Protezione della posta elettronica sotto Linux

Antonio TREPICCIONE
Pietro SPIEZIA
Raffaele FAELLA

Università di Salerno - Dipartimento di Informatica ed Applicazioni

Sistemi di elaborazione dell'informazione (Sicurezza su Reti)
Anno Acc.2000-2001

Introduzione

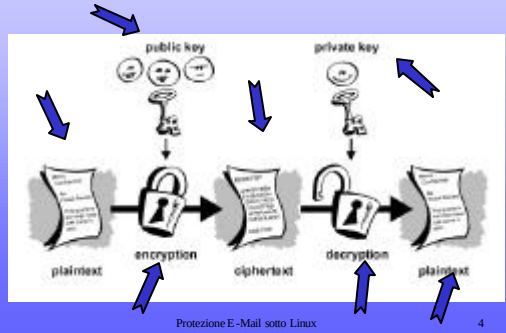
- Cifrare, Firmare, Decifrare
  - PGP (Pretty Good Privacy)
- Gestione Posta (con e senza Plugins)
  - Elm
  - Netscape Messanger
  - Pine

PGP: cos'è

E' un pacchetto freeware che fornisce protezione per la posta elettronica e la memorizzazione di file

Creato da P. Zimmermann nel 1991 e distribuito su Internet

PGP: Schema funzionale

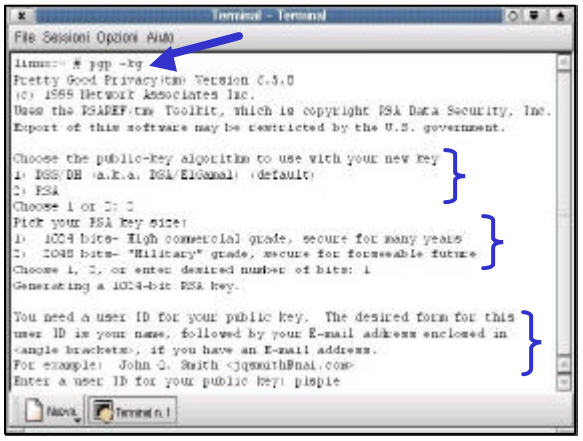


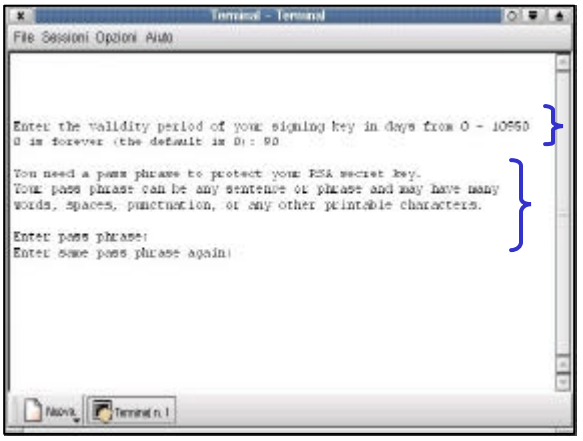
PGP: versione 2.6.3i e 6.5.8

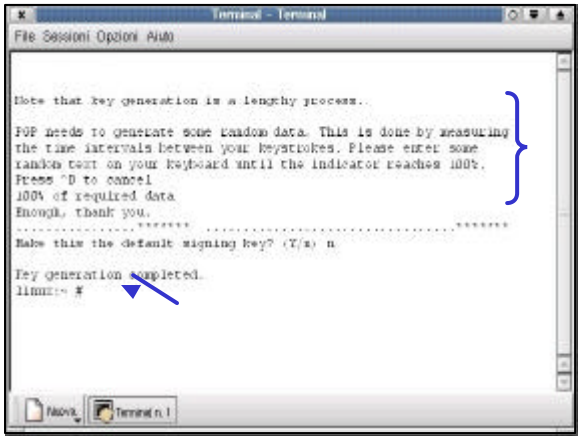
- Versione 2.6.3i
  - Per tutti coloro che non risiedono negli USA
  - Basata sul PGP 2.6.2 e modificata per l'uso internaz.
  - E' compatibile con tutte le versioni precedenti
  - Crea chiavi di dim. 512 bit, 768 bit oppure 1024 bit
- Versione 6.5.8
  - Risolve piccoli bug delle versioni precedenti
  - Crea chiavi di dimensione di 1024 bit oppure 2048 bit

PGP: Generazione chiavi

- L'utente deve generare la sua coppia di chiavi (comando: *pgp -kg*)
- Si sceglie l'algoritmo da utilizzare
- Si sceglie la lunghezza della chiave
- Si sceglie il proprio ID
- Si sceglie il periodo di validità
- Si sceglie la passphrase





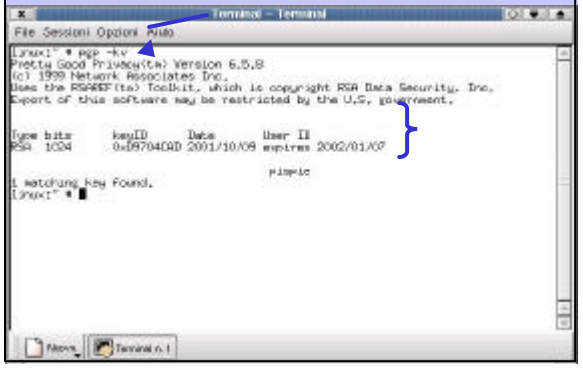


Key-ring

Le chiavi sono memorizzate nei key-ring

- Private Key-Ring
  - Memorizza la coppia di chiavi, pubblica e privata, dell'utente
  - La chiave privata è cifrata con la passphrase
- Public Key-Ring
  - Usato per memorizzare le chiavi pubbliche delle persone note all'utente

Key-Ring: Visualizzazione



PGP: Protezione chiavi

- I due keyring securing.skr e pubring.pkr sono memorizzati sul proprio HD
- PGP suggerisce una copia di backup al termine della generazione
- La copia può essere memorizzata sul proprio hd o su un FD

