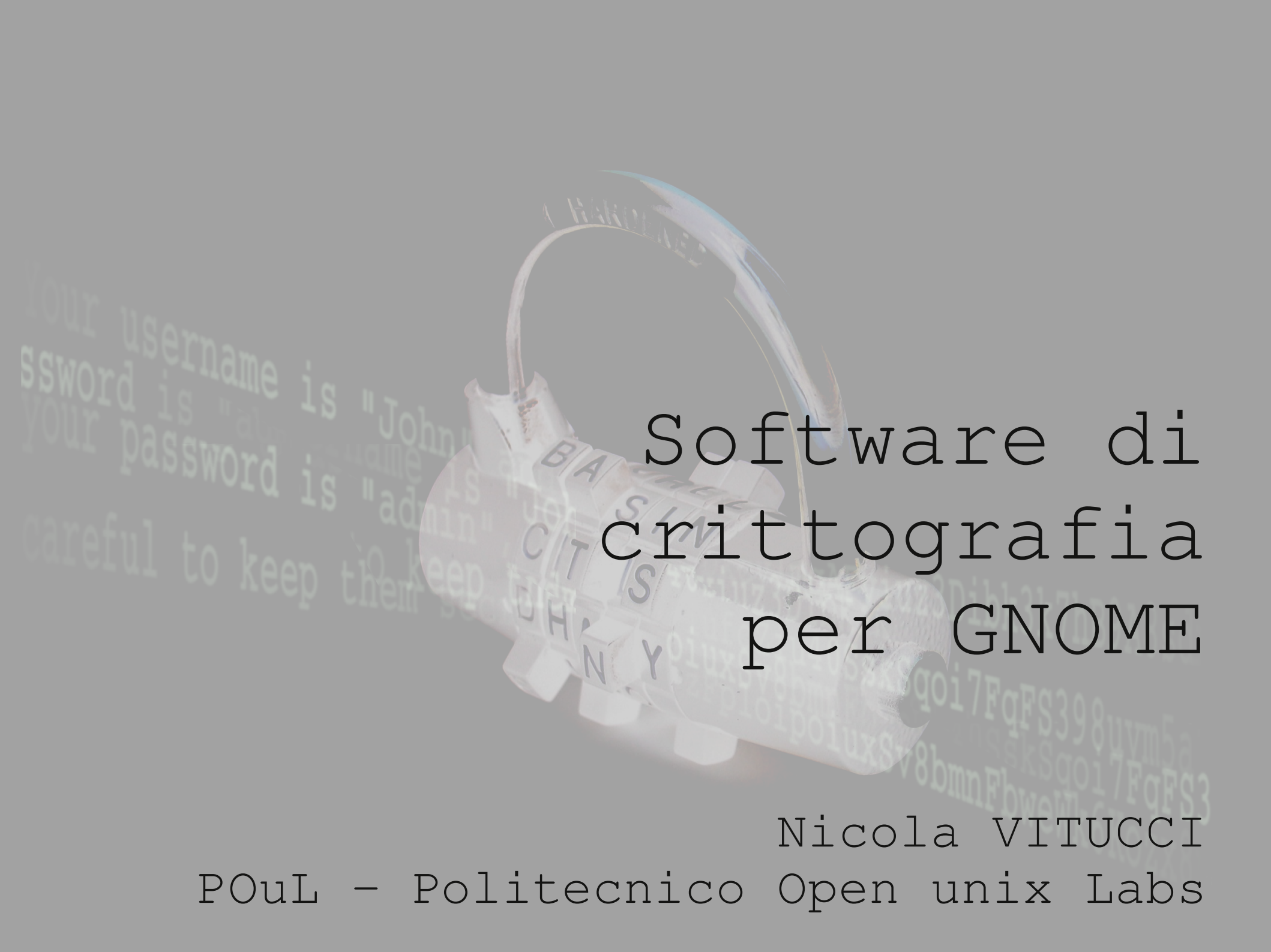


Software di crittografia per GNOME

Nicola VITUCCI
POuL - Politecnico Open unix Labs

Crittografia: definizione

- Dal greco *kryptós*, "nascosto", e *gráphein*, "scrivere"
- Crittografia: l'arte dello "scrivere cifrato"
- I soggetti della comunicazione possono scambiarsi messaggi con la certezza che nessuno possa interpretarli
- L'unico modo per decifrare un messaggio è conoscerne la *chiave* (oltre allo schema di cifratura)

Crittografia asimmetrica

- Un utente genera una coppia di chiavi, una pubblica e una privata
- La chiave pubblica è, appunto, di dominio pubblico: chiunque può usarla per cifrare un messaggio
- Solo il possessore della chiave privata, però, può effettuare la decifratura
- Si risolve così il problema della distribuzione della chiave di cifratura

Possibili utilizzi

- Gli algoritmi a chiave pubblica possono essere usati anche in altri modi:
  - per trasmettere in modo sicuro la chiave di un cifrario simmetrico
  - per poter apporre la firma digitale a un messaggio
  - per apporre la firma digitale alla chiave pubblica di un altro utente
- Ma... cos'è una *firma digitale?*

Firma digitale

- È l'analogo elettronico della firma a penna su un documento
- Ha però dei vantaggi:
  - non è riproducibile da altri soggetti
  - identifica in modo univoco il suo proprietario
  - certifica che il suo proprietario ha effettivamente emesso il messaggio cui è apposta
  - dipende strettamente dal messaggio
- Come viene realizzata?

