

# 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

Protezione E-Mail sotto Linux

1

## Introduzione

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

Protezione E-Mail sotto Linux

2

## PGP: cos'è

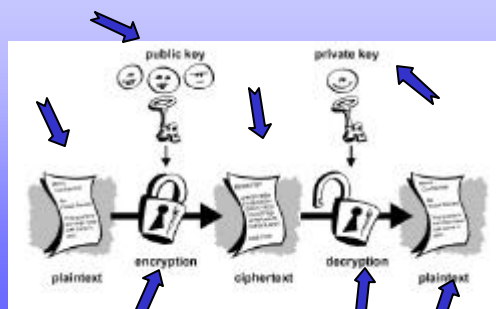
E' un pacchetto freeware che fornisce protezione per la posta elettronica e la memorizzazione di file

Creato da P. Zimmermann nel 1991 e distribuito su Internet

Protezione E-Mail sotto Linux

3

## PGP: Schema funzionale



Protezione E-Mail sotto Linux

4

## 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

Protezione E-Mail sotto Linux

5

## 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

Protezione E-Mail sotto Linux

6

```

Terminal - Terminal
File Session Options Auto
linux:~ # gpg -kg
Pretty Good Privacy(tm) Version 6.5.0
(c) 1999 Network Associates Inc.
Use the PGP(tm) Toolkit, which is copyright PGP Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Choose the public-key algorithm to use with your new key
1) DSS/DH (a.k.a. DSA/EIGamal) (default)
2) RSA
Choose 1 or 2: 2
Pick your RSA key size:
1) 1024 bits- High commercial grade, secure for many years
2) 2048 bits- "Military" grade, secure for foreseeable future
Choose 1, 2, or enter desired number of bits: 1
Generating a 1024-bit RSA key.

You need a user ID for your public key. The desired form for this
user ID is your name, followed by your E-mail address enclosed in
angle brackets, if you have an E-mail address.
For example: John C. Smith <jcsmith@aol.com>
Enter a user ID for your public key: people
  
```

```

Terminal - Terminal
File Session Options Auto

Enter the validity period of your signing key in days from 0 - 10550
0 is forever (the default is 0: 90)

You need a pass phrase to protect your RSA secret key.
Your pass phrase can be any sentence or phrase and may have many
words, spaces, punctuation, or any other printable characters.

Enter pass phrase:
Enter same pass phrase again:
  
```

```

Terminal - Terminal
File Session Options Auto

Note that key generation is a lengthy process.

PGP needs to generate some random data. This is done by measuring
the time intervals between your keystrokes. Please enter some
random text on your keyboard until the indicator reaches 100%.
Press 'D' to cancel.
100% of required data.
Enough, thank you.
.....*****
Make this the default signing key? (Y/n) n

Key generation completed.
linux:~ #
  
```

## 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

Protezione E-Mail sotto Linux 10

## Key-Ring: Visualizzazione

```

Terminal - Terminal
File Session Options Auto
linux:~ # gpg -kv
Pretty Good Privacy(tm) Version 6.5.0
(c) 1999 Network Associates Inc.
Use the PGP(tm) Toolkit, which is copyright PGP Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Type bits   keyID      Date       User ID
RSA 1024    0x897040AD 2001/10/09  expires 2002/01/07
                                people

1 matching key found.
linux:~ #
  