PGP: Gestione chiavi pubbliche

- Per ottenere la chiave pubblica di qualcuno si può chiedere direttamente alla persona interessata…
- …oppure si possono usare i Key-Server:
  - Server presenti su Internet, dedicati al deposito e prelievo di chiavi pubbliche
  - Sono in rete tra loro, per cui ogni chiave immessa in un server viene diffusa a tutti gli altri

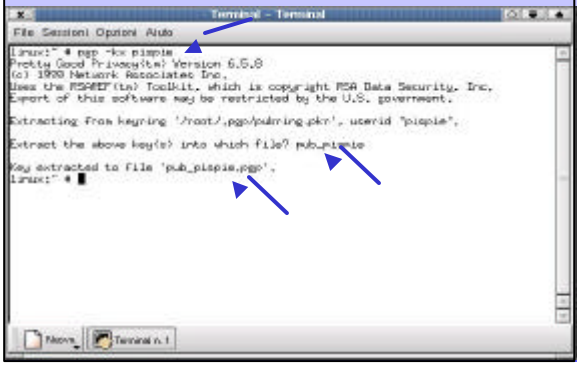
PGP: Distribuzione delle chiavi

- E' necessario distribuire la nostra chiave pubblica
  - per consentire agli altri di mandarci messaggi cifrati
  - per verificare la nostra firma
- Ciò può essere fatto in vari modi:
  - mandando la chiave ad un Key-Server
  - includendo la chiave in un messaggio di e-mail
  - esportando la chiave copiandola in un file di testo

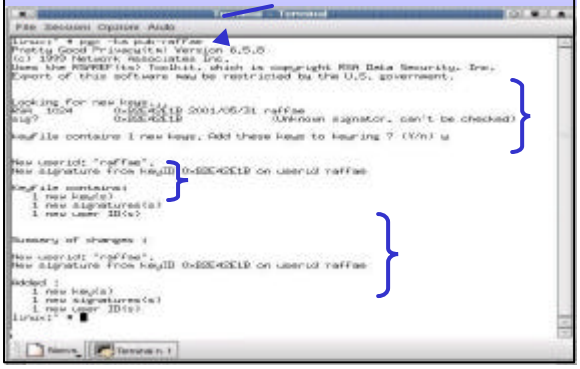
PGP: Distribuzione delle chiavi

- Per **estrarre** la propria chiave pubblica dal key-ring:
  - *pgp -kx userid*
- Per **aggiungere** una chiave pubblica nel key-ring:
  - *pgp -ka keyfile*
- Per **visualizzare** il contenuto del key-ring:
  - *pgp -kv*

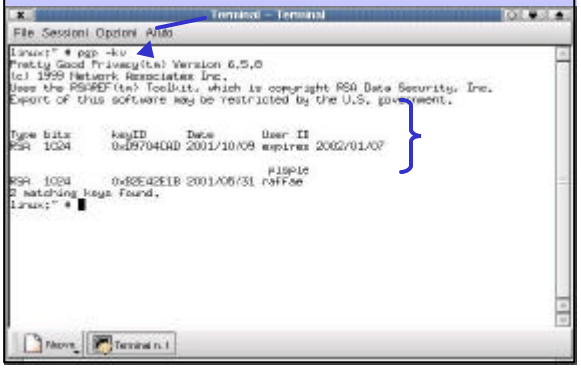
PGP: Estarre una chiave pubblica



PGP:Aggiungere una chiave pubblica



PGP: Visualizzare il Key-Ring



PGP ed e-mail

- Possibilità di cifrare una e-mail
- Possibilità di firmare una e-mail, lasciando il testo in chiaro
- Possibilità di fare entrambe le operazioni

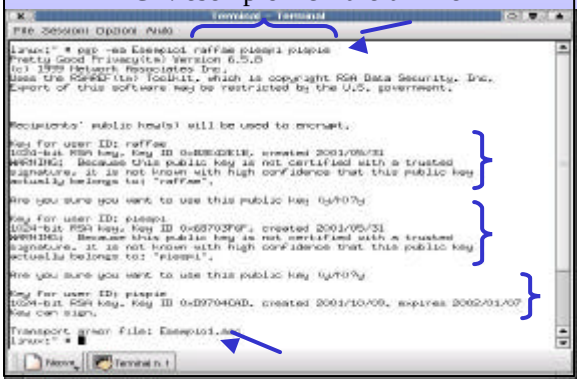
PGP: un esempio

Testo in chiaro

File Esempio1

"Quel ramo del lago di Como, che volge a mezzogiorno, tra due catene non interrotte di monti, tutto a seni e a golfi, a seconda dello sporgere e del rientrare di quelli, vien, quasi a un tratto, a restringersi, e a perder corso e figure di fiume, tra un promontorio a destra, e un'ampia costiera dall'altra parte; e il ponte, che ivi congiunge le due rive, par che renda ancor più sensibile all'occhio questa trasformazione, e segna il punto in cui il lago cessa, e l'Adda ricomincia, per ripigliar poi nome di lago dove le rive, allontanandosi di nuovo, lascian l'acqua distendersi e rallentarsi in nuovi golfi e in nuovi seni."

