Introduzione all'Informatica

Loriano Storchi

loriano@storchi.org

http://www.storchi.org/

GPG e LINUX

Generare una coppia di chiavi

- gpg -h

```
     --fingerprint              list keys and fingerprints
-K,  --list-secret-keys         list secret keys
     --gen-key                  generate a new key pair
     --quick-gen-key            quickly generate a new key pair
     --quick-adduid             quickly add a new user-id
     --quick-revuid             quickly revoke a user-id
```

- gpg –-gen-key

```
gpg (GnuPG) 2.1.15; Copyright (C) 2016 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/luvi/.gnupg' created
gpg: new configuration file '/home/luvi/.gnupg/dirmngr.conf' created
gpg: new configuration file '/home/luvi/.gnupg/gpg.conf' created
```

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
```

Uso della chiave privata

- gpg -K per vedere la lista delle chiavi private
- Crittare un documento:

```
[redo@buchner ~]$ fortune > test.txt
[redo@buchner ~]$ cat test.txt
Good day for overcoming obstacles.  Try a steeplechase.
```

- Adesso usiamo la nostra chiave privata :

```
[redo@buchner ~]$ gpg -a -e -r loriano@storchi.org test.txt
[redo@buchner ~]$ cat test.txt
Good day for overcoming obstacles.  Try a steeplechase.
[redo@buchner ~]$ cat test.txt.asc
-----BEGIN PGP MESSAGE-----

hQIMA+U4XULyDYGEAQ/8COocYQltQXulXMdh6scCx6/tF+fkrDPaHojpyxJaCplp
YOXG+GoaVoJPFCdJdFfQRVsGe+zrlpUZh/OUmdP2qKzAzj5f8azTyypoBhxcoJfI
KnwbLqjzYbhJ+i/ikiRYln3tAoNKuwuTzOWk7xnUWLxR/JZi3KYjbIoz1B6DX7V8
RjSR6p9eubCP1Qn8lhWPxEsPOYwszTAsf1zi01JVUPEdG+QhaZAkQrSi0F+mFR9G
duhWgqHSQNqmA53h7twC4Mtqu2BE1bRhsAOF5Df6kJvfZqkwwMTTOZtxmokvHyk8
Xnb8dIH5aDd72Df/RRvPxnT0QrRiBpsKz4c11/uO19PVmQlyQcp+aSOd7rMhA3w0
```

Decrittare

- gpg -a -d test.txt.asc

```
      "Loriano Storchi <loriano@storchi.org>"
Good day for overcoming obstacles.  Try a steeplechase.
```

- Cancellare in modo sicuro il messaggio in chiaro:

```
[redo@buchner ~]$ wipe test.txt
Okay to WIPE 1 regular file ? (Yes/No) yes
Wiping test.txt, pass 34 (34)
Operation finished.
1 file wiped and 0 special files ignored in 0
```

- EncFS per crittare una directory intera o LUKS un intero disco o filesystem