```

## PGP: Protezione chiavi

- I due keyring `secring.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

Protezione E-Mail sotto Linux 12

## 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

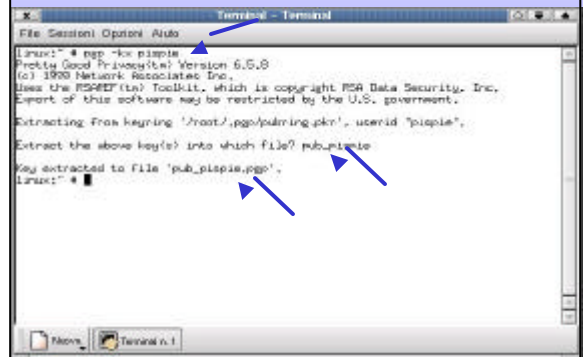
## PGP: Distribuzione delle chiavi

- 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`

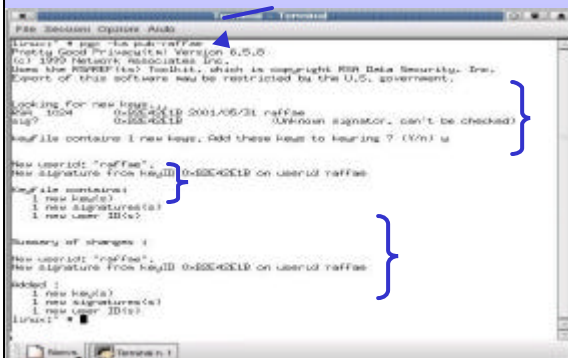
## PGP: Estarre una chiave pubblica



```
Linux:~# pgp -kx pispie
Pretty Good Privacy(tm) Version 6.5.0
(c) 1999 Network Associates, Inc.
Use the PGP(tm) ToolKit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Extracting from keyring '/root/.pgp/pubring.pkr', userid 'pispie',
Extract the above key(s) into which file? pub/pispie
Key extracted to file 'pub_pispie.pgp'.
Linux:~#
```

## PGP: Aggiungere una chiave pubblica



```
Linux:~# pgp -ka pub-raffae
Pretty Good Privacy(tm) Version 6.5.0
(c) 1999 Network Associates, Inc.
Use the PGP(tm) ToolKit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Looking for new keys: id 0 2001/06/31 raffae
Key 1024 0x8542E1B Unknown signator... can't be checked)
Keyfile contains 1 new keys. Add these keys to keyring? (Y/n) y

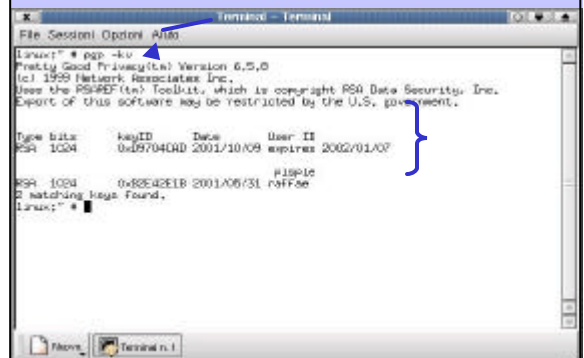
New userid: 'raffae'.
New signature from keyID 0x8542E1B on userid raffae.

Keyfile contains:
  1 new key(s)
  1 new signature(s)
  1 new user ID(s)

Summary of changes:
New userid: 'raffae'.
New signature from keyID 0x8542E1B on userid raffae.

Added:
  1 new key(s)
  1 new signature(s)
  1 new user ID(s)
Linux:~#
```

## PGP: Visualizzare il Key-Ring



```
Linux:~# pgp -kv
Pretty Good Privacy(tm) Version 6.5.0
(c) 1999 Network Associates, Inc.
Use the PGP(tm) ToolKit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

KeyID      Date      User ID
-----
RSA 1024   0x8542E1B 2001/06/31 raffae
RSA 1024   0x8542E1B 2001/06/31 raffae
2 matching keys found.
Linux:~#
```

# 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

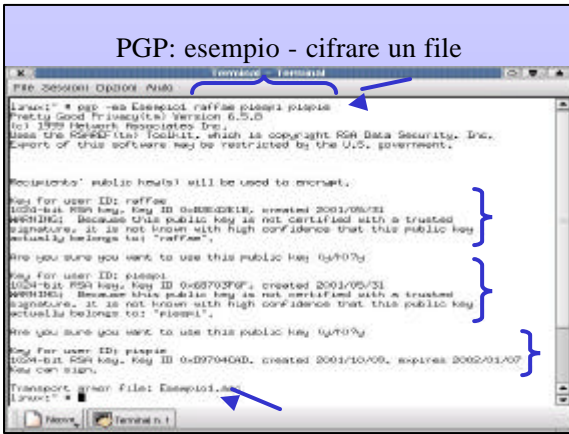
# PGP: un esempio

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 perdersi 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



