



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 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 "tritattutto" 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

The image shows a screenshot of the Ubuntu desktop environment. On the left, the application menu is open, displaying various categories like 'Accessori', 'Altro', 'Audio e Video', etc. The 'Password e chiavi di cifratura' application is highlighted, with a tooltip that reads 'Gestisce le proprie password e chiavi di cifratura'. On the right, the Seahorse application window is open, showing a 'Crea nuovo...' dialog box. This dialog box prompts the user to 'Selezionare il tipo di oggetto da creare:' and lists three options: 'Chiave PGP' (Utilizzata per cifrare email e file), 'Portachiavi' (Usato per salvare le password delle applicazioni e di rete), and 'Chiave Secure Shell' (Utilizzata per accedere ad altri computer (es. attraverso un terminale)). The 'Chiave PGP' option is selected. A blue callout bubble points to this option.

1) Questo è il percorso standard per aprire l'applicazione su Ubuntu

2) Dopo aver aperto l'applicazione, cliccando qui si apre la finestra di selezione del tipo di chiave

3) Scegliamo di creare una chiave PGP

Creazione delle chiavi

Applicazioni Risorse Sistema mer 3 giu, 20.50 nick

Nuova chiave PGP

Una chiave PGP consente di cifrare email o file ad altre persone.

Nome e cognome: Tizio Caio

Indirizzo email: tiziocaio@xmail.net

Commento: Questa è la mia chiave

Opzioni avanzate

Aiuto Annulla Crea

Genera una nuova chiave

Password e chiavi di cifratura

File Modifica Remoto Visualizza Aiuto

Proprietà Esporta... Cerca chiavi remote... Filtro:

Chiavi personali Chiavi fidate Chiavi collezionate Password

Nome ID chiave

Passphrase per la nuova chiave PGP

Inserire due volte la passphrase per la nuova chiave.

Password: ●●●●●●●●●●●●●●●●

Conferma: ●●●●●●●●●●●●●●●●

Annulla OK

Inserire qui nome, cognome e mail (il commento non è necessario)

Scegliere una password SICURA

Password e chiavi di ... Nuova chiave PGP

Ricerca delle chiavi

1) Cliccando qui...

Cerca chiavi remote

Questo cercherà altre chiavi attraverso Internet. Queste chiavi possono poi essere importate nel proprio portachiavi.

Cerca chiavi contenenti:

Dove cercare:

Annulla Trova

Password e chiavi di cifratura

File Modifica Remoto Visualizza Aiuto

Proprietà Esporta... Cerca chiavi remote... Filtro:

Chiavi personali Chiavi fidate Chiavi collezionate Password

Nome	ID chiave	Validità
Nicola Vitucci nick_vitucci@yahoo.it	9761B531	
Nicola Vitucci nick_vitucci@yahoo.it	9761B531	

2) Selezioniamo un risultato...

