Istruzioni e consigli per l'utilizzo del programma PGP (Pretty Good Privacy)

(aggiornamento del 6 giugno 2015)

Cari compagni e sinceri democratici,

queste istruzioni hanno lo scopo di permettervi di instaurare rapidamente la libera circolazione di informazioni senza che gli apparati repressivi "veglino" sulle vostre idee e la vostra organizzazione.

Voler migliorare la società, cambiare lo stato delle cose è illegale per chi detiene il potere nelle cosiddette "democrazie occidentali". Quindi armatevi degli strumenti tecnici adatti a cambiare lo stato attuale delle cose.

Le istruzioni sono divise in capitoli. All'interno di ogni capitolo abbiamo numerato le istruzioni: questo perché ogni eventuale nostro corrispondente che ha osservazioni da fare su qualche istruzione, possa indicare facilmente a quale si riferisce.

INDICE

1. Pillole di teoria

1. Il programma PGP permette di corrispondere in modo riservato**(1)** senza che i due corrispondenti debbano scambiarsi una password. I vantaggi di questo metodo è che si possono creare corrispondenze riservate facilmente senza dover fisicamente incontrare il proprio corrispondente per scambiarsi le password.

   Alla base di tutto c'è la **vostra chiave pubblica (*una password da inviare a chi vuole corrispondere con voi*)**. Prima di scendere nel dettaglio sappiate che grazie a questa chiave, tutti coloro che useranno il PGP potranno inviarvi dei messaggi riservati e voi che avete diffuso la **vostra chiave pubblica** potrete decifrarli senza bisogno di accordi con i corrispondenti.

   Uno dei vantaggi del programma PGP è che chi conosce la **vostra chiave pubblica** può scrivervi in qualunque momento e senza dover prendere degli accordi particolari con voi.

   Ad esempio il (n)PCI, per facilitare le comunicazioni riservate, ha pubblicato la **sua chiave pubblica** nel suo sito (più avanti, è indicato dove).

   Le istruzioni che seguono vi illustreranno come fare per comunicare con il Partito e come fare per permettere al Partito di inviare a voi dei messaggi riservati.

2. Vi domanderete come mai pur essendo la chiave *pubblica*, i messaggi criptati con essa rimangono riservati. Ecco in sintesi la spiegazione.

   La **chiave pubblica** è creata assieme ad una **chiave privata:** queste due chiavi sono **legate tra loro** da un metodo

matematico.

La sicurezza del metodo dipende dal fatto che la funzione che lega le due chiavi è molto complessa. Questa funzione si basa su dei grandi numeri primi ed ha la caratteristica di essere così complessa che i più veloci computer attualmente disponibili impiegano alcuni secoli per venirne a capo: di sicuro il socialismo lo instaureremo prima!

3. Ma la cosa da sottolineare è che chi cripta il messaggio con la **chiave pubblica** del Partito, non può lui stesso fare l'operazione inversa. Come non la possono fare neanche gli sbirri che intercettano un messaggio che anche a loro risulta criptato con PGP. Se per sbaglio il corrispondente con il Partito cancella il file originale, egli non sarà in grado di ripristinarlo a partire dal file criptato. Solo il Partito può ripristinare il messaggio perché è in possesso anche della propria **chiave privata** (quella generata **in coppia** con la chiave pubblica del Partito). Solo il possessore della **chiave privata**, se riceve il messaggio trattato con la **sua chiave pubblica,** può ripristinarne il contenuto.

4. In sintesi:
    - **Solo** chi ha la **chiave privata** e la sua **relativa chiave pubblica** può ripristinare un messaggio criptato.
    - **Tutti** possono criptare dei messaggi con la **chiave pubblica del Partito** e inviarli ad esso.
    - Se volete ricevere dei messaggi riservati dal Partito, dovete inviare al Partito la **vostra chiave pubblica**.
    - La **vostra chiave pubblica** è **diversa** da quella del Partito e si combina con **la vostra chiave privata**.
    - Le chiavi private devono essere gelosamente conservate: vedremo più avanti che (capitolo 4.) Kleopatra vi consente di farlo facilmente.

2. Recuperare e installare il programma PGP

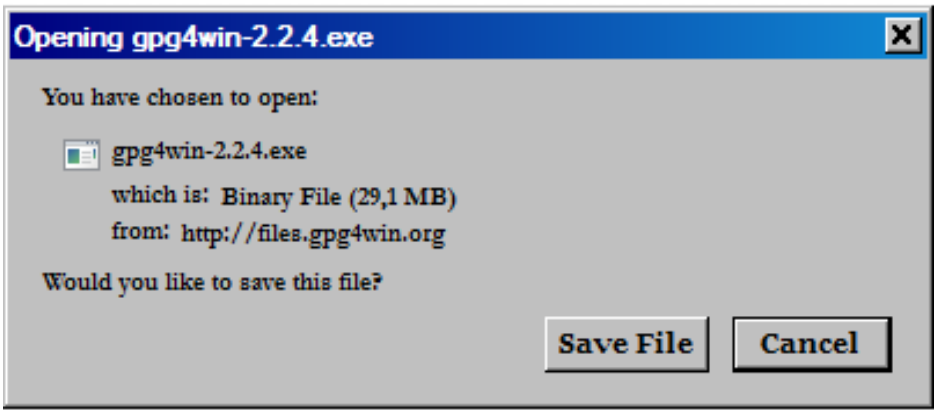
1. Non esiste una sola versione di programma PGP, ne esistono sia a pagamento che gratuite (Open Source).

   Noi abbiamo scelto di descrivere l'uso di GPG4win (http://www.gpg4win.org), perché è facile da installare su Windows. È quindi alla portata delle maggior parte degli utilizzatori di computer. Chi usa Linux o Apple deve scegliere un programma PGP adatto, ma molte delle indicazioni date in queste istruzioni gli saranno utili.

   Il file per installare il programma si trova al seguente indirizzo internet: http://www.gpg4win.org/download.html

   Quando si apre la pagina fate click su **Gpg4win 2.2.4** nell'area verde

2. Il Browser vi chiede se eseguire o salvare il file **gpg4win-2.2.4.exe**, come mostra l'immagine che segue (esempio con Firefox).



Fate click su "Save file".

3. Una volta salvato il file, possiamo iniziare l'installazione del programma.

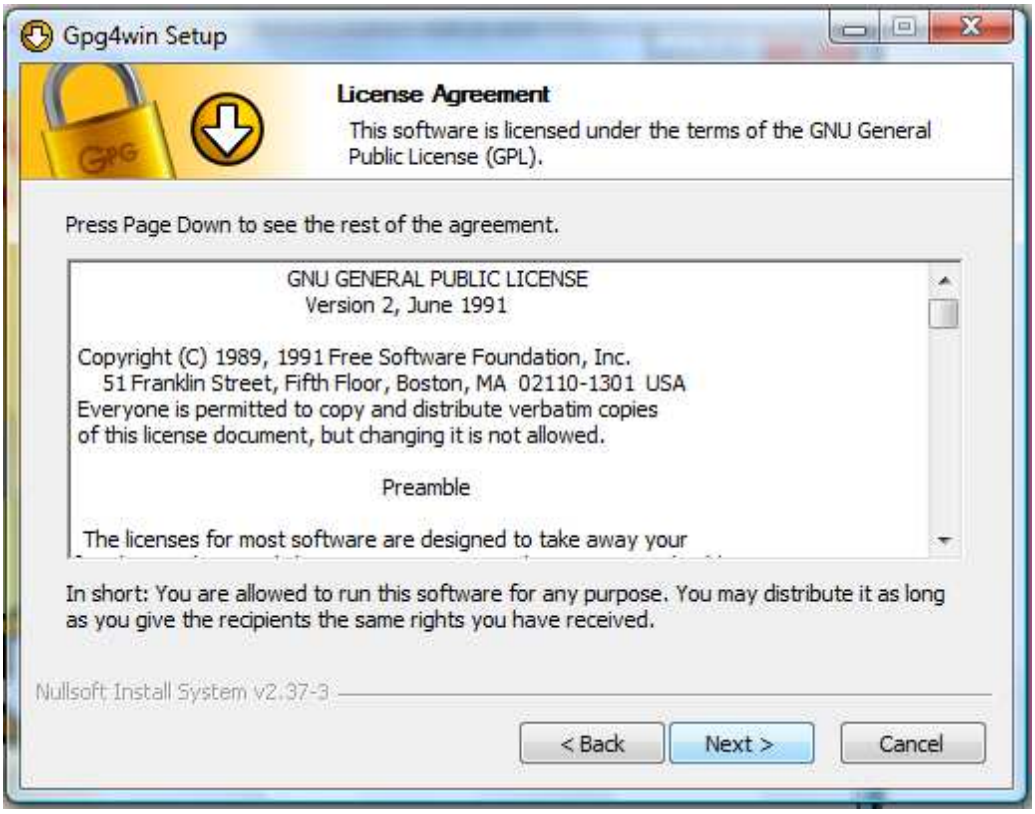
   Aprite la cartella in cui avete registrato il programma **gpg4win-2.2.4.exe**. L'immagine che segue mostra come appare l'icona del programma. Fate doppio click sull'icona per avviare il programma che installerà PGP.

4. Appena avviato, il programma vi chiederà di scegliere quale lingua deve utilizzare per i menu e i messaggi del programma: scegliete l'inglese. Vi consigliamo questa scelta perché le istruzioni che seguono sono basate sui menu e finestre con messaggi in inglese. Purtroppo l'italiano non è disponibile.

