

PGP

Nel giugno 1991 lo statunitense **Philip Zimmermann** realizza e distribuisce gratuitamente il programma PRETTY GOOD PRIVACY (PGP), un programma di crittografia diventato ormai uno standard (tanto che l'insegnamento del suo utilizzo è previsto nel Master per la Security al Politecnico di Milano), che permette di mantenere la privacy e la sicurezza dei propri dati personali in formato elettronico.

L'autore, che si è dato molto da fare per consentire a tutti di comunicare in modo sicuro, nel manuale d'uso del suo programma spiega perché è importante usare la crittografia: «Che accadrebbe se tutti pensassero che i cittadini onesti usano solo cartoline per la loro posta? Se qualche persona per bene volesse usare una busta chiusa per proteggere la sua privacy, desterebbe dei grossi sospetti. Forse le autorità aprirebbero la sua posta per controllare cosa nasconde. Fortunatamente non viviamo in un mondo fatto così, perché tutti proteggono la maggior parte della loro posta chiudendola in una busta. Sarebbe bello se tutti usassero abitualmente la crittografia per la loro posta elettronica, indipendentemente dal contenuto più o meno riservato, e in tal modo nessuno desterebbe sospetti».

Per la realizzazione di PGP, Zimmermann viene citato in tribunale dalla *RSA Data Security Inc.* per violazione del brevetto sull'algoritmo *RSA*, e accusato dal governo degli Stati Uniti di esportazione illegale di strumenti crittografici. Entrambe le cause finiscono nel nulla. L'accusa di esportazione illegale viene ritirata nel 1996, mentre la controversia con *RSA* verrà mediata da una successiva collaborazione tra le due parti per la realizzazione delle versioni successive del software. PGP, è il programma di crittografia per eccellenza, che garantisce la segretezza della posta (ma non solo), l'autenticazione con firma digitale. Il software in questione non fa altro che implementare i moderni sistemi di crittografia, utilizzando un sistema crittografico misto con tre algoritmi:

- **il sistema a chiavi pubbliche RSA**
- **sistema a chiavi private IDEA (oppure altri algoritmi a scelta)**
- **algoritmo di hashing SHA-1 (oppure MD5)**

È distribuito gratuitamente per uso personale e può essere scaricato dal sito <http://www.pgp.com> o <http://www.pgpi.org>, oppure dai cd-rom allegati nelle riviste del settore. Sul sito si trova anche il codice sorgente del programma. Ci sono anche altre versioni del programma (a pagamento) con incluse altre funzionalità, per le esigenze più diverse, specie per le aziende (tra cui la **VPN**).

Il suo funzionamento è molto semplice: l'utente A cifra i messaggi (o file) da spedire all'utente B, utilizzando la chiave pubblica (la stessa che si pubblica sui keyserver) dell'utente B. La chiave pubblica dell'utente B è generata a partire dalla chiave privata della persona B, proprio per questo solo chi possiede la chiave privata sarà in grado di leggere il messaggio (quindi attenti a non far circolare la vostra chiave privata).

Come detto nei paragrafi precedenti, gli algoritmi a chiave pubblica risolvono anche il problema della firma digitale e con PGP è possibile firmare i messaggi, o meglio una loro sintesi creata tramite l'algoritmo **SHA-1** o **MD5**.

Il programma contiene anche l'utility *PGPdisk*. Questa, a differenza del programma in generale, è a pagamento e permette la creazione di un disco virtuale criptato sul proprio hard disk. Esso può contenere documenti di ogni tipo e persino programmi che girano normalmente su un computer.

Sotto questa utility sono presenti anche i Plug-in, utilità che permettono l'integrazione del programma nei software di posta elettronica. Tuttavia questi Plug-in potrebbero non funzionare correttamente. Nelle procedure di utilizzo sotto indicate, escludo l'utilizzo di queste aggiunte, anche perché sono inutili. Infatti impostando le scorciatoie da tastiera (come vedremo più avanti) si sarà in grado di utilizzare PGP nelle operazioni di cifratura in modo molto veloce.

INSTALLAZIONE E CONFIGURAZIONE

Quando si avvia la procedura di installazione (che è guidata) il programma chiede se si è un nuovo utente o se si hanno già a disposizione una o più chiavi. Se si è un nuovo utente, prima di creare la chiave (o le chiavi) consiglio di impostare alcune voci dei tab "**General**", "**Servers**" ed "**Advanced**" come indicato man mano che si legge:

avviare *PGPkeys* (dal menu Start o dalla voce *PGPtray* accanto all'orologio) cliccare sul menu *Edit>Options*, appare così il tab "**General**". Queste sono le voci presenti:

- **Always encrypt to default key** se attivato, tutti i messaggi o i file, cifrati con la chiave pubblica di un destinatario, saranno cifrati anche con la propria chiave pubblica impostata come default, in modo da poter essere in grado di decifrare il documento.
- **Faster key generation** è consigliabile disabilitare tale voce, così facendo si avrà una generazione delle chiavi molto più sicura.
- **Comment block** commento visualizzato in tutti i file cifrati.
- **Cache passphrase while logged on** per ogni tipo di azione, memorizza la passphrase in memoria fino al logoff dell'utente.
- **Cache passphrase for** memorizza la passphrase in memoria per il tempo indicato e per l'azione indicata.
- **Do not cache passphrase** non memorizza la passphrase in memoria.
- **Share passphrase cache among modules** permette di passare da un modulo all'altro senza digitare nuovamente la passphrase (se memorizzata in memoria).
- **Number of passes** numero di passaggi da effettuare sull'hard disk quando si esegue la cancellazione sicura di un file (3 passaggi possono bastare).

Nel tab "**Files**" sono indicati i percorsi del portachiavi pubblico e del portachiavi privato. La coppia di chiavi, PGP la memorizza in due file criptati: **pubring.pkr** che contiene le chiavi pubbliche e **secring.skr** che contiene le chiavi private.

Se si perde la chiave segreta, non sarà possibile decifrare nessuna informazione e la chiave pubblica associata sarà quindi inutilizzabile.

Prestare molta cura al file *secring.skr* poiché contiene la chiave privata personale (o più di una). C'è da dire che, al contrario del file di chiavi pubbliche, questo file viene memorizzato in modo criptato: per questo motivo quando si utilizza la chiave privata viene chiesto l'inserimento della passphrase personale. Per maggiore sicurezza (non si sa mai) consiglio di: non condividere tale file in rete, non lasciarlo memorizzato su un computer che non è il proprio (e magari neanche su quest'ultimo), eventualmente crittografare ulteriormente questo file con il metodo "*Conventional Encryption*" (descritto più avanti).

In poche parole: mai nessuno deve entrare in possesso del file *secring.skr* perché analizzandolo potrebbe scoprire la propria passphrase segreta (cosa credo impossibile al 99,999%).

Un'efficace precauzione sarebbe quella di memorizzare il file *secring.skr* su di un supporto mobile (una penna USB o un semplice floppy) ed impostare il programma in modo che quando lo si utilizza andrà a ricercare la chiave privata nel file sul supporto mobile anziché sull'hard disk.

Un altro trucco può rivelarsi molto efficace per gli amministratori di Server: rinominare i file di default che usa il programma (*secring.skr* e *pubring.pkr*) e quindi impostare il programma per usare i file chiamati diversamente.

Tab "**Email**":

- **Use PGP/MIME when sending email** se il programma di posta elettronica che si usa supporta il formato PGP/MIME, attivando questa opzione si farà sì che il messaggio sarà criptato o firmato automaticamente. Il destinatario deve avere un programma compatibile con il formato PGP/MIME (ora chiamato **OpenPGP**), ad esempio Eudora.
- **Encrypt new messages by default** cifra automaticamente tutti i messaggi in uscita.

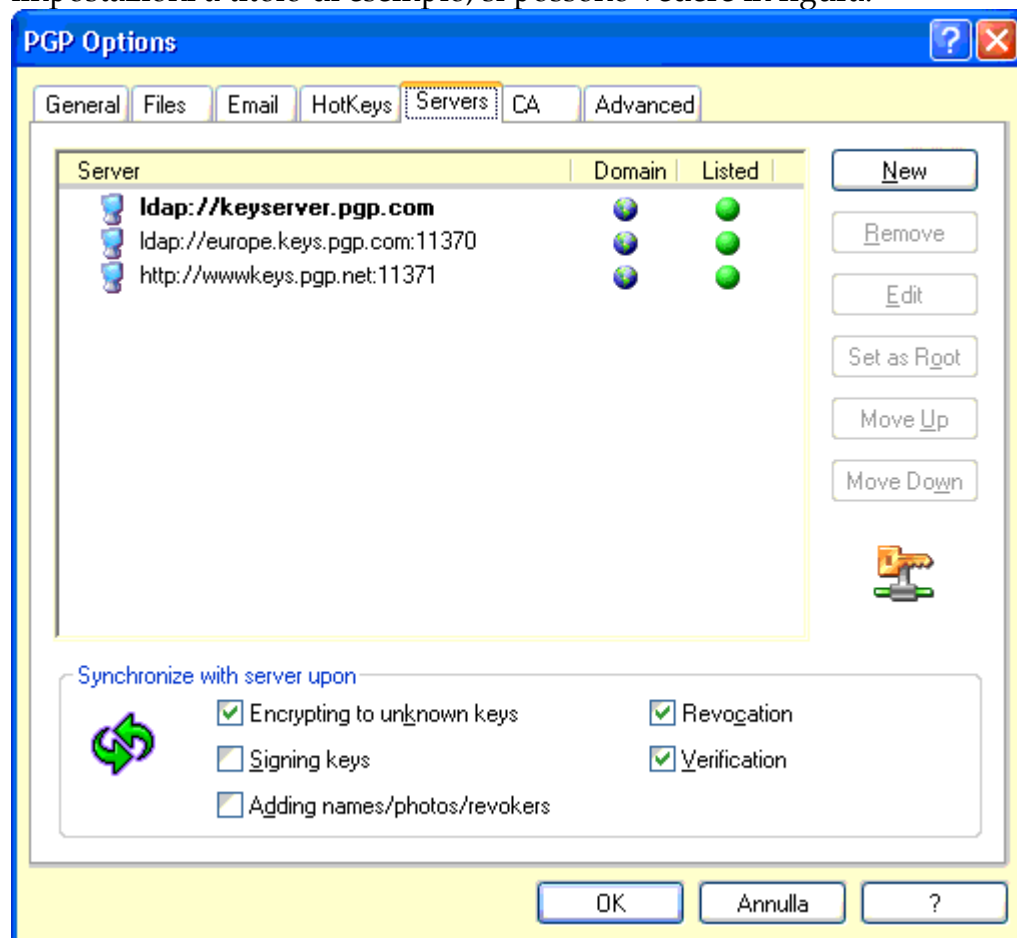
- **Sign new messages by default** firma automaticamente tutti i messaggi in uscita.
- **Automatically decrypt/verify when opening messages** procede a decriptare/verificare i messaggi in modo automatico quando vengono aperti.
- **Always use Secure Viewer when decrypting** permette di visualizzare i messaggi decifrati con caratteri speciali in una finestra chiamata "*Secure Viewer*". I messaggi cifrati con questa opzione non possono essere salvati in chiaro quando li si visiona.
- **Word wrap clear-signed messages** indica il numero di colonne dopo il quale sarà applicato un ritorno a capo all'interno del testo che contiene la firma digitale. Questo comando è stato introdotto perché alcuni programmi di posta inseriscono un ritorno a capo in modo errato, compromettendo la leggibilità.
- **Wrap at column** la colonna a cui applicare obbligatoriamente il ritorno a capo.

