Introduzione a GPG

GNU Privacy Guard: proteggere le proprie comunicazioni da sguardi indiscreti

giomba

GOLEM Empoli

24 Ottobre 2015

Problema

Comunicare in maniera sicura e impedire la lettura dei messaggi alle persone non autorizzate.

Esempi

- Durante una guerra, impedire al nemico di leggere le comunicazioni militari
- Durante un acquisto online, impedire ad un ladro di intercettare il numero della nostra carta di credito
- ...

Problema

Comunicare in maniera sicura e impedire la lettura dei messaggi alle persone non autorizzate.

Esempi

- Durante una guerra, impedire al nemico di leggere le comunicazioni militari
- Durante un acquisto online, impedire ad un ladro di intercettare il numero della nostra carta di credito
- ...

Soluzioni

Steganografia nascondere il messaggio

Esempio

Riproduzione leggermente alterata di un'immagine, di un suono, di una fotografia, della traccia di un disco, ...

Crittografia modificare la natura del messaggio

Esempio

Sostituzione delle lettere con simboli o altre lettere, secondo criteri prestabiliti con l'interlocutore, come nei cifrari alfabetici (Cesare, Leon Battista Alberti, Enigma) e nei cifrari perfetti (Vernam)

Soluzioni

Soluzioni

Steganografia nascondere il messaggio

Esempio

Riproduzione leggermente alterata di un'immagine, di un suono, di una fotografia, della traccia di un disco, ...

Crittografia modificare la natura del messaggio

Esempio

Sostituzione delle lettere con simboli o altre lettere, secondo criteri prestabiliti con l'interlocutore, come nei cifrari alfabetici (Cesare, Leon Battista Alberti, Enigma) e nei cifrari perfetti (Vernam)

Steganografia

Figura 1: Originale

Steganografia

Figura 1: Originale

Figura 2: Steganografata

Crittosistema: il Cifrario Perfetto

Definizione

La probabilità di determinare quale sia il messaggio originale non dipende dalla conoscenza del messaggio cifrato.

Figura 3:
Claude Shannon

Problemi

- La chiave di cifratura deve essere completamente casuale
- La chiave deve essere lunga almeno quanto il messaggio
- La chiave può essere utilizzata solamente una volta
- Non è garantita l'autenticità del messaggio ricevuto
- La chiave deve essere trasmessa attraverso un mezzo sicuro

Crittosistema: il Cifrario Perfetto

Definizione

La probabilità di determinare quale sia il messaggio originale non dipende dalla conoscenza del messaggio cifrato.

Figura 3:
Claude Shannon

Problemi

- La chiave di cifratura deve essere completamente casuale
- La chiave deve essere lunga almeno quanto il messaggio
- La chiave può essere utilizzata solamente una volta
- Non è garantita l'autenticità del messaggio ricevuto
- La chiave deve essere trasmessa attraverso un mezzo sicuro

Crittosistema: il Cifrario Perfetto

Definizione

La probabilità di determinare quale sia il messaggio originale non dipende dalla conoscenza del messaggio cifrato.

Figura 3:
Claude Shannon

Problemi

- La chiave di cifratura deve essere completamente casuale
- La chiave deve essere lunga almeno quanto il messaggio
- La chiave può essere utilizzata solamente una volta
- Non è garantita l'autenticità del messaggio ricevuto
- La chiave deve essere trasmessa attraverso un mezzo sicuro

Crittosistema: Crittografia Asimmetrica

Una cifratura accettabile

Svantaggi

Non è perfetto

Cosa significa?

Avendo a disposizione una notevole capacità di calcolo e un lunghissimo tempo, si può recuperare il messaggio.

Vantaggi

- non può essere decifrato in tempi ragionevolmente utili;
- è necessario scambiarsi la chiave una volta sola,
- e non è necessario un mezzo di comunicazione sicuro;
- la chiave può essere essere utilizzata infinite volte;
- è possibile autenticare il mittente.