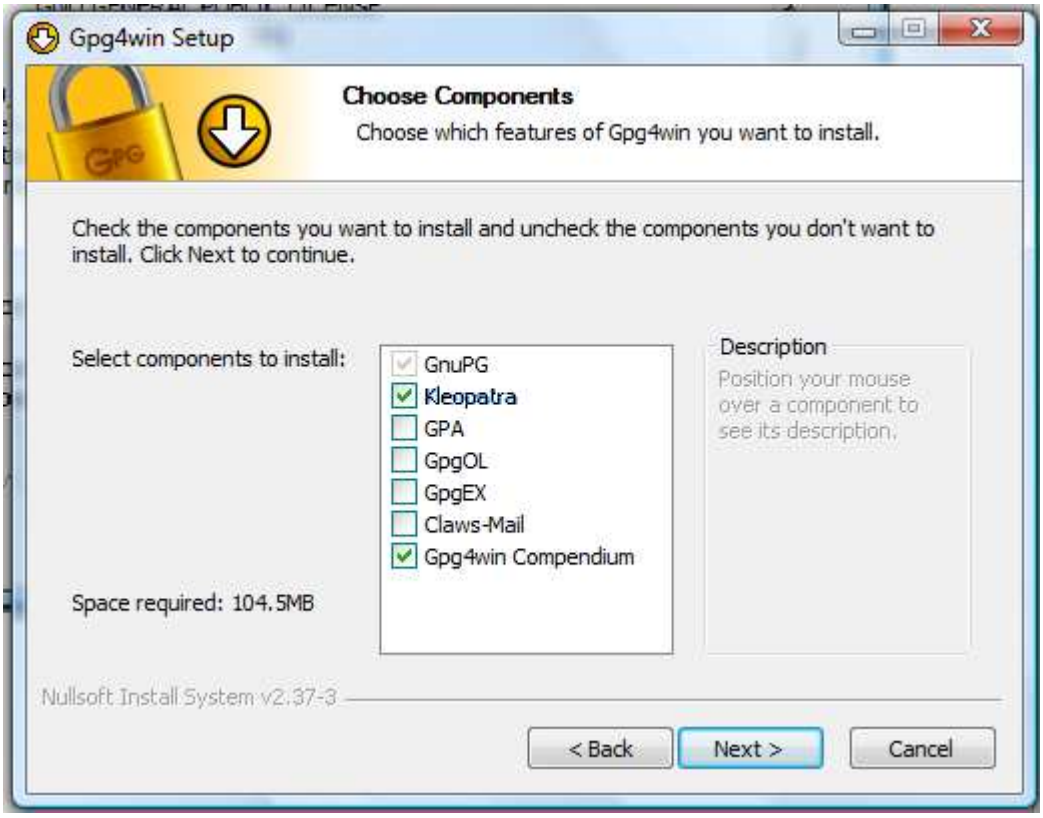
   L'immagine che segue mostra la finestra *Installer Language* da cui selezionare la lingua d'uso: fate click su OK per confermare la scelta.

Nell’immagine che segue, è mostrata la finestra che vi si presenta: fate click su **Next >**.

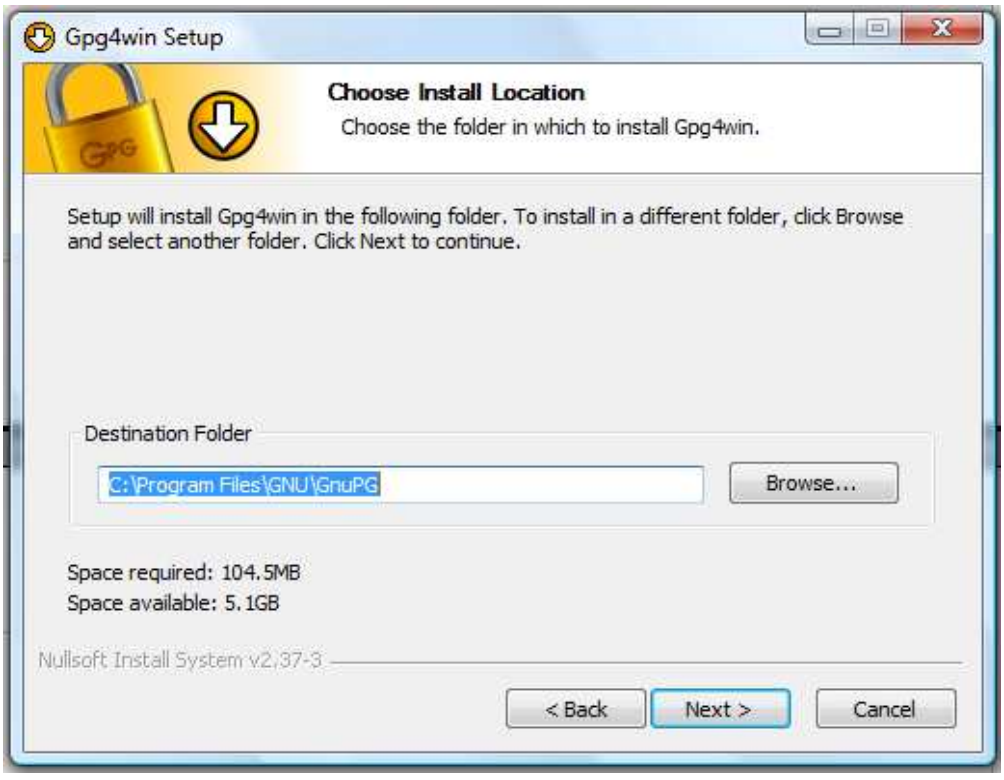
Nell’immagine che segue, è mostrata la finestra che vi si presenta: fate click su **Next >**.



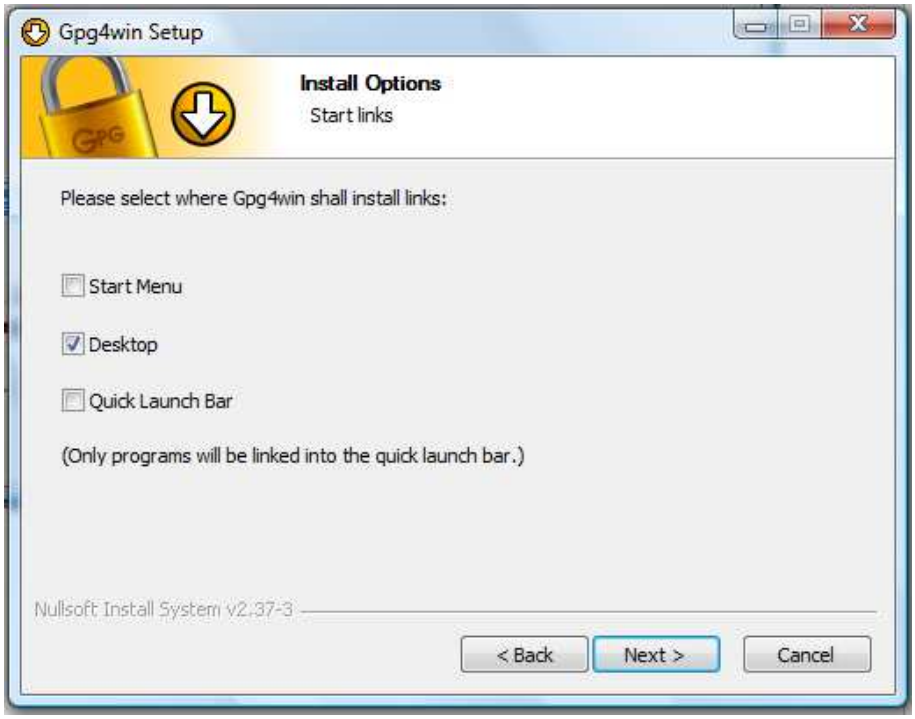
5. Dopo la finestra di presentazione della licenza d'uso, vi appare una finestra da cui scegliere quali componenti installare. Attivate solo le voci Kleopatra e Gpg4win Compendium, come nell'immagine che segue e fate click su **Next** >.



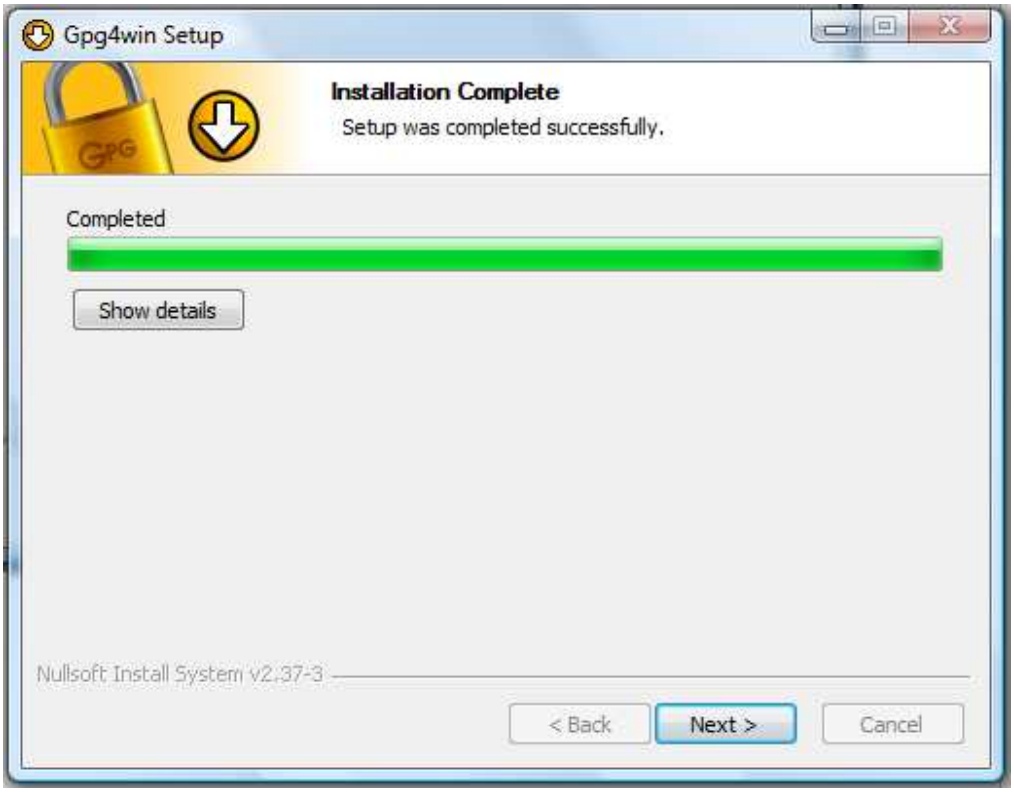
6. Abbiamo scelto di installare solo il minimo indispensabile per l'uso del PGP. Gpg4win Compendium comprende il manuale in inglese di questa versione di PGP.**(2)** Gli altri componenti sono descritti sul sito http://www.gpg4win.org.
7. Nell'immagine che segue, appare l'indicazione di dove verrà installato il programma Kleopatra (Destination Folder): fate click su **Next** >.



8. Nell'immagine che segue, è mostrata la nuova finestra che vi si presenta: attivate solo la voce **Desktop**.
   Facendo questa scelta il programma di installazione crea sulla vostra scrivania solo l'icona di Kleopatra. Questa scelta rende l'installazione di PGP meno visibile di quanto lo sia una installazione standard. Per la cronaca, Kleopatra è il programma che vi permetterà di usare PGP. Dopo l'installazione, l'icona comparsa sulla scrivania può essere spostata in una qualsiasi cartella. Fate click su **Next >** per continuare l'installazione.



9. Quella precedente era l'ultima scelta da eseguire: il programma inizia l'installazione, le due immagini che seguono mostrano la fase iniziale e finale del processo dell'installazione.
   L'immagine che segue mostra la finestra che indica la fine dell'installazione, fate click su **Next >**.