Parentesi: le funzioni hash

- Una funzione hash è un "tritatutto" che restituisce un "riassunto" del messaggio (il *digest*)
- Un messaggio di qualsiasi lunghezza può essere mappato in un messaggio (più corto) di lunghezza fissata
- Tale calcolo è "facile"
- Ovviamente, a più messaggi corrisponde lo stesso digest, ma da questo non si può risalire al messaggio originale

Firma digitale

- Si utilizza un algoritmo a chiave pubblica e una funzione di hash:
  1. si ricava il digest del messaggio
  2. si cifra il digest con la chiave privata
  3. si invia il messaggio (cifrato o in chiaro) insieme al digest cifrato
  4. il destinatario decifra il digest del messaggio con la chiave pubblica del mittente...
  5. ... e verifica se il digest ottenuto coincide con il digest del messaggio

Certificazione

- Il problema ora è: come essere sicuri che il mittente sia in effetti chi pensiamo che sia?
- Una possibile soluzione è avere un'entità fidata (PKI) che certifica l'attribuzione delle chiavi pubbliche
- Il problema è che, in caso di compromissione o malfunzionamento, l'intero meccanismo crolla

Il Web of Trust

- L'alternativa è lasciare la certificazione ai singoli soggetti
- Ogni chiave pubblica ha un identificativo unico (*fingerprint*)
- Si verifica su un canale sicuro (solitamente dal vivo) che il destinatario abbia realmente generato una chiave pubblica con il fingerprint di cui si è in possesso
- Se la verifica va a buon fine, si firma la chiave pubblica

GPG

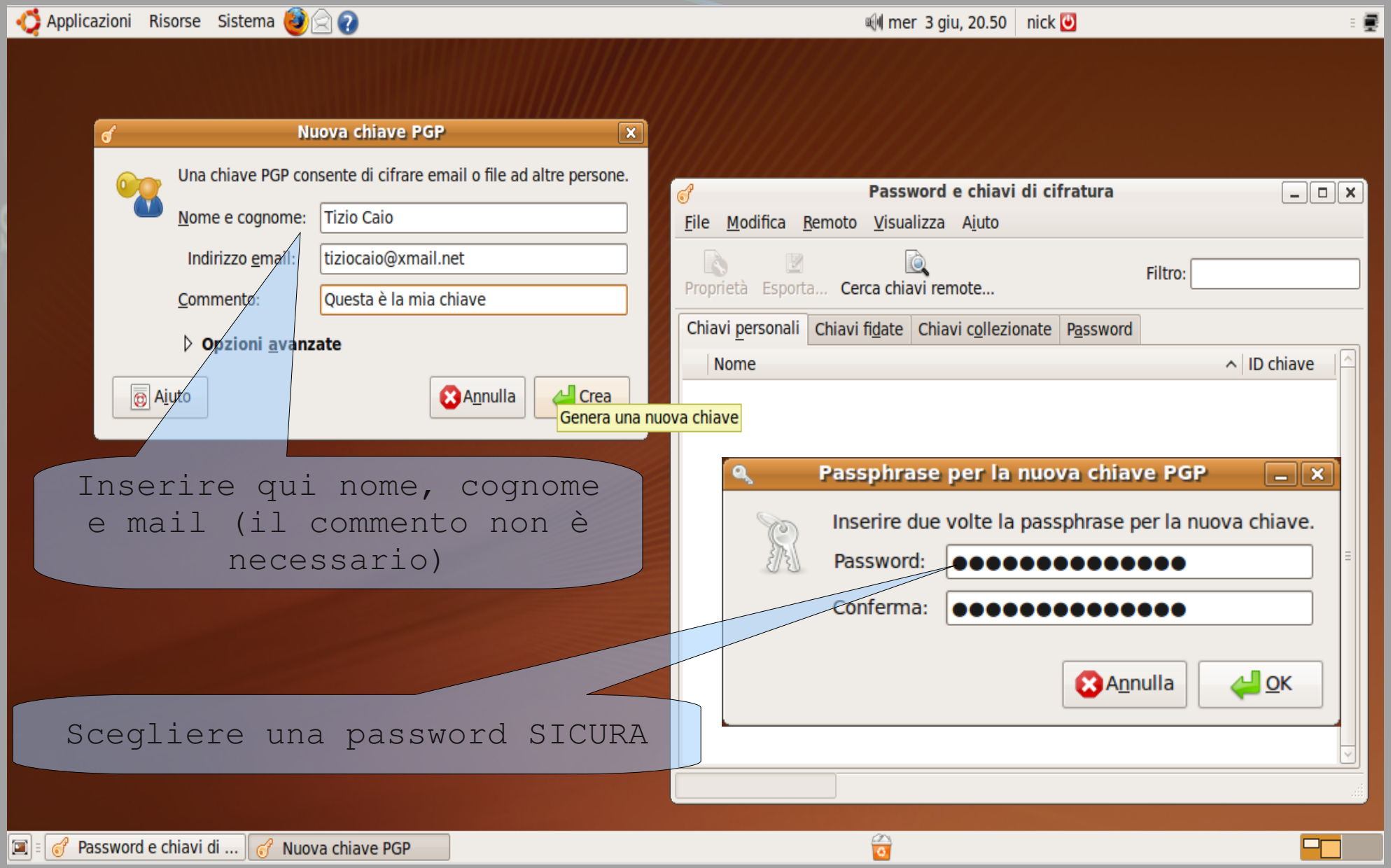
- GPG è una suite crittografica nata come risposta open source a PGP
- Come PGP, anche GPG si propone di portare in modo semplice una crittografia di livello militare ai singoli utenti
- GPG è una suite cross-platform, quindi si può trovare in varie versioni e per vari sistemi operativi, sia a riga di comando che con interfaccia grafica