Tab "**HotKeys**", consente l'impostazione delle scorciatoie da tastiera, per i comandi di maggior utilizzo, davvero utile in modo da non dover ricorrere sempre all'icona sulla Tray Bar:

- **Purge passphrase caches** cancella la cache che contiene la passphrase.
- **Encrypt current window** cripta il contenuto della finestra che possiede il focus.
- **Sign current window** firma il contenuto della finestra che possiede il focus.
- **Encrypt & Sign current window** cripta e firma il contenuto della finestra che possiede il focus.
- **Decrypt & Verify current window** decripta e verifica il contenuto della finestra che possiede il focus.

Tab "**Servers**":

impostazioni a titolo di esempio, si possono vedere in figura:



In genere i primi due keyserver sono presenti di default. E comunicano tra loro, scambiandosi le chiavi. Quindi basterà mandare la/e propria/e pubbliche ad uno dei due.

Se non esistono i keyserver, effettuare questa operazione:

- cliccare sul pulsante "New", nel campo "Type" selezionare dal menu a discesa la voce **PGP Keyserver LDAP**, nel campo "Name" digitare **keyserver.pgp.com**, premere il pulsante "Ok". Passiamo all'altro keyserver.
- clic ancora sul pulsante "New", nel campo "Type" selezionare la voce **PGP keyserver HTTP**, nel campo "Name" digitare **wwwkeys.pgp.net** e nel campo "Port" digitare **11371**. Questo keyserver ospita anche le chiavi pubbliche di **GnuPG**.
- cliccare sul pulsante "New", nel campo "Type" selezionare dal menu a discesa la voce **europe.keys.pgp.com**, infine digitare **11370** nel campo "Port".

Vediamo le opzioni di questo tab, che si riferiscono al momento in cui bisogna effettuare una sincronizzazione fra le chiavi del portachiavi locale e le chiavi sui *keyserver*:

- **Encrypting to Unknown Keys** se riceviamo un documento criptato, e non si possiede la chiave pubblica del mittente, il programma cerca di importare la chiave pubblica dal keyserver predefinito.
- **Signing Keys** prima di firmarla, controlla sul keyserver se la chiave è scaduta o revocata. Poi aggiorna la registrazione sul keyserver.
- **Adding Names/Photos/Revokers** prima di effettuare l'operazione di aggiunta nome, foto, o addetti alla revoca, controlla la validità delle chiavi e la invia nuovamente al keyserver.
- **Revocation** aggiorna la chiave che sarà revocata e la restituisce al keyserver dopo l'operazione.
- **Verification** alla verifica di un file o messaggio cifrato del quale non si possiede la chiave pubblica del mittente, il programma ricercherà ed importerà automaticamente la chiave dal keyserver.

Tutte le operazioni sopra indicate, andranno a buon fine se è attiva una connessione ad internet.

Tab "CA":

opzioni riservate all'uso dei certificati X.509.

- **URL** l'indirizzo della *Root Certificate Authority*.
- **Revocation URL** l'indirizzo alla quale è disponibile la *Certificate Revocation List* della CA.
- **TYPE** il tipo di CA utilizzato.
- **Root Certificate** informazioni sul certificato della root CA.
- **Clear Certificate** cancella quanto alla voce precedente.
- **Select Certificate** specifica un certificato di root CA.

Tab "Advanced":

- **Preferred algorithm** permette di specificare l'algoritmo simmetrico per criptare. Di default è impostato il *CAST*, personalmente consiglio *IDEA*, *Twofish* o *AES*.
- **Allowed Algorithms** solo gli algoritmi selezionati verranno usati per cifrare. Consiglio di disabilitare *CAST* e *TripleDES*.
- **Display Marginal Validity Level** visualizza le chiavi in parte non valide oppure permette di visualizzarne la validità mediante un cerchio colorato: verde per una chiave valida, grigio per chiavi non valide. Disattivare.
- **Treat Marginally Valid Keys as Untrusted** se attivato, tratta tutte le chiavi parzialmente valide come non degne di fiducia e avvisa di questo.
- **Warn When Encrypting Keys to keys with an ADK** avvisa prima di procedere con l'utilizzo di una chiave pubblica processata utilizzando l'*ADK (Additional Decryption Key)*.
- **Export format - Compatible** esporta le chiavi con un formato compatibile alle versioni precedenti di PGP.
- **Export format - Complete** esporta le chiavi nel nuovo formato, che comprende anche l'ID fotografico, i certificati X.509 ed altro.

Proprietà generiche di una chiave

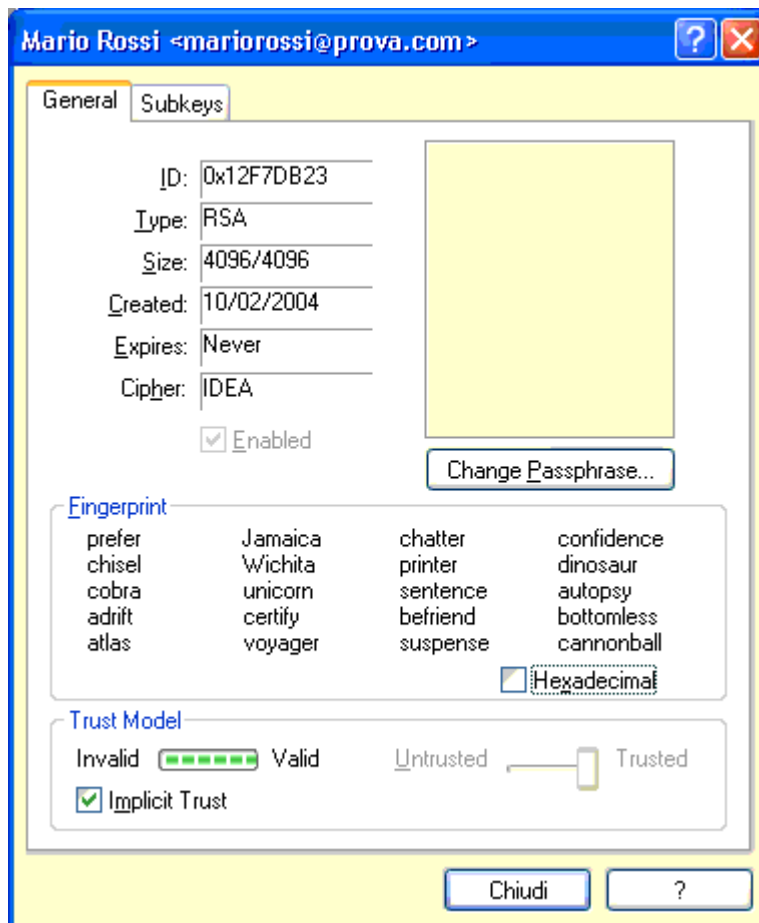
Per visualizzare le proprietà di una chiave, fare clic con il tasto destro del mouse su di essa, e dal menu contestuale scegliere la voce "Key Properties". Appariranno queste voci:

- **ID** identificativo univoco associato alla chiave. Per una chiave di tipo **V3** (versione 3, utilizzato dalla versione 5.x di PGP) significa i 64 bit meno significativi del modulo pubblico della chiave RSA. Nella versione **V4** (da PGP 6.x in poi) corrisponde ai 64 bit meno significativi del **fingerprint**.
- **Type** l'algoritmo a chiave pubblica utilizzato. Esso può essere:
RSA per le operazioni di cifratura della chiave e di firma verrà utilizzato l'algoritmo RSA. Con le nuove chiavi *V4* si utilizzano due coppie di chiavi, una per le operazioni di cifratura, un'altra per le operazioni firma/verifica.
DH/DSS per cifrare la chiave verrà utilizzato l'algoritmo *DH* mentre per firmare si ricorrerà a quanto previsto dal *Digital Signature Standard (DSS)*.
- **Size** la dimensione varia in base all'algoritmo utilizzato.
- **Created** data di creazione della chiave.
- **Expires** data di scadenza della chiave. Se indicato *Never* come in figura sopra non scadrà mai.
- **Cipher** algoritmo simmetrico utilizzato.
- **Enabled** se disabilitato, impedisce l'utilizzo della chiave.
- **Fingerprint** se la chiave è *V3*, consiste nel risultato dell'applicazione dell'algoritmo *MD5* alla chiave pubblica, senza considerare la lunghezza della chiave stessa. Per una chiave *V4* invece, sono considerati i 160 bit risultanti dall'utilizzo dell'algoritmo *SHA-1* avente in ingresso: *packet tag*, che indica la tipologia di pacchetto (chiave pubblica, chiave privata,...) di dimensione di un otteetto; *lunghezza del pacchetto*, di dimensione pari a due ottetti; tutto il pacchetto chiave pubblica a partire dal campo versione.
- **Hexadecimal** permette di visualizzare il *fingerprint* in formato esadecimale. Quando è disattivato, il *fingerprint* è visualizzato con delle parole in inglese la cui pronuncia è inconfondibile con altre parole se dettate al telefono.

Poi ci sono le opzioni legate al concetto di *Web of Trust* (ragnatela di fiducia) nel riquadro **Trust Model** e sono:

- **Implicit Trust** permette di dichiarare una chiave valida implicitamente, caratteristica che hanno le chiavi create di persona.
- **Untrusted-Trusted** livello di validità della chiave; essa può essere "non valida", "marginalmente valida" e "valida".