10. Nell'immagine che segue, è mostrata la nuova finestra che vi si presenta: attivate la voce **Root cetificate defined or skip configuration** e fate click su **Next >**.

11. Di seguito l'ultima finestra del programma di installazione. Fate click su **Finish**: il programma si chiude e vi apparirà un testo in inglese in cui sono descritte le caratteristiche del programma appena installato.

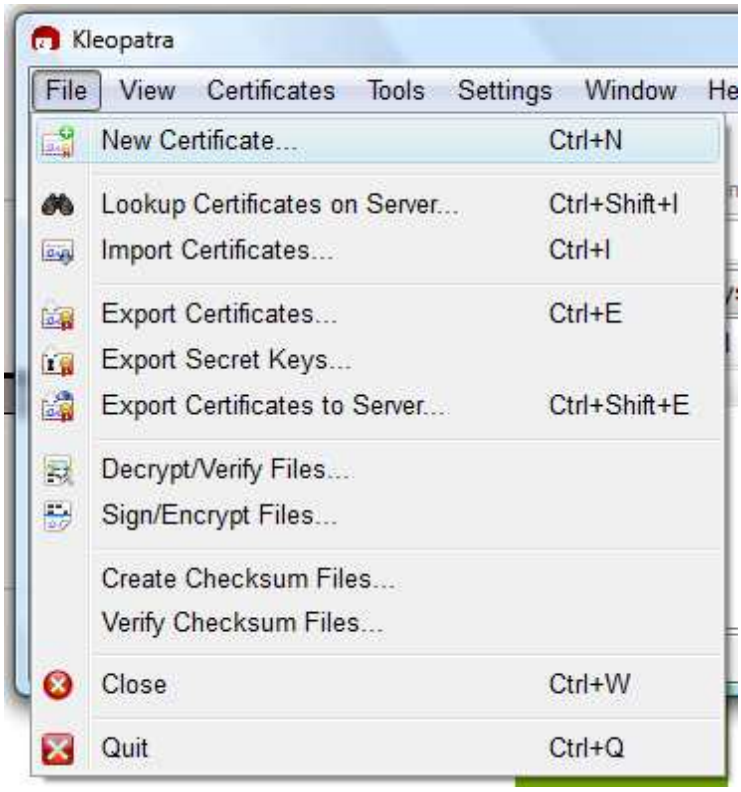
Chiudete il testo in inglese. A questo punto il programma di installazione ha finito il suo compito.

Sulla scrivania del computer apparirà l'icona del programma Kleopatra. I capitoli che seguono ne illustrano l'uso.

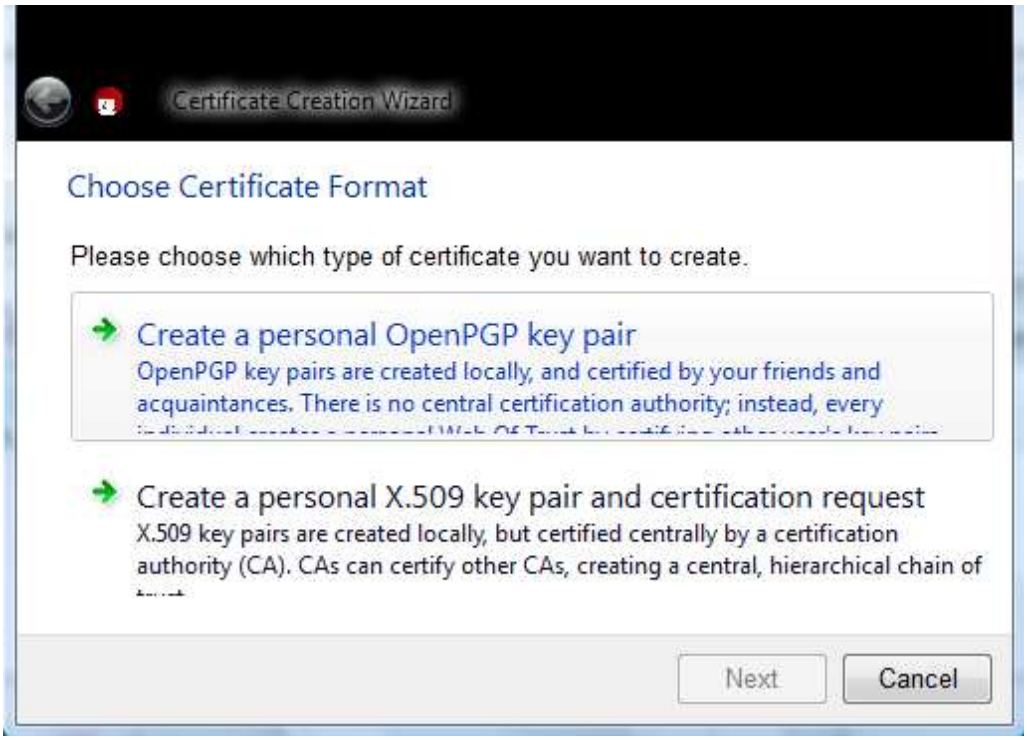
3. Creare la propria chiave privata e pubblica

1. Prima di iniziare a leggere la descrizione in dettaglio, è bene sapere che Kleopatra è la plancia di comando di PGP.
   Vale a dire che è stata creata per inviare dei comandi al programma PGP, ma sopratutto per semplificare il suo uso.
   Questo capitolo vi mostra come costruire la vostra coppia di chiavi (**privata** e **pubblica**). Come detto nel primo capitolo, questa coppia di chiavi vi permette di stabilire uno scambio di file riservati, tra voi e un qualsiasi corrispondente, senza bisogno di accordi diretti. La sola condizione per chi voglia inviarvi un documento riservato è conoscere **solo** la **vostra chiave pubblica**. Ho evidenziato "solo" perché è la **vostra chiave privata** che garantisce la riservatezza delle comunicazioni e questa **non deve essere a conoscenza di nessuno tranne voi!!!**
   Ecco la descrizione di come si costruisce la coppia di chiavi.
   L'immagine che segue vi mostra l'aspetto dell'icona del programma Kleopatra.
   Fate click due volte su di essa per avviare il programma Kleopatra.

   Il programma si apre. Dal menu file scegliete la voce **New Certificate**.



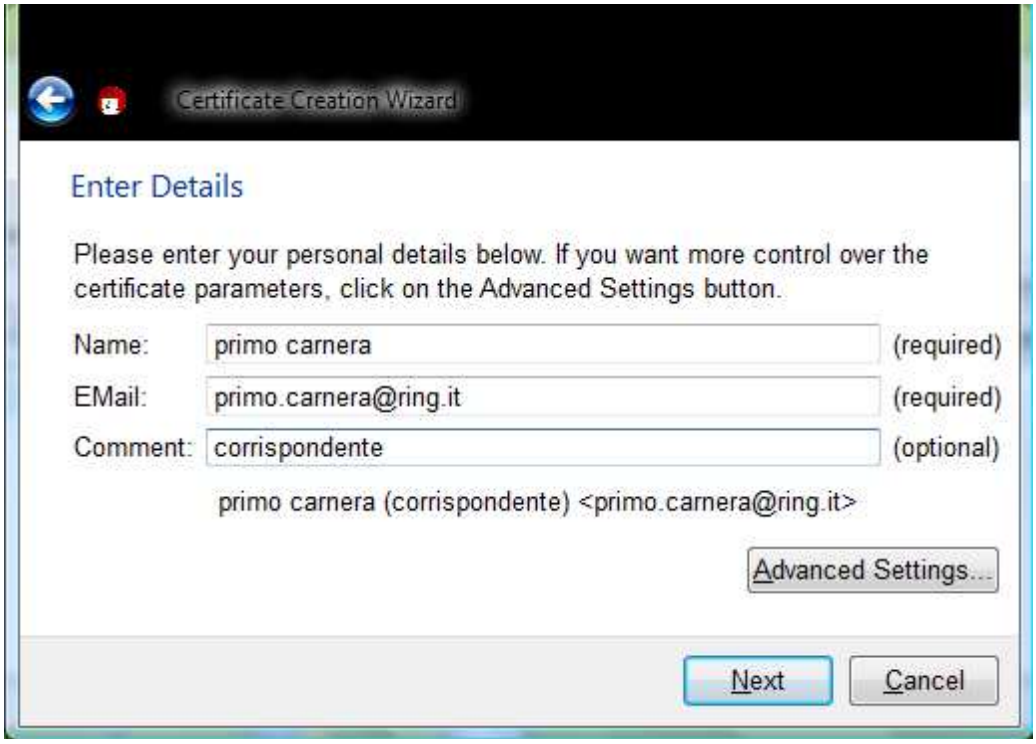
2. Nell'immagine che segue, è mostrata la finestra che vi si presenta *Certificate Creation Wizard*. Fate click su "Create a personal OpenPGP key pair".



Si apre nella finestra un modulo, compilatelo. Per illustrare come fare, adotto dati di fantasia.

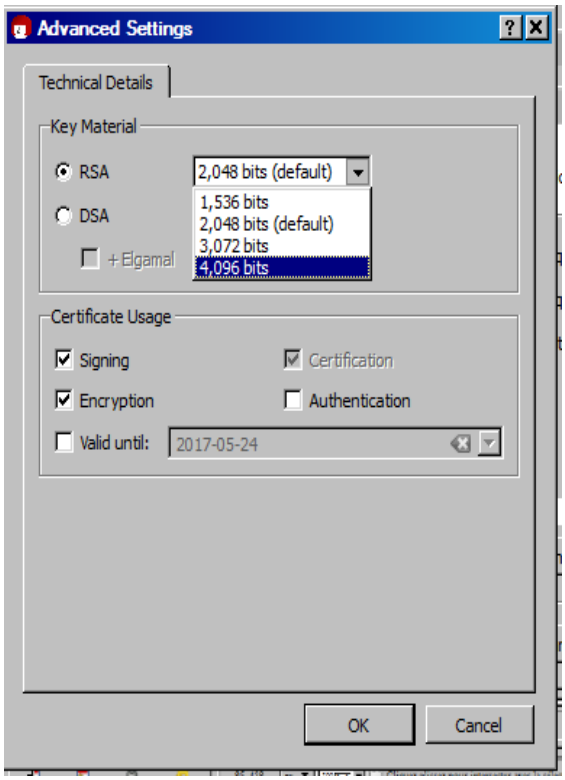
3 ATTENZIONE QUI!

Se volete che tutti i futuri utenti della vostra chiave pubblica sappiano chi è il titolare della chiave, mettete i vostri veri dati. Se invece volete che lo sappiano solo a quelli a cui voi lo comunicate, mettete anche voi dati di fantasia.