Crittosistema: Crittografia Asimmetrica

Una cifratura accettabile

Svantaggi

Non è perfetto

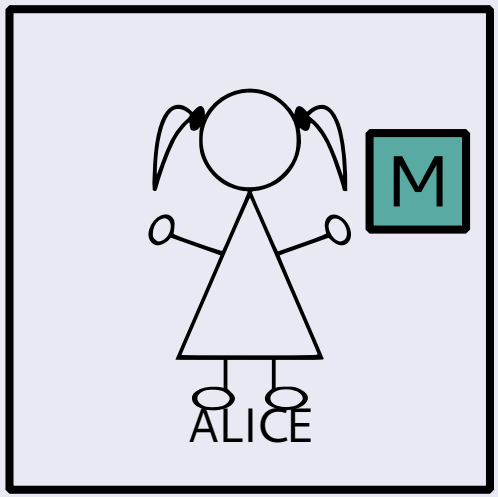
Cosa significa?

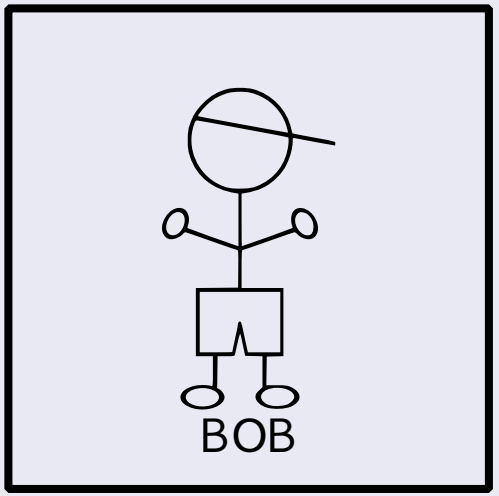
Avendo a disposizione una notevole capacità di calcolo e un lunghissimo tempo, si può recuperare il messaggio.

Vantaggi

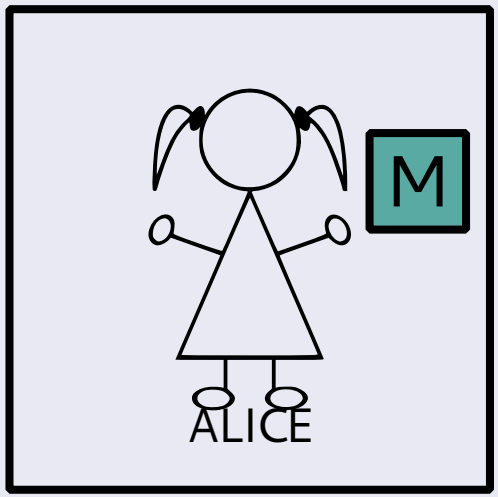
- non può essere decifrato in tempi ragionevolmente utili;
- è necessario scambiarsi la chiave una volta sola,
- e non è necessario un mezzo di comunicazione sicuro;
- la chiave può essere essere utilizzata infinite volte;
- è possibile autenticare il mittente.

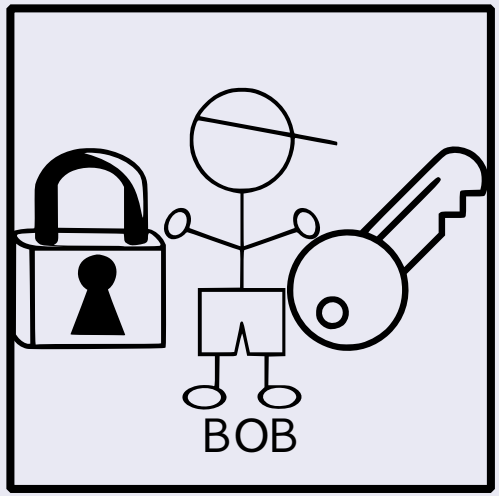
Come funziona in pratica?





