Esercitazione su PGP

Loris Tissino

Indice

1 Esercitazione su PGP

1.1 Introduzione

La crittografia è uno degli aspetti più importanti della sicurezza e della tutela della privacy nelle comunicazioni moderne. Questo documento ha lo scopo di illustrare come usare un software molto diffuso, PGP, nella versione 6.5.8 per Windows (reperibile all'indirizzo www.pgpi.com).

Nota importante. Il documento è pensato come supporto ad una esercitazione svolta in laboratorio con l'aiuto di un docente. Per questo motivo è previsto l'azzeramento di tutte le chiavi registrate precedentemente. Il passaggio si potrà eventualmente saltare se ritenuto superfluo.

1.2 Installazione di PGP

Non fa parte dell'esercitazione. Si assume che il software sia già correttamente installato. Controllare che nella barra delle applicazioni (normalmente in basso a destra) compaia l'icona del programma in esecuzione.

1.3 Rimozione delle chiavi esistenti

Per poter avere una situazione comune in laboratorio, rimuoviamo tutte le chiavi presenti nel nostro portachiavi.

1. Cliccare sull'icona di PGP (vista sopra) e scegliere la voce ***PGPkeys***
2. Selezionare tutte le chiavi presenti (***Edit*** / ***Select All***)
3. Cancellare le chiavi selezionate (***Edit*** / ***Delete***)
4. Al messaggio di richiesta di conferma (*Are you sure you want to delete this key?*) rispondere *Yes to All*

1.4 Generazione di una nuova coppia di chiavi

Generiamo la nostra coppia di chiavi (chiave pubblica e chiave privata), sempre utilizzando PGPkeys.

1. Iniziare la procedura di generazione della coppia di chiavi (***Keys*** / ***New key...***)
2. Nell'apposita finestra di dialogo, indicare il nome completo (*Full name*) e il proprio indirizzo di posta elettronica (*Email address*); cliccare su *Avanti*
3. Scegliere la generazione di una chiave di tipo *Diffie−Hellman/DSS*; cliccare su *Avanti*
4. Scegliere la dimensione della chiave (2048 bits); cliccare su *Avanti*
5. Indicare che non si desidera una scadenza per la chiave (*Key never expires*); cliccare su *Avanti*
6. Scrivere (due volte, nelle due caselle di testo apposite) una "passphrase", ossia una frase segreta che ci dovremo ricordare (volendo, si può decidere di mostrare ciò che si sta scrivendo, deselezionando la casella *Hide typing*); cliccare su *Avanti*
7. PGP genera la coppia di chiavi; al termine cliccare su *Avanti*
8. Visto che non dobbiamo pubblicare la nostra chiave pubblica su Internet, deselezionare la voce *Send my key to the root server now*; al termine cliccare su *Avanti*
9. Cliccare su *Fine*

Dovrebbe comparire la nostra coppia di chiavi nella finestra.

1.5 Firma digitale di un documento

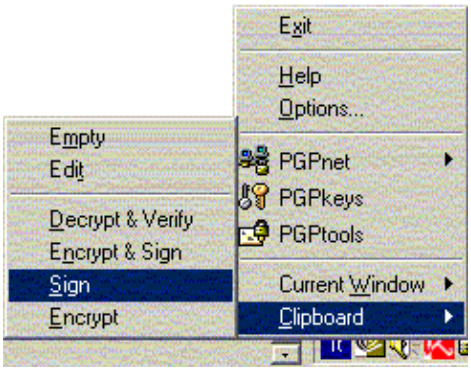
Esistono molti modi per firmare un documento (direttamente da un programma per cui funziona il modulo PGP, attraverso gli appunti, con PGPtools, oppure cliccando con il pulsante destro del mouse su di un documento). In questa esercitazione ne vedremo, per semplicità, solo uno, quello basato sugli appunti.