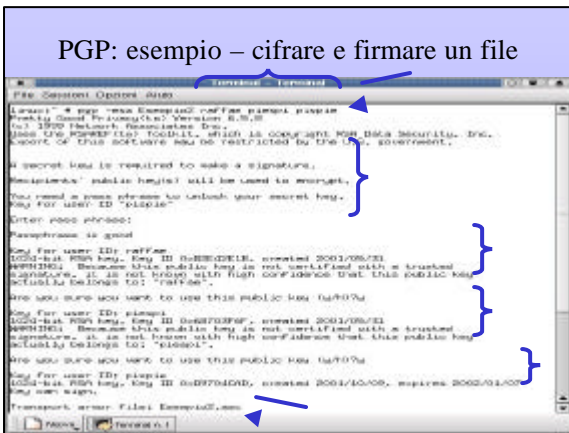
# PGP: esempio - cifrare un file

Comando: `pgp -ea Esempio1 rafae piespi piespi`

(File generato: Esempio1.asc)

```
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5.8
hQMA2w94Yz0YdQpAGP/VSMWd4Y5d0J6L222RzCtTyoPX901Nc0y8V0eYLnX1dV05/7WofcDm
1pWGSa5Vv81EzAQR0+3sk1wZV5th8cclQmwa0ZU0VtZp/aP5uty071893jy3d8jz1M+5j3CHZ
zL+bVfVv/uo8Q0/+3v7B8d4r7+fp0777PFA1wdaWj1bLkLhBA/ah7qyFaeocxj6H5Z1Wz8Tq
67759t8mFMX1pccm3j6cY11IKL/G6b9wPcTmFyLyu08g7e441Kx61e587H0U12/2P4e07
KZL4g3R8+nv0/P0dHSH11gA0Q0c8Pz0e1E1M1KXWJHJh3z83byH6Lz6kQF48w4D1J3Ghu6
rxzHA/bwED/0Fp6h+3S82V0G80cJW6dKbtM/1P5ePrlm0U0+e615VfVb0eV0eVtqKd1a
1ctRAeKCT09+M2E0+ey82b0U9e9G8Qz0P0U1mM/L5c1hwV6qF7v8PM0M1jKwXwzf2DSSK1L
dgs-0Dz12y0b1Z2B0PFW6LcpQ0F4Yc2a0G1p1PFI08M1D6ePa09xaxaEDT7eLTD3M6x09W
7Hx41zppdM0a16W8K0X0AP4X8+smV0C234cFHLz2z2zW2682Vn10Xnu7y7b1VbH24n4nJ3
QPNBzL7L3D7Qc7M4U1V97U0134zY1+q07aoVovr20wVAoLR8REIRE1mVoX6Jm36h4H0G
bsoPac9F9g+2dE1K48Rv+8J31dXulx28+mqeM1XW1J21Pqbwppgrwms8R8r13QQd+
Cz0uW0C8802A827a1Z4E8P1k0t0001K86+3vT1E0fDyV4zrsg0+1M11E2TAV1P
RV4qg1VVE1x2i12bz0rhu9Av+mG1E00X0A0Adg49g3c0tF3q0e6mhkH5d+4XD731hRRV6
PBM1nBmp0pVtM990AJ9H1u1ObzD10x8S2E0VeJgYbDcczaJz6a+mbu0+XNLEBFA80272uc4e2
Cub+gntV2Z5V2P+TqH
-----END PGP MESSAGE-----
```

# PGP: esempio - cifrare e firmare un file



# PGP: esempio - cifrare e firmare un file

Comando: `pgp -esa Esempio2 rafae piespi piespi`

(File generato: Esempio2.asc)

```
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5.8
hQMA2w94Yz0YdQpAGP/VSMWd4Y5d0J6L222RzCtTyoPX901Nc0y8V0eYLnX1dV05/7WofcDm
1pWGSa5Vv81EzAQR0+3sk1wZV5th8cclQmwa0ZU0VtZp/aP5uty071893jy3d8jz1M+5j3CHZ
zL+bVfVv/uo8Q0/+3v7B8d4r7+fp0777PFA1wdaWj1bLkLhBA/ah7qyFaeocxj6H5Z1Wz8Tq
67759t8mFMX1pccm3j6cY11IKL/G6b9wPcTmFyLyu08g7e441Kx61e587H0U12/2P4e07
KZL4g3R8+nv0/P0dHSH11gA0Q0c8Pz0e1E1M1KXWJHJh3z83byH6Lz6kQF48w4D1J3Ghu6
rxzHA/bwED/0Fp6h+3S82V0G80cJW6dKbtM/1P5ePrlm0U0+e615VfVb0eV0eVtqKd1a
1ctRAeKCT09+M2E0+ey82b0U9e9G8Qz0P0U1mM/L5c1hwV6qF7v8PM0M1jKwXwzf2DSSK1L
dgs-0Dz12y0b1Z2B0PFW6LcpQ0F4Yc2a0G1p1PFI08M1D6ePa09xaxaEDT7eLTD3M6x09W
7Hx41zppdM0a16W8K0X0AP4X8+smV0C234cFHLz2z2zW2682Vn10Xnu7y7b1VbH24n4nJ3
QPNBzL7L3D7Qc7M4U1V97U0134zY1+q07aoVovr20wVAoLR8REIRE1mVoX6Jm36h4H0G
bsoPac9F9g+2dE1K48Rv+8J31dXulx28+mqeM1XW1J21Pqbwppgrwms8R8r13QQd+
Cz0uW0C8802A827a1Z4E8P1k0t0001K86+3vT1E0fDyV4zrsg0+1M11E2TAV1P
RV4qg1VVE1x2i12bz0rhu9Av+mG1E00X0A0Adg49g3c0tF3q0e6mhkH5d+4XD731hRRV6
PBM1nBmp0pVtM990AJ9H1u1ObzD10x8S2E0VeJgYbDcczaJz6a+mbu0+XNLEBFA80272uc4e2
Cub+gntV2Z5V2P+TqH
-----END PGP MESSAGE-----
```