Esempio di proprietà di una chiave:



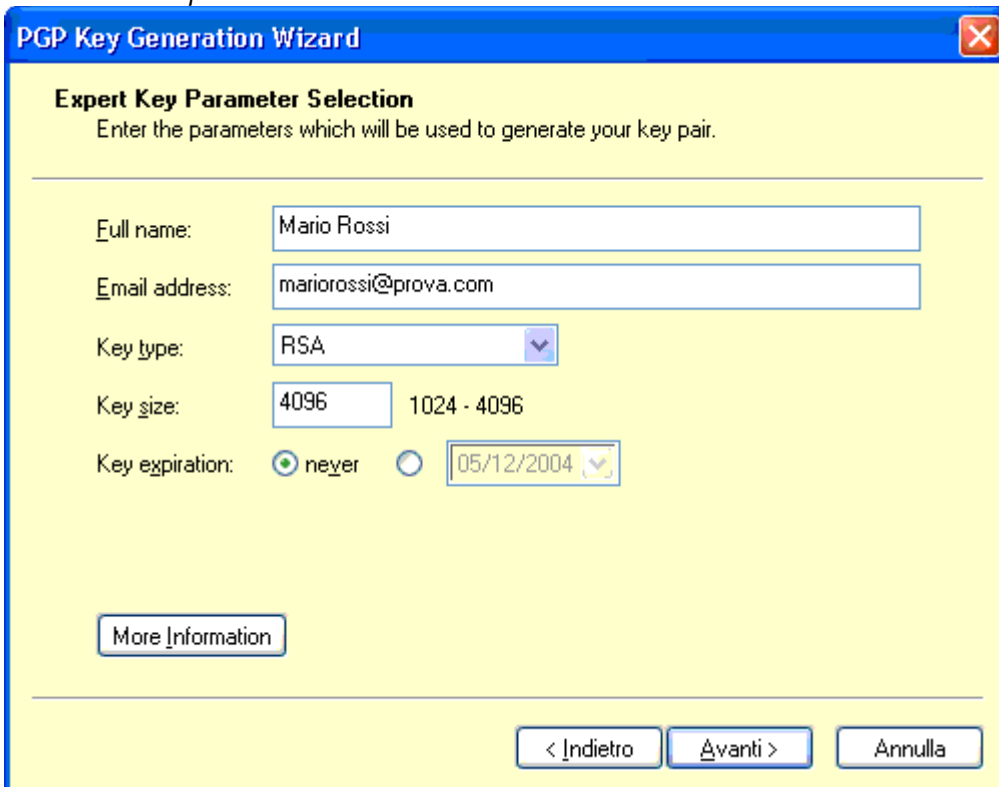
Per creare una nuova coppia di chiavi procedere nel seguente modo: avviare *PGPkeys*, fare clic sul menu *Keys>New key...*, apparirà la seguente finestra:



Se si fa clic sul pulsante **"Expert"** si passa alla modalità per esperti. Cliccando sul pulsante **"Avanti"** inserire il nome e l'indirizzo e-mail nei rispettivi campi. Cliccare ancora sul pulsante **"Avanti"** ed apparirà la finestra in cui inserire nel primo campo la *Passphrase*, che può includere qualsiasi combinazione di caratteri della tastiera. L'avanzamento della barra *"Passphrase Quality"* indicherà la *"bontà"* della combinazione immessa. Dopo aver immesso la passphrase

anche nel campo *Confirmation*, fare clic su “*Avanti*” ed attendere la generazione della chiave muovendo il mouse e premendo tasti a caso sulla tastiera, infine cliccare su “*Fine*”.

Per quanto riguarda la modalità **Expert**, le informazioni da inserire sono quasi identiche: quello che si imposta manualmente è il tipo della chiave e la dimensione. Ecco la finestra che appare se si accede alla modalità *Expert*:



The image shows a Windows-style dialog box titled "PGP Key Generation Wizard" with a yellow background. The main heading is "Expert Key Parameter Selection" with the instruction "Enter the parameters which will be used to generate your key pair." Below this, there are several input fields: "Full name:" with the text "Mario Rossi"; "Email address:" with "mariorossi@prova.com"; "Key type:" with a dropdown menu set to "RSA"; "Key size:" with a text box containing "4096" and a range "1024 - 4096" to its right; and "Key expiration:" with two radio buttons, the first labeled "never" (which is selected) and the second with a date "05/12/2004" and a dropdown arrow. At the bottom left is a "More Information" button, and at the bottom right are three buttons: "< Indietro", "Avanti >", and "Annulla".

A titolo di esempio ho inserito le voci nei campi.

Il tipo della chiave (campo “*Key type:*”) può essere:

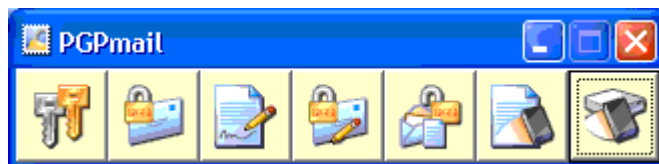
- **Diffie-Hellman/DSS** la cui coppia di chiavi generata sarà compatibile con le versioni PGP a partire dalla 5.x in poi. In teoria, la dimensione massima è di 4096 bit. In genere però le chiavi generate saranno di 1024 o al massimo 2048 bit.
- **RSA** nuova versione dell’algoritmo RSA V4 con grandezza di 4096 bit. Con questo algoritmo si può impostare la dimensione massima di 4096 bit e le chiavi saranno generate effettivamente con questa dimensione. Le chiavi tuttavia saranno compatibili a partire dalla versione 7.x di PGP.
- **RSA Legacy** grandezza massima delle chiavi è di 2048 bit. Le chiavi saranno compatibili con tutte le versioni di PGP.

Quale scegliere? Ovviamente per la massima sicurezza è consigliabile *RSA*. Non è importante che serva una versione più aggiornata del programma per leggere questo tipo di chiavi (7.x come detto), visto che si può scaricare gratuitamente dal sito.

Ricapitolando, terminata l’installazione e riavviato il computer, l’icona del programma si posiziona accanto a quella dell’orologio (area SysTray), e si hanno a disposizione due chiavi: una privata (da conservare molto scrupolosamente come descritto più avanti) e una pubblica. Se dopo il riavvio del computer non dovesse comparire l’icona del programma accanto all’orologio, fare clic su *Start>Programmi>PGP>PGPtray*.

L’utility PGPmail

PGP contiene una utility che si chiama *PGPmail* (quella in figura).



Volevo sottolineare che non è necessario utilizzarla, in quanto tutti i comandi che svolgono i pulsanti presenti, sono richiamabili dall'icona *PGPtray* (o dalle scorciatoie da tastiera). A qualcuno può piacere questa utility.

Nelle procedure di seguito non sarà usata questa utility, ma saranno usate le vie più semplici e veloci, appunto per velocizzare le operazioni di cifratura/firma digitale e decifratura.

La prima cosa da fare dopo aver installato il programma e create le chiavi, è salvare la chiave personale su un supporto, perché se la perdiamo non potremo più leggere i nostri documenti. Dopo aver avviato *PGPkeys*, selezionare la chiave desiderata e dal menu "Keys" cliccare su "Export", selezionando anche l'opzione 'include private keys'. Sarà salvata in un file .asc. Conservare e camuffare scrupolosamente il file generato (come descritto per il file *secring.skr* a pagina 2), poiché se andrà in possesso delle mani sbagliate, questo potrà decifrare i file personali che si sono protetti con questa chiave. In ogni caso comunque dovrebbe conoscere anche la nostra passphrase segreta associata, o analizzare il file per cercare di scoprire la passphrase memorizzata (cosa credo impossibile al 99,99%)

PGP prevede un archivio pubblico elettronico dove sono conservate le chiavi pubbliche degli utenti (sono i *keyserver* che abbiamo visto prima). Per inviare le chiavi ai *keyservers* selezionare il menu *Server>Send to* e poi ad uno ad uno le voci che compaiono.

Creata la chiave è possibile in futuro cambiare la passphrase. Per cambiare la passphrase, selezionare la chiave desiderata, clic sul menu *Keys>Properties...>clic* sul bottone "Change Passphrase".

Dopo ogni modifica ricordarsi di aggiornare la chiave sul *keyserver* e di mandare la chiave aggiornata ai propri amici. L'aggiornamento si ottiene mediante il tasto destro del mouse sulla chiave interessata e scegliendo la voce "Update" dal menu contestuale.

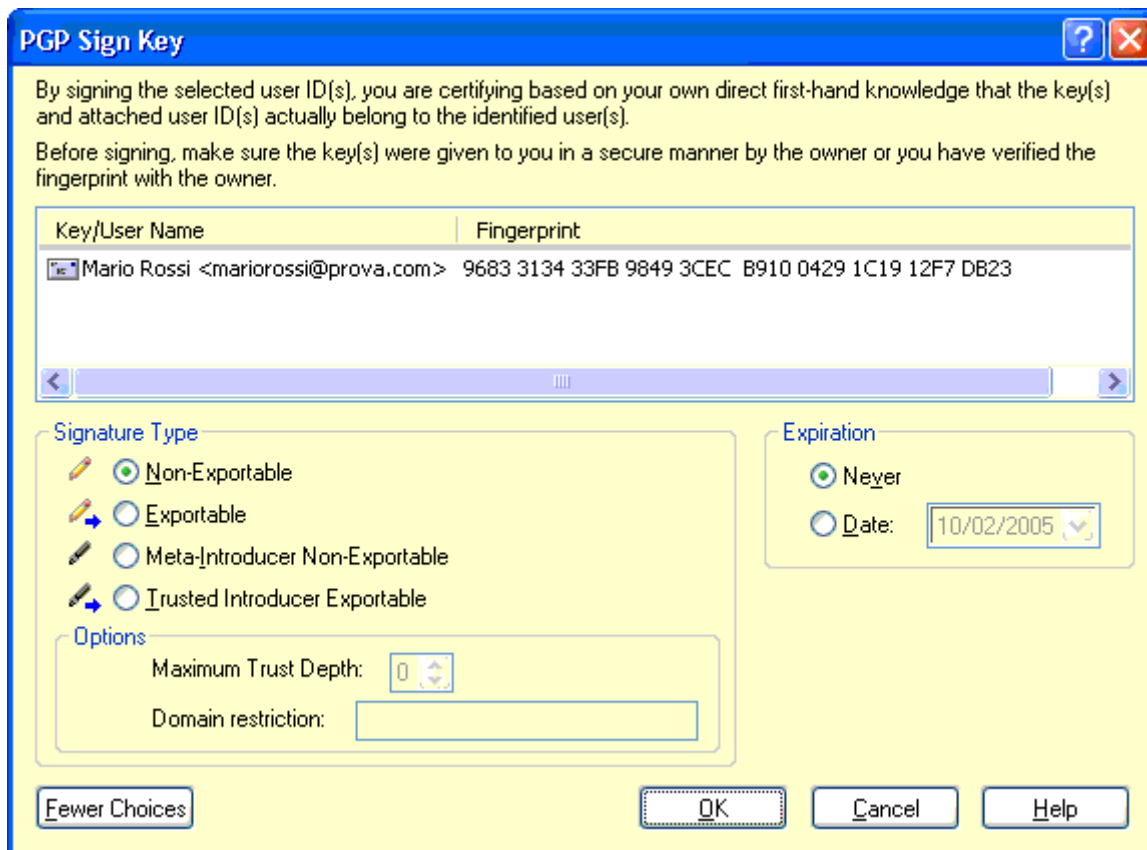
Se invece non desideriamo pubblicare la chiave su di un *keyserver*, salviamo la chiave pubblica (quindi non includere quella privata), e mandiamo poi il file .asc a chi desideriamo.