1. Con un semplice programma di videoscrittura (va benissimo il *Blocco note*) scrivere un testo che si vuole firmare. Ad esempio:

```
Testo che voglio firmare.
Voglio che tutto il mondo sia sicuro
che l'autore di questo documento
sono proprio io.

                    Loris Tissino
```

2. Selezionare l'intero testo e copiarlo negli appunti (***Modifica*** / ***Seleziona tutto*** e ***Modifica*** / ***Copia***)
3. Cliccare sull'icona di PGP e scegliere la voce ***Clipboard*** / ***Sign***



4. Inserire nella finestra di dialogo che appare la *passphrase* associata alla chiave che utilizziamo per firmare, e poi cliccare su *Ok*
5. A questo punto, il contenuto degli appunti è stato firmato digitalmente. Tornare al *Blocco note* e incollare il testo ottenuto. Si dovrebbe ottenere qualcosa di simile a questo:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Testo che voglio firmare.
Voglio che tutto il mondo sia sicuro
che l'autore di questo documento
sono proprio io.

                    Loris Tissino

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>

iQA/AwUBPeDNdnVyeS6y6zGjEQK0nACg23ZhHks+l2kH2lvDBVYH49F7d0oAoJor
gNJzcodM22x/lLBL7XJAXCGz
=uIML
-----END PGP SIGNATURE-----
```

1.6 Esportazione della chiave pubblica

Pubblicare la nostra chiave è essenziale per dare la possibilità a qualcun altro di verificare l'origine del messaggio firmato digitalmente da noi.

1. Da ***PGPkeys***, selezionare la chiave ed esportarla (***Keys*** / ***Export***)
2. Nella finestra di dialogo che appare, scegliere in che file esportare la chiave. Salvare il file, che avrà una forma simile alla seguente:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>

mQGiBD3gxUIRBADqcw4VZE0nGqawcqpHGGodJyu9N7x6QyzMdM1O3RODe1QuvtaG
kgOChh2cuyIjDxeTdp7NuFbEtA7MZmI1jjNfEqJd2DZUj/hnub5oR6EugpogbPv2
IHr+5GyuTj3EgcIUMDsjbL72kWlM5fGBLxWlbxHRoCt000LD7LobRj4BgwCg/67R
ntd0AQmYb8ovby6hqw5QVo8D+wfkt3AwazbZ5WQKW3/oMAth4s2SJc86eYilWQFs
x1XLYhxvRSSxGZcyEOYNVdalcBiYJHkSS57L9QL44aRYSvfYTOp6QCi6BA6FXDw+
3DzGaSPYMiHf31OkXC7BhC8r+h7sTosgtJGuM2ieSi9bSZS1BHgh1WmzWxWrcWpc
kdAWA/4xNO5fs+jma7drqt+ztP+uP90u6YfgoPq3P/cR0fBdoaIbloHWdB7wfCgO
dh/9H6YPr+1RQDmFYmgCSpoHmC5JCteHwXP1qQYmL0+7LHaDL+mEnFPrJgwlByo5
uIznmSu92R48uQovM7doZclwgP/rVGRKDBs1wda9FdKDOB29mrQgTG9yaXMgVGlz
c2lubyA8bG9yaXNAdGlzc2luby5pdD6JAE4EEBECAA4FAj3gxUIECwMCAQIZAQAK
CRB1cnkususxoysyAKC+78IjmIvk8DFUrAw8J8SQqkmNRQCgogDkwzvjYzSHZWtl
X53vJqfWbD+5Ag0EPeDFQhAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65Szgg
2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09jdvO
meFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brwv0YA
WCvl9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiNjrtV
jLhdONM0/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrKlQzZ
lp+r0ApQmwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIIAK97HnNanRn2
+cFBVWUsSx5rtZ7tg4k7GIoyE0kHBsbYpmmrr1gBLPlgXqnhhahzUIp7GtbOE076
3hH/s8LbHwaf+xcQfguXf+HhWfW+EC6Dmy6lDOZ/58Sc4bYGmv0Cnemj7zyZj9rX
Trkvvl9Bmd1AFzREzMQPgpLCIO/w4B1iN5x2XSgZ4vgVeugKR7sohXxDSyE8xDee
+bOsviwTemo9gIYL+p1hv91GhEeVHTXh4xMM41eBIpN/9eguAZEF1YfW11A5fCV/
2EVLqPtyVuXONZoE63nGPG1pZ9xQMwzX5fz8Fx82CLcj3tqZYDH9kRhg84hOCzRb
xltN7+jl/5WJAEYEGBECAAYFAj3gxUIACgkQdXJ5LrLrMaPxCACcCnDxCzN6Rrtr
opgPZtb3bAV2TDkAoILIJl+4eOTxgDX1mtBrg7CLUwlK
=4YkC
-----END PGP PUBLIC KEY BLOCK-----
```