## PGP: esempio - firma di testo in chiaro

```

Terminal - Terminal
File Sessioni Opzioni Aiuto
Linux:~ # pgp -sa Esempio3
Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates Inc.
Uses the RSA#REF(ta) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

A secret key is required to make a signature.
You need a pass phrase to unlock your secret key.
Key for user ID "piespie"
}
Enter pass phrase:
Passphrase is good
Transport error file: Esempio3.asc
Linux:~ #
    
```

## PGP: esempio - firma di testo in chiaro

Comando: `pgp -sa Esempio3raffae piespie`

(File generato: `Esempio3asc`)

```

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5.8
oW1kxstFE8QxjGQRQe8+A/YhOaEaPMY18jBA2LRwshYfpDNT0yp6R7MchGkHLLIdgEFFPkQ
eC4EXFBC85VFPyGDT1HkCQ0Wj2Lr+7qg9+9VXPM5262MDU5dUqIGrVDR24695f64787TE
461W970X06d+3c0b2j4818/c0u4H2sk3+4f0/r3+H13MEF3acDm/g3j5f61z08910/0gq
8VvcN46/fb0c20s9X+Xul9un56d3u0z+VlvzeeDy9MaaOdvT42dz194ub6y2n61zh7LX08vN8
M+P1Pq37397vfh9y/XU7KULW5U219pVboe1Day1ShwQcmDyJGKN+EU+8KE11IKT1oN2mPM1ofn
801aDdIKU0UFTFPg88Qc0aDME1008781ixQaMIMpFsdTc0y8B9K8A5a0Q6877AllyC5Iam
1ia1I1Gcy72801az0vAw1BstD1hntLGE5MTT0wS9gR2k0haTD1HkM+qw6M7BGB1wksHmQ
Qd8RS8rko2SBK0d0hhYK1UVapQ+XS0BjhnPQ153LomIUFcr500TKUPCaZLD2640wyeqavMhHj
hoY0outyM1Bn+34k1420rKYLQmPls12K1W82SLcuungFahP7D9dyo1EM1pb49noe4746Y8pQe8
h8o7v0wv8S85u11p504+VR1ndv48baS80182700q4LAVKkynoY0w0281v1r5a257ev47Pe
nQw3hge1EKy68Gt/5hWwZEPFD0=chK3
-----END PGP MESSAGE-----
    
```

## PGP: esempio - decifrare un file

Comando: `pgp "nomefile.txt"`

(File generato: "nomefile")

```

Terminal - Terminal
File Sessioni Opzioni Aiuto
Linux:~ # pgp Esempio3.asc
Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates Inc.
Uses the RSA#REF(ta) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

File is signed. Good signature from user "piespie".
Signature made 2001/10/19 16:03 GMT
}
Plaintext filename: Esempio3
Linux:~ #
    
```

## PGP: Revoca di una chiave

```

Terminal - Terminal
File Sessioni Opzioni Aiuto
Linux:~ # pgp -hr raffae
Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates Inc.
Uses the RSA#REF(ta) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Key for user ID: raffae
1024-bit RSA key, Key ID 0x8E42E1B, created 2001/05/31
}
Are you sure you want this key removed (y/N)? y
Key removed from key ring.
Linux:~ #
    
```