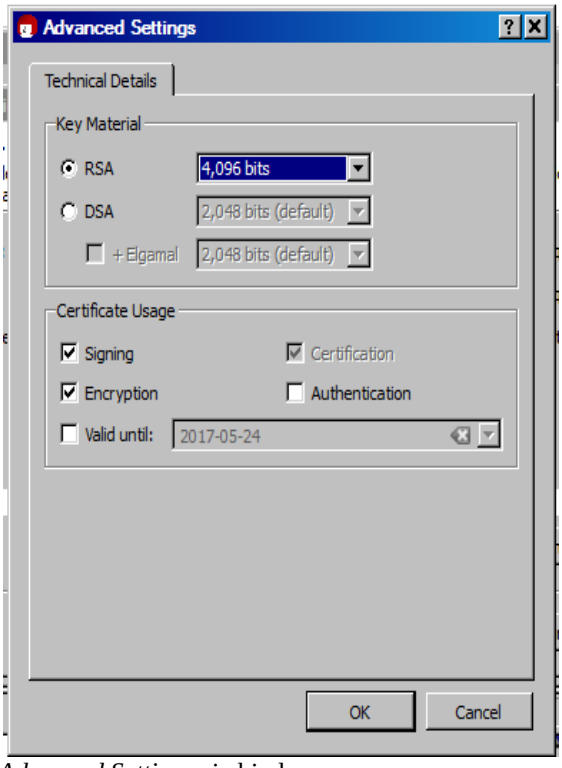


Dopo aver compilato il modulo fate click su **Advanced Settings...**. Nell'immagine che segue, è mostrata la finestra *Advanced Settings.*

4 Nella finestra *Advanced Settings* vi viene proposta l'opzione *RSA 2,048 bits (default)*. Modificatela facendo click sul triangolino nero che punta verso il basso. Dal menu che vi si presenta, selezionate *4,096 bits* (quanto maggiore è questo valore, tanto migliore è il livello di protezione dei dati).

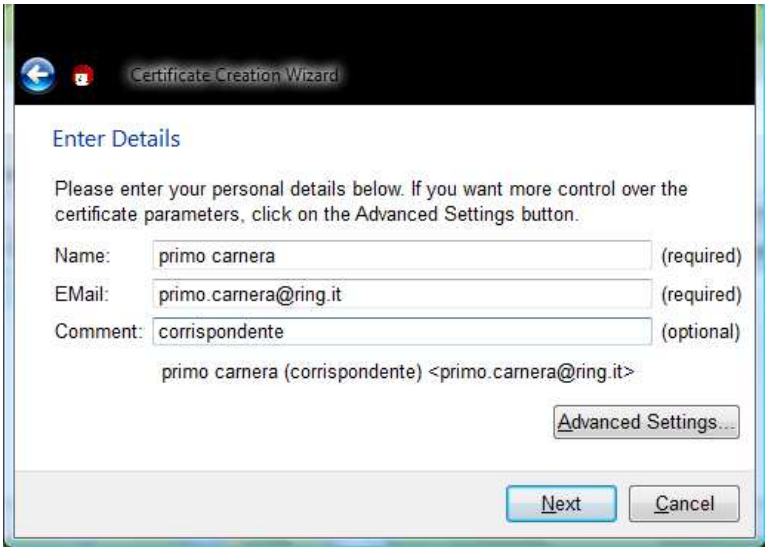


5. Qui di seguito è mostrata la finestra *Advanced Settings* con i valori corretti per la creazione della vostra chiave privata e pubblica. Se sono differenti, modificateli in modo che siano uguali a quelli mostrati nell'immagine.



Fate click su **OK**: la finestra *Advanced Settings* si chiude.

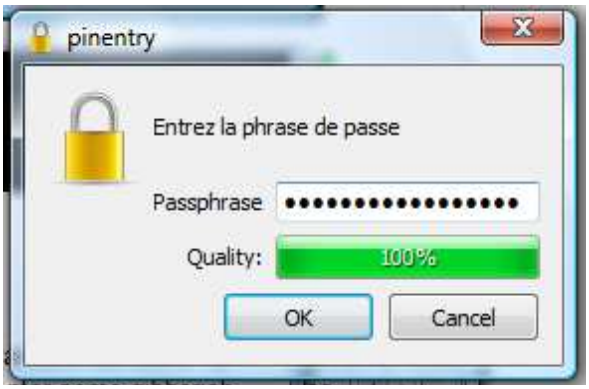
6. Tornate quindi alla finestra con il modulo appena compilato, che è rimasta aperta e fate click su **Next**.



Si apre una finestra con il riepilogo dei dati inseriti, come mostrato nell'immagine che segue. Fate click su **Create Key**.

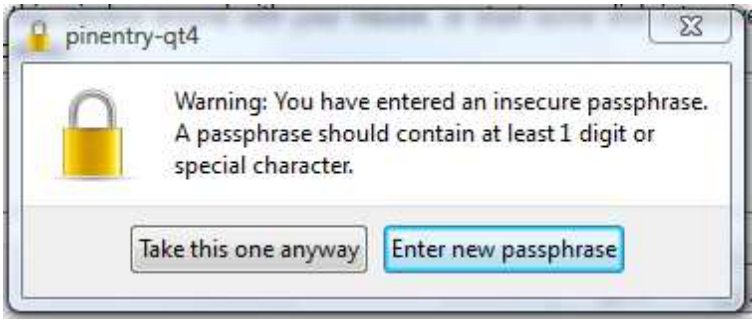
7. Si apre la finestra *pinentry*: inserite una password con almeno una cifra e lunga almeno 9 caratteri.

8 Se la password inserita è sufficientemente sicura, la barra **Quality** diventa verde, come mostra l'immagine che segue e la percentuale indicata è 100% se la password è adeguata**(3)**.



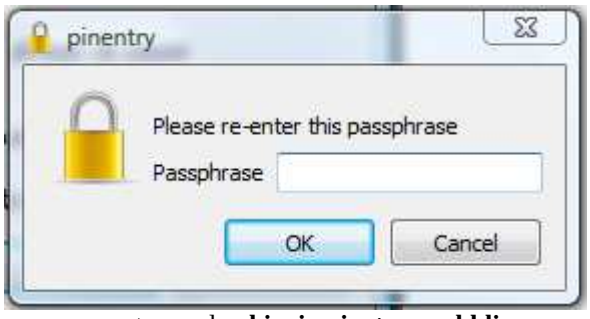
Fate click su **OK**.

9. Se la password inserita non contiene almeno una cifra o è troppo semplice, appare una finestra di avvertimento in cui vi viene richiesto di utilizzare almeno una cifra nella password, come viene mostrato nell'immagine che segue. Riportatevi alla nota 3 di queste istruzioni per utilizzare una password adeguata.



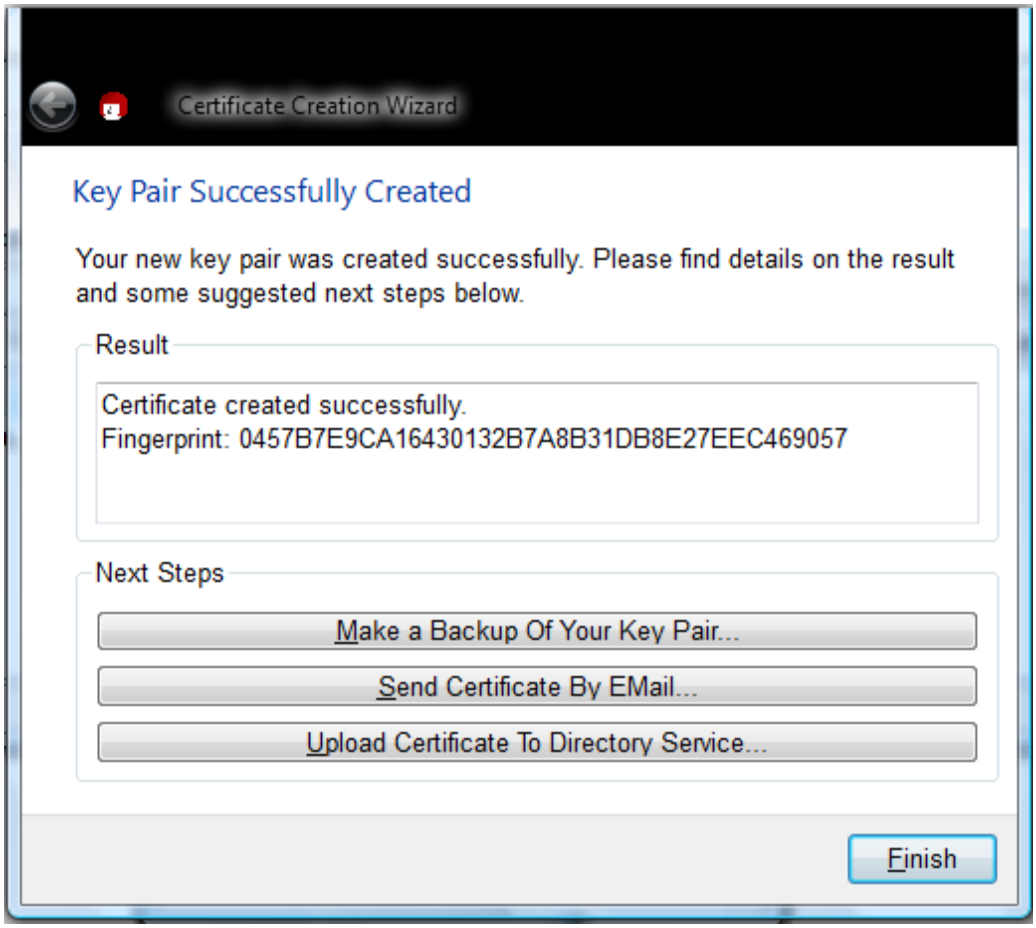
Fate click su **Enter new passphrase**: vi si ripresenta la finestra *pinentry*. Inserite una password con almeno una cifra e fate click su **OK**.

10 Vi si ripresenta la finestra *pinentry*: vedi l'immagine che segue. Inserire la nuova password per la verifica e fate click su **OK**.



