Lambros Petrou

"We are what we repeatedly do. Excellence then, is not an act, but a habit!" — Aristotle

CV LINKEDIN GITHUB TWEETS

Encrypt files with password on Linux

JANUARY 06, 2018 | SATURDAY

Problem

I have some important private files that I want to store in Google Drive and on my USB flash drive, but I don't want them to be in plain sight for anyone to see.

I would like to at least password-protect them before storing them, but without too much hassle with asymmetric cryptography where I need to fiddle with keys.

Solution

It turns out pretty much all UNIX systems have GnuPG installed which allows me to just run a command to encrypt a file using a passphrase, and a corresponding command to decrypt it when I need to open it.

I found out that this method is also used inside NASA when transferring files.

In order to **encrypt and password-protect a file** run the following command:

```
gpg -c --cipher-algo AES256 private-file.txt
```

The `-c` option specifies that we want to do symmetric encryption using a passphrase. The `--cipher-algo 256` option specifies that we want to use the AES256 cipher instead of the default CAST5 cipher, although this is not required.

The above command will ask you for the passphrase to use, and then will create a new file named `private-file.txt.gpg`, which is the encrypted and password-protected file we want to store.

In order to **decrypt the file** run the following command:

```
gpg private-file.txt.gpg
```

Once you enter the passphrase used during the encryption of the file, you will get back the decrypted file which will have the same name without the `.gpg` extension, hence `private-file.txt`.

Tips

- If you want to encrypt a whole directory (folder), then you have to first zip/tar the folder into a single file and then apply the same command above to the zipped/tarred file.
- Use long passphrases for important files consisting of multiple words with letters, spaces, symbols, and numbers to maximise the entropy and security of the encryption.

References

- NASA - Using GPG to Encrypt Your Data
- How to use a password stored in separate file as passphrase