PGP: esempio - cifrare un file



PGP: esempio - cifrare un file

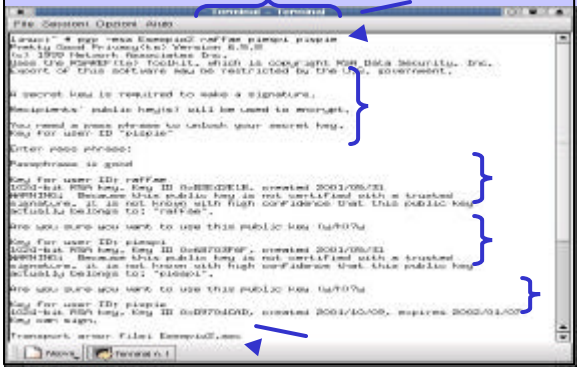
Comando: *pgp -ea Esempio1 raffae piespi pispie*

(File generato: Esempio1.asc)

```
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5.8

hQCMA2w94VEzOTyBAQP/VSMWvdA4y5dojK6u222EzObTVyoPX9OiNGOwy8VGeYLnX1dVO5/7WofrDm
I6pWGGSsVVv81EzARO+O3sK1sw2VSUh8cc1QMwa0ZUOVtzp/zAP5uty07i89J9by3d8jzLM+SjcHHZ
zL+BvPVy/uoQ8Q/+3vYH84dP7r+fpvO7V7mFAIwDmJWylbLkLhsBA/sH7qAyFseoxxj6GH5ZiWZsTq
677S9HTKnnY8X4lpcZmGjc6Cy1IlKL/J6bgwwPrJfmTyiLyu6Kq7rL4dIKsxi6+Sw7hUIh/Z3Pe07
K2LaWb39R+w0vrF0vU+pHllGtAQ0QwSpZEPxiEIAh1SKIWHjPhz9E0byxWL62wkQU4BWw4UAjADhu6
rxaHA/bwED/0Fqp6h+JS8ZvPGf80cJWweDkbtM/IFyEerLlmGU0+e6I5VYFVbYebuFOevMJqKkOdls
IctRArBKT09rN2E0+eyc8ZbOUqsgGsGEQrOPOUiJmX/L5c1baWY6qETvsPMXM71jKwXKmqfZDSGKTl
dqk+0Nu2bYcbIp2zBU8FCvM6LcpQGPfyNczzGo1GtrpPFIo8IM1DU6Fa89GzxraDTnrLJD3Mo6xD9W
7HX4IqzpdUMGs16vHK00XQAF4hXrsnVOCZS4cfHloZxrzzWZH6B2Vm10XnuTyP7bJiVhbfZ4n4ndLN
QPNBZuk7L3D7Qu7MAulyVG7uU3IzdrYIw+gQ7soVoaryZCw+VAoLRkRECIREimVoXEGjmxj0hw4HQG
bsoPaca9PKgr+2sDrfX4aRRve+B3tC4nulxZSs+mOQeM1xVd1jB2iPqbuwqbprawn8ZRbST3QQxb+
GcruNMOKC88oEQ2AsR27mJrZ4IRFzA1ksoToGO03GKm5JwIUIqWUhDvfAzraqgS+hMlIEqTJaV2IP5
RVfaQg1vVEALxziw2bsQzruhgAv+mFGleU0XAOvADag49gdC5otF3Qeo6mSmhKJ5d+4XD731nBREV6
P8MUInBMp0pVTMGgQ9OJJ9HJuiObzDi0xESzEOVejqYbDxczajz6a+mbuO+NXLBEFsDs8O27Zuc4eZ
Cu0+qmtVzZ52VPrB=Iphh
-----END PGP MESSAGE-----
```


PGP: esempio – cifrare e firmare un file



PGP: esempio - cifrare e firmare un file

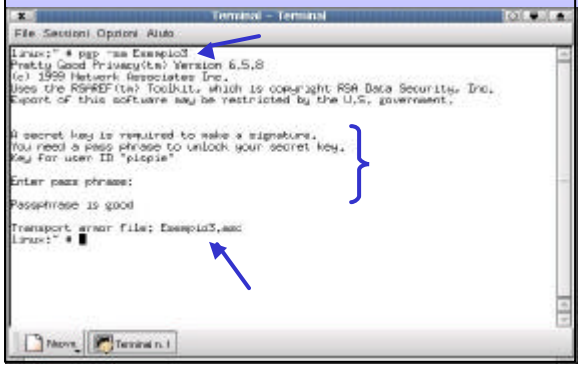
Comando: *pgp -esa Esempio2 raffae piespi pispie*

(File generato: Esempio2.asc)

```
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5.8

hQCMA2w94VEzOTyBAQQAt5825ttB5aZ0B6kUliT6G/aEBZ9YdDtn5SE9o8fvYAGvXwi8imB5ziheEiKVk
f8QYYDaRFo+A466cJmsErtkYa8e/jZjkv+MdWl18Dqir2I2lqf6lp2eKqa9v8sejnhRQE7raXM/4fVol4K
B5fRvo0St7lVSb12Cc7muMAxwJeFAIwDmJWylbLkLhsBA/9o0eKmGBNxii9dtC3PmL59hPjV5jIxgTmALc
OKqo79kYTqLjsuql9TcZCKYKAb8HIVY951plZfuCYVB6zcmichL3wHwDaj2jEWHJu4zFZX2m5YFxwFojf6
5pTByV9Q2wFHhOWKOTR54EuzBvKfK0uCpKw42MJ8poWNIgKCsVBqcoUAjAOhu6rxaHA/bwED/i0BGn9ZdX
PRtBe/IeVDeMVEdE7/2PaCv5JwStPbfb0y84RtopFFr4lsTUgAI2H7BRvJBiU09mY161AITOR9QTd+BTQu
KgtG0mFYWx4K+9tHMHLfmZ48ZmXkEFHIGAFTeduziNw9q1nEa5b7rv9c25uwL1geEi981PFGriV3Mls6pQ
Jr1u1SI0F/OWgnpfc2phXKXrvAyMbVezzZXsScMFt4bZf+efj1UzxHRQ0ZeLR4Rsw+vkdvkQmlzTxhrpI5
UatAYyswutnZCKmgqx8a/vPKppA3XHy3s27W6sxeRdeANkUq1/KSnhpod6pi2gIBBoubDmpaXqDDmLSzJJ
eVTZCH5vY8Dds1/tjjgQKvO1M/hE+Te8pZymLQ6jXhw8vk+hMqTl4jAt8pMQq13Qj3Z/4xsm3Ovv89whD
pu4wk5bQFQQls+XiFZuQi7Px3RxbQZJa+wo8E0lGBhF5LhGMXotQvldvmEmG79glg3XwUCWv+6eVF6fSxJ
aMy5IcxNnWxMPKGme0yM7vixq4J+JXzcteWMmpiMEDqGFH2eBbHIQCmLH/+pZQdvglzxkn35DisMUs05Dy
WQ6raHhXmTX1R9UGrdaFJtf5Dgc1+W5fwcNWw31m1lrOQDK5wcMCT7BwcVNJBxVtVbHzpoO5wLCSB680g9
amcbtPK7aa2v6x6UY4vJxlF22EYMbzHm23+zT8ak6rUiluEWmrBbHxbeks77yDJrYg91L6n7WlbVsUAL61
OWrineEjm6BE6vp9dt0EnrEQnyuBMXSHN0uhcByzjTbTN2hq4fyC7/KukrrII1hPGbAlLHkvu9G0UCT9uT
UCBv8rmbHNLyqcp9LkhdLvNxMvstdIuMrcPouKaMwmVz+rU87nEmZN4HmCANAr+rKiATvBPlT1V+tyyoL
vjoQYXeL8koer/cvKCjWkWBpXKRXYY5mxBe4KOuh0w2RUbuQRwYiX+z900lKCuRUFPbFSTzrs8qR8h9NID
NwknNZeA===GwLx
-----END PGP MESSAGE-----
```