## PGP: Visualizzare il Key-Ring

```

Terminal - Terminal
File Sessioni Opzioni Aiuto
Linux:~ # pgp -kv
Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates Inc.
Uses the RSA#REF(ta) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Type bits      keyID      Date      User ID
-----
RSA 1024      0x29704CRD 2001/10/09  piespie 2002/01/07
}

1 matching key found.
Linux:~ #
    
```

## 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

```

File Sessions Options Audo
Terminal - Terminal
Linux:~# pgp -kc raffae
Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates, Inc.
Uses the RSPREF(tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

A secret key is required to make a signature.
You specified no user ID to select your secret key.
Using default signing key if set, otherwise the default user ID
and key will be the most recently added key on your secret keyring.

Key for user ID: raffae
1024-bit RSA key, key ID 0x8E42E1B, created 2001/05/31
Key fingerprint = 3D 52 5C 2B 2A 47 92 72 42 0C 26 0F 91 21 8F 93

PGP CAREFULLY: Based on your own direct first-hand knowledge, are
you absolutely certain that you are prepared to solemnly certify that
the above public key actually belongs to the user specified by the
above user ID (y/n)? y

You need a pass phrase to unlock your secret key.
Key for user ID: raffae
Enter pass phrase:
Passphrase is good

Attach a regular compression to this signature, or
press enter for none:
Linux:~#
    
```

## PGP: Controllo di un certificato

```

File Sessions Options Audo
Terminal - Terminal
Linux:~# pgp -kc raffae
Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates, Inc.
Uses the RSPREF(tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Key ring: '/root/.pgp/pubring.pkr'
Type bits  keyID      Date      User ID
RSA 1024   0x8E42E1B 2001/05/31 raffae
sig!      0x8E42E1B           raffae
sig!      0x87040AD           pipole
1 matching key found.

KeyID      Trust  Validity User ID
0x8E42E1B  untrusted complete raffae
untrusted complete raffae
ultimate         pipole
Linux:~#
    
```

## PGP: Controllo di tutti i certificati

```

File Sessions Options Audo
Terminal - Terminal
Linux:~# pgp -kc
Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates, Inc.
Uses the RSPREF(tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Key ring: '/root/.pgp/pubring.pkr'
Type bits  keyID      Date      User ID
RSA 1024   0x8E42E1B 2001/05/31 pipole
sig!      0x8E42E1B           pipole
sig!      0x87040AD 2001/10/09 expires 2002/01/07
RSA 1024   0x8E42E1B 2001/05/31 raffae
sig!      0x8E42E1B           raffae
sig!      0x87040AD           pipole
3 matching keys found.

KeyID      Trust  Validity User ID
0x8E42E1B  untrusted invalid pipole
untrusted complete pipole
0x8E42E1B  untrusted complete raffae
untrusted complete raffae
ultimate         pipole
0x87040AD  ultimate complete pipole
Linux:~#
    
```

## PGP: Revoca di un certificato

```

File Sessions Options Audo
Terminal - Terminal
Linux:~# pgp -krc raffae
Pretty Good Privacy(tm) Version 6.5.8
(c) 1999 Network Associates, Inc.
Uses the RSPREF(tm) Toolkit, which is copyright RSA Data Security, Inc.
Export of this software may be restricted by the U.S. government.

Removing signatures from userid 'raffae' in key ring: '/root/.pgp/pubring.pkr'

Key for user ID: raffae
1024-bit RSA key, key ID 0x8E42E1B, created 2001/05/31
Key has 2 signature(s):

Signatures for userid raffae:
sig      0x8E42E1B           raffae
Remove this signature (y/n)? y
sig      0x87040AD           pipole
Remove this signature (y/n)? y

2 key signature(s) removed.
Linux:~#
    
```

## Gestione e-mail

- Elm
- Netscape Messenger
- 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...

