File Encrypter and Decrypter

In this article I am going to show you how to make a command line tool that will encrypt a file or decrypt a file. This command line tool is going to be a shell script.

Before diving into the development phase let’s clear some concepts and terminologies.

**What is encryption?**

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simple terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key. It is a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

**What is decryption?**

The conversion of encrypted data into its original form is called decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

Now that you have a basic understanding of encryption and decryption, the image of this project is becoming clear, but now you want to know that how will we do this. So for that we will be using GPG, and you will be thinking that what this “GPG” is.

**GPG** or **GnuPG**, stands for GNU Privacy Guard. GPG is a different implementation of the open PGP standard and a strong alternative to Symantec’s official PGP software.

GPG is defined by RFC 4880 (the official name for the Open GPG standard.) The GPG project provides the tools and libraries to allow users to integrate encryption with emails and operating systems like Linux. GPG can open and decrypt files encrypted by PGP or open PGP, meaning it works well with other products.

Enough theory let’s start coding our file encrypter and decrypter.

1. Step one make a shell script file using touch command and give whatever name you want to give it. I am giving it encrypt.sh
   1. Touch encrypt.sh
2. Make sure to make changes in the file permissions so that you can execute this shell script file, you can do it like this
   1. Chmod 744 encrypt.sh
3. Now start coding the script. First prompt a message to the user and ask what they want to do encrypt or decrypt.
   1. Echo –e “File encrypter/decrypter”
   2. Echo “Please select what you want to do”
   3. Choise=”Encrypt Decrypt”
4. Then we will use a select statement and make a decision on the basic of input
   1. Select option in $choise; do

Done

1. Then use if-else statement and perform encryption or decryption.
2. If user entered 1 than write the logic of encrypting a file, if user enter 2 than write the logic to decrypt the file and if the user enter something other than this, that prompt an error.

So the code for it will be like this

If [ $REPLY = 1 ];

Then

Echo “You have selected Encryption”

Echo “Please enter the name of the file (including extension)”

Read file;

Gpg –c $file

Echo “File is encrypted”

Break

Elif [ $REPLY = 2 ]

Then

Echo “You have selected decryption”

Echo “Please enter the name of the file (including extension)”

Read file2;

Gpg –d $file2

Echo “File is decrypted”

Break

Else

Echo “You have selected invalid option”

Fi

Done

The code for file encryption and decryption completed. You can also see the complete code here (<https://github.com/rahulMishra05/file_encrypter_decrypter>)

So this was all about file encrypter and decrypter. Hope you liked it and learned something new from it.

If you have any doubt, question, quires related to this article or just want to share something with me, than please feel free to contact me.