PGP: esempio - firma di testo in chiaro



PGP: esempio - firma di testo in chiaro

Comando: *pgp -sa Esempio3raffae piespi pispie*

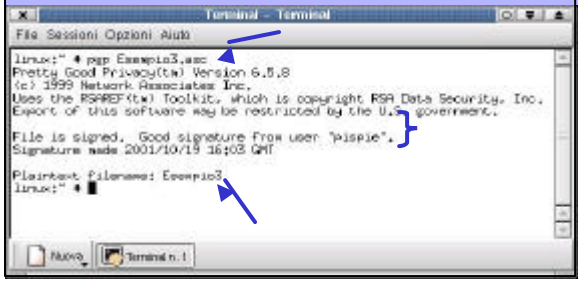
(File generato: Esempio3asc)

```
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5.8
owE1kstrFEEQxjcGRQe8+A/YhOAaEmPMYlBjBA2LErwsnhYfpDNTQynp6Rr7MchGkHiLiJdgEEFFxQ
eC4EXFBC85JVFQyd6TiHhXCEQ0Wj2Lt+7qqq9+9VXPVm52b62MDJ5dUqNfGrVDR2a6ug5f6f478fTE
46UHw279UXW6d+3cgb2j481f8/ODcuH4zrkP+dFn/trP+p+H215MfF3acfDN/Epj5t6lzdvNj0/G9q
8VvcN46/fb0c2osW9x+Xu19unU6d03uoZ+vLvzeeDy9MmsOdvT42dWz194ub6y2ne1b2hj7tX08vvN
M+P1PQt37397vfh8y/XJ7XULWY5U21WpVBoelDAyI5HwQcmUDyjGKKN+EU+BKEilKTIoN2mFMlofn
BGisSDiKUDDUKTFhFqB8aQcxAEMtIOOdE7R1xtQaMIMimpFsdDJCadyNBVkbA5mRQMcE7AiAyC5iam
1LrIlqLCg72801aZAGvAwbLBzUD1hnULQE5MTTKwSRgREzGkohAtDO1HbkW+gw6M78Ch1iWksHAmQ
QdGRS8rko2SbKCdQhhYKlUVapQF+XSOBjhNFQ153LomIUFcrSO0TOKUFCaZLDqZ64oUwyEqaVmMJHj
hojYGouTyMlBn+J4ikl4ZOtkYLQtMplsI2kIWBZSLcuunqEFahF7DPdyc1EM1pb4qnos4T4GY8pQx8
hBdoTvOaYKmSUn5Li1pSOdrVNRIndwI4bhuaSWOiH2m7O0p4LNVtKynOYOMuZd8IvlT5AE57mv4Tpe
nQw3hgs1KKJy68Gt/5HwHwZEFP0D=cHk3
-----END PGP MESSAGE-----
```

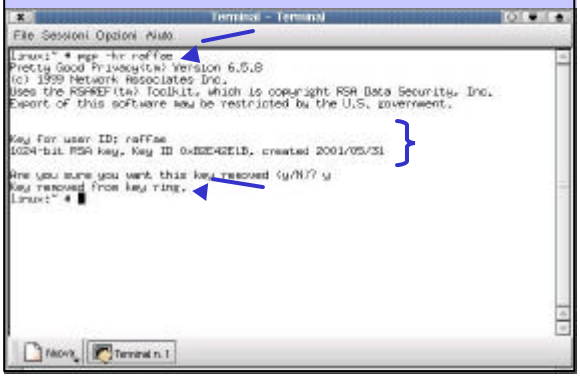

PGP: esempio – decifrare un file

Comando: *pgp "nome file.ext"*

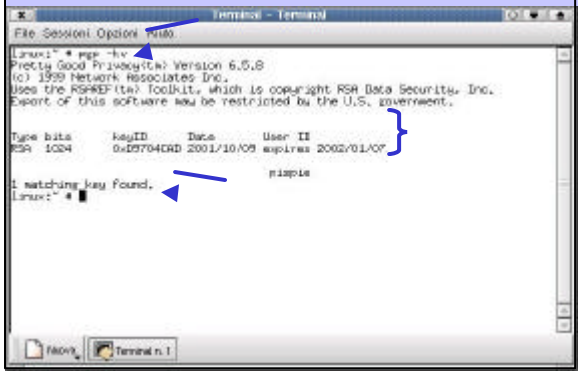
(File generato: "nome file")