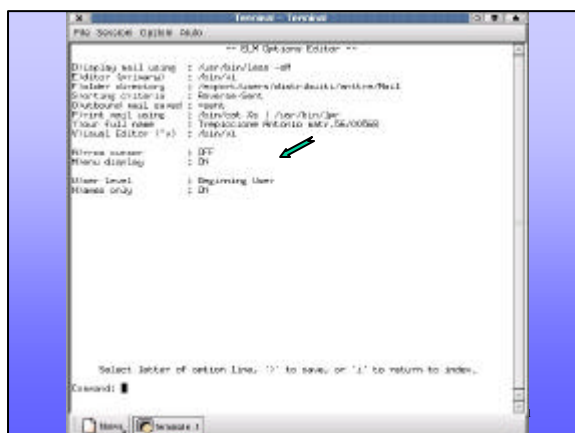
...dobbiamo diventare **ESPERTI !?!**

## 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

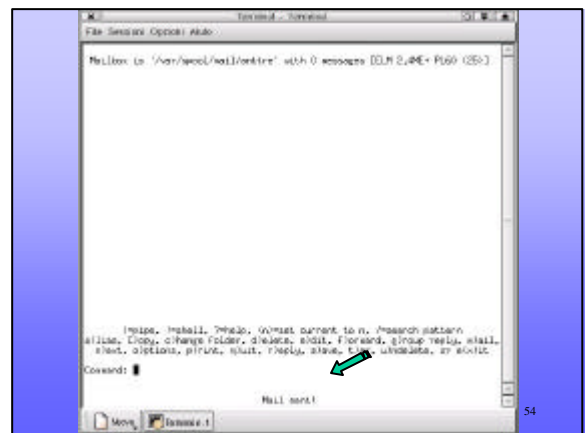
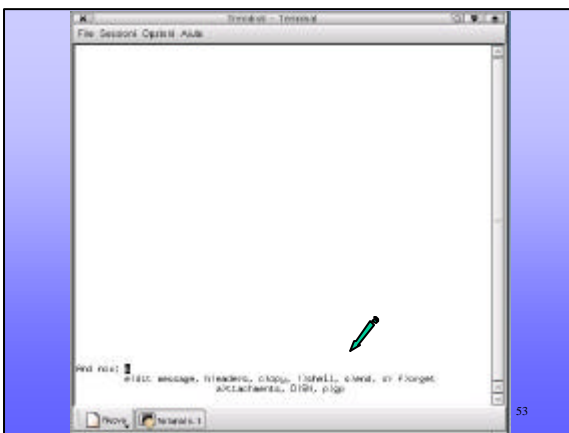
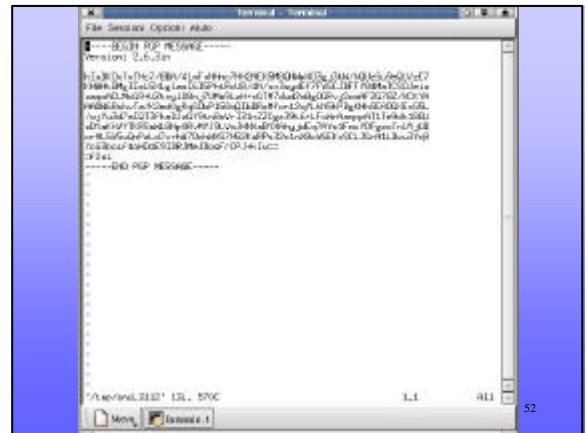
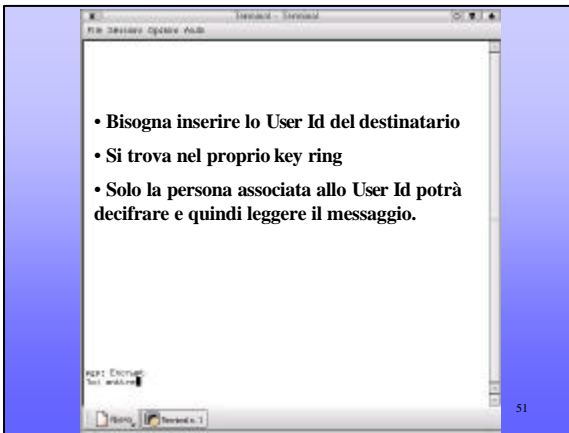
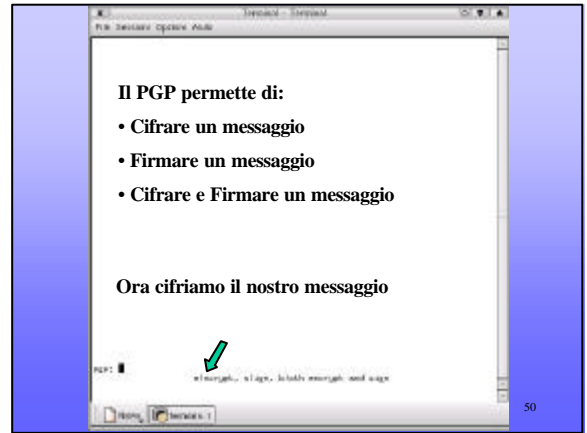
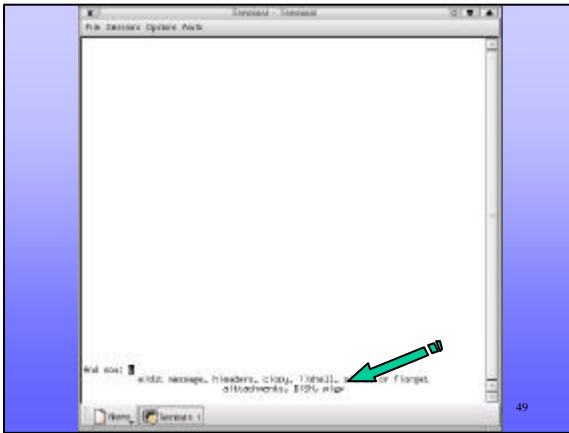
**E allora ?**