Seahorse

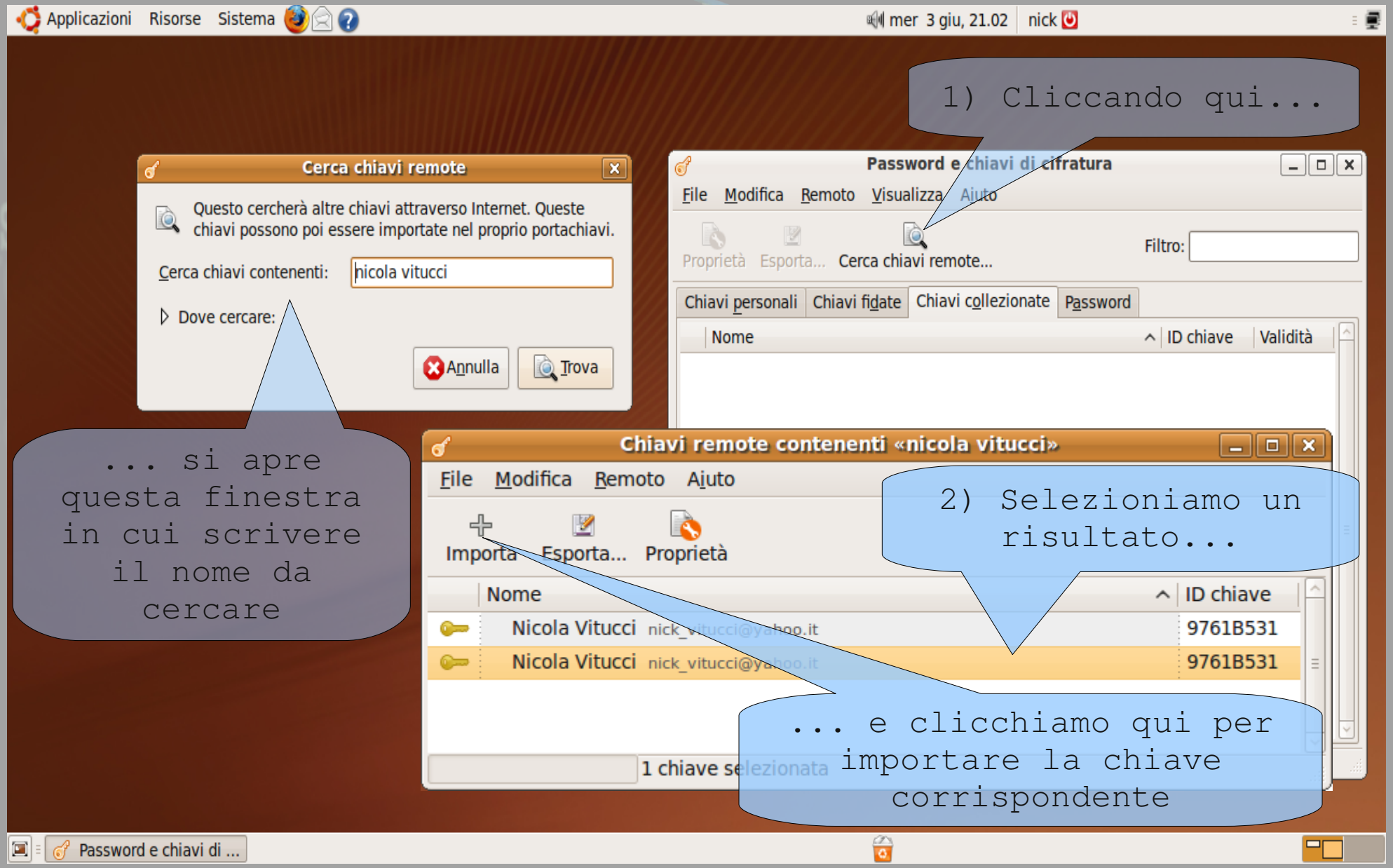
- Seahorse è un software per GNOME per la gestione di chiavi crittografiche
- Si interfaccia con GPG
- Può anche gestire chiavi SSH e password di applicazioni (come le password di login per siti Internet)
- È ben integrato con varie applicazioni di sistema come Nautilus, gedit ecc.