PGP: Revoca di una chiave



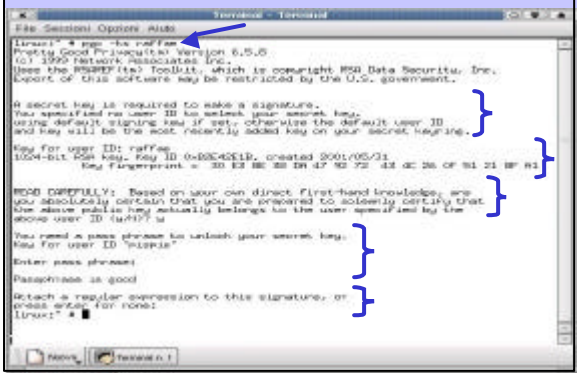
PGP: Visualizzare il Key-Ring



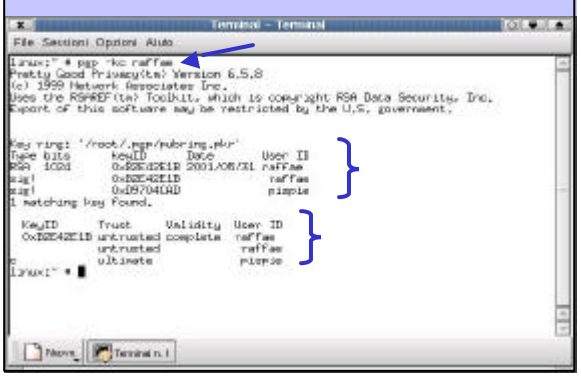
PGP: Certificati

- Per **creare** il certificato PGP di una chiave pubblica:
  - *pgp -ks her_userid*
- Per **controllare** il certificato di una chiave pubblica:
  - *pgp -kc userid*
- Per **rimuovere** il certificato di una chiave pubblica:
  - *pgp -krs userid*

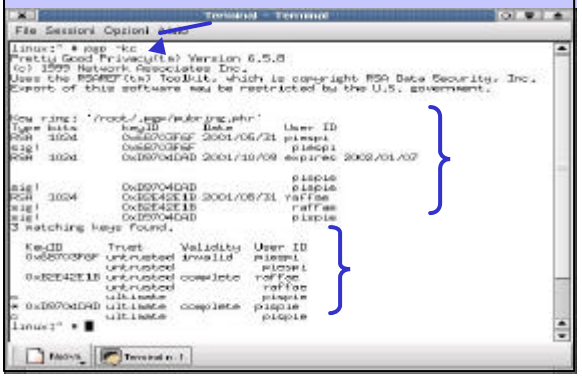
PGP: Creare un certificato



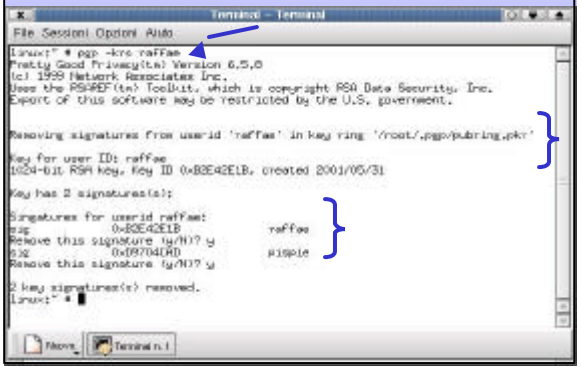
PGP: Controllo di un certificato



PGP: Controllo di tutti i certificati



PGP: Revoca di un certificato



Gestione e-mail

- Elm
- Netscape Messanger
- Pine

Elm

- E' un client di posta elettronica per piattaforme Unix-Linux
- Interfaccia non grafica, poco User Friendly
- In rete sono disponibili 72 versioni di Elm, tra distribuzioni e patch list

Posta sicura con Elm

- Gestire la propria posta elettronica lontano da occhi indiscreti

Come si fa?

Con il **PGP (Pretty Good Privacy)**

Elm senza il supporto PGP

- La maggior parte delle versioni di Elm non supportano il PGP
- Elm 2.4 pl 20
- Elm 2.5 pl 3
- Elm 2.5 pl 20
- Elm 2.5.3-6
- Elm 2.5.5-0.52

…

Elm con il supporto PGP

- Le versioni **ME+** (development by Michael Elkins) hanno integrato il PGP.

Lavoreremo con
Elm 2.4 ME+ pl 60

Ma prima…

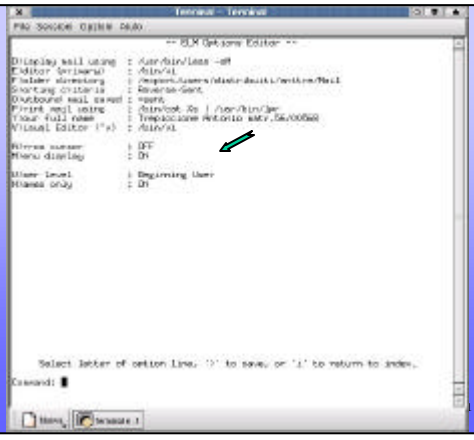
…dobbiamo diventare ESPERTI !?!?

Elm con il supporto PGP

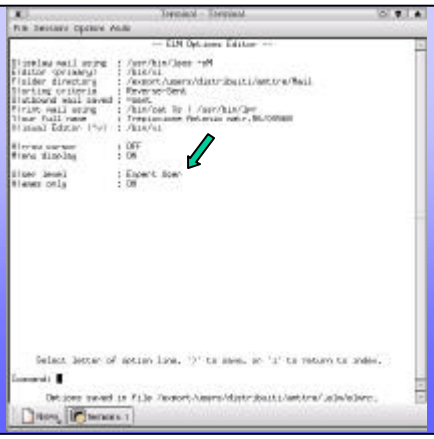
- Di default Elm 2.4ME+ pl 60 non presenta nessuna funzione PGP
- La reference guide e il Man non ne parlano

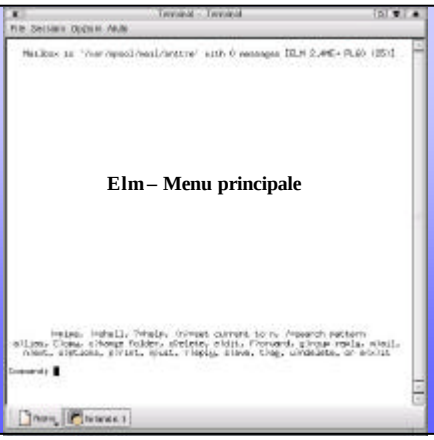
E allora ?