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



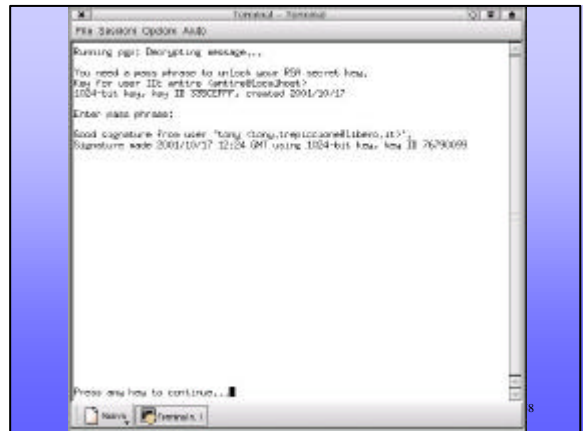
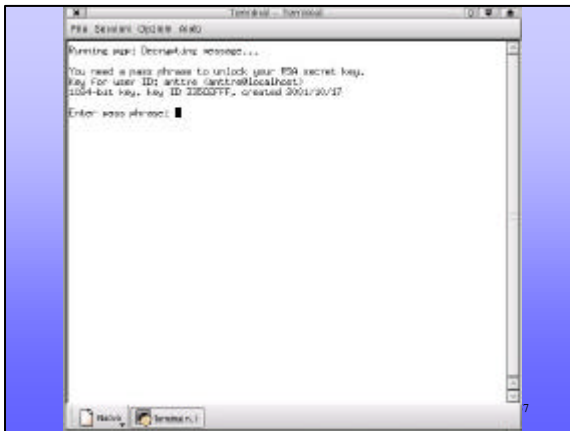
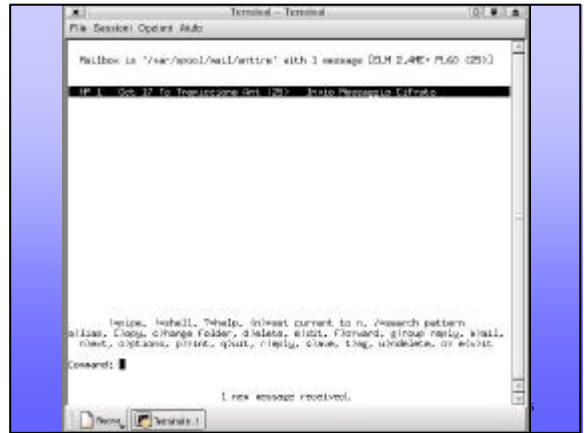
**Fissarlo a EXPERT .....**





