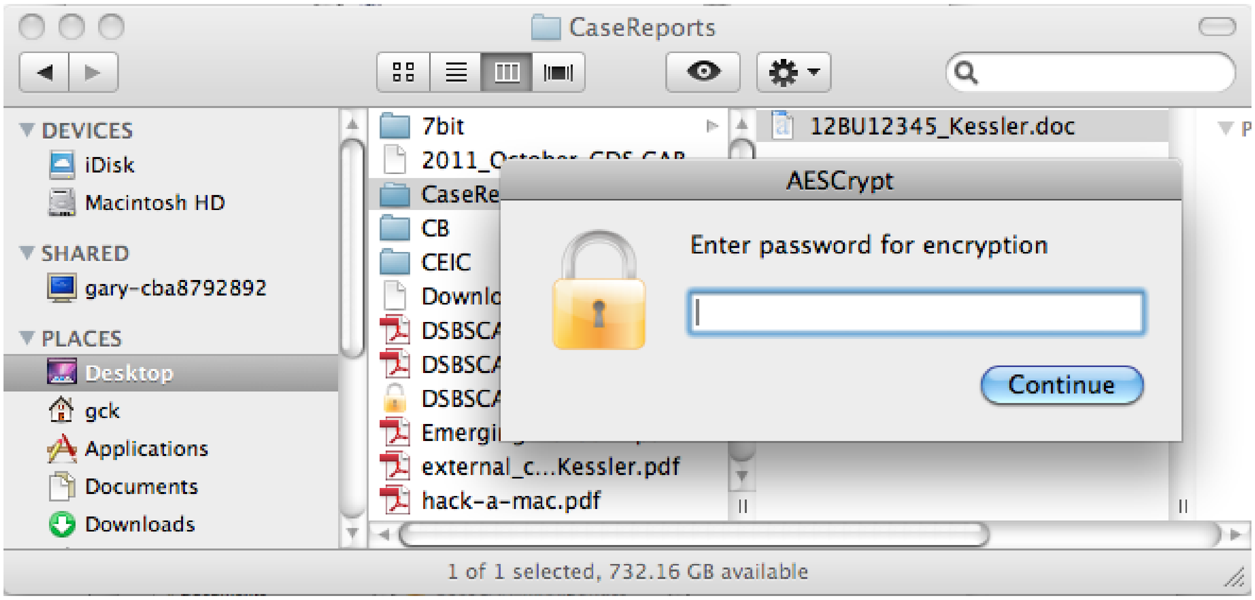
Drag the file to encrypt onto the *AESCrypt.app* file in the Applications directory ***or***…



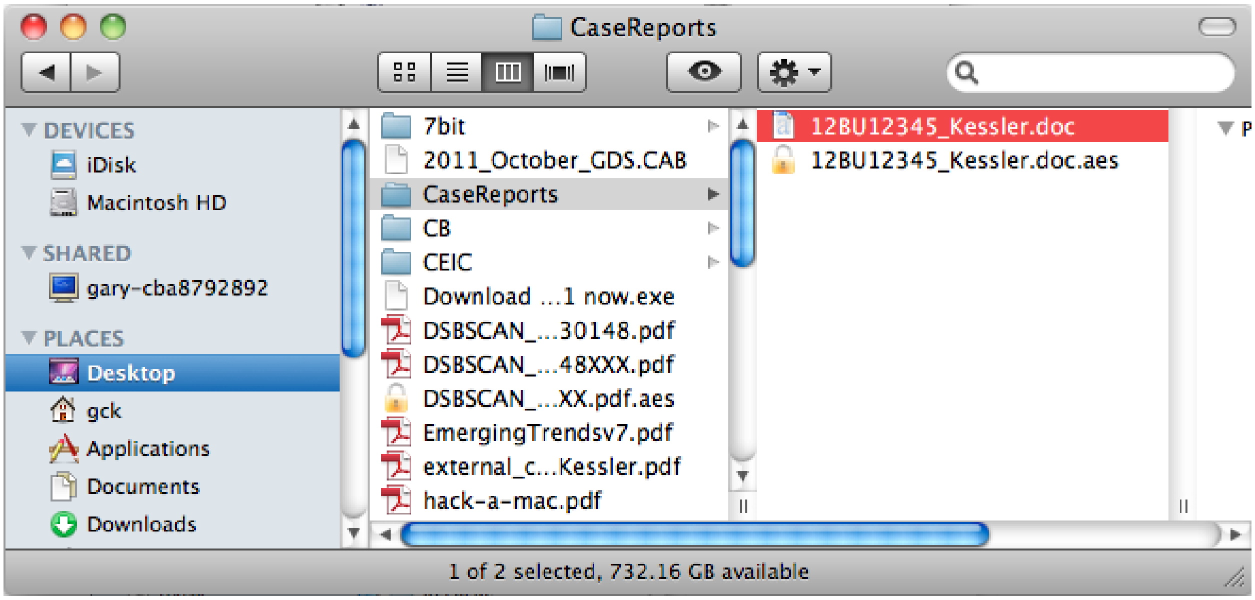
… drag the file onto the AES Crypt “lock” icon on the dock.



