

DES con OpenSSL in Linux

L'encryption (**Cifratura**) e il Decryption (**Decifratura**) con algoritmi **a chiave simmetrica** prevede l'uso di **una sola chiave** per cifrare il testo in chiaro o decifrare il testo cifrato.

OpenSSL è un toolkit robusto, di livello commerciale e completo di funzionalità per la crittografia generica e la comunicazione sicura.

Per lavorare con OpenSSL il tool deve essere installato. Per verificare che il tool sia correttamente installato digitare il comando seguente:

```
openssl version
OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)
```

Esercitazione 1. Cifrare un testo in chiaro con algoritmo DES

1. Creare una cartella e nominarla “DES”:

```
(psygnosys@psygnosys)-[~]
$ mkdir -p DES
```

2. Spostarsi in “DES” e creare il file “clear.txt”:

```
(psygnosys@psygnosys)-[~]
$ cd DES
(psygnosys@psygnosys)-[~/DES]
$ touch clear.txt
```

3. Scrivere la frase “ciao questo è un file in chiaro da rendere segreto” nel file “clear.txt”:

```
(psygnosys@psygnosys)-[~/DES]
$ echo "ciao questo è un file in chiaro da rendere segreto" >> clear.txt
```

4. Cifriamo il file “clear.txt” con algoritmo DES inserendo la password (a scelta) quando richiesto e creando il nuovo file “chyper.txt” che conterrà il testo cifrato:

```
(psygnosys@psygnosys)-[~/DES]
$ openssl enc -des -e -iter 1000 -a -provider legacy -provider default -in clear.txt -out chyper.txt
enter DES-CBC encryption password:
Verifying - enter DES-CBC encryption password:
```

5. Visualizziamo il contenuto di “chyper.txt”:

```
(psygnosys@psygnosys)-[~/DES]
$ cat chyper.txt
U2FsdGVkX1/TdXg7fgEL1TdI1nTE/eqogbPgB2hpLyj3oDzqME/NgrtYIwotqePp
c4NcNupbI4qVoKKkKDRwKWgx8tg+mqGm
```

6. Analizziamo il comando:

1. **openssl** è il comando del tool che offre circa 140 algoritmi di cifratura
 2. **enc** abilita il tool di encryption e decryption
 3. **-des** abilita l'algoritmo da utilizzare (in questo caso DES)
 4. **-e** specifica che vogliamo fare encryption
 5. **-iter 1000** esegue 1000 iterazioni per derivare la chiave
 6. **-provider legacy** è necessario abilitare gli algoritmi deprecati
 7. **-provider default** abilita il provider di default degli algoritmi
 8. **-in** testo in chiaro
 9. **-out** testo cifrato
7. Vediamo come decifrare il file “chyper.txt” scrivendo l'output sul file “decifrato.txt”. Inserire la password quando richiesta. Nel comando specificheremo -d (per il decryption) e ovviamente il file di input sarà “chyper.txt” mentre in output il file verrà creato in modo automatico.

```
(psygnosys@psygnosys)-[~/DES]
$ openssl enc -des -d -iter 1000 -a -provider legacy -provider default -in chyper.txt -out decifrato.txt
enter DES-CBC decryption password:
```

8. Analizzare il contenuto del file “decifrato.txt”:

```
(psygnosys@psygnosys)-[~/DES]
$ cat decifrato.txt
ciao questo è un file in chiaro da rendere segreto
```

E' possibile anche fornire la chiave ed un vettore di inizializzazione IV a 64 bit. Per la chiave verranno utilizzati solo 56 bit:

```
(psygnosys@psygnosys)-[~/DES]
$ openssl enc -des -e -K 3d4325a3676f34bb -iv be1d78bd53f11a02 -a -provider legacy -provider default -in clear.txt -out chyper.txt
```

Analizzando il testo cifrato otterremo:

```
(psygnosys@psygnosys)-[~/DES]
$ cat chyper.txt
UaUtgHrvqGTu0K8X/GBNDYSEZOhrC8fhNiZm35ERSKW8zmAjUV609FgjAtUJVPoE
cdcVgt5T3fs=
```

Decifriamo il file “cypher.txt” ed analizziamo il file “decifrato.txt”:

```
(psygnosys@psygnosys)-[~/DES]
$ openssl enc -des -d -K 3d4325a3676f34bb -iv be1d78bd53f11a02 -a -provider legacy -provider default -in chyper.txt -out decifrato.txt
(psygnosys@psygnosys)-[~/DES]
$ cat decifrato.txt
ciao questo è un file in chiaro da rendere segreto
```