DECENC
Introduction & User Guide

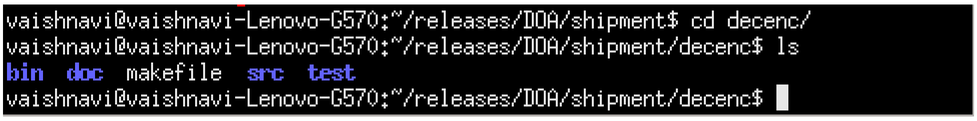
Ravi Sankar Konidena, CSP-SM
IT Consultant

Introduction

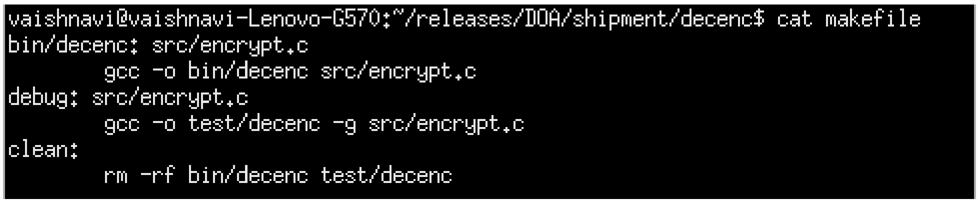
DECENC is a IT product developed on Ubuntu Linux platform using C language. It is a command line product. The purpose of this product is to give file users the benifit of encryption, decryption and authentication.

Open Source

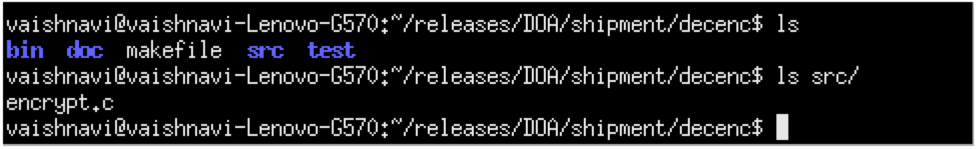
DECENC is a open source product. It has the following structure.



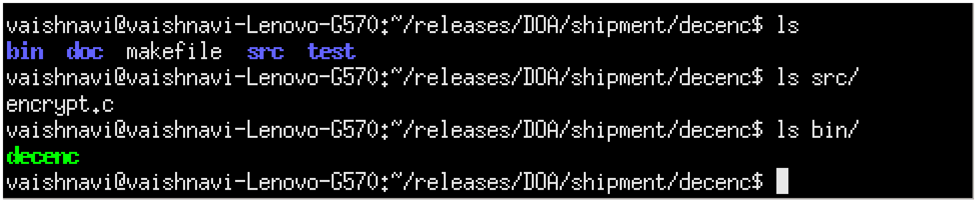
```
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment$ cd decenc/
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$ ls
bin  doc  makefile  src  test
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$
```



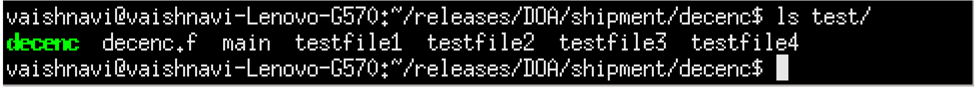
```
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$ cat makefile
bin/decenc: src/encrypt.c
        gcc -o bin/decenc src/encrypt.c
debug: src/encrypt.c
        gcc -o test/decenc -g src/encrypt.c
clean:
        rm -rf bin/decenc test/decenc
```



```
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$ ls
bin  doc  makefile  src  test
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$ ls src/
encrypt.c
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$
```



```
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$ ls
bin  doc  makefile  src  test
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$ ls src/
encrypt.c
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$ ls bin/
decenc
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$
```



```
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$ ls test/
decenc  decenc.f  main  testfile1  testfile2  testfile3  testfile4
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc$
```

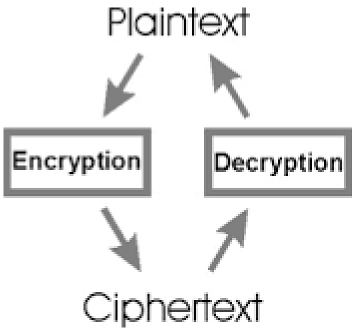
The following sections brief you about encryption, decryption and authentication.

Encryption

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference but denies the readable content in information. Information which is plain text is encrypted using a encryption algorithm which generates a cipher text that can be read only if decrypted.

Decryption

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system.



Authentication

Authentication is the process of reserving the encryption/decryption process by a product user. This IT product can be shared by any number of people and purely encryption/decryption process will be not be sufficient for user level protection. The product user can provide his own key while encrypting the information. The cipher text generated cannot be decrypted by the product unless the user provides the key.

User Guide

This section will give the possible ways of using the product. Each use case scenario is shared using a screen shot and simple text.