DICHIARARE VALIDE LE CHIAVI PUBBLICHE

Quando desideriamo comunicare in sicurezza con un destinatario, dobbiamo dichiarare valida la chiave pubblica del nostro corrispondente per poterla utilizzare. Se possediamo il file .asc (o .txt) del nostro destinatario, basta fare clic sul menu *Keys>Import...* e poi selezionare il file con la chiave dal percorso in cui risiede.

Per recuperare una chiave da un *keyserver*, clic sul menu *Server>Search...* e inserire un qualsiasi dato che identifica la persona che si vuole cercare (può essere il nome, l'indirizzo e-mail o altre informazioni).

Scaricata la chiave, come si può notare, se non si dichiara valida la chiave importata o scaricata, essa non può essere utilizzata correttamente, come mostra il cerchio di colore grigio nel campo 'Validity'. Per validare la chiave, fare clic su di essa con il pulsante destro del mouse e scegliere la voce "Sign...". Dovrebbe apparire una finestra simile a questa:



Se non appare il riquadro "Signature Type", fare clic sul pulsante "More Choices". Ecco cosa significano le varie voci:

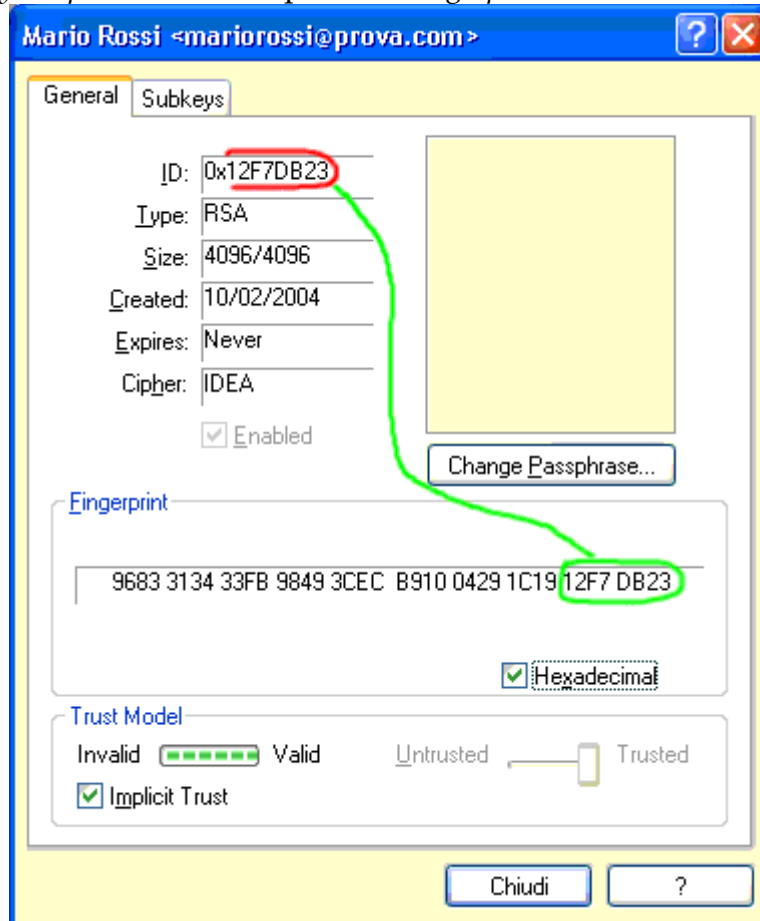
- **Non-Exportable** la chiave è per noi valida, ma non desideriamo che altri si basino sulla nostra validazione. La nostra fiducia dunque non sarà inviata al keyserver, ma rimarrà in locale.
- **Exportable** come per la precedente opzione, in questo caso però si acconsente la decisione della fiducia ad altri.
- **Meta-Introducer Non-Exportable** firmando la chiave, si darà fiducia al proprietario della stessa ed a quelle dichiarate valide da quest'ultimo, nonché ai *trustud introduced* creati dalla stessa chiave. In poche parole le chiavi dichiarate valide da un meta-introducer (paragonabile ad una CA root) saranno valide anche per noi.
- **Trusted Introducer Exportable** oltre a dar fiducia al proprietario della chiave, è considerato garante per le chiavi che ha firmato (un delegato, simile ad un delegato di una CA root). E che quindi sono valide anche per noi. E' possibile indicare la profondità con cui è nidificata una chiave.

Il riquadro "Expiration" indica la data di validità:

- **Never** significa che non scadrà mai.
- **Date** la firma scadrà nella data specificata.

In genere è sufficiente utilizzare una delle prime due voci (*Non-Exportable* oppure *Exportable*). C'è un caso particolare: se una chiave importata ne contiene delle altre al suo interno, è possibile dichiarare valide o meno quelle che contiene agendo nel riquadro 'Trust Model' che appare quando si aprono le proprietà di una chiave. Questa voce è da collegare a quelle sopra elencate (*Meta-Introducer Non-Exportable*, ecc). Anche se non si modifica il concetto di 'Trust Model' questa chiave è comunque utilizzabile, al contrario di quelle che definisce al suo interno. Prima di procedere a firmare la chiave assicurarsi che la stessa appartenga veramente alla persona interessata mediante la verifica del *fingerprint* (detto anche *impronta digitale*).

Nota: per controllare il *fingerprint*, cliccare con il pulsante destro del mouse sulla chiave, scegliere la voce "Key Properties" e nel riquadro "Fingerprint" attivare la voce "Hexadecimal".



Se solo un carattere dell'**ID** non corrisponde alla stringa cerchiata in verde, vuol dire che la chiave pubblica è stata modificata o che si tratta di un'altra persona e non di quella desiderata. Espandendo la chiave, fra le altre firme noteremo anche la nostra. Ricordarsi che una chiave pubblica può contenere anche altre firme, non solo quella del proprietario.

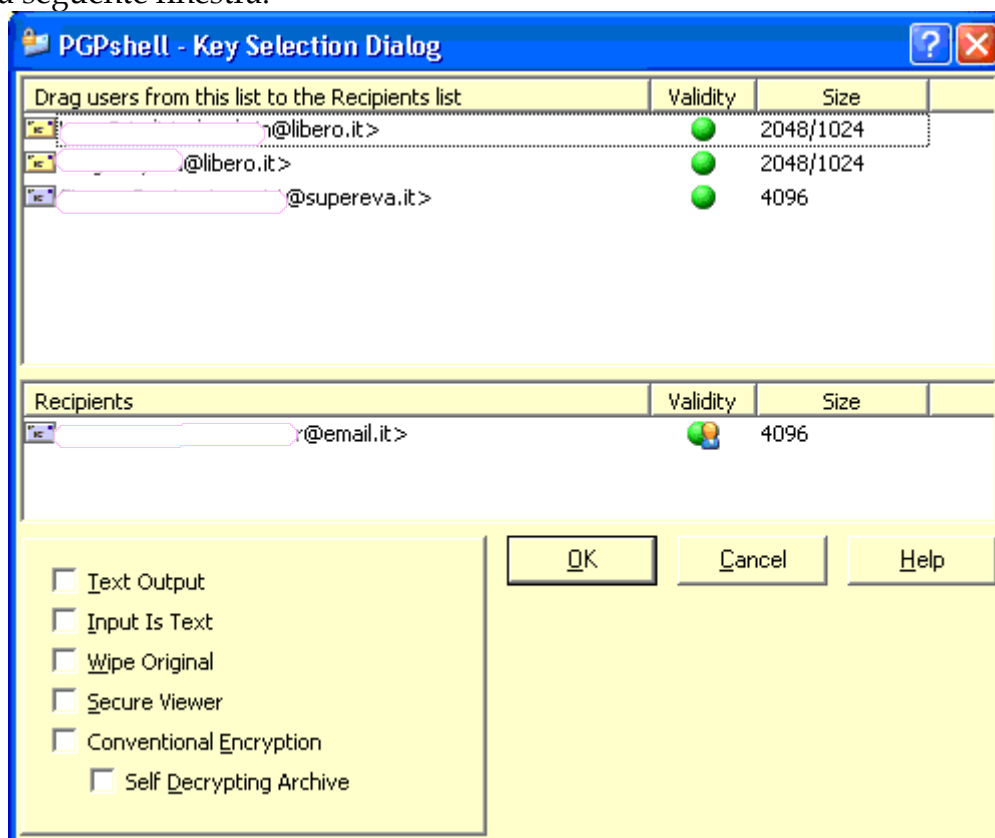
REVOCARE UNA CHIAVE

Se si ha la necessità di revocare una propria chiave, l'operazione è molto semplice: basta cliccare con il tasto destro del mouse sulla chiave e scegliere la voce **Revoke**. Se poi si aggiorna la chiave revocata anche sul *keyserver*, quando qualcuno la scarica non sarà funzionante. Ricordarsi che quando si revoca una chiave con cui era stata firmata una chiave pubblica di un certo destinatario, quest'ultima non sarà più utilizzabile se non la si firma nuovamente con la nuova chiave.

Quando si deve cifrare un documento, dobbiamo porci una sorta di domanda: chi deve essere in grado di decifrare il messaggio che stiamo per inviare? La risposta sarà nelle chiavi pubbliche che utilizzeremo.