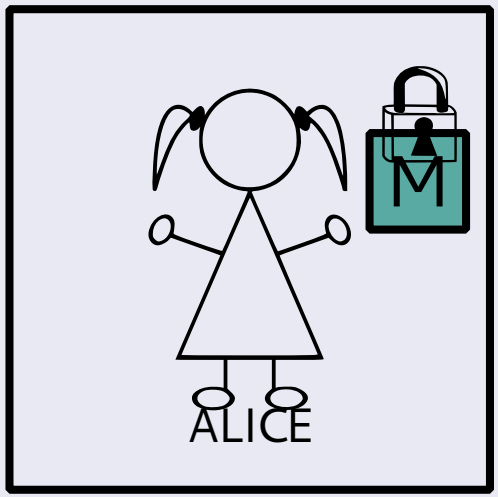
Come funziona in pratica?

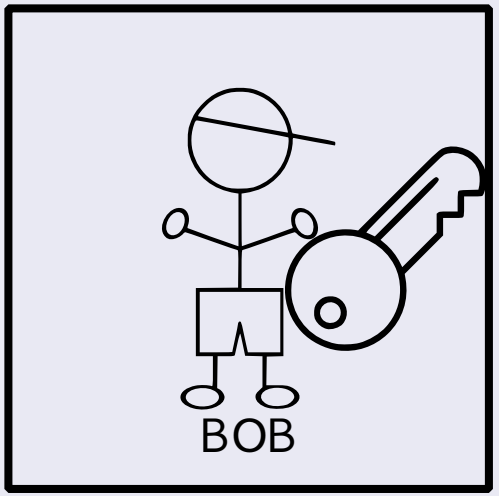




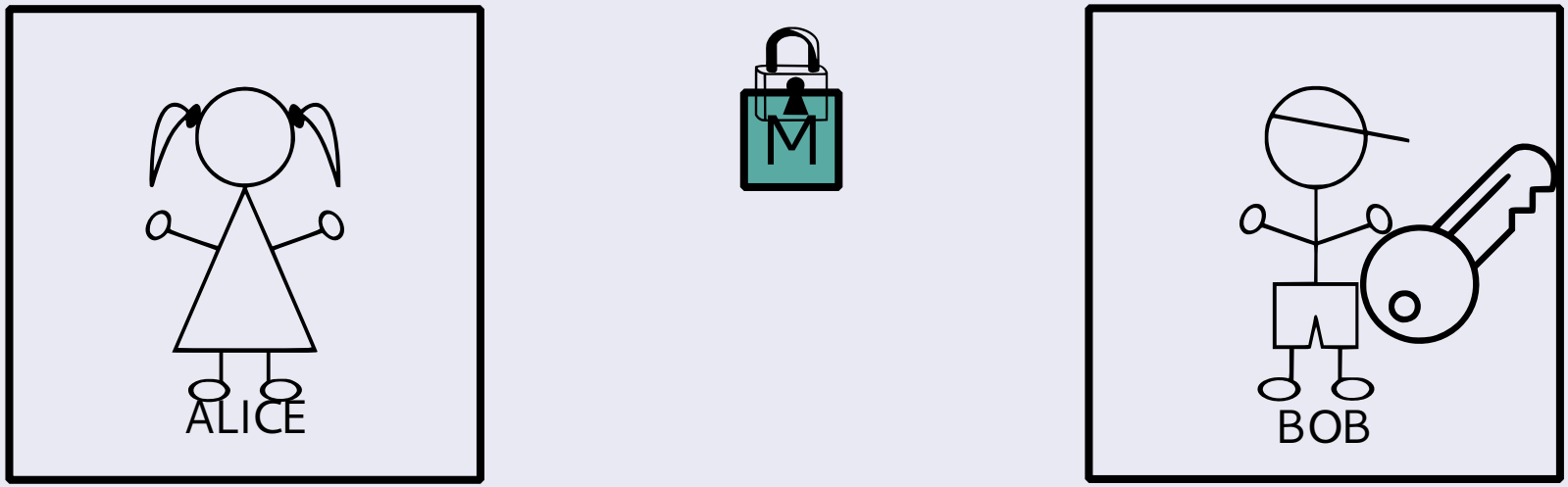
Come funziona in pratica?