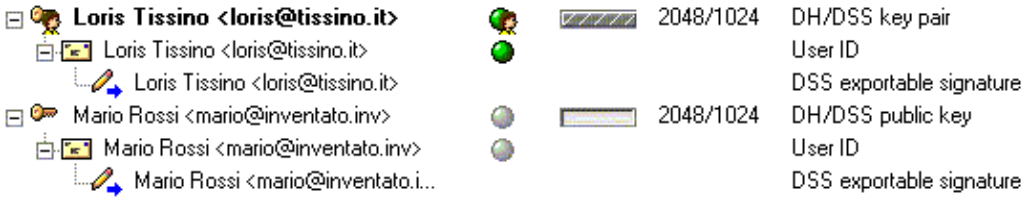
3. Si potrebbe pubblicare questo file in molti modi (ad esempio, nel nostro sito web, oppure in un apposito *keyserver*). Ai fini di questa esercitazione, inviaro semplicemente via posta elettronica ai propri corrispondenti.

1.7 Importazione nel portachiavi di chiavi pubbliche di altri

Supponiamo che qualcuno ci abbia inviato un file contenente la sua chiave pubblica, esportara come mostrato nel punto precedente.

Per importarla nel nostro portachiavi:

1. fare un doppio click sul file corrispondente
2. cliccare sul pulsante *Import*
3. verificare che il portachiavi contenga quindi la chiave pubblica importata



1.8 Verifica della firma digitale di un documento

Immaginiamo a questo punto di ricevere un documento firmato digitalmente, come ad esempio il seguente:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Questo è un messaggio firmato
digitalmente da me, Mario Rossi.

Voglio che tutti siano sicuri che
sia stato scritto proprio da me.

               Mario Rossi

-----BEGIN PGP SIGNATURE-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>

iQA/AwUBPeDUyDWxq3zxdhTkEQKCCACg7WYPzi4zyvRrGpjPt90j2v4ri88An0IE
Rgv8feWQAL9xfWzPyLt0IRKq
=CMJR
-----END PGP SIGNATURE-----
```

Vogliamo essere sicuri che la firma corrisponda alla chiave pubblica in nostro possesso (nel senso che l'abbiamo importata nel nostro portachiavi).

1. Selezionare il testo e copiarlo negli appunti (***Modifica*** / ***Seleziona tutto*** e ***Modifica*** / ***Copia***)
2. Dall'icona di PGP, selezionare la voce ***Clipboard*** / ***Decrypt & Verify***
3. Controllare l'esito della verifica. Se è positivo, dovremmo vedere un messaggio analogo al seguente:

   ```
   *** PGP Signature Status: good
   *** Signer: Mario Rossi <mario@inventato.inv>
   *** Signed: 24/11/2002 15.31.51
   *** Verified: 24/11/2002 15.39.30
   *** BEGIN PGP VERIFIED MESSAGE ***

   Questo è un messaggio firmato
   digitalmente da me, Mario Rossi.

   Voglio che tutti siano sicuri che
   sia stato scritto proprio da me.

                  Mario Rossi


   *** END PGP VERIFIED MESSAGE ***
   ```

   Altrimenti, otterremmo:

   ```
   *** PGP Signature Status: bad
   *** Signer: Mario Rossi <mario@inventato.inv>
   *** Signed: 24/11/2002 15.31.51
   *** Verified: 24/11/2002 15.43.52
   ```

```
*** BEGIN PGP VERIFIED MESSAGE ***

Questo è un messaggio firmato
digitalmente da me, Mario Rossi.