## Ricezione di un messaggio CIFRATO

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



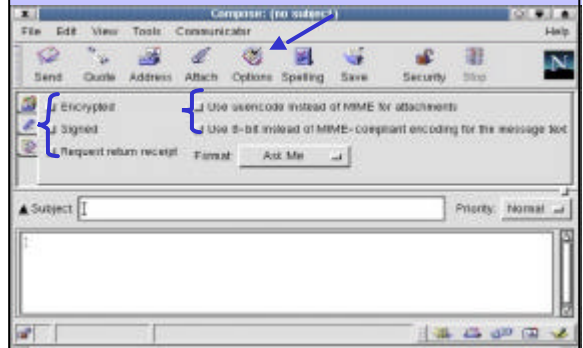
## Netscape Messenger

- Messaggio cifrato in allegato
- Messaggio cifrato

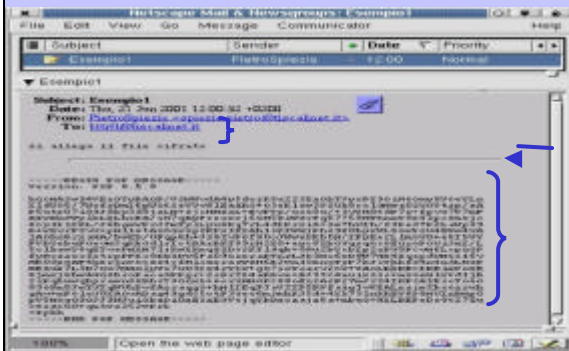
## Netscape Messenger: Premessa

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

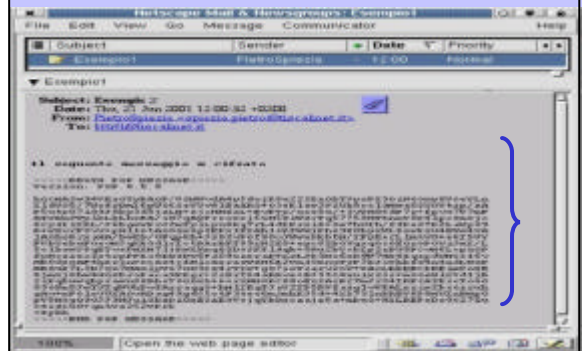
## Netscape Messenger: Premessa



## 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 così il testo in chiaro.

## Plugins

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

## NETSCAPE MESSANGER con Plugin

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

## NETSCAPE MESSANGER con Plugin per Windows

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

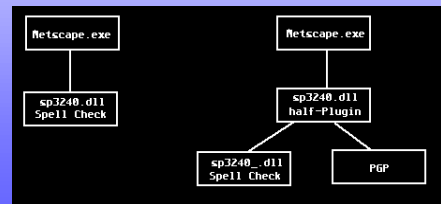
## NETSCAPE MESSANGER con Plugin per Windows

- Come Lavora



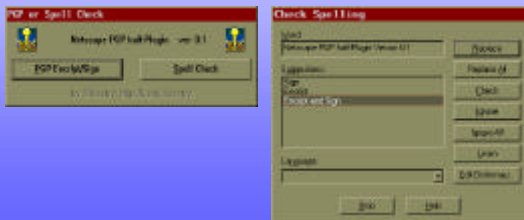
## NETSCAPE MESSANGER con Plugin per Windows

- 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:

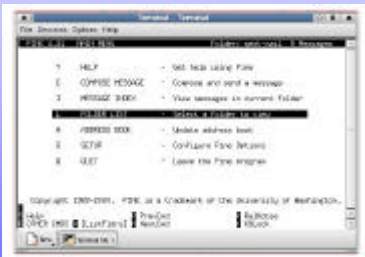
occorre creare il file PGP con il comando:

```
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:

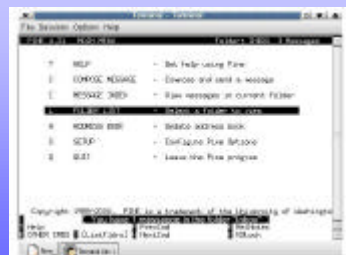


inserirlo nel body



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

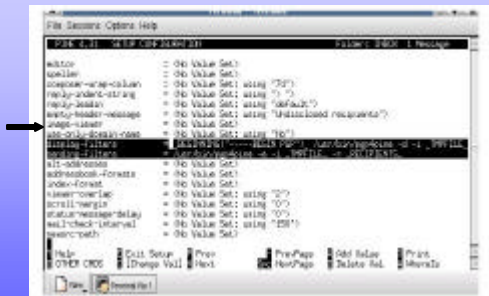


si accede alla configurazione nel setup



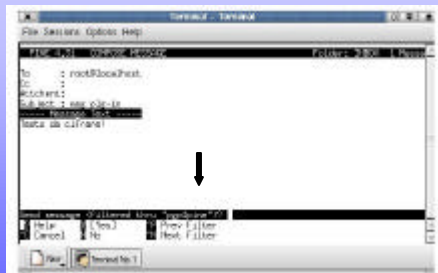
nella parte alta

nella parte bassa



adesso siamo pronti per ricevere e spedire

dal menu principale digitando <c> si accede al composer



sceita del plugin installato



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 riscontrati "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