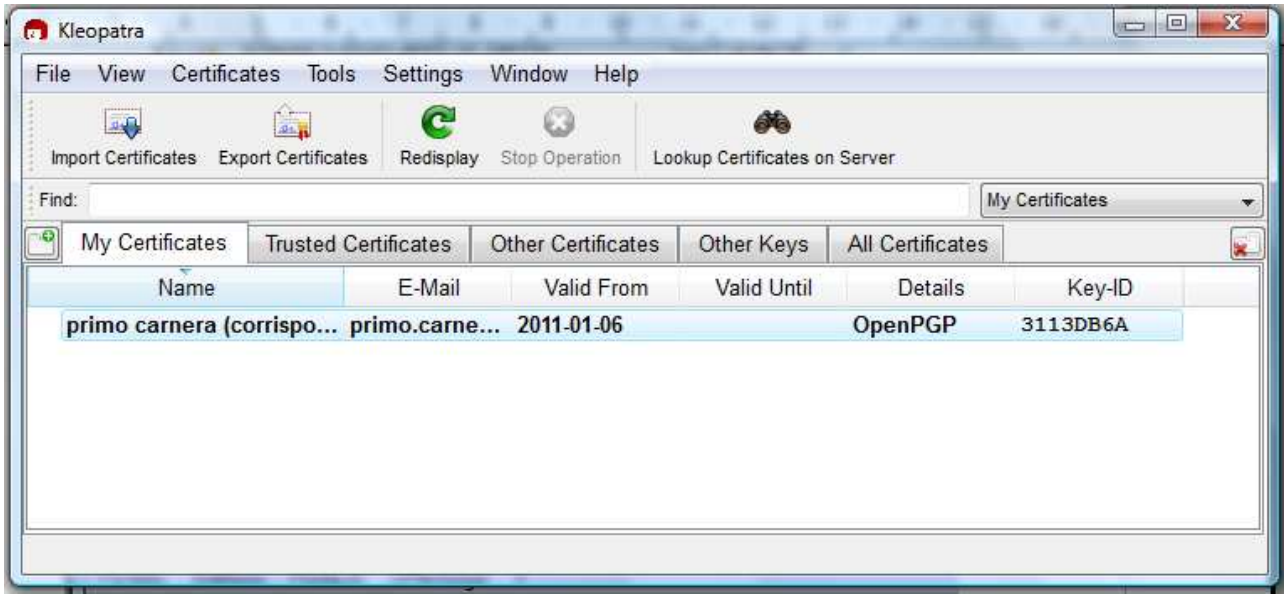
11 Nota bene che questa password serve a mantenere le **chiavi privata e pubblica** nascoste sul vostro computer. Questa password non partecipa allo scambio di messaggi tra voi e il vostro corrispondente. Questa password deve essere conservata in modo discreto, non deve essere diffusa.

Se la password è adeguata, vi appare una finestra, mostrata nell'immagine che segue, in cui viene indicato che la coppia di chiavi privata e pubblica è stata creata (*Key Pair Successfully Created*).



Fate click su **Finish**.

12. La finestra del programma Kleopatra ora vi mostra nella scheda *My Certificates* in grassetto la voce **primo carnera (corrispondente)**, come mostrato nell'immagine che segue.



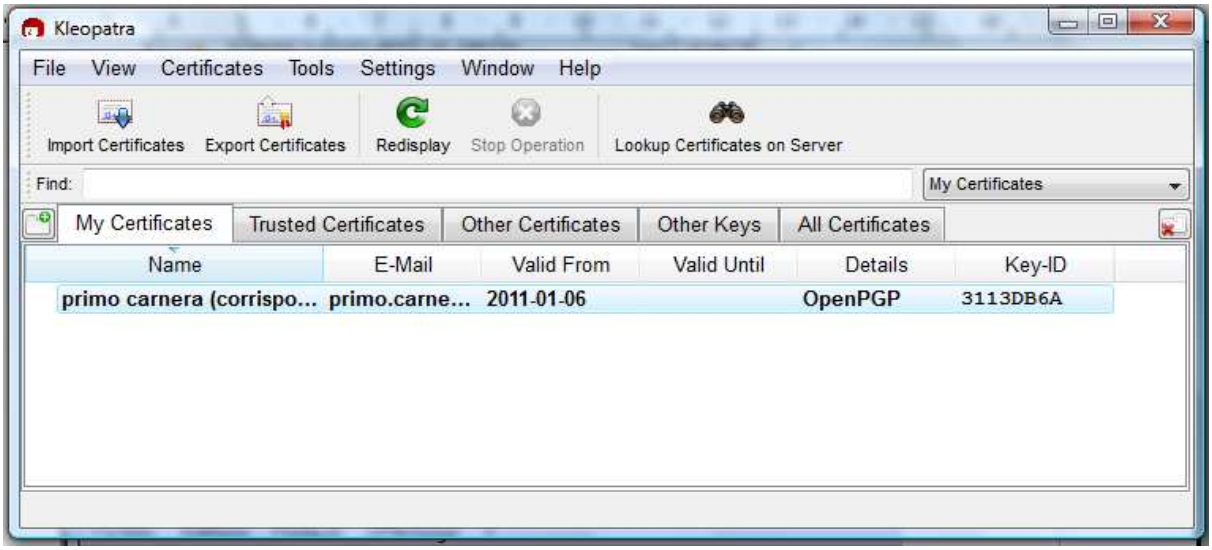
13. Questa sequenza di operazioni ha creato la vostra coppia di **chiavi privata e pubblica**. La *password* che avete utilizzato per creare le chiavi, vi sarà richiesta ogni volta che dovrete fare delle operazioni di criptazione o decriptazione. Questa *password* è un'ulteriore difesa per i vostri dati. Questa *password* è propria del programma Kleopatra e permette di conservare le vostre chiavi in modo criptato sul vostro computer.
14. Questa stessa operazione, la creazione della vostra coppia di chiavi privata e pubblica, l'ha fatta anche il Partito.
    La creazione di una coppia di chiavi è necessaria per poter corrispondere con un'altra persona che usa il sistema PGP.
    Vedremo più avanti che inviando **la vostra chiave pubblica** al Partito, voi permettete al Partito di inviare a voi messaggi riservati. Da parte sua il Partito mette a disposizione la propria chiave pubblica sul sito. Con essa voi siete in grado di inviare al Partito i messaggi riservati. Nel capitolo 5. viene illustrata la procedura per inviare al Partito o a qualunque altro corrispondente la **vostra chiave pubblica**. Vi ricordo che è proprio la diffusione della chiave pubblica che permette a tutti gli altri corrispondenti di inviare messaggi riservati a voi. Voi **non potete mandare messaggi riservati se non conoscete la chiave pubblica della persona a cui volete inviare un messaggio riservato** con il sistema PGP

4. Esportare la propria chiave privata per conservarla

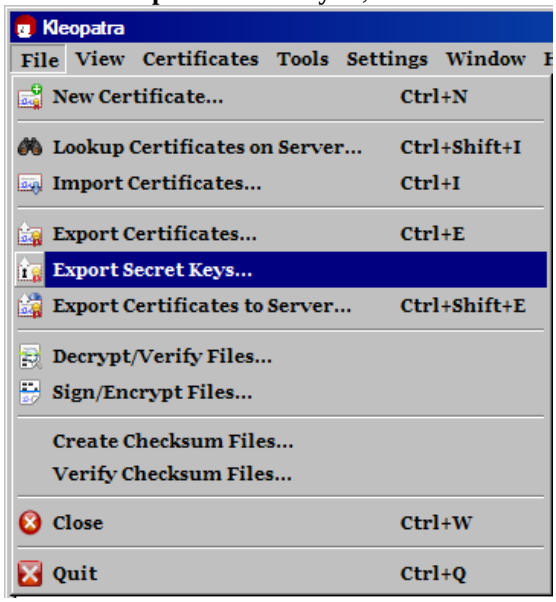
Ora che la vostra coppia di chiavi privata e pubblica è stata creata, avete posto le basi per farvi contattare in modo riservato dal Partito.

1. Prima di continuare **è d'obbligo fare una copia di sicurezza della vostra coppia chiave privata e pubblica** e conservare questa copia su un altro computer, chiavetta o disco esterno. Se la perdete per un guasto al computer o il suo furto, rischiate di compromettere la vostra corrispondenza o di non poter più recuperare un vostro archivio criptato. Se occorre, potrete importare la coppia in Kleopatra dopo aver installato Kleopatra su un altro computer.

   Per fare la copia di sicurezza della vostra coppia chiave privata e pubblica, aprite Kleopatra e evidenziate la chiave di cui volete ottenere una copia. Aprite la linguetta *My Certificate*,

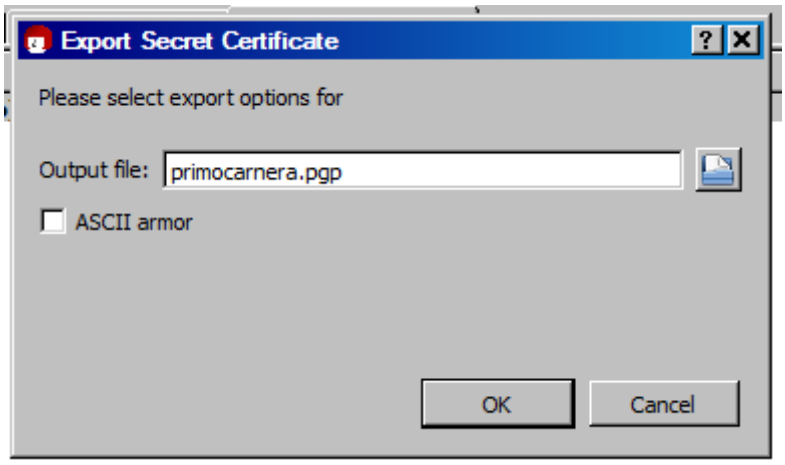


fate click sul menu *File* e selezionate la voce **Export Secret Keys...**, come mostrato nell'immagine che segue.



Dopo aver selezionato la voce **Export Secret Keys...** vi appare la finestra *Export Secret Certificate* mostrata nell'immagine che segue.

2. Nel campo, inserite un nome che vi aiuti a ricordare che chiave è contenuta nel file che state per registrare.
   Poi fate click sul pulsante a destra del campo *Output file:*, quello con l'icona della cartella aperta.



3. Dopo aver fatto click sul bottone con l'icona della cartella aperta, si apre la finestra di sistema che vi chiede dove registrare il file contenente la vostra chiave privata. Salvatelo su una chiavetta USB o disco esterno, in modo che se il vostro computer va fuori servizio, reinstallando Kleopatra su un altro computer potrete importala nella stessa maniera con cui si importano le chiavi pubbliche. Tale procedura è descritta al capitolo 6.
   Il file così registrato è criptato e per essere utilizzato vi verrà richiesta la password che è la stessa che avete usato per creare la vostra coppia di chiavi privata e pubblica come descritto al capitolo 3. di queste istruzioni.