Si deve cambiare nel menu Option lo **User Level** che di default è fissato a **Beginning**



Fissarlo a EXPERT …..



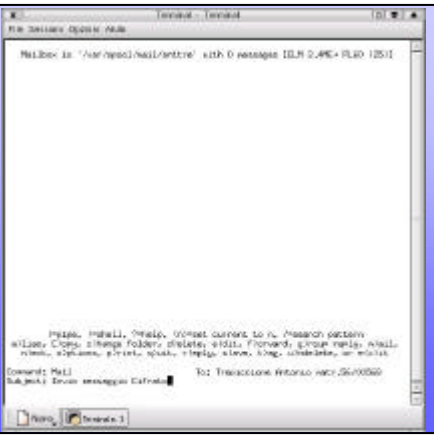


Elm – Menu principale

Invio di un messaggio CIFRATO

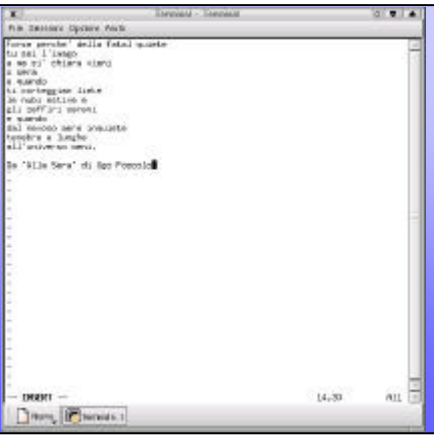
- Utilizzeremo i comandi PGP che Elm supporta per cifrare il messaggio da inviare
- Il destinatario deve essere presente nel nostro key ring
- Se il destinatario ancora non possiede la nostra chiave pubblica…

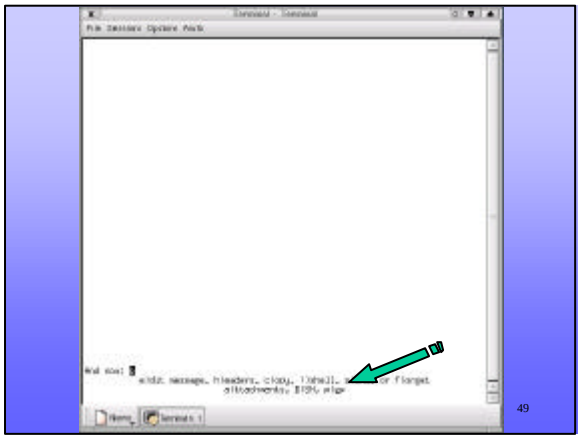
  …forniamogliela, ad es., in allegato



Invio di un messaggio CIFRATO

- Inseriti i campi To, Subject e Copy to, si accede all'editor di testo per comporre il messaggio
- Di default l'editor è il **VI**
- <i> per inserire il testo
- <ESC :wq> per salvare e uscire





49

Il PGP permette di:

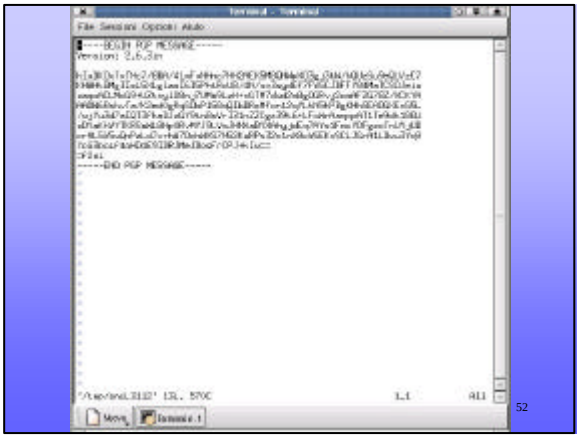
- **Cifrare un messaggio**
- **Firmare un messaggio**
- **Cifrare e Firmare un messaggio**

Ora cifriamo il nostro messaggio

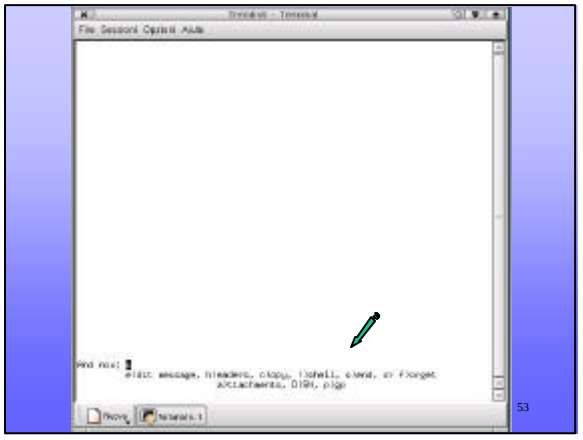
50

- **Bisogna inserire lo User Id del destinatario**
- **Si trova nel proprio key ring**
- **Solo la persona associata allo User Id potrà decifrare e quindi leggere il messaggio.**