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



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.

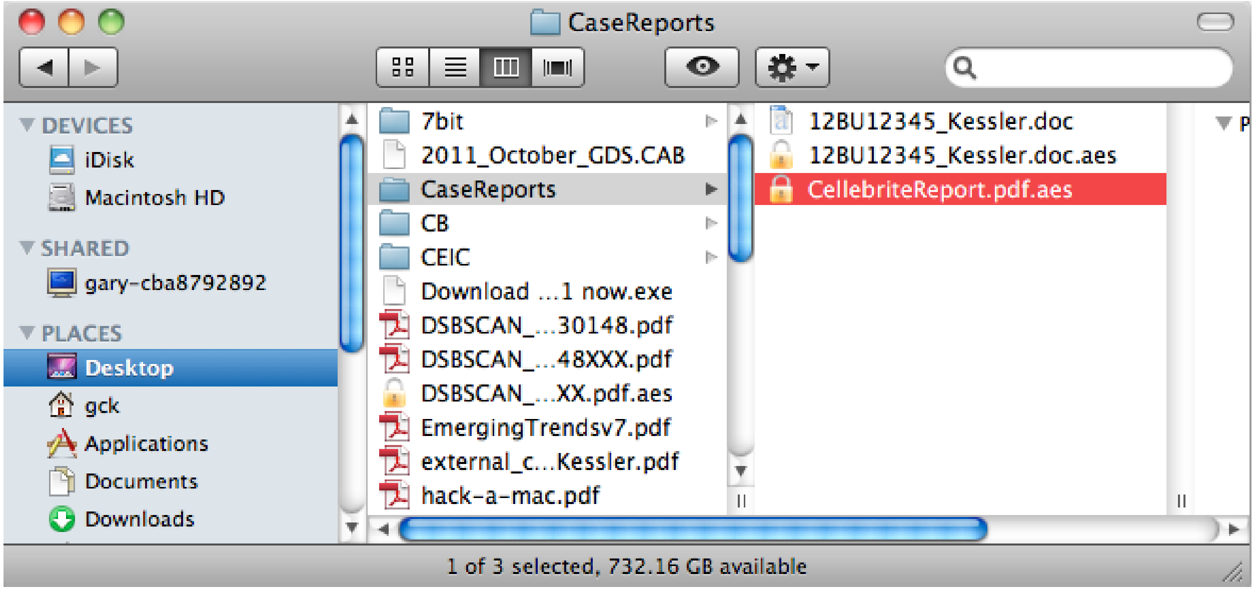
3.2.2 Decrypting Files

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.

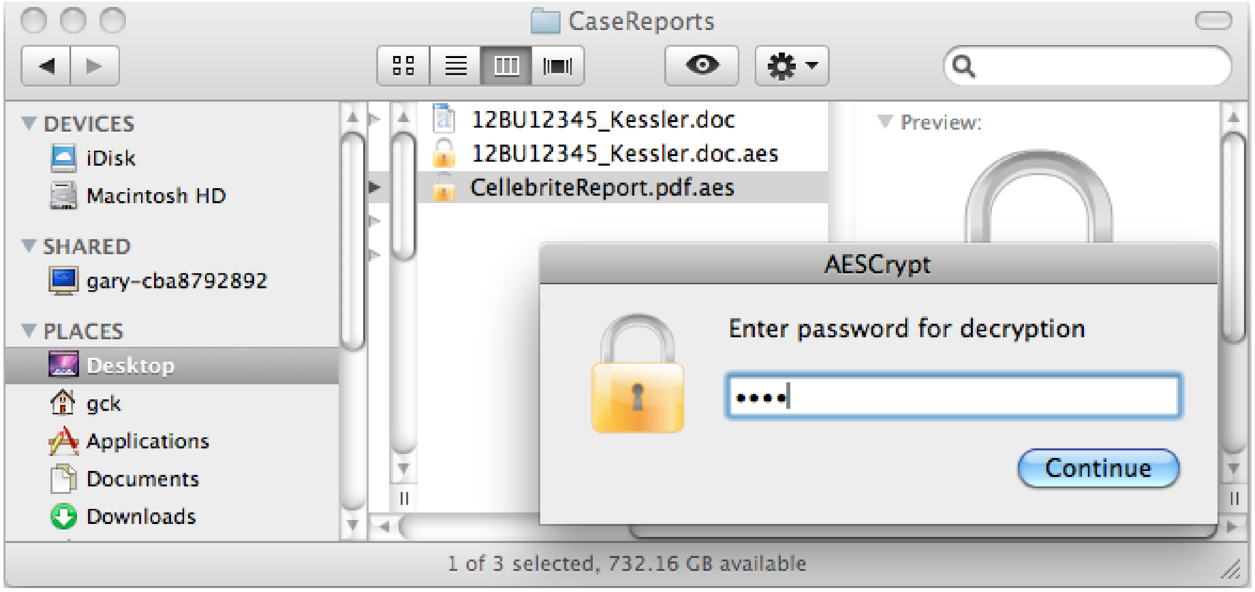
WARNING: If you already have a file with the same name as the encrypted file, but without the “.aes” extension, this process will over-write the existing file!