Voglio che tutti siano sicuri che
sia stato scritto proprio da me.

(Ma il messaggio è stato contraffatto
da un maligno che ha introdotto questa
nota)

                Mario Rossi


*** END PGP VERIFIED MESSAGE ***
```

1.9 Invio di un messaggio cifrato

Un'esigenza diversa potrebbe essere quella di inviare un messaggio ad un nostro corrispondente cifrandolo in maniera tale da renderlo illeggibile a chiunque altro (compresi noi stessi). Procediamo così:

1. Con il *Blocco note*, scrivere il messaggio:

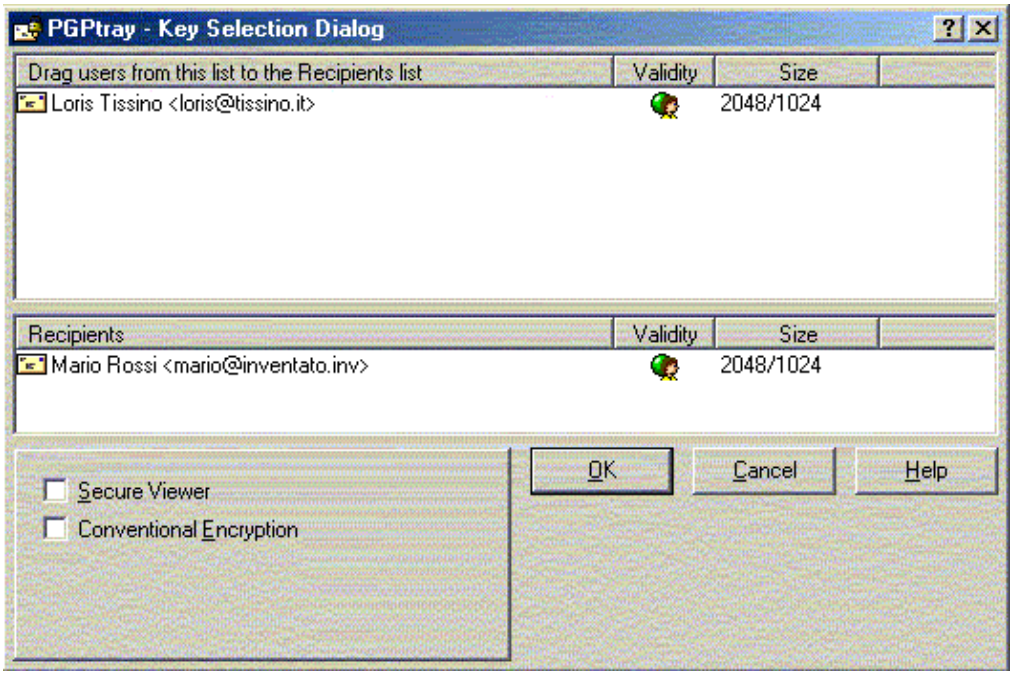
   ```
   Messaggio riservato per Mario Rossi

   Caro Mario, ti invio questo messaggio con la speranza che,
   grazie alla cifratura offerta dal programma PGP, solo tu
   possa leggerlo. Userò la chiave pubblica che mi hai inviato
   per cifrarlo.