INVIO DI FILE CIFRATI

Cercare il file desiderato all'interno di 'Esplora Risorse', clic con il pulsante destro del mouse e scegliere la voce *PGP>Encrypt* (se si vuole anche firmarlo digitalmente scegliere *Encrypt & Sign*), poi appare la seguente finestra:



Nella parte alta della finestra, come si vede, sono presenti le chiavi pubbliche dei destinatari (in questo caso la lista ne contiene 3), cioè chi sarà in grado di decifrare il nostro messaggio (ecco lo scopo della domanda precedente). Tramite un semplice drag-and-drop, trascinare il/i destinatario/i che deve essere in grado decifrare il messaggio cifrato, nel riquadro "Recipients" sotto alla nostra chiave pubblica. Infatti chi esegue la cifratura è presente di default, se attiva la voce **Always encrypt to default key** vista prima.

Premendo sul tasto OK, il file sarà crittografato, sarà aggiunta l'estensione *.pgp* (apparirà l'icona a forma di lucchetto), ed è pronto per essere allegato, oppure decifrato da noi stessi.

Le opzioni disponibili significano:

- **Text Output** crea il file cifrato solo caratteri ASCII Armored, non in binario.
- **Input Is Text** da selezionare quando il documento in questione contiene solo caratteri alfanumerici.
- **Wipe Original** da usare con cautela, in quanto se attivo cancella in modo irrecuperabile il file originale.
- **Secure Viewer** aggiunge un elemento di sicurezza contro sofisticate tecniche di spionaggio industriale. In altre parole visualizza i file o testo decifrati, utilizzando caratteri speciali all'interno della *Secure Viewer*. E non è possibile salvare in chiaro questi messaggi né copiare il testo in memoria, appunto perché sono visibili esclusivamente nella finestra *Secure Viewer*. Tuttavia questa opzione non è compatibile con alcune precedenti versioni di PGP.
- **Conventional Encryption** permette di cifrare il messaggio senza usare la chiave pubblica, e possiamo scegliere una frase convenuta tra noi ed il destinatario. Così facendo quando il

destinatario riceverà la nostra e-mail (o file) crittografata, dal menu di *PGPtray*, gli basterà scegliere *Current Windows>Decrypt & Verify*, e quindi digitare la frase convenuta.

- **Self Decrypting Archive** nel caso in cui il destinatario non possiede PGP.

Se, invece di un intero file, vogliamo cifrare un testo, procedere nel seguente modo:

- per esempio all'interno di un programma di videoscrittura (o client e-mail), clic su *PGPtray>Current Window>Encrypt* (oppure impostare una scorciatoia da tastiera per questo comando, per esempio CTRL+SHIFT+E). Dalla finestra che appare trascinare i destinatari che devono essere in grado di decifrare il messaggio.
- In alternativa, selezionare tutto, premere CTRL+C (per copiare tutto il contenuto), clic su *PGPtray>Clipboard>Encrypt*. Trascinare i destinatari dalla solita finestra. Incollare poi il testo (premendo CTRL+V) per esempio nel programma di posta elettronica che si utilizza.

Il destinatario che riceve il messaggio cifrato, dovrà semplicemente selezionare dal *PGPtray* la voce *Current Window>Decrypt & Verify* (o scorciatoia da tastiera se l'ha impostata) ed inserire la sua parola chiave. Oppure copiare il testo e scegliere la voce *Decrypt & Verify* questa volta dal menu *Clipboard*.

La prima procedura è meno elaboriosa della seconda, e noterete comunque che il primo metodo effettua le stesse operazioni della seconda (cioè la copia in memoria del contenuto della finestra corrente), risparmiando qualche operazione all'utilizzatore del software.

Ricapitolando dunque avviene questo: il mittente cripta il messaggio che vuole inviare con la chiave pubblica del destinatario, a sua volta il destinatario decifra il messaggio cifrato con la sua chiave privata.

INVIO DI E-MAIL CRIPTATE

Scrivere il messaggio nella finestra del proprio client e-mail come al solito, inserire i destinatari nei campi "A:", in "Cc:", "Bcc:", e poi cliccare su *PGPtray>Current Window>Encrypt* (oppure *Encrypt & Sign*). Ci appare una finestra, come visto in precedenza, che presenta solo le opzioni **Secure Viewer** e **Conventional Encryption** descritti sopra.

Esempio: avviato il client e-mail preferito, inserire i dati come sempre. Supponiamo di scrivere questo testo:

Ciao,

tutto bene? Ci vediamo stasera?

cliccare poi su *PGPtray>Current Window>Encrypt* e come risultato la finestra del proprio client mostra qualcosa simile a questo:

-----BEGIN PGP MESSAGE-----

Version: PGP 8.0.3

```
qANQR1DBwUwDLzYFSIW5Z44BEAC0GsrWUZlmh9n/b/cXXTlewVQPZYHt36j8+UC/
DJwpTjiX0nhdJMEiE5wHiAXTxDDoexK0y9WRrbsxScTsmZneVgjEn0cK42S1oVzA
TmVmDZxlUoa9F9zyaomThe+4XxLT5m5pf/2zLbCsR07QDwBn2uE+Jpe4bwXzWl/8
5yRS/fHj2gk2w/N9eXCzvwUg8QrV23C6rBXnDqsa11iGLtQXOKVfrYGOt/FOdrP
YxfBfw6rWaVqwgM03/XmFk8vGUKfy9cFN4lBkzvuakNt955Eyg99Z6GfDx3XbGer
tYtWc0pyCWkgCKBufDZx+lrvjstuzddm3co4NctQRXfa4vBTADbBGegtyMHC9CKV
03slcM6tpWdAj7iN+w8Mgf8R/OxTAYWHptCQTW5KBZXqGMF1BdnCPpNtM9gufJsd
QuTHRQVjR7xX37eZylYgpYjGbEUvdu1rP8G/VaNewIk5dY5Ujef0m/TzaYvpVM/v
MTJN4yekxpad+HXZGz5ULZBwWs+FRFEoT5mdK8ApWh/ETmfgnzZUd8XOlzlCuMth
QJu/vvgvF8W7ANhG8vSmVasIC1DfbZsge2uBSb5mwYfuSb3DsiuqUR8VVPoKxWTT
krimxF56QavN01Ep9Znr18itRSg+S1ijzqsH5Gx6ItG1bnCaSHfb5DGKwxNSFqsu
```

ufzP8HBTAPAdgFdxp8mQEP/3ITHzH9KiQjp0VbGzW6jeAb3/gcqTpNhMOMCn/+
p5zDLN6Y5/wd/9pyKaBn69aO97dWuAiS1EYDHFUchUhc8NbZ4ASbocILv+6fyrHn
M4ikpK1+CO31kFjWuemawbqA3pLiS2jpdanJwmTFedN3BUB1ZvX4D283ZCvxSjL1
BK8gyv9DvLV30n8r4K9Gov1X+QG0L1Dh5ccsKO6bn0GD3KPxO2J1aTFRA//Q1CU4
y6CUDuPWLtEoMWGKigDE0dIL21b4xWU2yt/+tF5BVj+424g4YbTv6YY/i1yOWmqg
w+TIDf8V2TQpUbbGA0MdrQcaCULZRYkWQmW7W582qrCs7jQTHhfDZlgR8BqhrcxF
n3eMnXtPu0HNI3yupyY0IK2cM5hBqZbb8d7qAXqBFYC/jADuY22li+v+2eqBjS0
cVxBaUyVDqvQ0wsYqEox2dvUzPh4U3uSRHF4cbJ1/SBvvdDJ+H7WvgHW5IH6Prye
BSQQDJkRZd66aEzFd/AprLdhIXLBKO/Lhe/v3eaSbuA6/tIVm5eXUX5iNmHdr+3e
WevKDEjVnzjCWtTpL4LB7Hs24omV0ufa8A2ezaMxCrODtFMUPxmbz3f+mycUsSn1
R67ENlm9KjGWl18FNj9Imy0GtXABnM9KnFAygdWpXiyjQ9NDX2UAm99fhyaAKwB
1w1fyT2W4e1KhZynlkbjsLCKipa9SwpxSovJ/noWA0KuFx1A9EI3hze95JDn9e59
h4y3I6/n6dF6i/mokpwwzTju
=DniC
-----END PGP MESSAGE-----

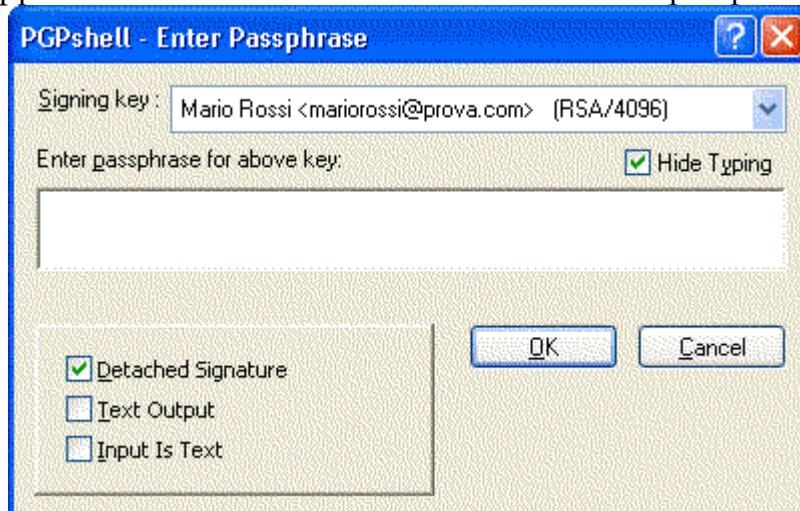
Se qualcuno vuole provare a risalire al messaggio originale “Ciao, tutto bene? Ci vediamo stasera?” partendo da quest'ultimo criptato, è libero di farlo ;-)

USARE LA FIRMA DIGITALE

Per firmare digitalmente un documento (non necessariamente solo testo, può contenere anche immagini o altro, oppure potrebbe essere un qualsiasi file) all'interno di un apposito software, non c'è altro da fare che cliccare su *PGP*tray>Current Window>Sign (oppure usare la scorciatoia da tastiera).

Per firmare un file sull'hard disk, cercarlo da “Esplora Risorse” (o da un qualsiasi cartella), clic con il tasto destro del mouse su di esso e dal menu scegliere *PGP*>Sign. Il programma aggiungerà l'estensione .sig (o .sign).