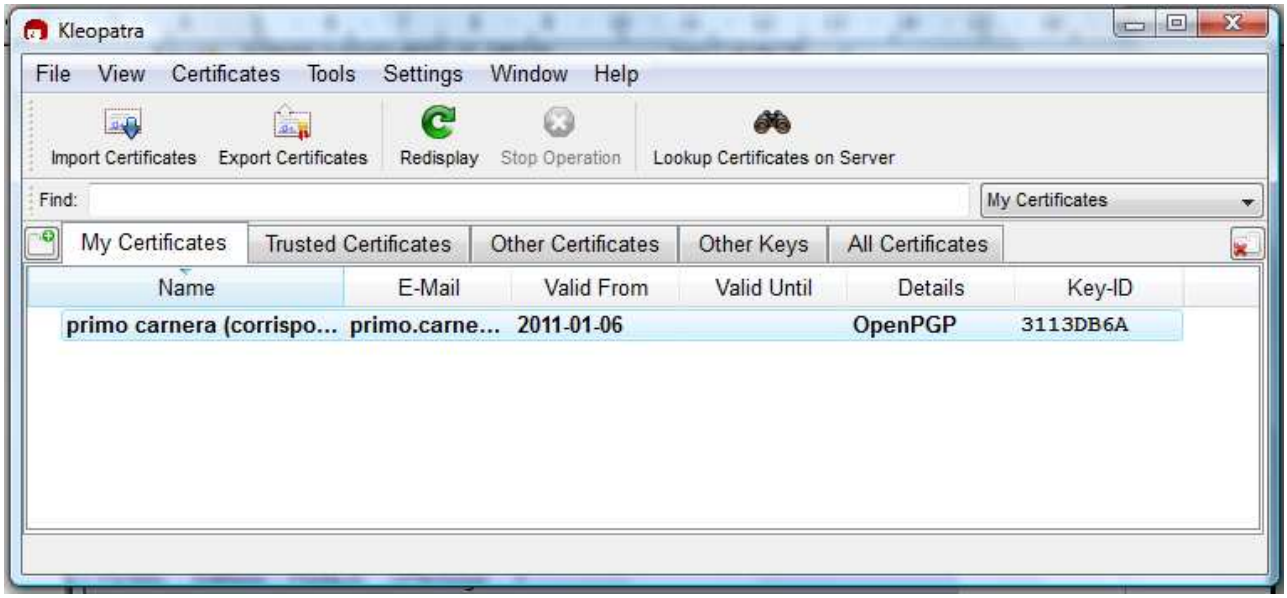
5. Esportare la vostra chiave pubblica per comunicarla a terzi

Nel capitolo seguente il 6. spieghiamo come inviare un messaggio criptato al Partito o a un altro corrispondente. Prima di inviare un messaggio dobbiamo fare in modo che il Partito o l'altro corrispondente sia in grado di rispondere subito a voi con il sistema PGP.

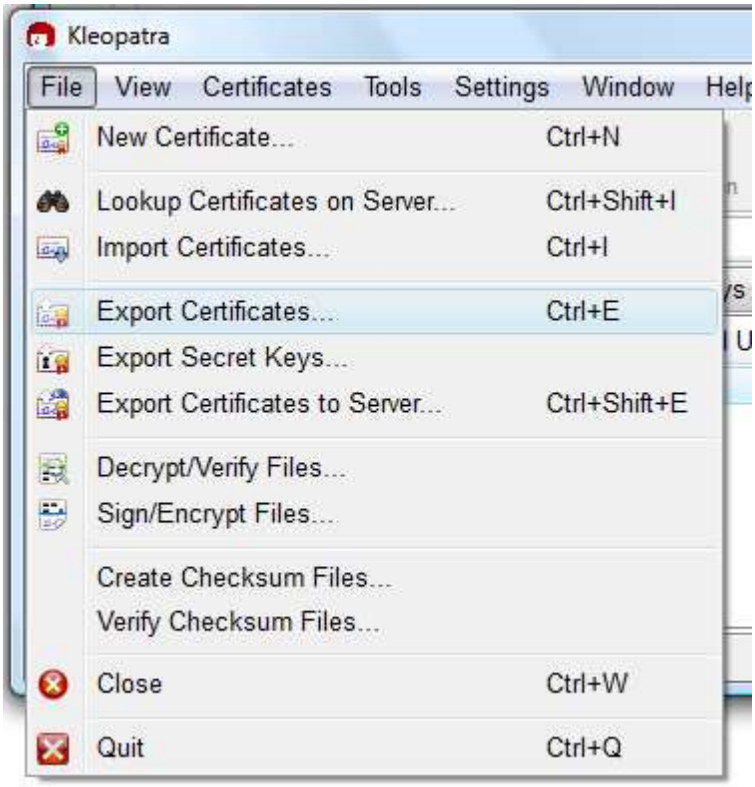
1. Per farlo dovete esportare la vostra chiave pubblica e inviarla al Partito o a un altro corrispondente. Solo conoscendo la vostra chiave pubblica il Partito o un altro corrispondente sono in grado di criptare un messaggio con la vostra chiave pubblica. Il messaggio criptato con la vostra chiave pubblica è decifrabile solo da voi.

2. **Questa operazione richiede attenzione, bisogna stare attenti a non confondersi tra chiave privata e pubblica:** la chiave pubblica è differente dalla chiave privata; la chiave pubblica deve essere messa a disposizione del vostro corrispondente separatamente da quella privata.
   L'operazione di esportazione della vostra chiave pubblica corrisponde a dividere la coppia chiave privata / chiave pubblica.
   Se vi sbagliate e inviate la chiave privata invece di quella pubblica, benché essa sia utilizzabile solo conoscendo la password con cui l'avete creata (vedi capitolo 3.), la protezione dei vostri dati diventa debole, poiché per gli spioni ora il compito diventa trovare la password (un compito incomparabilmente più facile che cercare di decriptare un file PGP). Se commettete questo errore il sistema PGP a questo punto non fa più argine agli spioni: dovete creare una nuova coppia di chiave privata e pubblica.
   Quindi seguite con attenzione le istruzioni che seguono.

3. Per inviare la vostra chiave pubblica ad un corrispondente evidenziate la vostra coppia di chiave privata e pubblica (nell'esempio **primo carnera …**) nella scheda *My Certificate*. In questo caso c'è una sola voce, ma in linea di principio il programma è fatto per gestire anche più coppie di chiavi pubbliche e private.

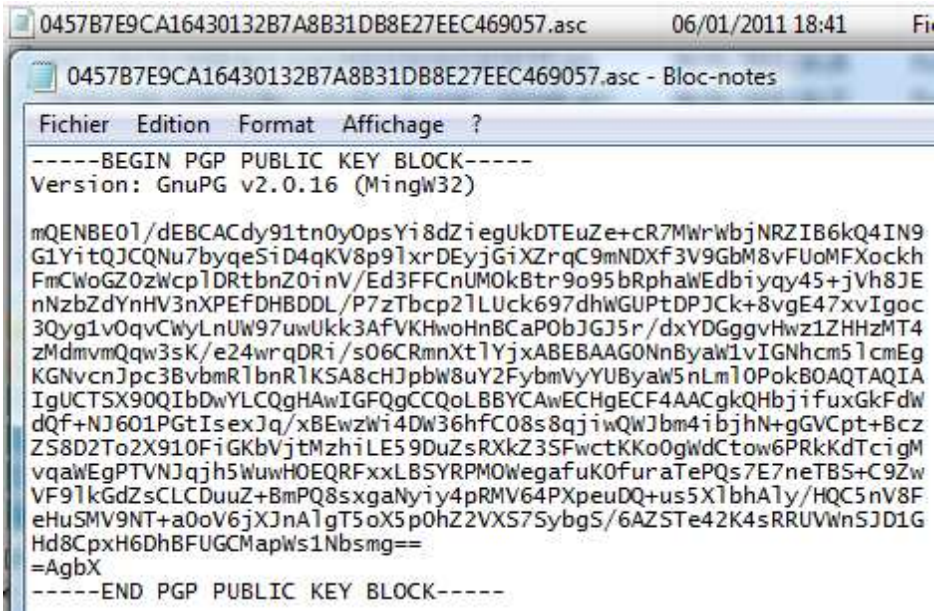


4. Dopo aver selezionato la voce "primo carnera ...", dal menu *File* di Kleopatra, scegliete la voce **Export Certificates...**, come nell'immagine che segue. Attenzione a non selezionare **Export Secret Keys …**, questa voce esporta la chiave privata che invece non deve essere a conoscenza di nessuno dei vostri corrispondenti.



5. Si apre la finestra di sistema che vi chiede dove registrare il file contenente la chiave pubblica.
   Scegliete la cartella in cui volete registrare il file e confermate la registrazione.
   Nell'immagine che segue è mostrato il file che viene registrato (il suo nome consiste di una serie di numeri e lettere con il suffisso .asc) e, se aprite il file con il programma Bloc-notes, potete vedere il suo contenuto. Come vedete, esso contiene l'indicazione che è una chiave pubblica del sistema PGP (PGP PUBLIC KEY BLOCK) e una lunga serie di

numeri e cifre (che rappresenta il famoso numero primo molto grande).



6. Inviando questo file come allegato ad un messaggio email al vostro corrispondente o mettendo a disposizione questo file sul vostro sito o blog, permetterete a tutti i vostri corrispondenti che utilizzano il sistema PGP di inviarvi messaggi riservati.

7. Il Partito ha fatto questa operazione ed espone questo file sul proprio sito per permettere a tutti di poter inviare messaggi riservati ad esso.

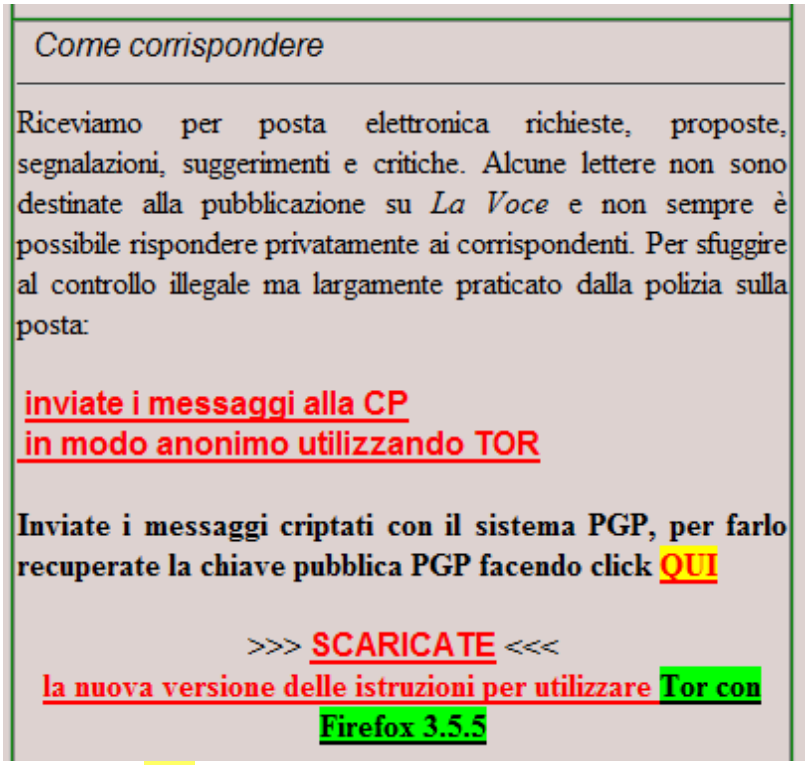
   Quando inviate il primo messaggio al Partito (procedura descritta al capitolo 6. che segue), dovete anche inviare la vostra chiave pubblica. Non inviatela così come è adesso dopo l'operazione di esportazione sopra descritta, ma criptatela con la chiave pubblica del Partito assieme al primo messaggio che inviate. Al capitolo 6. vi spiegheremo i dettagli di questo accorgimento.