Come funziona in pratica?

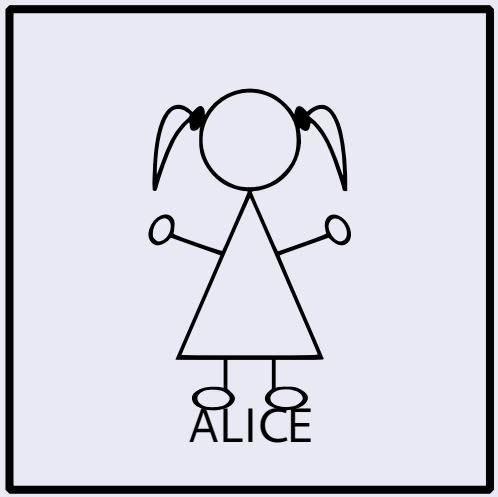


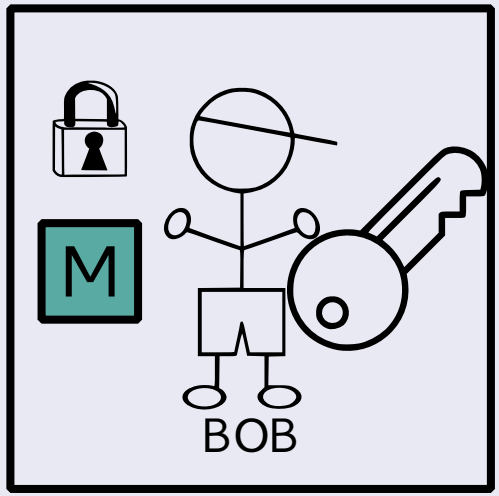


Come funziona in pratica?



Come funziona in pratica?





Utilità

Ma ho davvero bisogno di tutto questo?

Abbiamo tutti qualcosa da nascondere

- Origine razziale ed etnica
- Convinzioni religiose e filosofiche
- Orientamento politico
- Orientamento sessuale
- Stato di salute

Meglio prevenire che curare

Anche se oggi, probabilmente, non ce n'è bisogno, non fa sicuramente male prendere confidenza con questi utili strumenti.

Utilità

Ma ho davvero bisogno di tutto questo?

Abbiamo tutti qualcosa da nascondere

- Origine razziale ed etnica
- Convinzioni religiose e filosofiche
- Orientamento politico
- Orientamento sessuale
- Stato di salute

Meglio prevenire che curare

Anche se oggi, probabilmente, non ce n'è bisogno, non fa sicuramente male prendere confidenza con questi utili strumenti.

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`
  - `> fpr`
  - `> sign`
  - `> save`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`
  - `> fpr`
  - `> sign`
  - `> save`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`
  - `> fpr`
  - `> sign`
  - `> save`

GPG mini How-to

GnuPG

- `gpg --gen-key`
- `gpg --list-keys --fingerprint`
- `gpg -o file.txt.gpg -e -r user@example.org file.txt`
- `gpg -o file.txt -d file.txt.gpg`
- `gpg --keyserver pgp.mit.edu --send-key <ID>`
- `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- `gpg --edit-key`
  - `> fpr`
  - `> sign`
  - `> save`