In entrambi i casi apparirà la finestra che chiederà di immettere la passphrase personale:



- **Detached Signature** crea un file di firma (.sig) separato contenente l'hashing del file originale, invece che inserire direttamente la firma nell'originale.
- **Text Output** crea un file di firma usando i caratteri **ASCII Armored**.
- **Input Is Text** da selezionare quando si sta firmando, appunto, un documento che contiene solo caratteri alfanumerici.

Notare la differenza quando si seleziona il metodo “Text Output”:

-----BEGIN PGP SIGNATURE-----

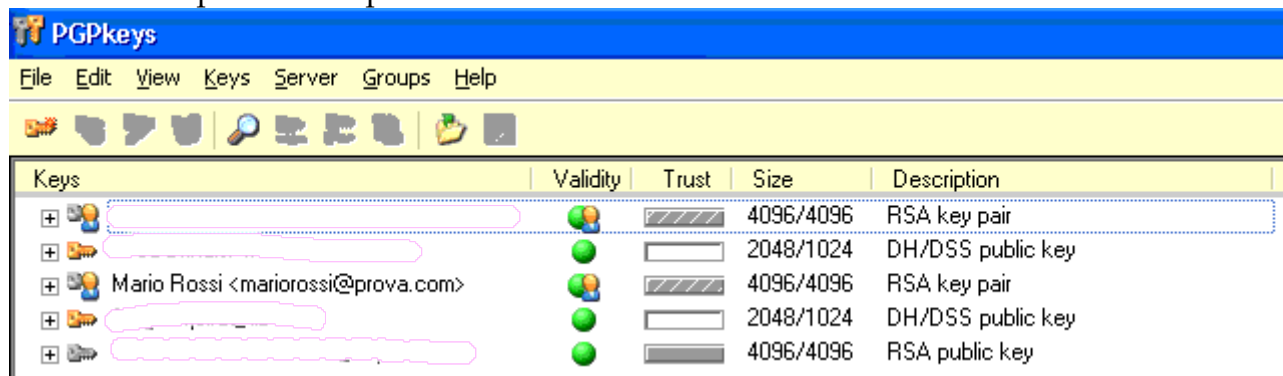
Version: PGP 8.0.3

elettronica, ed il destinatario lo potrà leggere inserendo la frase convenuta (che abbiamo scelto tra di noi prima) al momento dell'apertura.

La voce *Conventional Encryption* è disponibile anche per l'invio di e-mail, così facendo non si userà alcuna chiave pubblica, però in questo caso è necessario che il destinatario abbia installato il PGP, mentre nel caso visto sopra, come già detto, non c'è bisogno.

Struttura di un portachiavi

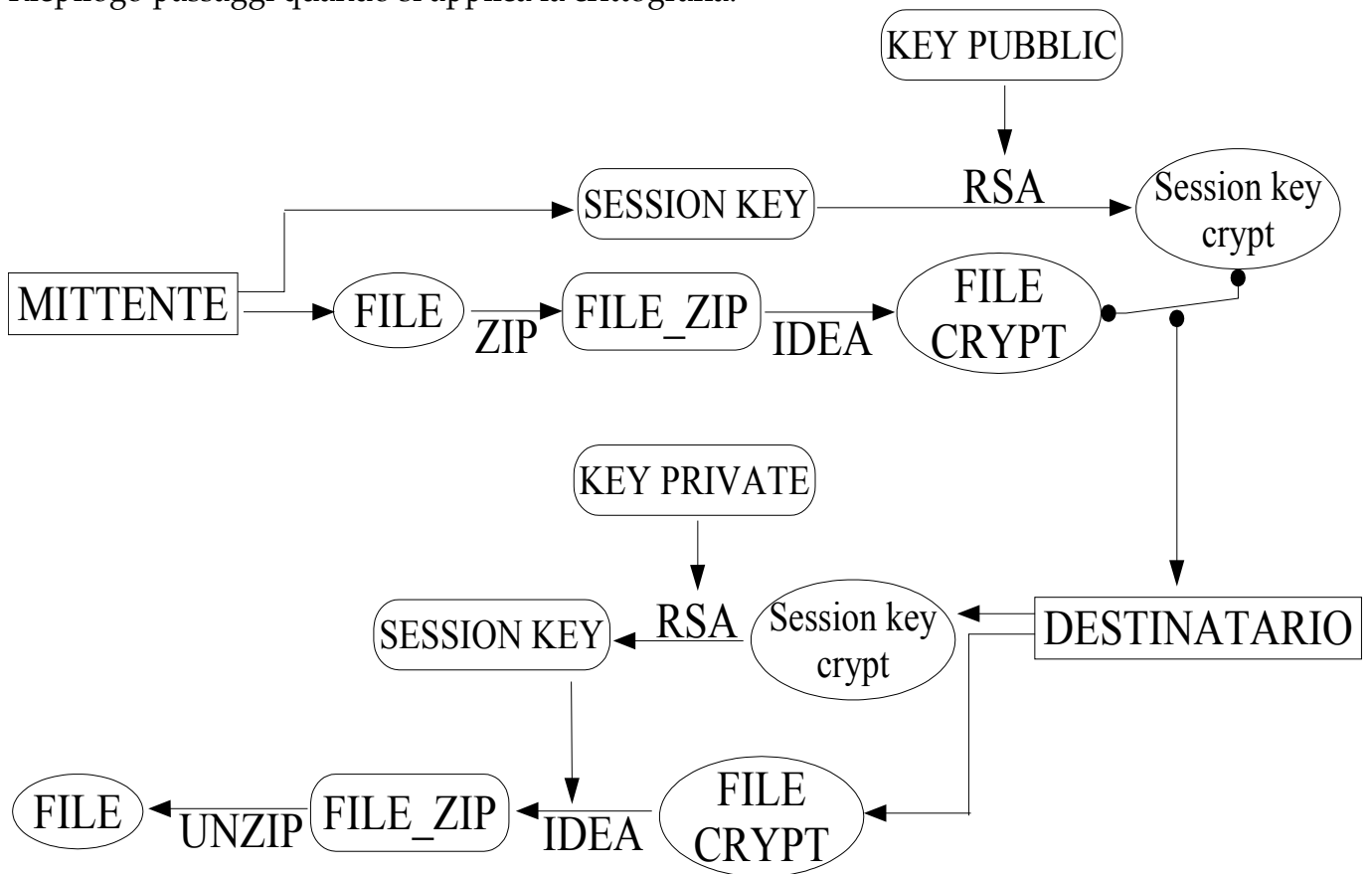
A titolo di esempio ecco un portachiavi:



Ho nascosto molti indirizzi e-mail, compaiono solo alcune intestazioni. Tutte queste informazioni sono salvate nei file indicati nel tab "Files". Se si salvano questi file in un'apposita cartella, e poi su un supporto, quando si formatta il computer e si reinstalla nuovamente PGP, non c'è bisogno di creare nuovamente tutte le chiavi personali. Basta copiare la cartella in un percorso (non è importante che sia lo stesso di quello prima della formattazione) e poi dal tab "Files" impostare il percorso, e saranno disponibili tutte le chiavi del portachiavi.

Come si può notare, le chiavi con il cerchietto verde e con un omino indicano le chiavi create da chi utilizza il programma. Mentre le chiavi che hanno solo il cerchietto verde sono chiavi importate e dichiarate valide.

Riepilogo passaggi quando si applica la crittografia:



- il file del mittente viene compresso con un algoritmo di tipo *zip*
- il file compresso viene criptato mediante l'algoritmo *IDEA*
- viene generata una sequenza casuale di 128 bit (o più) chiamata *session key* con appositi algoritmi per ottenere una sequenza di numeri pseudo casuali che hanno determinate proprietà statistiche, devono essere equiprobabili (come se si tirasse un dado: escono numeri da 1 a 6)
- la *session key* viene cifrata con l'algoritmo *RSA* (oppure con l'algoritmo *Diffie-Hellman/DSS*) utilizzando la chiave pubblica del destinatario ed il risultato è concatenato al documento
- la *session key* criptata viene concatenata al file criptato
- infine, viene applicato l'algoritmo di trasformazione reversibile a testo **ASCII** chiamato **Armor Radix-64** (a volte indicato **Base64** o **Armored**). Questo algoritmo produce un documento formato da solo caratteri ASCII compatibile con tutti i server e client di posta elettronica.

Brevemente, questo formato converte un input a gruppi di 24 bit come una stringa di 4 caratteri codificati ASCII. I 24 bit vengono formati a gruppi di 8 bit (quindi 3 byte) concatenati fra loro, e poi ogni gruppo di 6 bit è codificato con un carattere stampabile compreso tra un indice da 0 a 63. Alla fine si hanno dunque 4 caratteri stampabili. Ogni singola linea, nel file di output, non avrà più di 76 caratteri.

Questi 64 caratteri fanno parte del cosiddetto *ASCII 'basso'*, cioè i caratteri rappresentati dai numeri decimali nell'intervallo 0-127 (o esadecimali da 00 a 7F oppure ancora 2^7-1 bit).