Seahorse: panoramica

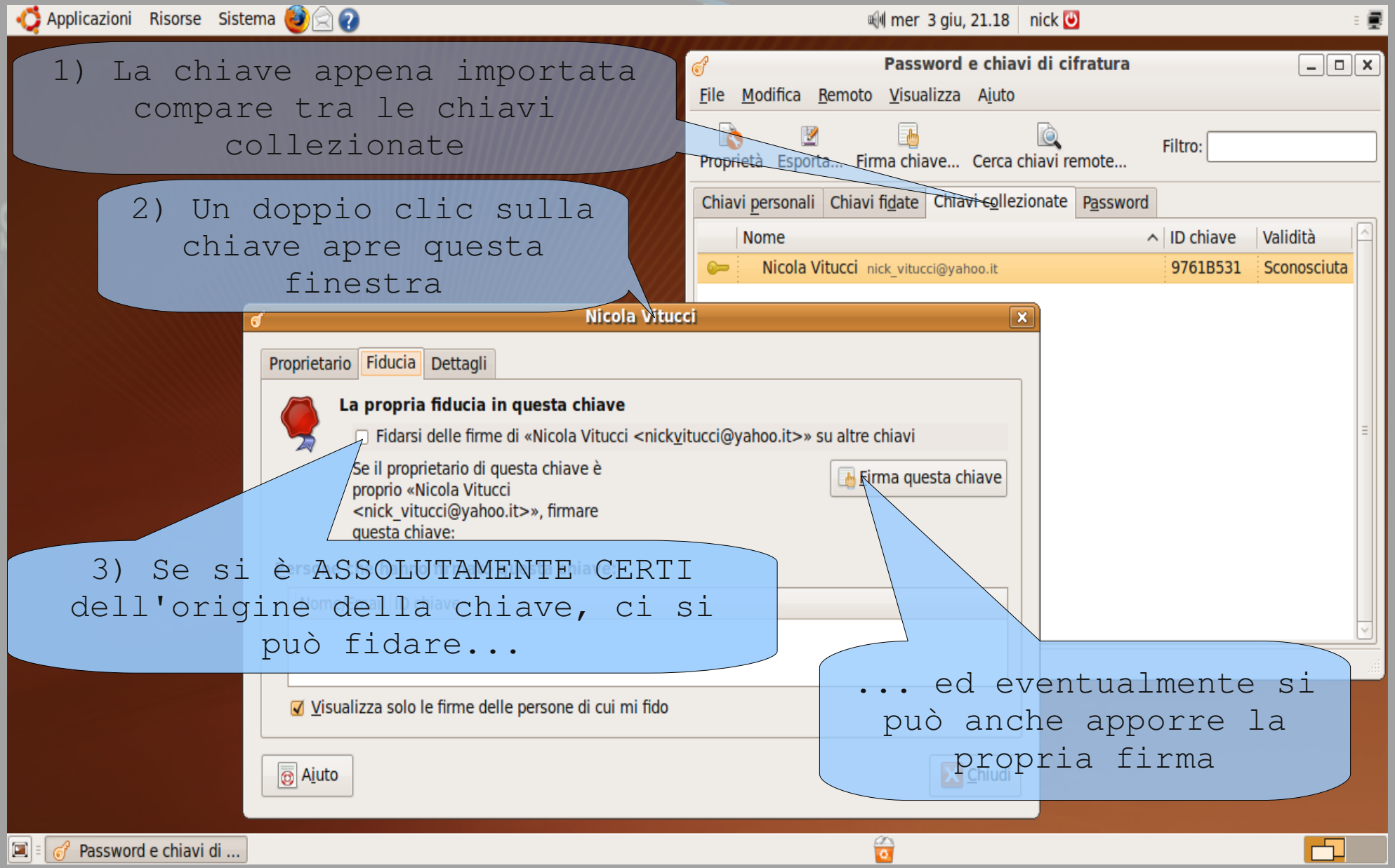
Creazione delle chiavi



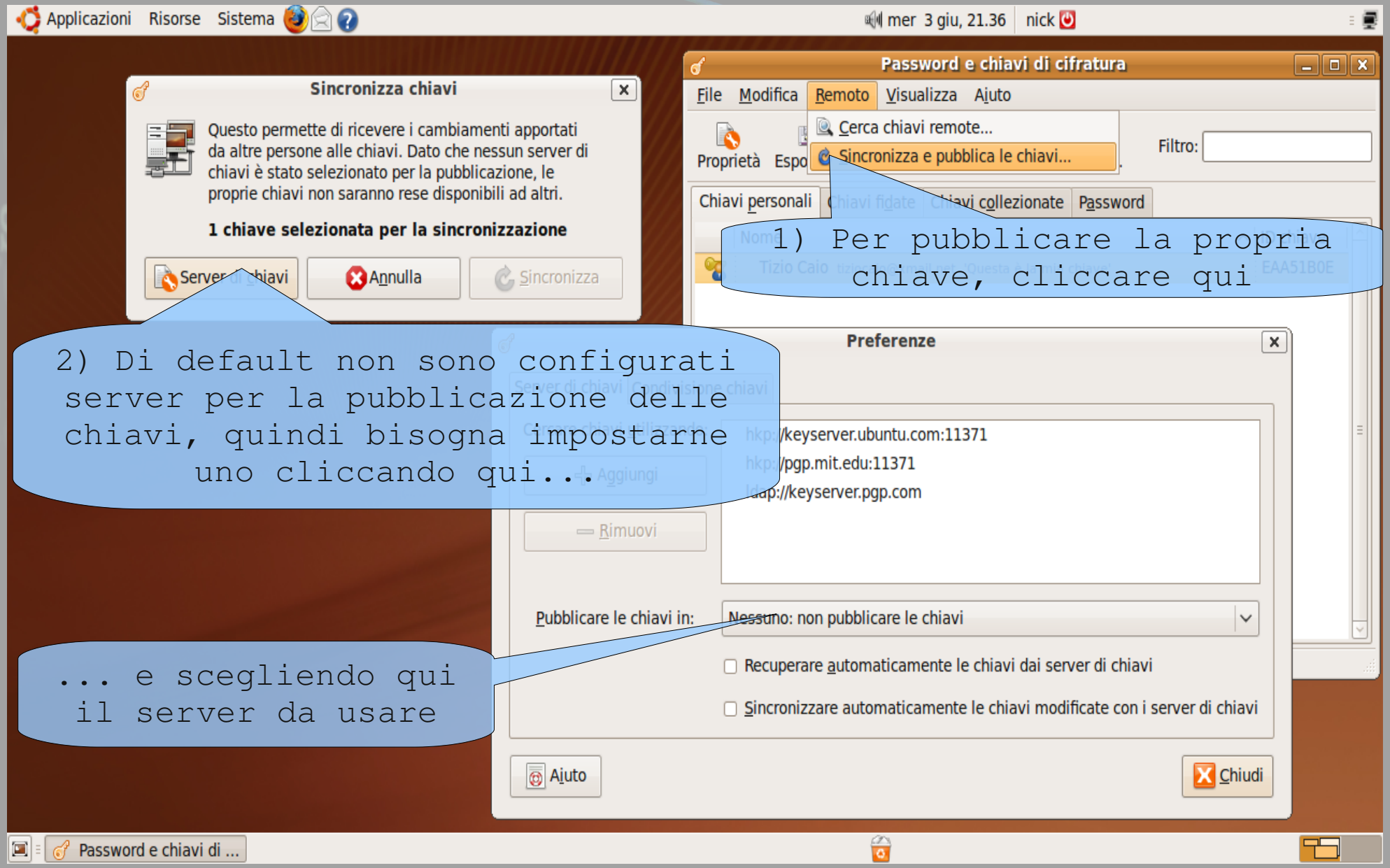
Ricerca delle chiavi



Firma delle chiavi



Pubblicazione delle chiavi



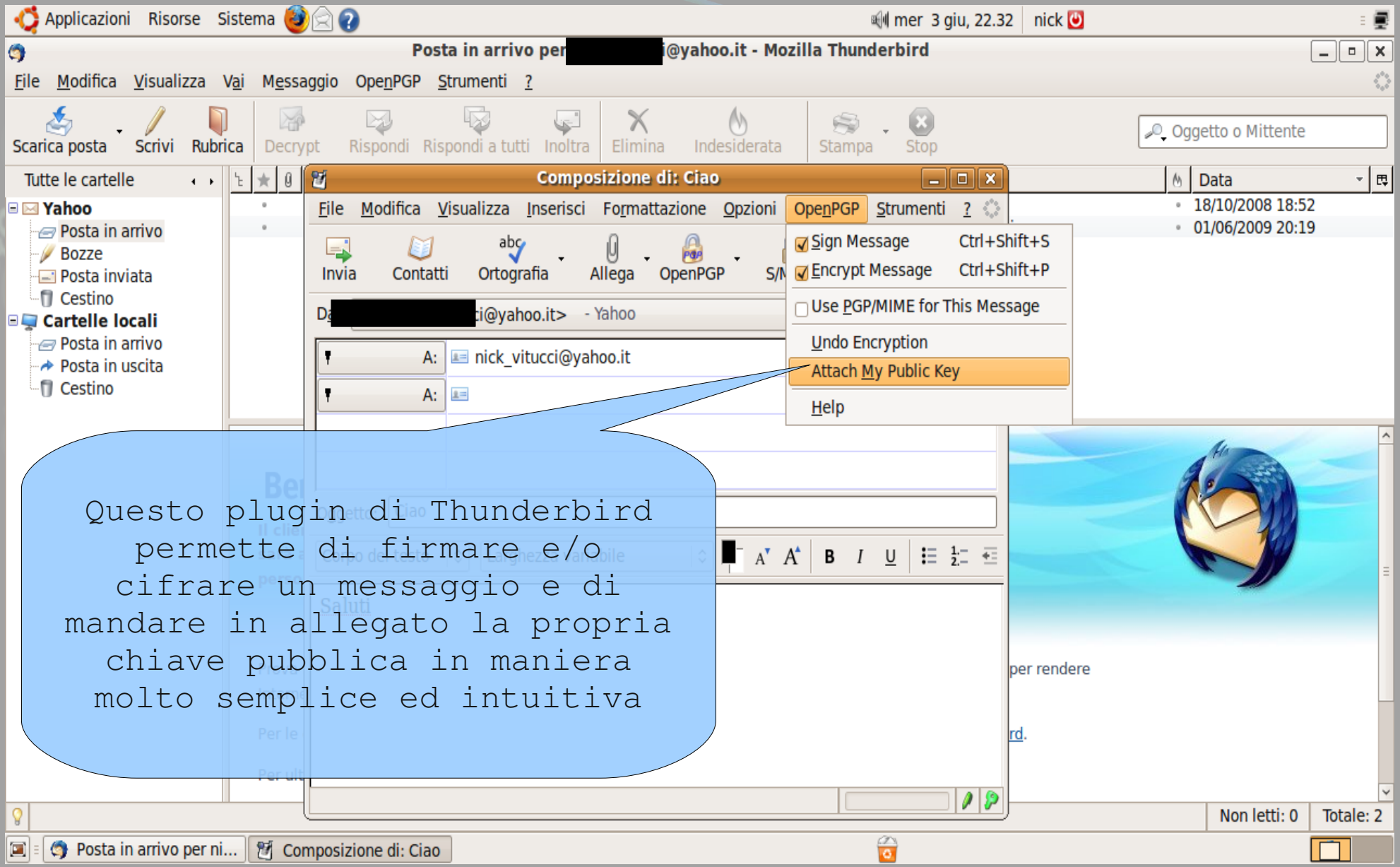
Note

- La pubblicazione delle chiavi è una cosa