GPG: Interfacce grafiche

Thunderbird + Enigmail

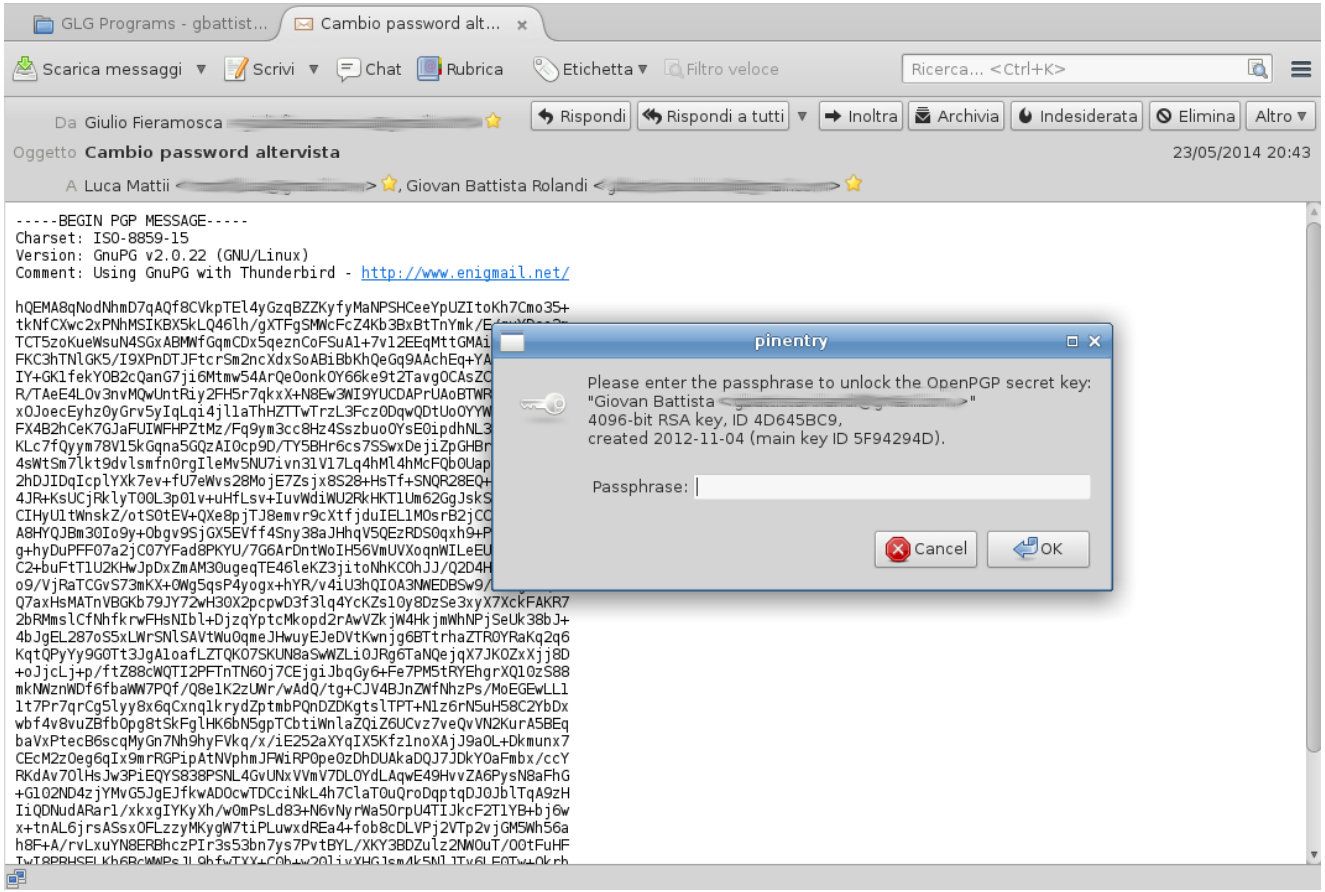


Figura 4: Enigmail

GPG: Interfacce grafiche

GNOME Seahorse

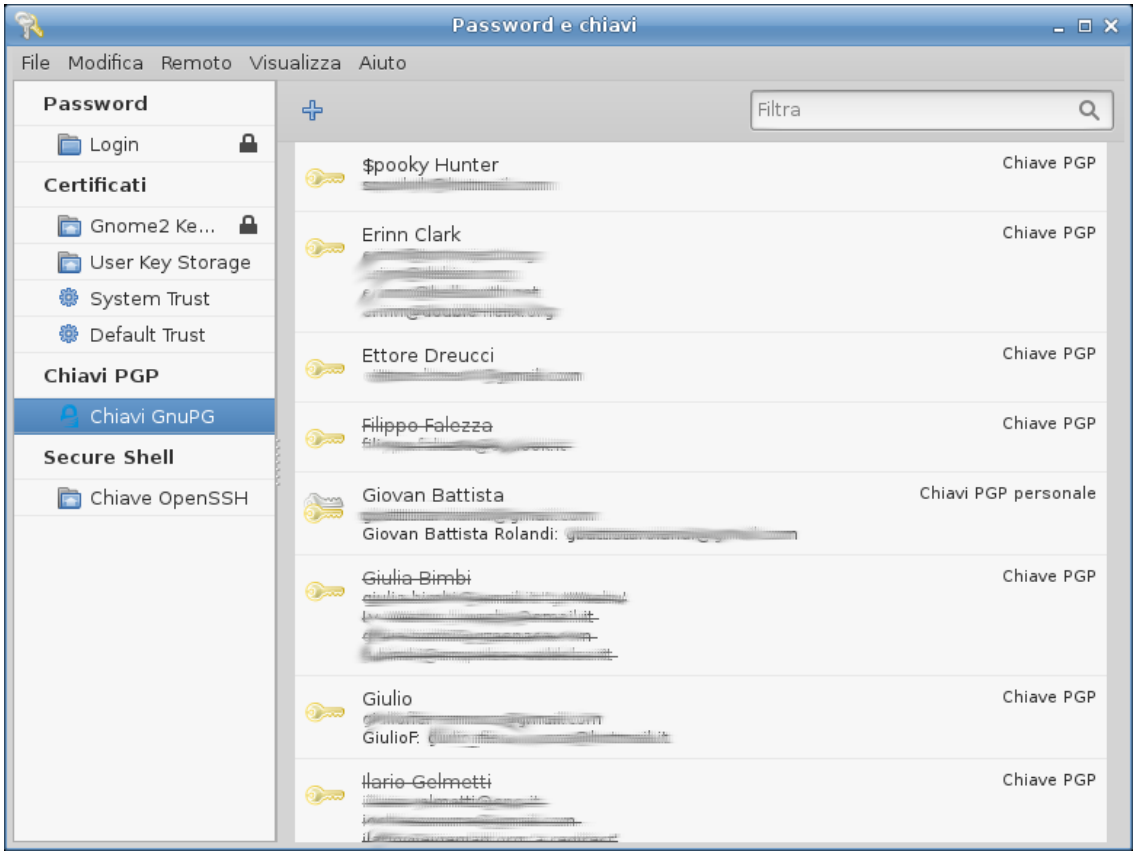


Figura 5: Seahorse

L'anello debole della catena

Il problema è tra la tastiera e la sedia

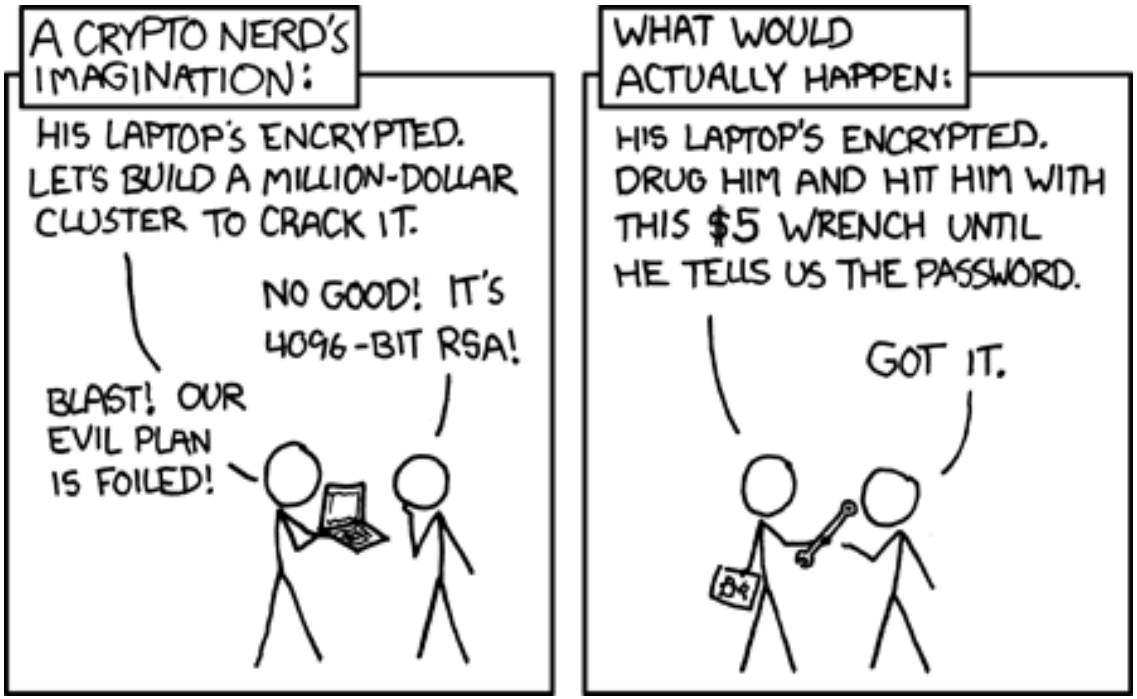


Figura 6: Security: http://xkcd.com/538

Che fare?

Andate, generate, e scambiatevi l'impronta di chiave.

GPG Keysignign Party: prima

- Generare coppia di chiavi

  ```
  gpg --gen-key
  ```

- Annotarsi l'impronta (*fingerprint*) della propria chiave

  ```
  gpg --fingerprint <ID>
  ```

- Preparare bigliettini col proprio nome, indirizzo email ID e impronta della propria chiave
- Inviare chiave pubblica ad un server

  ```
  gpg --keyserver pgp.mit.edu --send-key <ID>
  ```

Che fare?

Andate, generate, e scambiatevi l'impronta di chiave.