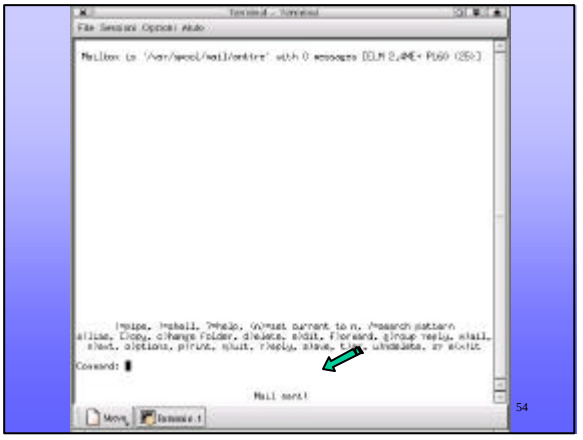
51



52



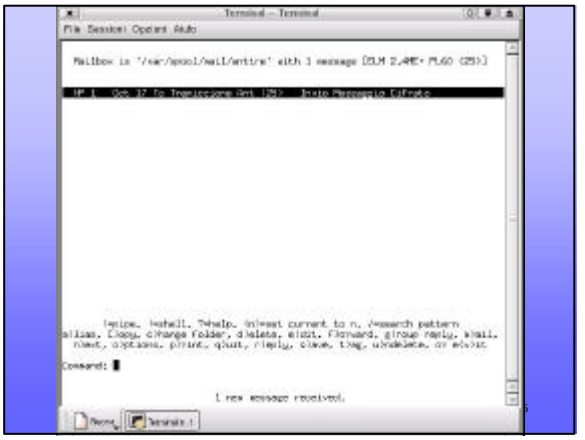
53

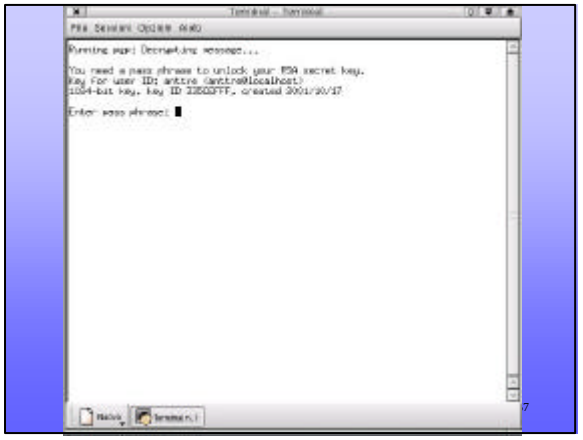


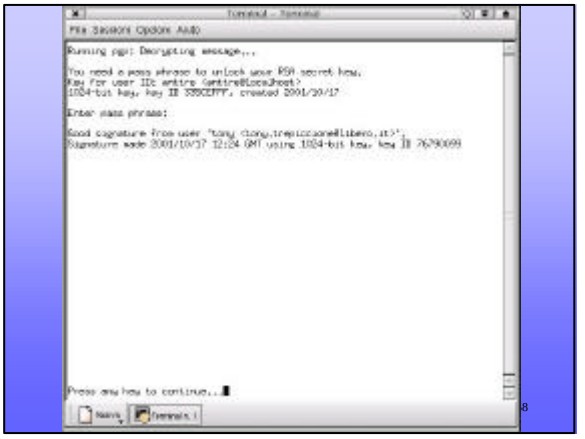
54

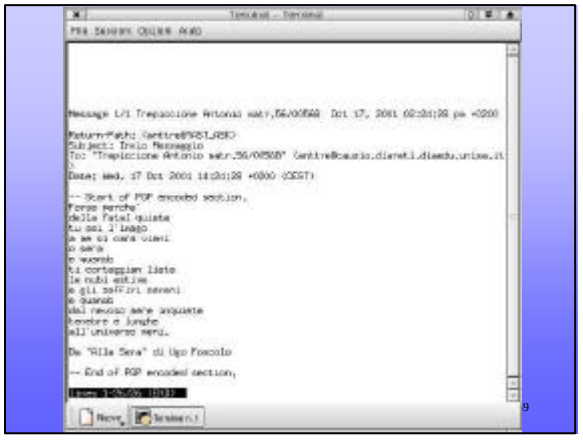
Ricezione di un messaggio CIFRATO

- Il destinatario del messaggio deve ricordarsi la propria passphrase, che lo autorizza a decifrare il messaggio.









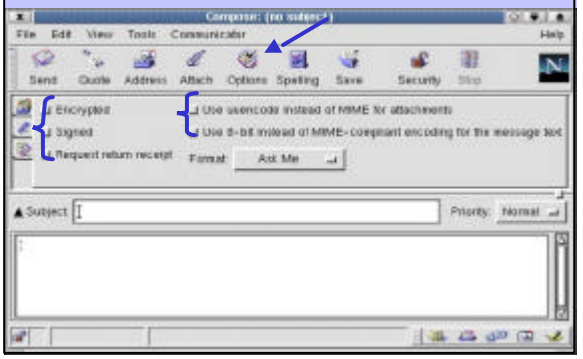
Netscape Messanger

- Messaggio cifrato in allegato
- Messaggio cifrato

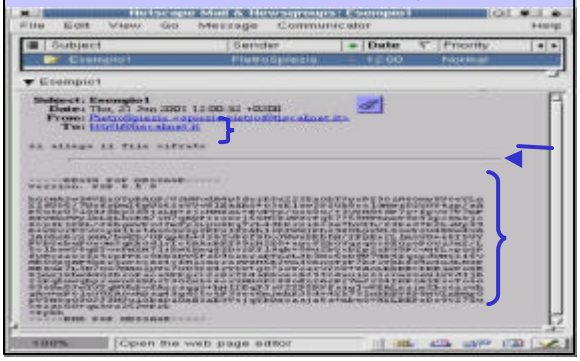
Netscape Messanger: Premessa

- Al fine di permettere al destinatario di poter leggere correttamente il messaggio, occorre:
  - Disattivare qualsiasi opzione propria del Messanger, utilizzando il pulsante “Options”

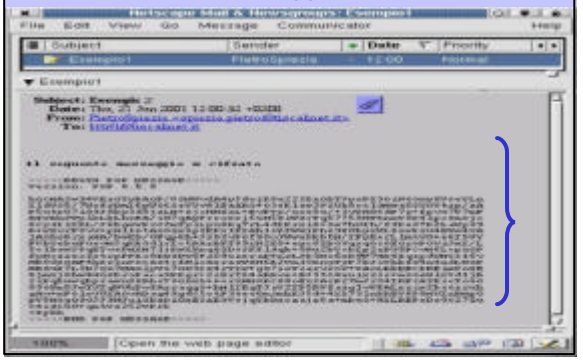
Netscape Messanger: Premessa



NETSCAPE MESSANGER esempio: invio file cifrato in allegato



NETSCAPE MESSANGER esempio: invio messaggio cifrato



LETTURA MESSAGGI

- Ricevuta l’e-mail con messaggi e/o file cifrati, bisogna decifrarli
- Per decifrare occorre, naturalmente, il PGP con la propria chiave privata
- Il Comando per decifrare un file è:
  pgp nome_file_cifrato
- …ottenendo cosi’ il testo in chiaro.