seria: bisogna essere sicuri di usare sempre quella coppia di chiavi per cifrare/decifrare
- Una chiave pubblicata non può essere cancellata ma deve essere revocata
- Le password scelte devono sempre essere robuste

Cifratura di file

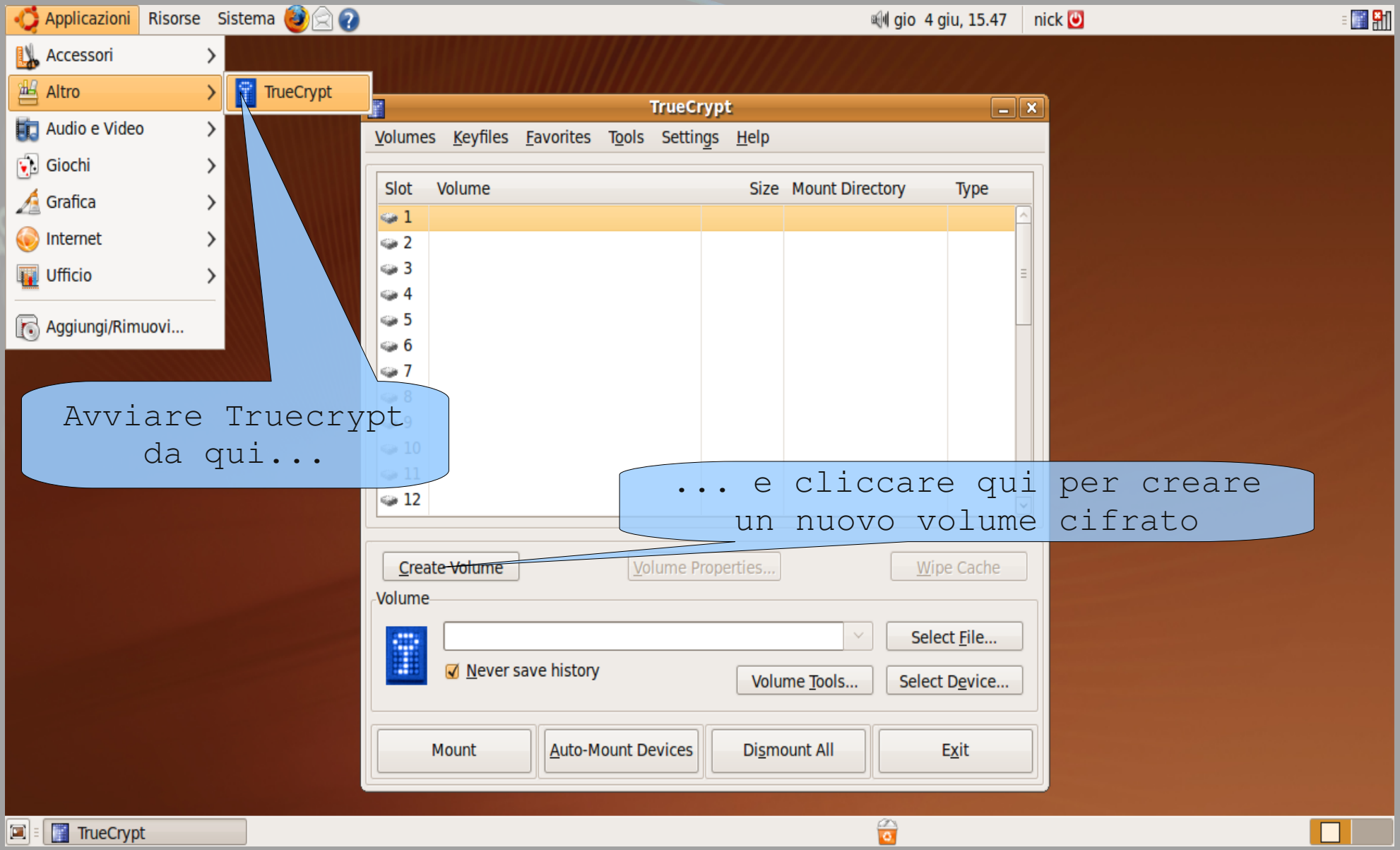
- È possibile cifrare e/o firmare un file con un semplice “clic destro”
- Si possono così spedire file cifrati via email
- Se il destinatario non ha la propria chiave pubblica, conviene spedirgliela come altro allegato
- Di norma viene prodotto un nuovo file mentre il file originale non viene toccato, quindi attenzione