Questa è la tabella di conversione del codice *Armor Radix-64*:

Value Encoding Value Encoding Value Encoding Value Encoding

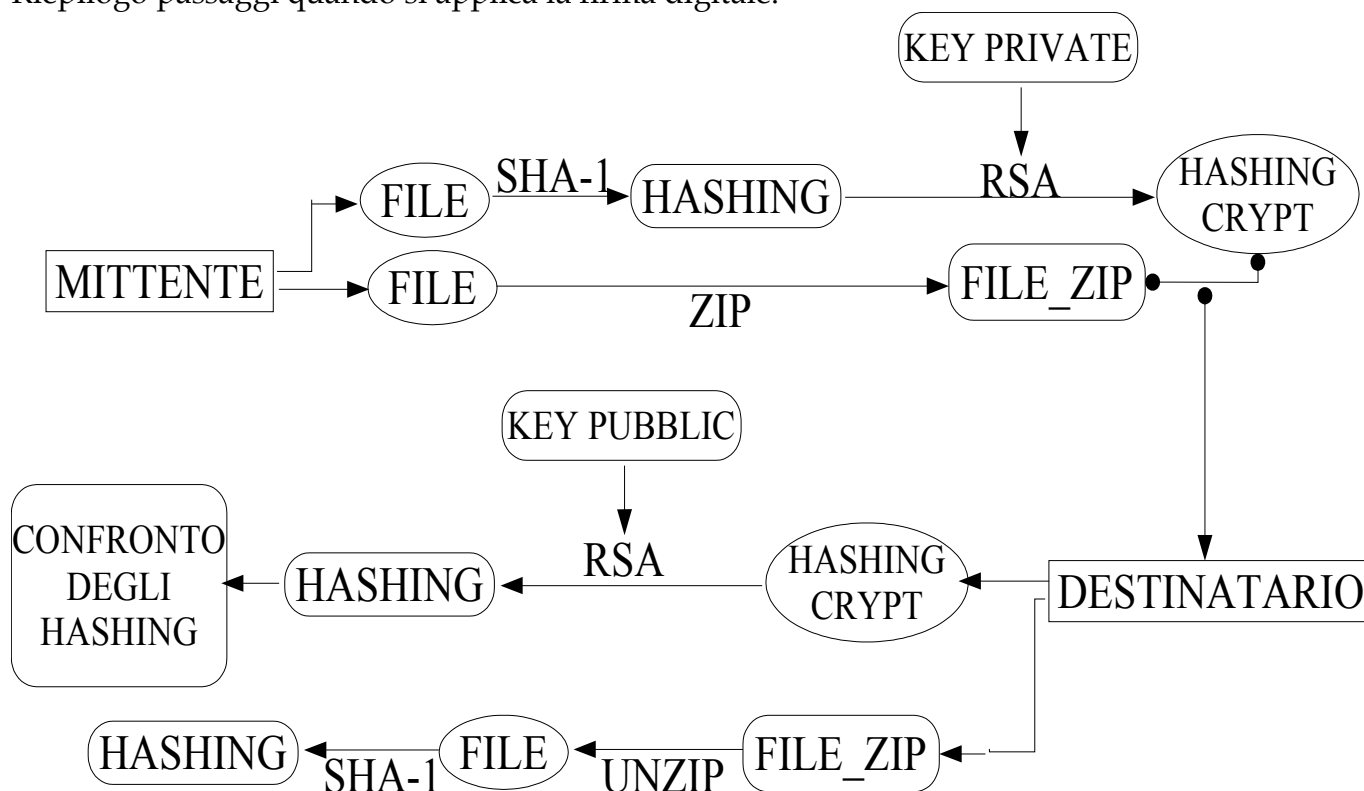
0 A	17 R	34 i	51 z
1 B	18 S	35 j	52 0
2 C	19 T	36 k	53 1
3 D	20 U	37 l	54 2
4 E	21 V	38 m	55 3
5 F	22 W	39 n	56 4
6 G	23 X	40 o	57 5
7 H	24 Y	41 p	58 6
8 I	25 Z	42 q	59 7
9 J	26 a	43 r	60 8
10 K	27 b	44 s	61 9
11 L	28 c	45 t	62 +
12 M	29 d	46 u	63 /
13 N	30 e	47 v	
14 O	31 f	48 w	(pad) =
15 P	32 g	49 x	
16 Q	33 h	50 y	

Per maggiori informazioni, cercare l'RFC2440 (che definisce lo standard di comunicazione **OpenPGP**) sul sito <http://www.ietf.org>.

La scelta di trasformare un file in codice *ASCII Armored* oppure no è a scelta dell'utente (in alcuni casi questa operazione è svolta dai sistemi software o hardware in modo trasparente se non l'ha fatto in modo esplicito l'utente)

- il destinatario, naturalmente, per leggere il file deve compiere le stesse operazioni al contrario.

Riepilogo passaggi quando si applica la firma digitale:



- il file del mittente viene compresso con un algoritmo di tipo *zip*
- viene calcolato l'*hashing* del file mediante l'algoritmo *SHA-1* (o *MD5*). Il codice *hash* generato viene criptato tramite *RSA* con la chiave privata del mittente ed accodato al file di origine
- eventualmente il file risultante dalle due operazioni precedenti viene trasformato in codice *ASCII Armored*

- il destinatario effettua le operazioni al contrario e verifica se i codici di *hashing* sono identici.

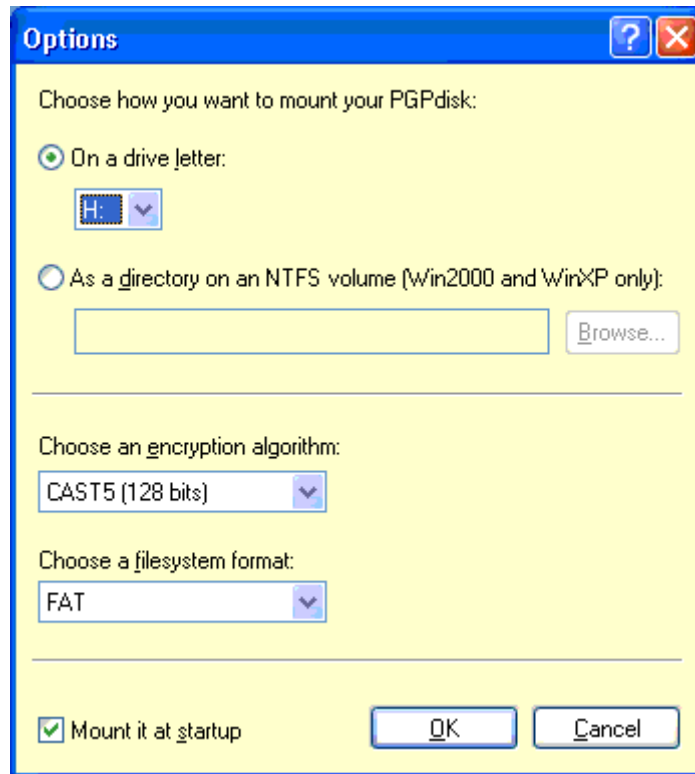
PGPdisk: disco virtuale o cartella protetta

Installando l'utilità PGPdisk, come già detto, è possibile creare uno spazio virtuale protetto da passphrase sull'hard disk, al cui interno è possibile memorizzare ogni tipo di file e persino installarci programmi. L'utilizzo di quest'aggiunta è a pagamento, al contrario del resto del programma. Se si procede all'acquisto, si ha a disposizione un'interessante aggiunta. Analizziamo l'utilizzo: clic sul menu *Start>Tutti i Programmi>PGP>PGPdisk*, se è la prima volta che lo si utilizza, apparirà la procedura guidata per la creazione del disco. Clic sul pulsante *Avanti* dovrebbe apparire questa finestra:



Come si può notare, si deve specificare una posizione fisica per il volume criptato e la dimensione.

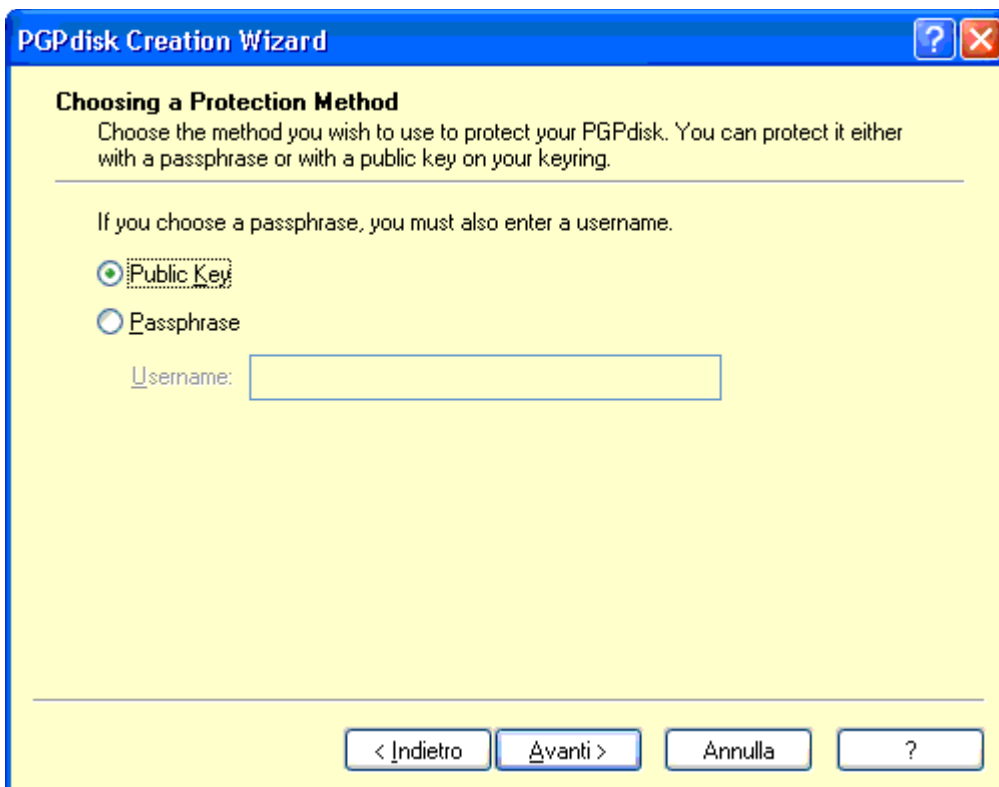
Il pulsante "Advanced Options..." permette di specificare altri parametri:



essi sono: la lettera con cui sarà montato il disco protetto oppure un percorso (directory) in cui saranno resi disponibili i file criptati.

Poi vi è la possibilità di scegliere l'algoritmo con cui sarà cifrato il volume (**AES**, **CAST5**, **TWOFISH**), ed il formato del file system (**FAT** o **NTFS**). Per il formato del file system è consigliabile scegliere **FAT** se ad accedere al volume cifrato è un solo utente. Scegliere **NTFS** per impostare dei criteri di protezione per i files del volume ad accesso multi utente.

La casella **Mount it at startup** consente di montare il volume criptato all'avvio del sistema operativo. Cliccare sul pulsante "OK", premere "Avanti" e dovrebbe apparire la finestra sottostante:



- **Public Key** scegliendo quest'opzione è necessario disporre della chiave privata abbinata a quella pubblica per decifrare il volume.
- **Passphrase** bisogna inserire anche un nome utente e sarà richiesto ogni volta che viene montato il volume.

Proseguendo, bisognerà digitare una passphrase. Poi completare la procedura.