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



1 of 3 selected, 732.16 GB available

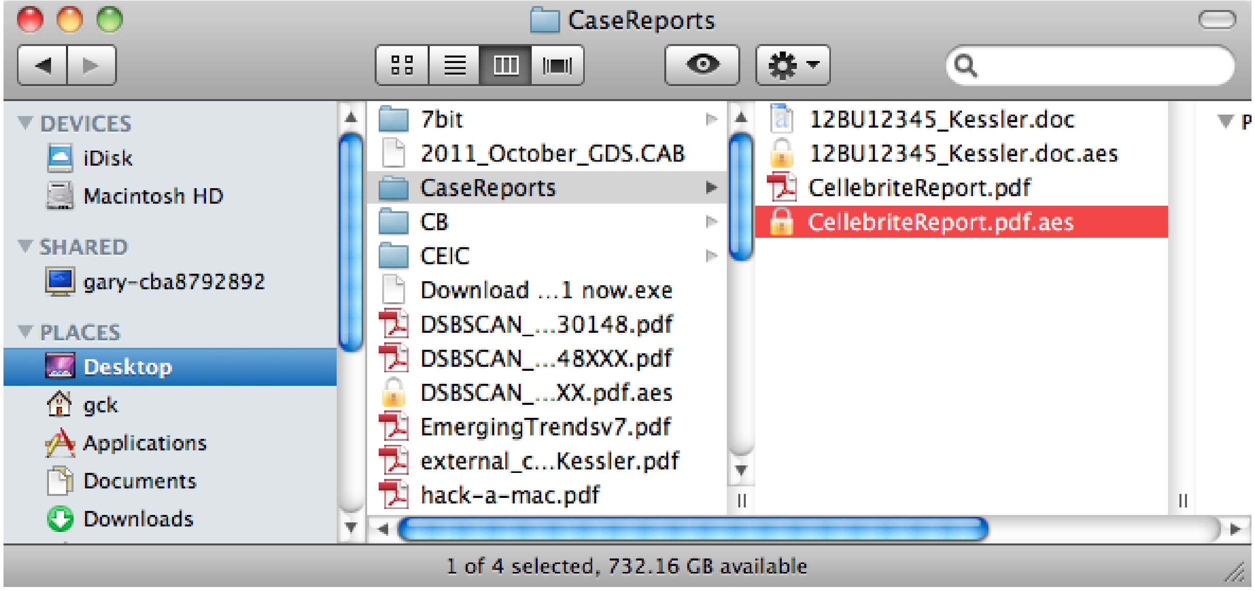
Double-click on the filename, enter the password in the dialogue box, and click “Continue”.