Plugins

- Programmi freeware che integrano il PGP con un programma di gestione e-mail
- Questi programmi, permettono, una gestiome di “posta protetta”, utilizzando soltanto il programma di gestione posta.

NETSCAPE MESSANGER con Plugin

- Non esistono ancora plugin per Messanger per **sistemi Unix-Linux**
- Esiste solo un Plugin per Messanger per **sistemi Windows**

NETSCAPE MESSANGER con Plugin per Windows

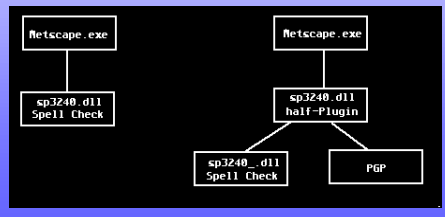
- Si tratta di un **Half-Plugin**:
  - Cifra e firma
  - **NON** Decifra e Verifica

NETSCAPE MESSANGER con Plugin per Windows

- Come Lavora

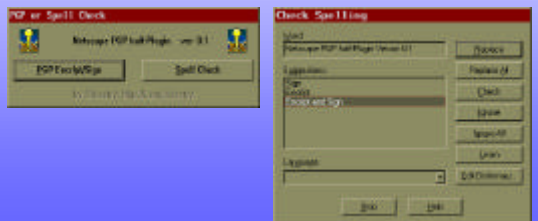
NETSCAPE MESSANGER con Plugin per Windows

- Installazione



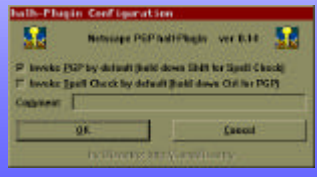
NETSCAPE MESSANGER con Plugin per Windows

- Come si usa



NETSCAPE MESSANGER con Plugin per Windows

- Come si usa



Inizialmente è sembrata una leggenda, ma adesso tutto è più *chiaro*…

Inviare un'e-mail cifrata con Pine

interfaccia non-grafica

…ma conoscendo i comandi, diviene semplice gestire la posta…

Premessa:

occorre creare il file PGP con il comando:

pgp –ea nome_file

l'opzione *–ea* produce un output tale da poter essere copiato in modalità testo

Entriamo in Pine

Il menu principale

come muoversi

quando spediamo un messaggio, le alternative sono:

inserirlo nel body

allegarlo all'e-mail

Quando riceviamo un e-mail

se il messaggio cifrato è nel body dell'e-mail

si salva con nome in un file di testo e si usano i comandi PGP

se è presente un allegato cifrato si usa PGP su questo file

Per rendere l'invio e la ricezione più pratici utilizziamo un plugin

pgp4pine-1.75-6.i386.rpm

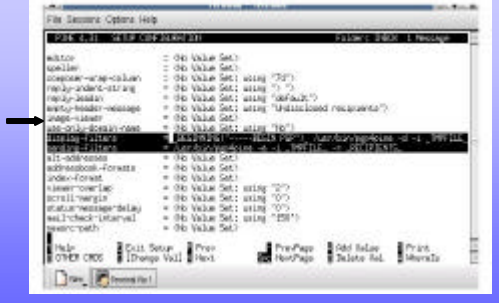
dopo averlo installato, si deve configurare il Pine

dal menu principale

si accede alla configurazione nel setup

nella parte alta

nella parte bassa

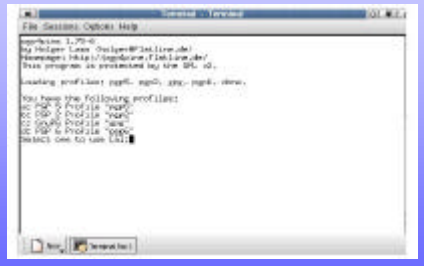


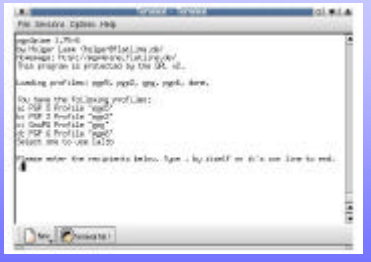
adesso siamo pronti per ricevere e spedire

dal menu principale digitando <**c**> si accede al composer

scelta del plugin installato

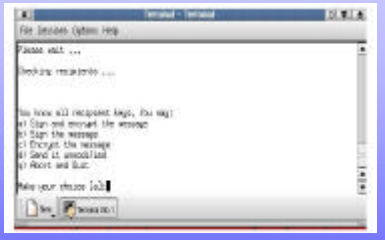
la versione del PGP da usare





indicare il recipient da utilizzare

Vengono visualizzate le chiavi contenute nel file



le opzioni sono funzioni PGP

leggendo la posta

Si seleziona un messaggio e se è stato cifrato

viene chiesta la versione del PGP

la passphrase…

se l'inserimento fallisce…

Messaggio cifrato con poche informazioni aggiuntive

Ma se tutto è andato a buon fine…

…si può continuare con altri messaggi

Non sono stati riscontati "appesantimenti" evidenti del sistema

Il plugin semplifica l'utilizzo del PGP in fase di invio/ricezione e firma dell'e-mail, ma è necessario conoscere i comandi PGP