Enigmail



Questo plugin di Thunderbird permette di firmare e/o cifrare un messaggio e di mandare in allegato la propria chiave pubblica in maniera molto semplice ed intuitiva

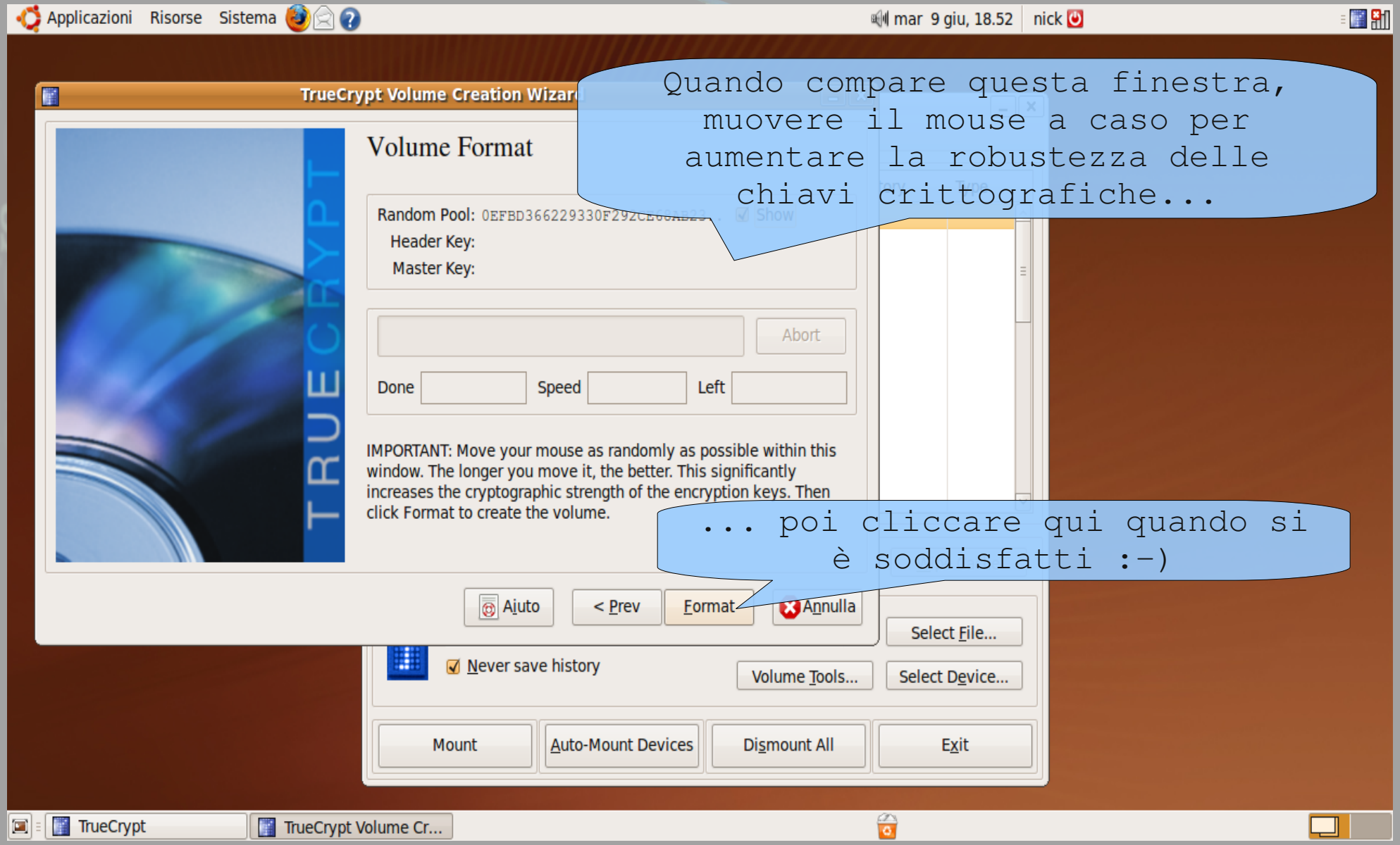
Truecrypt


Applicazioni
Risorse
Sistema
gio 4 giu, 15.47
nick
Accessori
Altro
Audio e Video
Giochi
Grafica
Internet
Ufficio
Aggiungi/Rimuovi...
TrueCrypt
TrueCrypt
Volumes
Keyfiles
Favorites
Tools
Settings
Help
Slot
Volume
Size
Mount Directory
Type
1
2
3
4
5
6
7
12
Create Volume
Volume Properties...
Wipe Cache
Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit
Avviare Truecrypt da qui...
... e cliccare qui per creare un nuovo volume cifrato
TrueCrypt