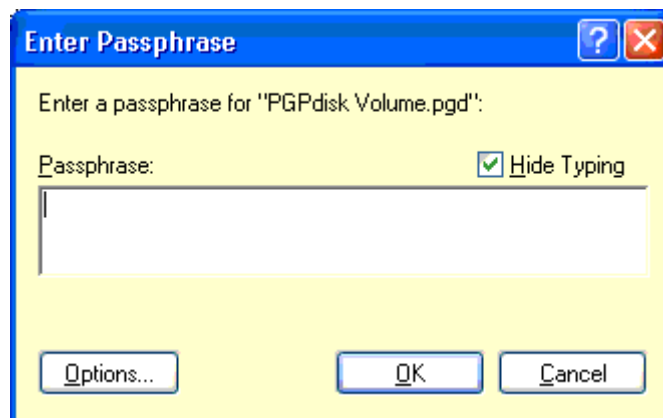
Aperto "Risorse del computer" dovrebbe apparire il volume criptato, oppure la cartella nel relativo percorso, se si era scelto quest'ultima opzione.

Se invece non si è un nuovo utente, bisogna interagire su di esso tramite l'icona *PGPtray>PGPdisk* e poi scegliere la voce desiderata dal sottomenu che apparirà.

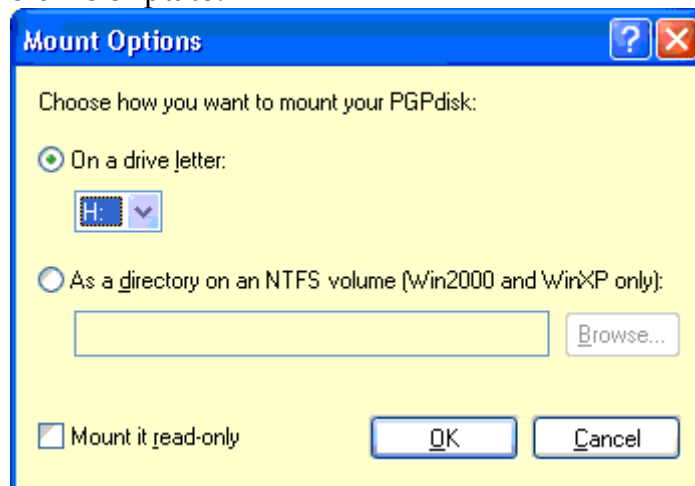
PGPdisk, "mount" e "unmount" di un volume

Il file cifrato che rappresenta il volume (o la cartella), non consente di effettuare nessuna operazione su di esso, come per esempio l'accesso ad un documento. Per questo è necessario effettuare un "montaggio" del volume stesso, operazione che consente al sistema operativo di "vedere" il volume come un'unità disco o come una cartella. Il "mount" di un volume può essere effettuato anche a mano tramite la voce presente in PGPdisk. Non è necessario che il 'mount' sia impostato in automatico all'avvio del sistema.

Cliccando su *PGPtray>PGPdisk>Mount Disk...*, apparirà la finestra che permette di selezionare il file di volume PGPdisk (.pgd). Raggiunto il percorso in cui è memorizzato il file, all'apertura apparirà la finestra di inserimento della passphrase, se si è scelto di utilizzare l'opzione **Public Key**. Ecco l'immagine:



Osservare anche la presenza del pulsante "Options...": cliccando su di esso è possibile cambiare il comportamento del volume criptato.



Come si può vedere nell'immagine, è possibile 'montare' in un volume virtuale, in una directory (su Windows 2000/XP e hard disk formattato con file system NTFS); ed anche in sola lettura.

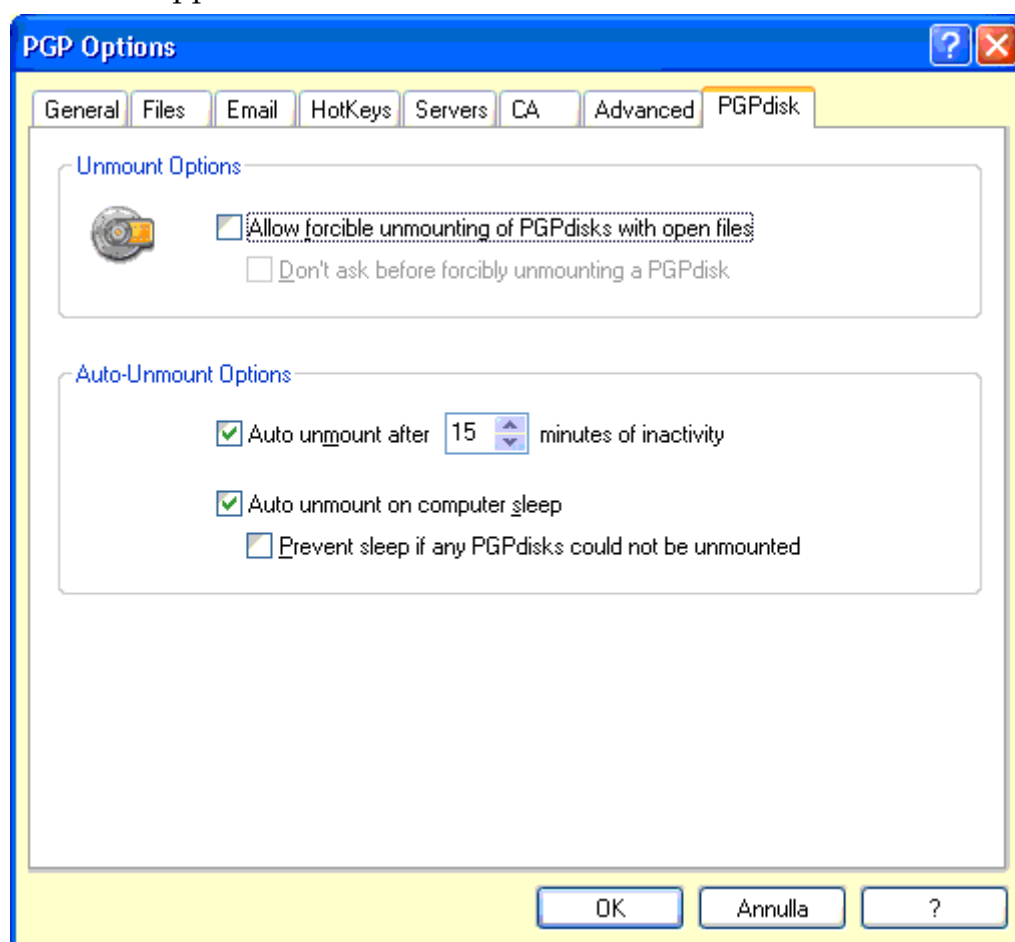
Come si intuisce, effettuando un "unmount" di un volume si effettua l'operazione opposta di "mount". Prima di effettuare lo smontaggio di un volume, è necessario che nessun file contenuto all'interno sia in uso. L'operazione si effettua all'intero di 'Edit Disk' oppure mediante il comando *PGPTray>PGPdisk>Unmount All Disks*

PGPdisk, editing del volume

La funzione di editing di un disco virtuale criptato consente di effettuare le operazioni messe a disposizione del programma. Cliccare su *PGPTray>PGPdisk>Edit Disk...*, selezionare il file di volume e cliccare sul pulsante "Apri".

Dalla finestra che appare, è possibile aggiungere utenti, scegliere un altro algoritmo di criptazione per il volume, cambiarne le proprietà, modificare la passphrase per un utente.

Quando è installata l'utility PGPdisk, sarà presente un nuovo tab nelle opzioni del programma, e il nuovo tab si chiama appunto "PGPdisk":



- **Allow forcible unmounting of PGPdisks with open files** permette lo smontaggio forzato dei file aperti, e non saranno disponibili per il programma che ne faceva uso.
- **Don't ask before forcibly unmounting a PGPdisk** disabilita la visualizzazione di un messaggio di conferma di chiusura file in uso prima dello smontaggio del volume.
- **Auto unmount after xx minutes of inactivity** effettua lo smontaggio automatico di un volume dopo xx minuti di inattività.
- **Auto unmount on computer sleep** smonta automaticamente i volumi alla chiusura del sistema operativo.
- **Prevent sleep if any PGPdisks could not be unmounted** non spegne il computer se ogni volume non può essere smontato.

Note

In alternativa a PGP si può usare **GPG (GNU Privacy Guard)**, <http://www.gnupg.org> di cui è presente anche una versione compilata per sistema Windows e molte altre piattaforme. GPG può leggere anche le chiavi PGP e viceversa (comunque ci sono delle limitazioni in entrambi i casi).

Se desideriamo crittografare un file sull'hard disk che contiene dati importanti per noi, e che dunque vogliamo proteggere da occhi indiscreti, possiamo utilizzare la voce '*Conventional Encryption*' quando appare la finestra per la selezione delle chiavi. Così facendo si scavalca il metodo della doppia chiave e, cosa più importante, anche se qualcuno riesce a scovare il file che contiene la chiave privata non sarà in grado di decifrare i file criptati con questo metodo. Oppure valutare l'uso di **PGPdisk** al posto di usare questo metodo o altri programmi.

Esistono altri software di crittografia, anche se, secondo me, il migliore è PGP; gli altri software non permettono la gestione a doppia chiave (ed alcuni sono davvero insicuri), quindi possono andare bene per file che devono restare sul proprio computer, senza scambio, altrimenti si è costretti a rivelare la propria password ad altri.

Volevo fare un'altra precisazione: chiunque abbia bisogno di proteggere un file, o più di uno, magari comprimendolo, avrà usato il famoso Winzip. Questo programma infatti, permette anche di assegnare una password agli archivi compressi. Io consiglio di non usarlo. Perché?

Perché esiste un programma che si chiama *Advanced ZIP Password Recovery*, prodotto dalla **Elcomsoft**, il quale permette di trovare la password degli archivi Winzip in pochi minuti. Quindi il Winzip è un valido programma per la compressione dei file (deve la sua diffusione soprattutto in merito al vecchio formato *.zip*, gestito dal programmino DOS *PkZip*; i programmi WinRAR e WinACE possiedono un algoritmo di compressione dei dati più potente del famoso WinZIP), ma per la sicurezza di dati importanti, non è il caso.

Attenzione: non tutti i programmi permettono di proteggere gli archivi compressi.

Stesso discorso possiamo farlo con i file di Word, Excel, Access. Esistono programmi, sempre prodotti dalla casa russa Elcomsoft che permettono di scovare le password di questi file.

In questo guida si è parlato della sicurezza dei file personali sul proprio computer e della comunicazione in sicurezza via internet.

Tuttavia, per proteggere adeguatamente il proprio computer sia da attacchi esterni (via internet, specie per chi possiede una connessione sempre attiva, tipo ADSL), sia dai virus, sono necessari anche altri strumenti: un buon antivirus ed un firewall.