Encryption/Decryption

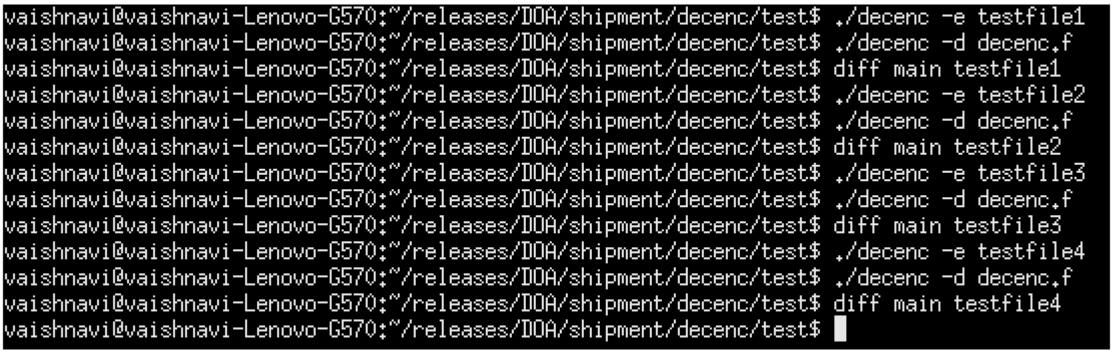
```
decenc -e <inputfile>
```

This command will encrypt the input file and gives the cipher text in a file decenc.f decenc -d decenc.f

This command will decrypt the cipher text and gives the original file in a file with name “main”

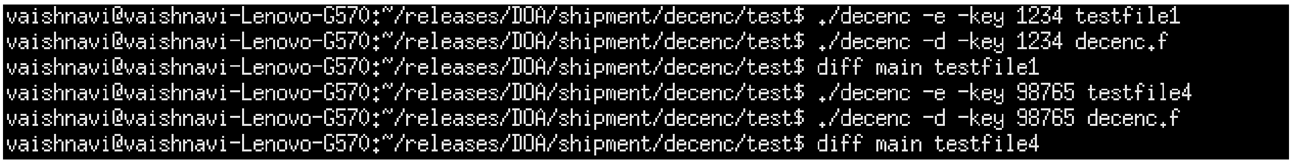
diff inputfile main

This command will give the evidence of encryption and decryption.



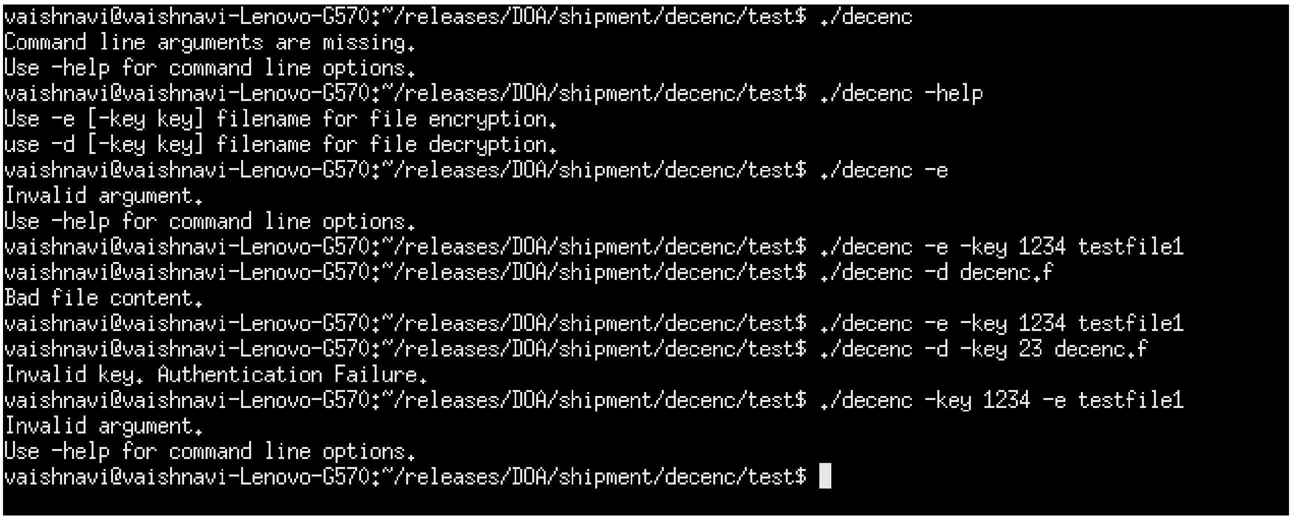
```
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e testfile1
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -d decenc.f
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ diff main testfile1
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e testfile2
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -d decenc.f
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ diff main testfile2
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e testfile3
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -d decenc.f
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ diff main testfile3
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e testfile4
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -d decenc.f
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ diff main testfile4
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$
```

Authentication



```
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e -key 1234 testfile1
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -d -key 1234 decenc.f
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ diff main testfile1
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e -key 98765 testfile4
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -d -key 98765 decenc.f
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ diff main testfile4
```

Errors



```
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc
Command line arguments are missing.
Use -help for command line options.
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -help
Use -e [-key key] filename for file encryption.
use -d [-key key] filename for file decryption.
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e
Invalid argument.
Use -help for command line options.
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e -key 1234 testfile1
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -d decenc.f
Bad file content.
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -e -key 1234 testfile1
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -d -key 23 decenc.f
Invalid key. Authentication Failure.
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$ ./decenc -key 1234 -e testfile1
Invalid argument.
Use -help for command line options.
vaishnavi@vaishnavi-Lenovo-G570:~/releases/DOA/shipment/decenc/test$
```