Creazione di volumi cifrati

- I passi successivi sono:
  1. Selezionare *Create an encrypted file container*
  2. Selezionare *Standard TrueCrypt volume*
  3. Selezionare la directory e scrivere il nome del file da creare
  4. Lasciare invariate le opzioni sulla cifratura
  5. Scegliere la dimensione del volume
  6. Scegliere una password robusta
  7. Scegliere il tipo di filesystem

Generazione delle chiavi



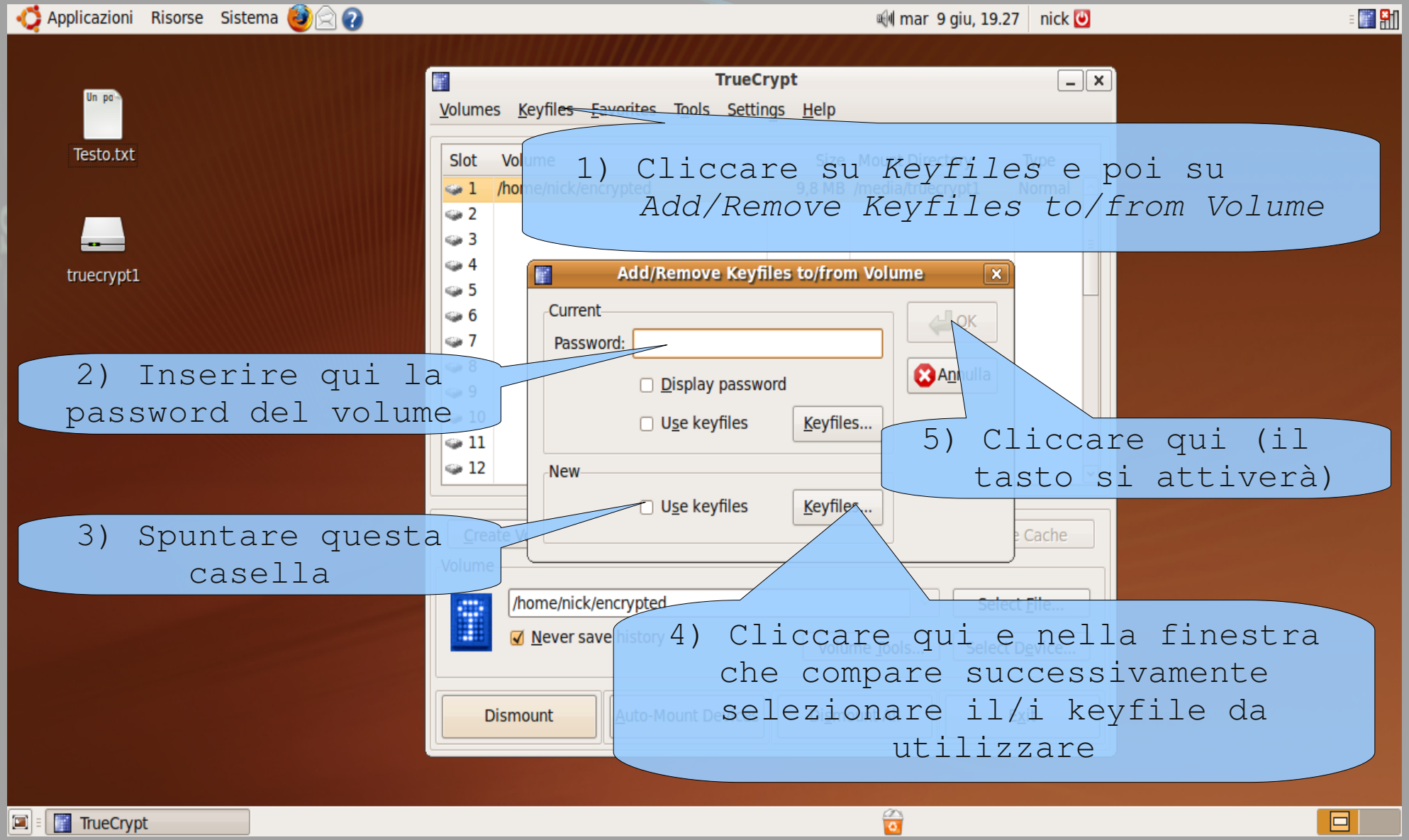
Montaggio di volumi cifrati

- Per montare un volume cifrato:
  1. Cliccare su uno slot vuoto nella finestra principale del programma
  2. Selezionare il file con *Select file...*
  3. Cliccare su *Mount*
  4. Scrivere la password del volume
  5. Scrivere la password di amministratore o di utente per montare il volume
- Per smontare un volume cifrato, cliccare sullo slot corrispondente e poi su *Dismount*

I keyfile

- Per una maggior protezione, si possono usare i *keyfile*
- Un keyfile è un file qualunque che può essere usato come chiave insieme alla password
- Il keyfile usato NON deve essere modificato, quindi non bisogna usare file come documenti o comunque soggetti a modifiche

Utilizzo dei keyfile



Utilizzo dei keyfile

- D'ora in poi, quando si vorrà montare il volume cifrato con i keyfile, oltre alla password bisognerà fornire i keyfile utilizzati
- Bisogna perciò tenere una copia di backup dei keyfile selezionati, altrimenti in caso di smarrimento non si potrà più accedere al volume cifrato