Enter password for decryption

••••

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



3.3 Using Linux (GUI)

3.3.1 Encrypting Files

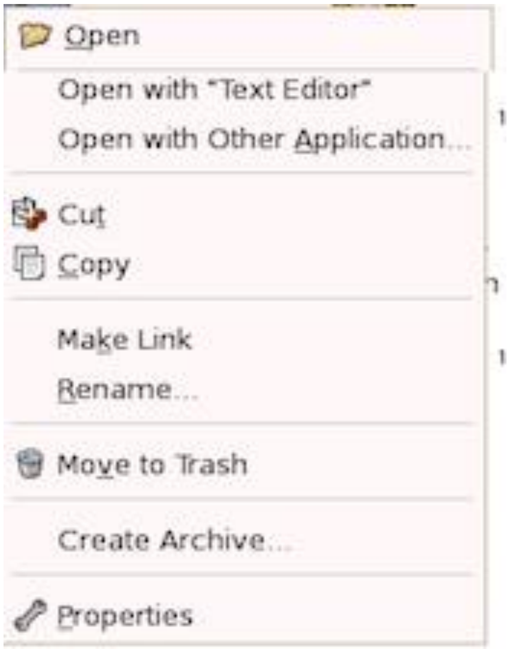
Use the following steps to encrypt a file with AES Crypt:

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

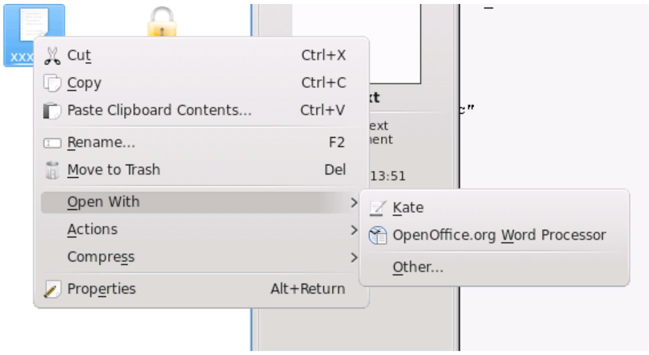
2. Select “AESCrypt” (you may have to select “Open with…” and locate the AES Crypt application the first time).
3. Enter the password in the dialogue box and click “OK”.
4. The encrypted file will appear with the same name as the original, but with an “.aes” file extension.

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.



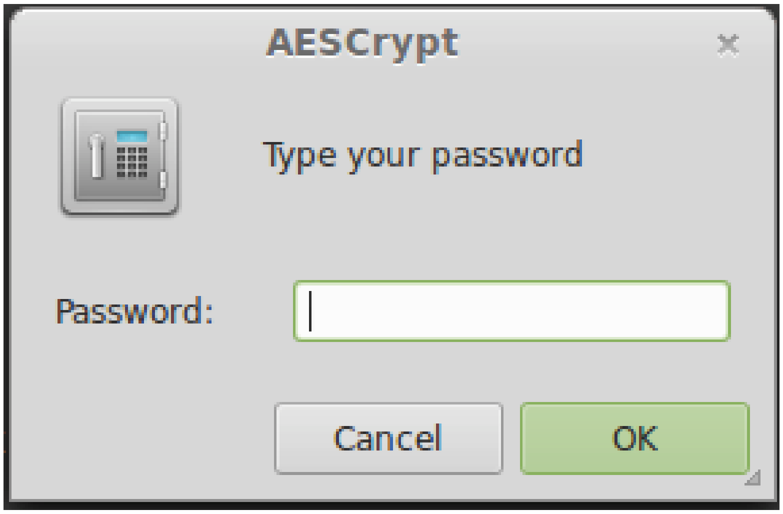
For Gnome, choose “**Open with Other Application…**”



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.

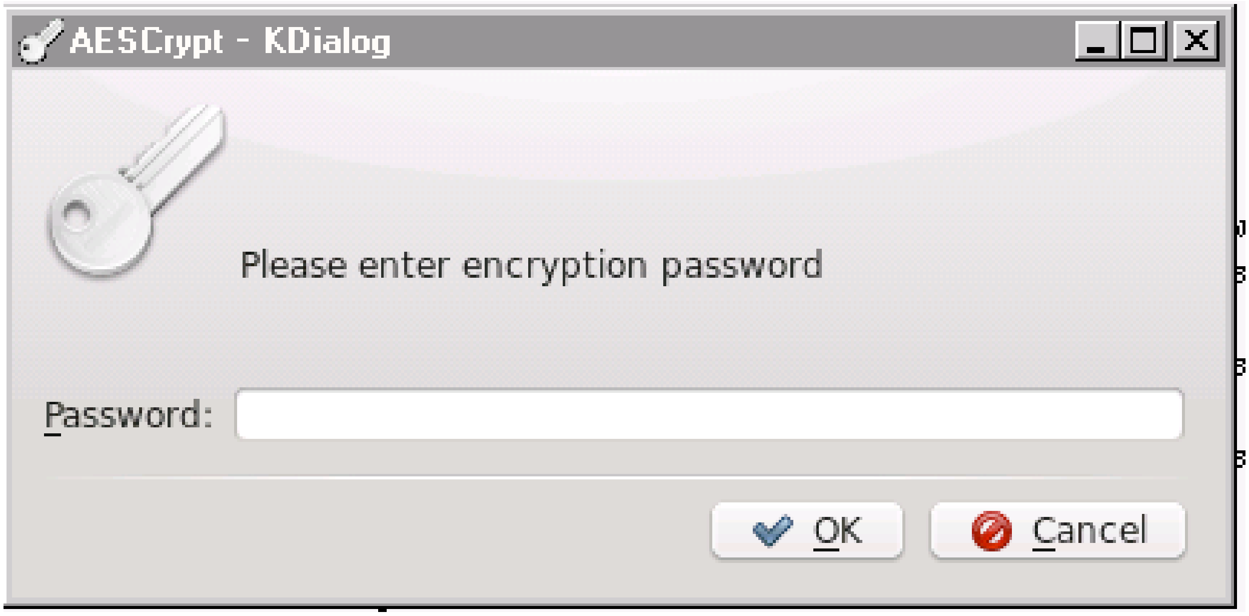
You will get a dialogue asking for your password twice:



