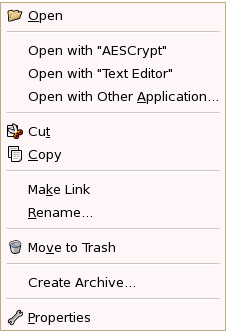
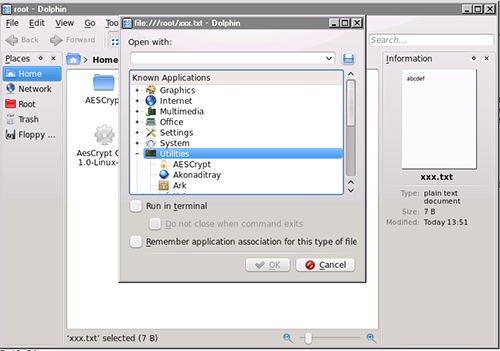
Using AES Crypt on Linux

Graphical User Interface (GUI) Option

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 right-click or left-click on the file (depending on your desktop) you wish to encrypt, and open the file with AES Crypt. You will be prompted to enter the desired password. AES Crypt will produce a file that cannot be read by anybody who does not know the secret password. It is as simple as that.

  
**Gnome Interface**

  
**KDE Interface**

The KDE screenshot is an example of using KDE's "Open With..." dialog, and the Gnome screenshot is an example of what it looks like when it is already in the primary menu. Both Gnome and KDE will add AES Crypt to the primary menu for files once it has been used once. It becomes the default application for the ".aes" extension after the first use in both Gnome and KDE.

AES Crypt will produce an encrypted file with the same name as the original file, but with an ".aes" extension.

Note that when you encrypt a file with AES Crypt, it does not delete the original file. Generally, people encrypt files for the purpose of sending a file securely via e-mail or copying it to a portable storage device that is more susceptible to loss. As such, most people do not want to delete the original. However, you may certainly delete the original file: just do not forget the password. It is impossible to recover the contents of an encrypted file if the password is lost.

Decrypting an encrypted file produced through the process described above is even easier. To decrypt the file, you simply double-click on the .aes file and enter your secret password when prompted.

**Note: The process of encrypting or decrypting a file will over-write any file in the target directory with the same name as would be produced by AES Crypt. Before encrypting or decrypting a file, ensure that another file with the same name and file extension does not already exist.**

Refer to the [User Guide](https://www.aescrypt.com/documentation/AES%20Crypt%20User%20Guide.pdf) for additional important usage information.

Command-Line Option

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.

It can't be any simpler than that!

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. Then 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.

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](http://en.wikipedia.org/wiki/Byte_order_mark) is preserved. See the Readme.txt in the source files for more details about the key file.