Encrypting a single file

John C. Nash

2024-03-31

Abstract

This document gives some suggestions on how to encrypt, decrypt and view a single (text) file in different computing environments.

Introduction

Encryption is a key aspect of modern computing and communications. In this article, we will focus on the encryption of a single **file** of data, normally assumed to be ordinary text, as well as its decryption and viewing. We will usually restrict our attention to **symmetric** encryption, where the same **password** or **passphrase** is used to encrypt and decrypt the file. However, there are a number of important tools that use **passkeys** and may use asymmetric or public-private key pairs.

Note that encryption can be applied to whole storage devices, volumes, directories or streams. Here we will not explore those possibilities, even if our tools could be used for such applications. Indeed we will look at encrypting a single file, which will often be a plain text file. This is particularly applicable to storing password or similar private lists.

Required facilities in the abstract

To simplify our discussion, we will give our tools the generic names

- **ecrypt**, a program that encrypts a file from FILE to FILE.CCC
- **dcrypt**, a program that decrypts a file from FILE.CCC to FILE
- **vcrypt**, a program that displays FILE.CCC or part thereof for human reading, hopefully removing all readable traces of the decrypted information as it exits. This facility is not available for all encryption tools, so the user may have to take measures to avoid leaving unencrypted information accessible to those not authorized to view it.

Some possible tools

ccrypt

ccrypt (http://ccrypt.sourceforge.net/) is intended for file encryption. I happen to be acquainted with its author, Peter Seligman of Dalhousie University. It is available for most platforms.

- ecrypt becomes

  ccrypt FILE

  and outputs FILE.cpt

The password must be entered twice, though there are options to include it on the command line, but such options are discouraged for reasons of security.

- dcrypt becomes (the user is prompted for the password)

  ccrypt -d FILE.cpt

- vcrypt becomes

  ccat FILE.cpt

Linux

ccrypt is present in most Linux distributions and can be installed from the appropriate repositories. For example, in Debian/Ubuntu/Mint family distributions, the command

sudo apt install ccrypt

will carry out the necessary installation steps. Note that there is a quite useful GUI wrapper called qccrypt (Philippe Beaureilles) which is in some Linux software repositories (certainly Linux Mint) or at http://qccrypt.free.fr/

Windows

We need to install ccrypt by downloading an appropriate archive file from https://ccrypt.sourceforge.net/

One example is (2023-3-30) ccrypt-1.11.cygwin-x64.zip. After extracting the files from this archive into a suitable directory, follow instructions in the text file README-WIN to install the necessary ccrypt files in an appropriate location so it can be used.

Mac ??

I don't have a Mac, but would welcome material to include here (with credit, of course)

Android

While the ccrypt web site shows an Android package, I have not yet sorted out how to make this work.

7zip

7zip (https://7-zip.org/) is free and open source software intended primarily for compressed archiving of collections of files. However, it includes strong AES-256 encryption in 7z and ZIP formats. Moreover, it is available for almost all platforms, including Android.

- ecrypt becomes

  ??

  and outputs FILE.??

- dcrypt becomes (the user is prompted for the password)

  ??

- vcrypt seems unavailable in a form that is "view only"

Linux

Debian family distributions can use

sudo apt install 7zip

Windows

Mac ??

Android

Google Play has the app installer for 7Z, a Zip, 7Zip, Rar, File Manager from Sociosoftware. I have installed and used this, though it is a GUI for mobile phones. I don’t particularly like how I have to use it, but it does let me decrypt a compressed and encrypted file, or indeed encrypt one.

gpg

- ecrypt becomes

  ```
  gpg –symmetric FILE
  ```

  and outputs FILE.gpg

  The password must be entered twice, though there are options to include it on the command line, but such options are discouraged for reasons of security.

- dcrypt becomes (the user is prompted for the password)

  ```
  gpg –decrypt FILE.gpg
  ```

- vcrypt becomes

  ??

Linux

Debian family distributions can use

```
sudo apt install gnupg2
```

This is an updated version of this tool.

Windows

Windows users need to install the **gpg4win** software

Mac ??

Android

There is the OpenKeychain project (https://www.openkeychain.org/) that apparently offers GPG capability for Android, but I have not tested how well this works for encryption or decryption of single files, especially with a single (symmetric encryption) passphrase.