6. Criptare e inviare un messaggio al Partito o a un altro corrispondente

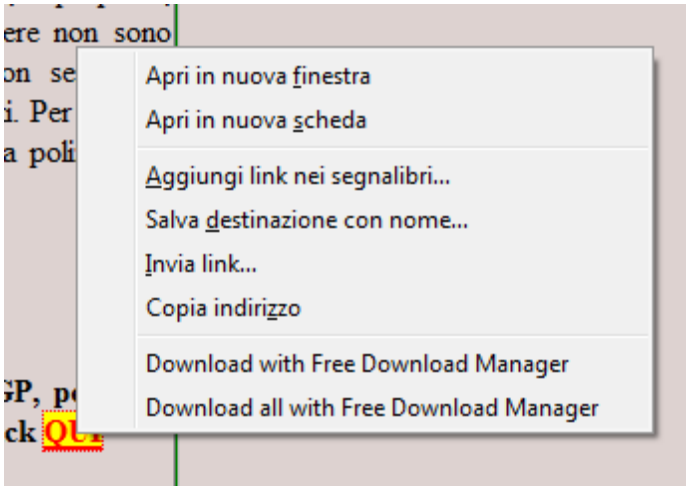
1. Prima di inviare un messaggio al Partito o a un altro corrispondente, dovete recuperare la **chiave pubblica del Partito (o del corrispondente a cui volete inviare un messaggio riservato)**.

   Se non avete ancora recuperato la **chiave pubblica del Partito,** recatevi nel sito del (n)PCI al seguente indirizzo internet:

   http://www.nuovopci.it/corrisp/risp03.html . Si apre la pagina, parzialmente mostrata nell'immagine che segue (le immagini seguenti si riferiscono a Firefox).



2. Portatevi con il mouse sul link **QUI**, schiacciate il bottone destro del mouse, vi appare, il menu contestuale mostrato nell'immagine che segue.



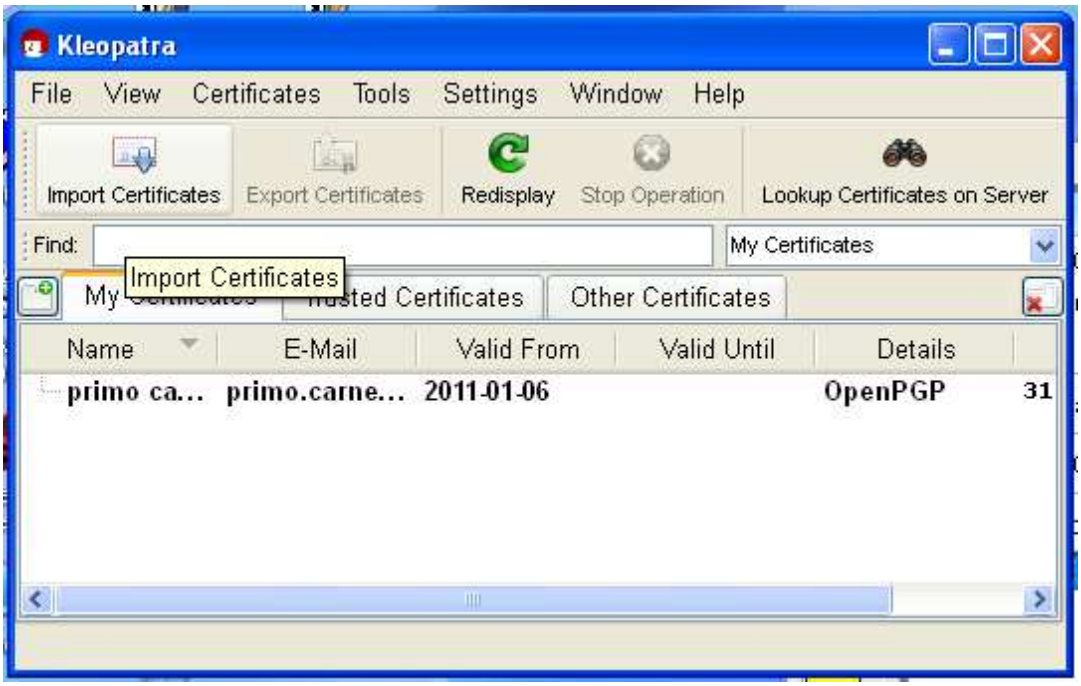
3. Scegliete la voce **Salva destinazione con nome...** . Si apre la finestra per scegliere dove registrare il file che per la cronaca si chiama: "*7435ACE5184B6A1D142993CF18BBACA7BD99C90B.asc*". Esso contiene la chiave pubblica del Partito.

4. Ora dovete importare la chiave pubblica del Partito o di un altro corrispondente utilizzando Kleopatra.

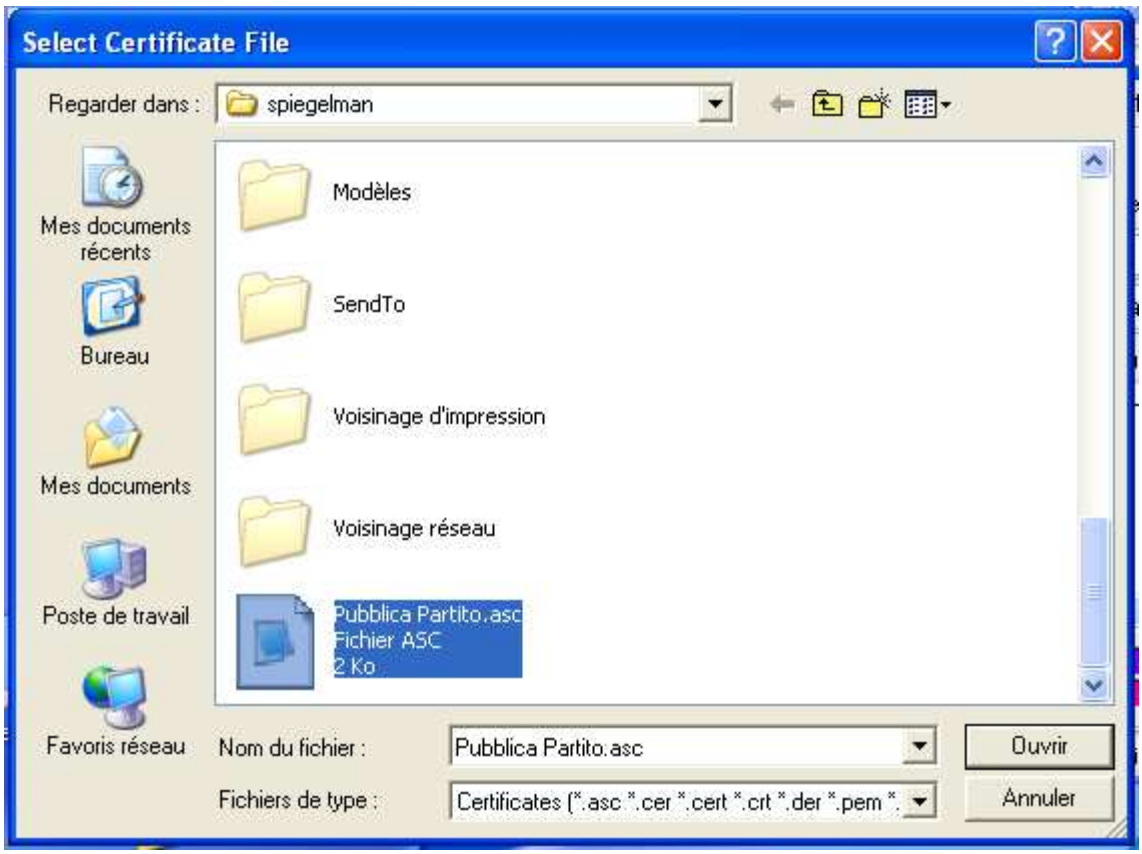
Una volta registrata la chiave pubblica del Partito sul vostro computer, avviate Kleopatra. Fate doppia click sull'icona sulla scrivania, immagine a sinistra, oppure un click, se Kleopatra è già avviato, sull'icona nella barra in basso a destra di Windows, immagine che segue.

Oppure portatevi con il mouse sull'icona sulla barra in basso a destra di Windows e scegliete la voce **Open Certificate Manager...**.