Type your password

Password:

Gnome Password Prompt

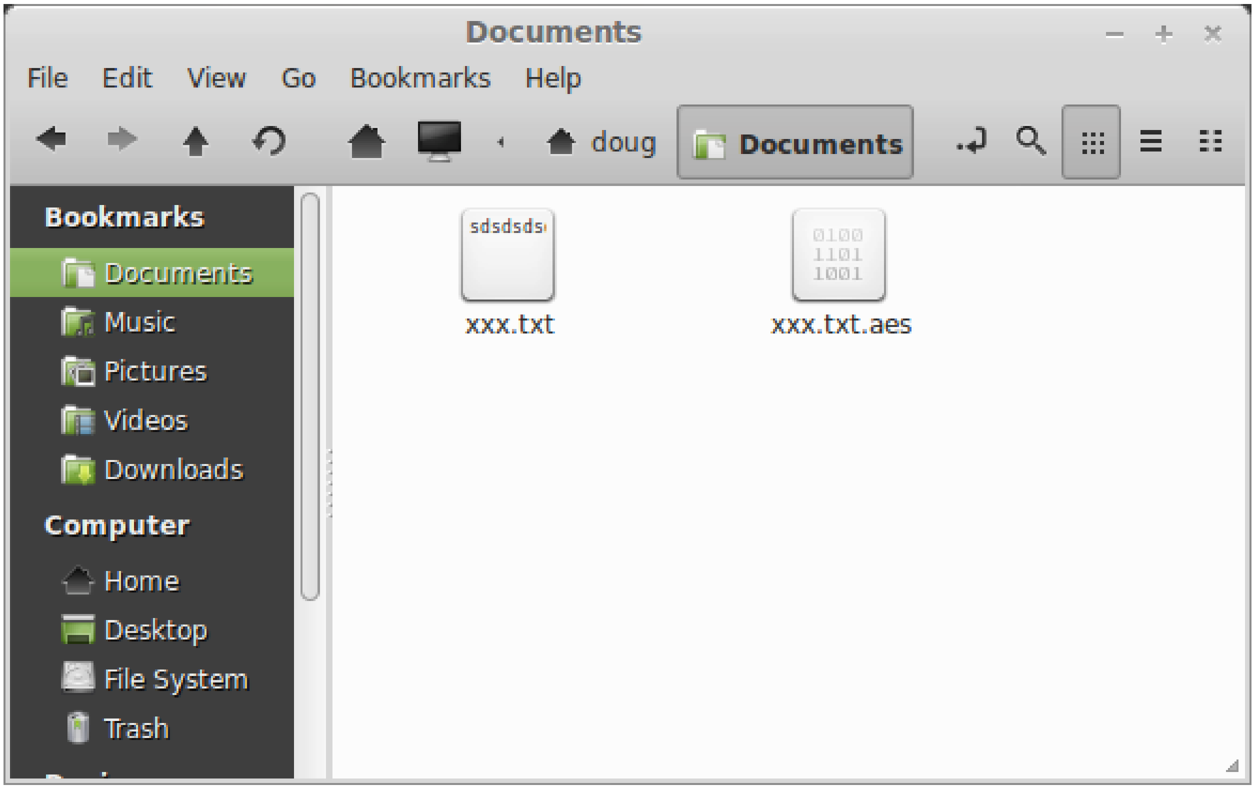


Please enter encryption password

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.

3.3.2 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!