... si apre questa finestra in cui scrivere il nome da cercare

... e clicchiamo qui per importare la chiave corrispondente

1 chiave selezionata

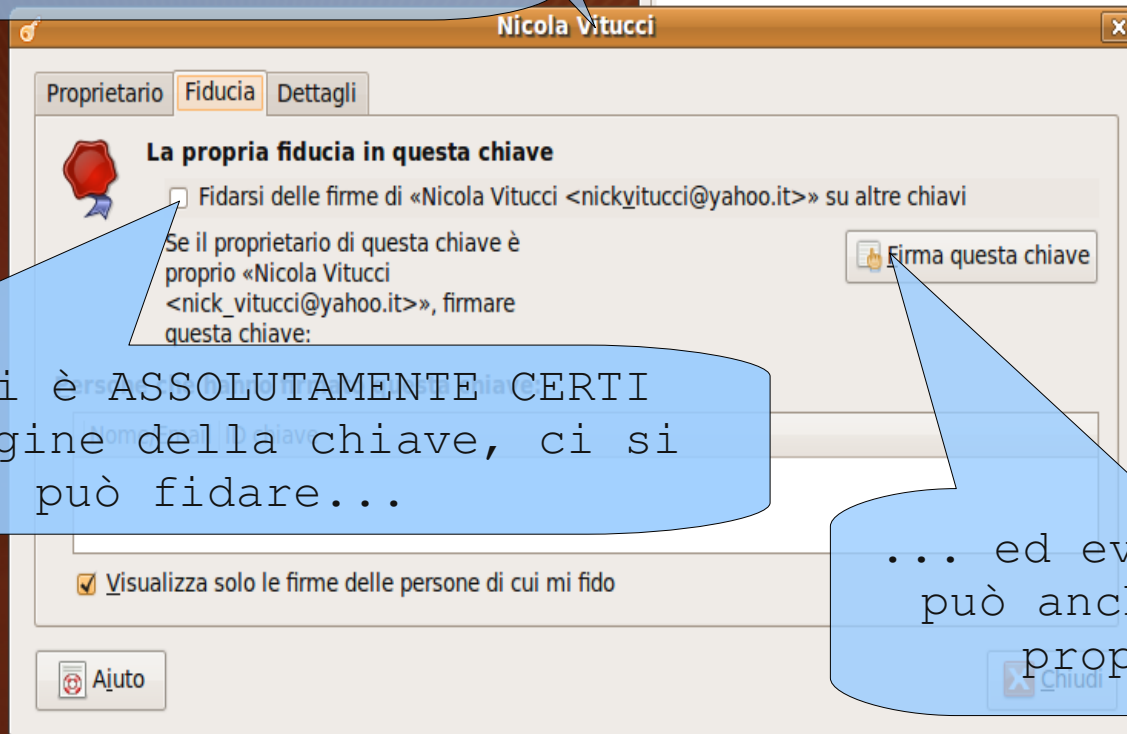
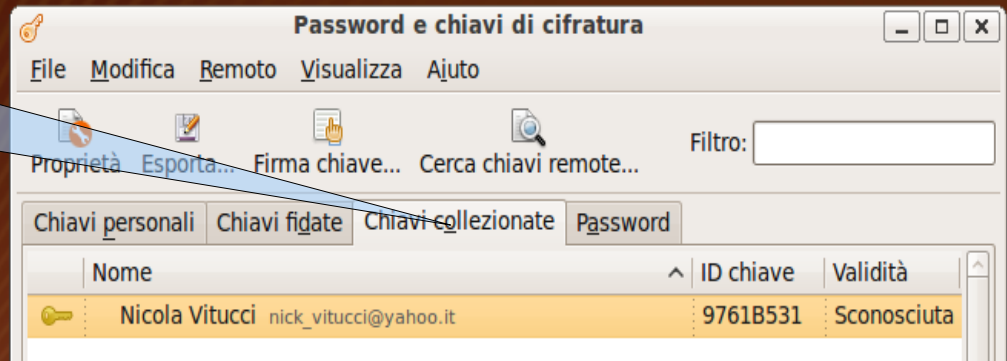
Passoword e chiavi di ...

Firma delle chiavi

1) La chiave appena importata compare tra le chiavi collezionate

2) Un doppio clic sulla chiave apre questa finestra

3) Se si è ASSOLUTAMENTE CERTI dell'origine della chiave, ci si può fidare...



... ed eventualmente si può anche apporre la propria firma

Pubblicazione delle chiavi

The image shows a screenshot of an Ubuntu desktop environment. The top panel displays the system menu with 'Applicazioni', 'Risorse', and 'Sistema' icons, along with the date 'mer 3 giu, 21.36' and the user name 'nick'. The main desktop area features three windows:

- Sincronizza chiavi:** A dialog box with the title 'Sincronizza chiavi'. It contains the text: 'Questo permette di ricevere i cambiamenti apportati da altre persone alle chiavi. Dato che nessun server di chiavi è stato selezionato per la pubblicazione, le proprie chiavi non saranno rese disponibili ad altri.' Below this, it states '1 chiave selezionata per la sincronizzazione'. At the bottom, there are three buttons: 'Server di chiavi' (highlighted with a blue callout), 'Annulla', and 'Sincronizza'.
- Password e chiavi di cifratura:** A window with a menu bar including 'File', 'Modifica', 'Remoto', 'Visualizza', and 'Ajuto'. The 'Remoto' menu is open, showing options like 'Cerca chiavi remote...' and 'Sincronizza e pubblica le chiavi...' (highlighted with a blue callout). Below the menu, there are tabs for 'Chiavi personali', 'Chiavi fidate', 'Chiavi collezionate', and 'Password'. A blue callout points to the 'Sincronizza e pubblica le chiavi...' option with the text: '1) Per pubblicare la propria chiave, cliccare qui'.
- Preferenze:** A window titled 'Preferenze' showing a list of key servers. The list includes: 'hkp://keyserver.ubuntu.com:11371', 'hkp://pgp.mit.edu:11371', and 'ldap://keyserver.pgp.com'. Below the list is a 'Rimuovi' button. Underneath, there is a dropdown menu labeled 'Pubblicare le chiavi in:' with 'Nessuno: non pubblicare le chiavi' selected. Below this are two checkboxes: 'Recuperare automaticamente le chiavi dai server di chiavi' and 'Sincronizzare automaticamente le chiavi modificate con i server di chiavi'. At the bottom, there are 'Ajuto' and 'Chiudi' buttons. A blue callout points to the dropdown menu with the text: '2) Di default non sono configurati server per la pubblicazione delle chiavi, quindi bisogna impostarne uno cliccando qui...'. Another blue callout points to the 'Chiudi' button with the text: '... e scegliendo qui il server da usare'.

The bottom panel shows the taskbar with the 'Password e chiavi di ...' window icon and a trash icon.

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

Applicazioni Risorse Sistema mer 3 giu, 22.32 nick

Posta in arrivo per [redacted]@yahoo.it - Mozilla Thunderbird

File Modifica Visualizza Vai Messaggio OpenPGP Strumenti ?

Scarica posta Scrivi Rubrica Decrypt Rispondi Rispondi a tutti Inoltra Elimina Indesiderata Stampa Stop

Oggetto o Mittente

Tutte le cartelle

- Yahoo
 - Posta in arrivo
 - Bozze
 - Posta inviata
 - Cestino
- Cartelle locali
 - Posta in arrivo
 - Posta in uscita
 - Cestino

Composizione di: Ciao

File Modifica Visualizza Inserisci Formattazione Opzioni OpenPGP Strumenti ?

Invia Contatti Ortografia Allega OpenPGP S/M

D: [redacted]@yahoo.it - Yahoo

A: nick_vitucci@yahoo.it

A:

Sign Message Ctrl+Shift+S

Encrypt Message Ctrl+Shift+P

Use PGP/MIME for This Message

Undo Encryption

Attach My Public Key

Help

per rendere

rd.

Non letti: 0 Totale: 2

Posta in arrivo per ni... Composizione di: Ciao

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

Avviare Truecrypt da qui...

... e cliccare qui per creare un nuovo volume cifrato

Slot	Volume	Size	Mount Directory	Type
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

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

Applicazioni Risorse Sistema mar 9 giu, 18.52 nick

TrueCrypt Volume Creation Wizard

Volume Format

Random Pool: 0EFBD366229330F292CE66AB22 Show

Header Key:

Master Key:

Abort

Done Speed Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Ajuto < Prev **Format** Annulla

Select File...

Never save history Volume Tools... Select Device...

Mount Auto-Mount Devices Dismount All Exit

TrueCrypt TrueCrypt Volume Cr...

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

The image shows a Linux desktop environment with the TrueCrypt application open. The application window has a menu bar with 'Volumes', 'Keyfiles', 'Favorites', 'Tools', 'Settings', and 'Help'. A table lists 12 slots, with slot 1 selected and showing the volume path '/home/nick/encrypted'. An 'Add/Remove Keyfiles to/from Volume' dialog box is open, showing a 'Current' section with a 'Password:' field and checkboxes for 'Display password' and 'Use keyfiles'. A 'New' section also has a 'Use keyfiles' checkbox. A 'Keyfiles...' button is visible in both sections. The dialog box has 'OK' and 'Annulla' buttons. The background shows a file manager window with 'Testo.txt' and 'truecrypt1' files.

1) Cliccare su **Keyfiles** e poi su **Add/Remove Keyfiles to/from Volume**

2) Inserire qui la password del volume

3) Spuntare questa casella

4) Cliccare qui e nella finestra che compare successivamente selezionare il/i keyfile da utilizzare

5) Cliccare qui (il tasto si attiverà)

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