GPG Keysignign Party: prima

- Generare coppia di chiavi

  ```
  gpg --gen-key
  ```

- Annotarsi l'impronta (*fingerprint*) della propria chiave

  ```
  gpg --fingerprint <ID>
  ```

- Preparare bigliettini col proprio nome, indirizzo email ID e impronta della propria chiave
- Inviare chiave pubblica ad un server

  ```
  gpg --keyserver pgp.mit.edu --send-key <ID>
  ```

GPG Keysigning Party: durante

- Recarsi ad un *GPG Keysigning Party* con i bigliettini e muniti di documento di identità
- Scambiarsi la chiave con i presenti, controllando la loro identità

GPG Keysigning Party: dopo

- Tornare a casa `cd ~`
- Scaricare le chiavi `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- Controllare la *fingerprint* `gpg --fingerprint <ID>`
- Firmare

```
gpg --edit-key <ID>

> sign
```

- Rispedire al server `gpg --keyserver pgp.mit.edu --send-key <ID>`

GPG Keysigning Party: durante

- Recarsi ad un *GPG Keysigning Party* con i bigliettini e muniti di documento di identità
- Scambiarsi la chiave con i presenti, controllando la loro identità

GPG Keysigning Party: dopo

- Tornare a casa `cd ~`
- Scaricare le chiavi `gpg --keyserver pgp.mit.edu --recv-key <ID>`
- Controllare la *fingerprint* `gpg --fingerprint <ID>`
- Firmare
  `gpg --edit-key <ID>`

  `> sign`
- Rispedire al server `gpg --keyserver pgp.mit.edu --send-key <ID>`

Licenza

Il sorgente di questa presentazione
è software libero,
viene rilasciato sotto licenza GPLv3,
ed è consultabile presso golem.linux.it

GPL Free Software
Free as in Freedom

Linux Day @ Empoli 2015

Questa presentazione è stata preparata per
GOLEM - golem.linux.it
in occasione del Linux Day 2015
da Giovan Battista Rolandi (giomba)
gbattistarolandi@gmail.com
GPG Public ID: 5F94294D

LINUX
D A Y