   Ciao

                           Loris Tissino
   ```

2. Selezionare il testo, copiarlo, e poi dall'icona di PGP scegliere la voce ***Clipboard*** / ***Encrypt***
3. Nella finestra di dialogo che appare, trascinare la chiave del destinatario legittimo del nostro messaggio nella parte inferiore:



4. Cliccare sul pulsante *Ok*
5. A questo punto negli appunti c'è il messaggio cifrato:

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>

qANQR1DBwU4DoIsJLsFeUtMQCADrBlbGl0yuqF9Uz+D55AmFvRM/W9+LeX1e1ery
y9Ip1VEETZET/0BTZEb+HLtUJJvwdP1NWoHEimA32IjTolgVEkMchit9CPn3N3yb
GyvLq3li5sR7i1w79iP/Az/mpR3Sx23y+3RfB8q3aivIzDaFeGeFRkWWrpeZYovK
WC/iWtNyUSY/a+DiO3CpHQlxeYbRIa7DY6O2TgwcuZ4Knb/MssGqpPMMCHEgMW6h
a+MtsUrb1RjEWfB8+0DoFiEQdqsSPpgTOMOHe+47vjN/MSHMcnRScXkexXjLejYr
SUOP9izmYXPFbCr2cYW+xP767EI/txKzKqMubN05KwDb8CYQCAD018sPLx7AhZ37
H/JqNU11AVMIFqNb/st86bqGvPkqT1Io+vLRN1ziOLVYuLVH+Qj262m7jt88CTi/
kp73lzz2V0/O90jYuTkExS32W01PENjgKAW55wH+HPN9YQiKoGz6OthAkeRBl4v1
XlRvL8r1ciU6cuRvOGXhLW8br4edU95eDPc7jHJM+Sgfus9mLmkTGfWgMdnI014+
hioi14ew1DmRL4AXp5Cui8iRaoamz25H2WzJOoRk9zCRWbCIFzohnT9y6xNHKh0d
Ern/VsXtoB+Yud2RO3O+Wo4NAofqhyN8fRYYwu6u2S6tLhdoILsBW2N+0CtNBaCY
Uveo9CGHycAUibpu7KxdCiPJszojeHLLVXW34ZT9s+UUS0oD0kpm/Pk+qe3r3IYY
NVqiwXk1JhSiVIg3RQc3KTfPTKzRtqoQxCmckBwf/7gbmUZuqllN+XMM+g2xGtZ+
ZfDnb/Qu29wZCVE7cn6kaO0TpvCjsHvWAtEMs3+qDtnc2efert2ZwiRiNQ0ayL0J
WPaByYV+eJYfVOH5mXqDL5OflXgAYijtXrp/20SQ4T6tg//bdC0s3wW4r67LevSM
BT+SAk6eyZ4O7KcjAj1f5yEQfdkiLvDQ0NKBZA0=
=jfhm
-----END PGP MESSAGE-----
```

1.10 Lettura di un messaggio cifrato

Supponiamo di ricevere un messaggio cifrato, e di essere i legittimi destinatari. Per leggerlo:

1. Selezionare il messaggio e copiarlo negli appunti
2. Scegliere la voce ***Clipboard*** / ***Decrypt & Verify*** di PGP
3. Viene chiesta la *passphrase* corrispondente alla nostra chiave privata. Digitarla correttamente per vedere il contenuto del messaggio.

1.11 Altre funzionalità

Con PGP si possono fare anche altre cose, che dovrebbero risultare abbastanza facili se si sono capiti i punti precedenti:

- Firmare e cifrare un messaggio in un'unica operazione
- Cifrare un messaggio con più destinatari
- Cifrare / firmare il contenuto della finestra corrente (anziché degli appunti)
- Cifrare / firmare un file arbitrario o il contenuto di una cartella
- Firmare una chiave pubblica, garantendone l'autenticità
- Utilizzare PGP come modulo aggiuntivo per altri programmi
- ...

Si noti che i concetti qui esposti saranno utili anche nel caso di uso di altri programmi, come ad esempio GPG (GNU Privacy Guard). L'interfaccia è una cosa, le funzionalità un'altra.

A cura di Loris Tissino

L'autore spera che queste note possano essere utili pur nella loro essenzialità. Chi dovesse riscontrarvi delle inesattezze o volesse suggerire delle integrazioni, può scrivere un messaggio di posta elettronica (*loris@tissino.it*). (Attenzione: messaggi in formato HTML o con allegati vengono direttamente cestinati dal filtro di posta)

Questo documento dovrebbe essere rintracciabile all'indirizzo http://www.tissino.it/docs/