5. Si apre la finestra di Kleopatra, vedi immagine che segue: fate click sul pulsante **Import Certificate**.



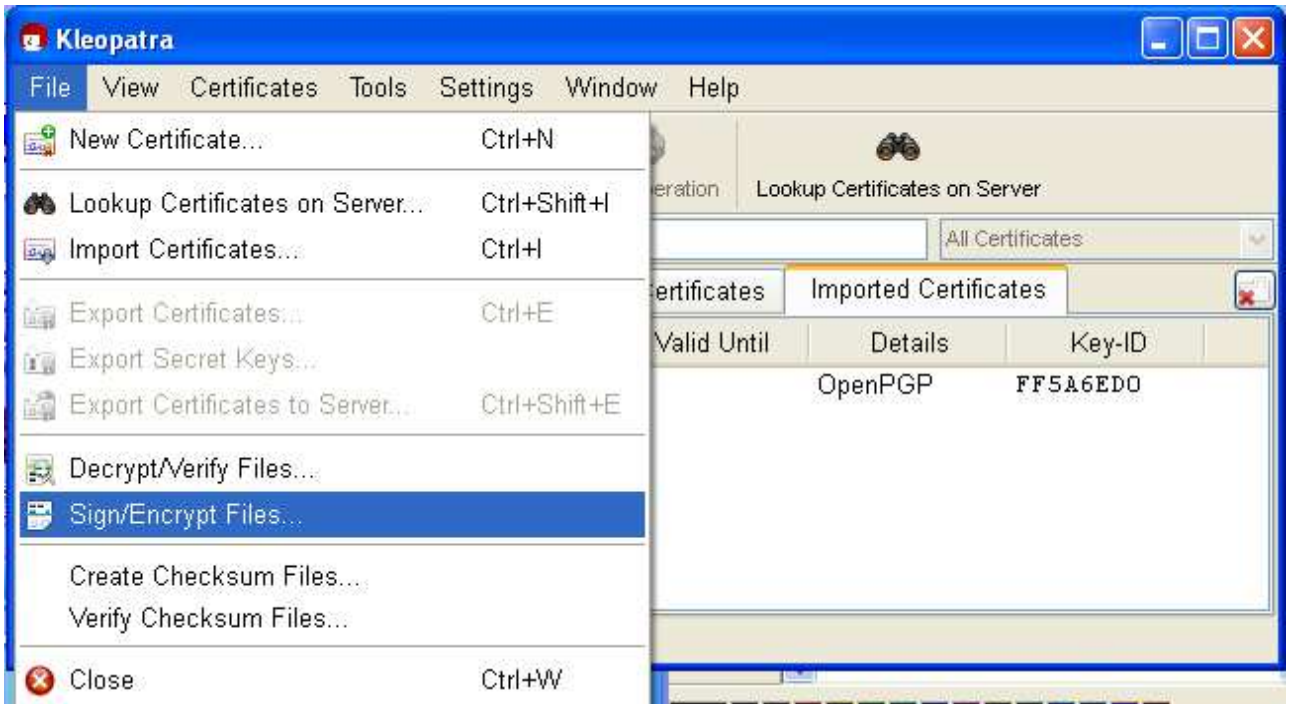
6. Dopo aver fatto click sul pulsante **Import Certificate**, si apre la finestra di sistema dalla quale potete scegliere il file che contiene la chiave pubblica del corrispondente a cui volete inviare un messaggio riservato. Nell'immagine che segue è mostrato un file .asc che contiene la **chiave pubblica del Partito**. Selezionate il file e fate click sul bottone **Apri (*Ouvrir*, nella versione francese e *Open* in inglese).**



Si apre la finestra mostrata nell'immagine che segue. Questo indica che l'operazione di importazione della chiave pubblica del vostro corrispondente è riuscita (*Imported: 1*).

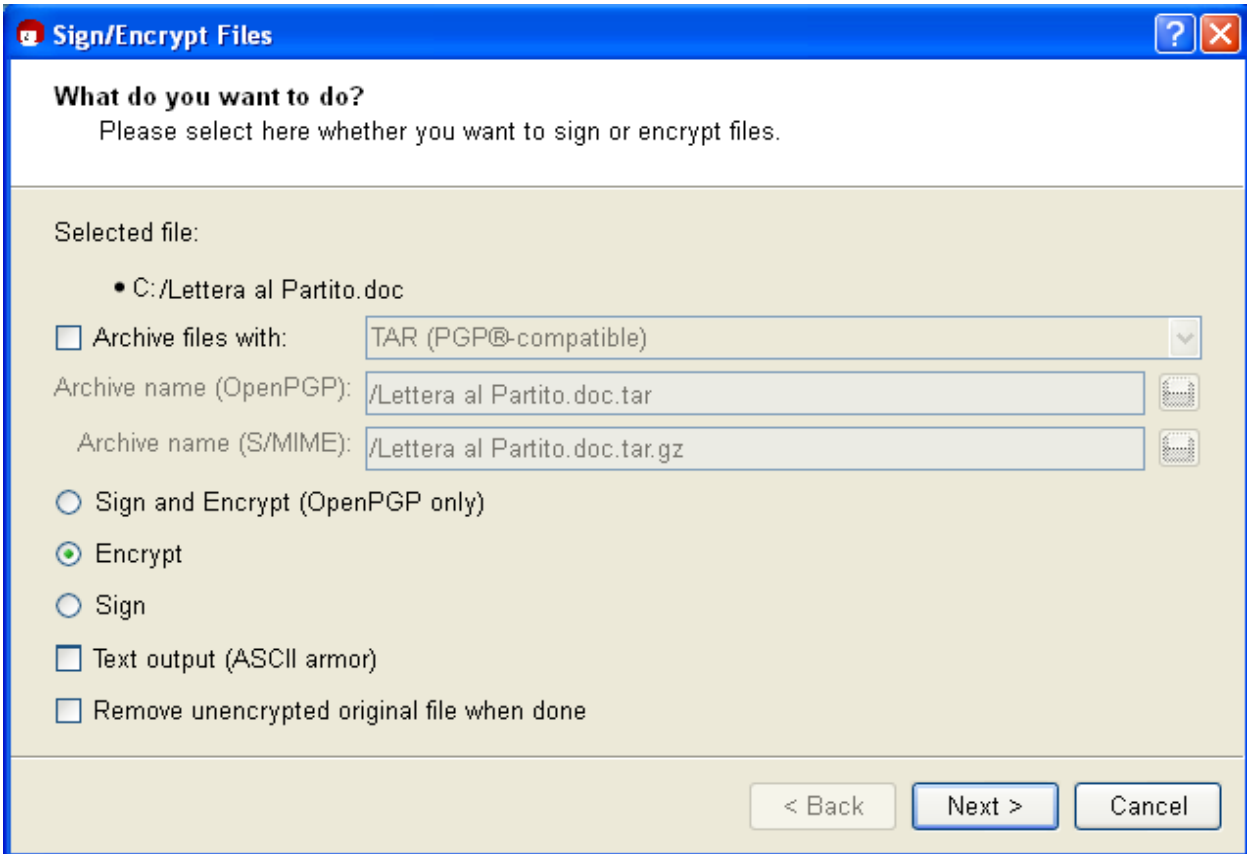
Fate click su **OK**. Se aprite la scheda *Imported Certificates*, vedrete che c'è la voce **il partito …,** a conferma del fatto che Kleopatra ha **importato la chiave pubblica del Partito**. Ora potete criptare con la chiave pubblica del Partito il messaggio riservato che volete inviare ad esso.

8. Se è la prima volta che scrivete al Partito o a un altro corrispondente, dovete assolutamente inviare insieme al messaggio anche la vostra chiave pubblica. Riunite in unica cartella il vostro messaggio e la vostra chiave pubblica (Per creare il file contenente la vostra chiave pubblica riportatevi alle istruzioni del capitolo 5.). Il file contenente la vostra chiave pubblica avrà un nome tipo: "*A1D142993CF18BBACA77435ACE5184B6BD99C90B.asc*". Selezionate i due file (il messaggio e la vostra chiave pubblica) e comprimeteli con Winzip, Winrar o 7zip (i tre programmi di compressione più diffusi e gratuiti per Windows). Otterrete un unico file con il suffisso .zip, .rar o .7z a secondo del programma di compressione che avete usato. Questo è il file che dovrete criptare usando la chiave pubblica del Partito. Per far questo dovete scegliete dal menu *File* la voce **Sign/Encrypt Files...**

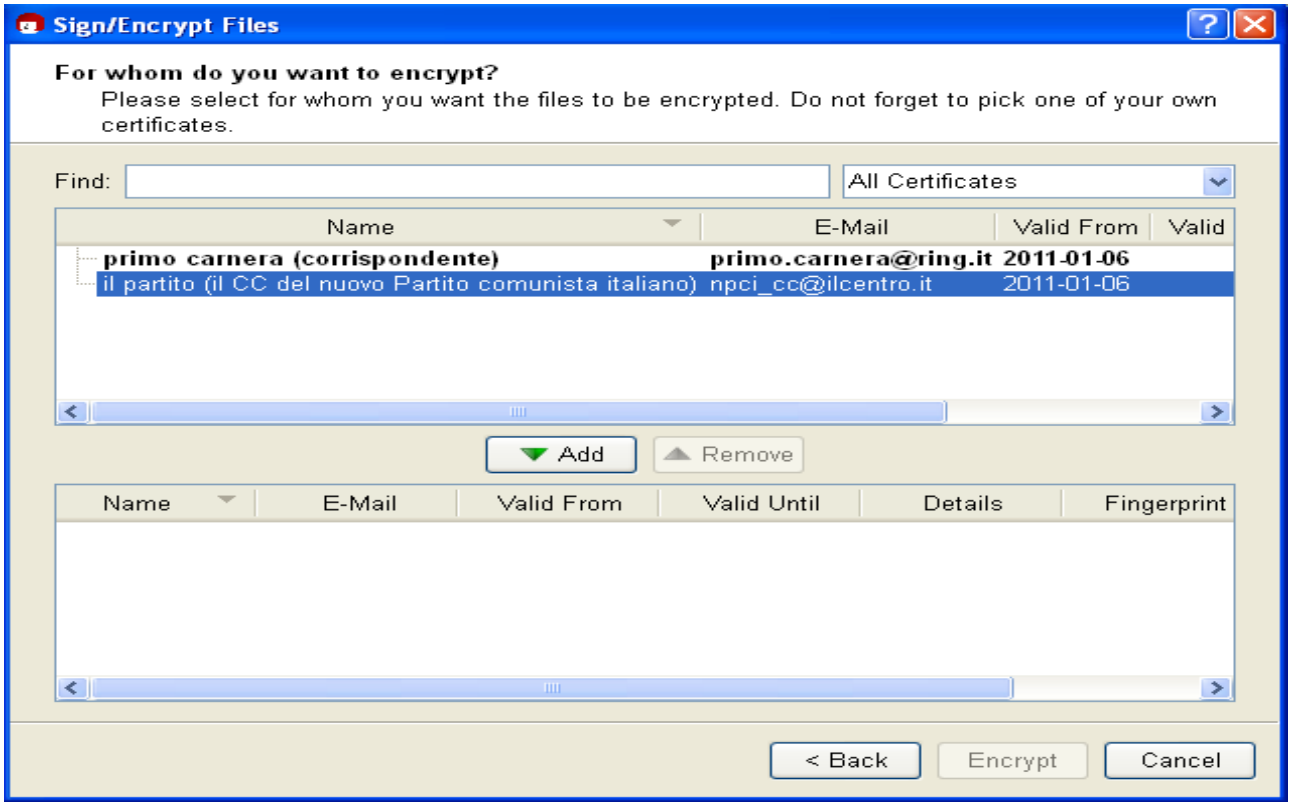


9. Si apre la finestra di sistema per scegliere il file da criptare. Selezionatelo e fate click su **Apri** *(Ouvrir, Open a seconda dei sistemi operativi)*, come mostrato nell'immagine che segue. Nell'esempio criptiamo il file "Lettera al Partito.doc", ma potrebbe anche essere il file "Lettera al Partito.zip" che contiene sia il messaggio che la vostra chiave pubblica, se è la prima volta che inviate il messaggio al Partito od ad un altro corrispondente. Se avete già inviato la vostra chiave pubblica allora basta criptare il documento "Lettera al Partito.doc" come nell'esempio che segue.

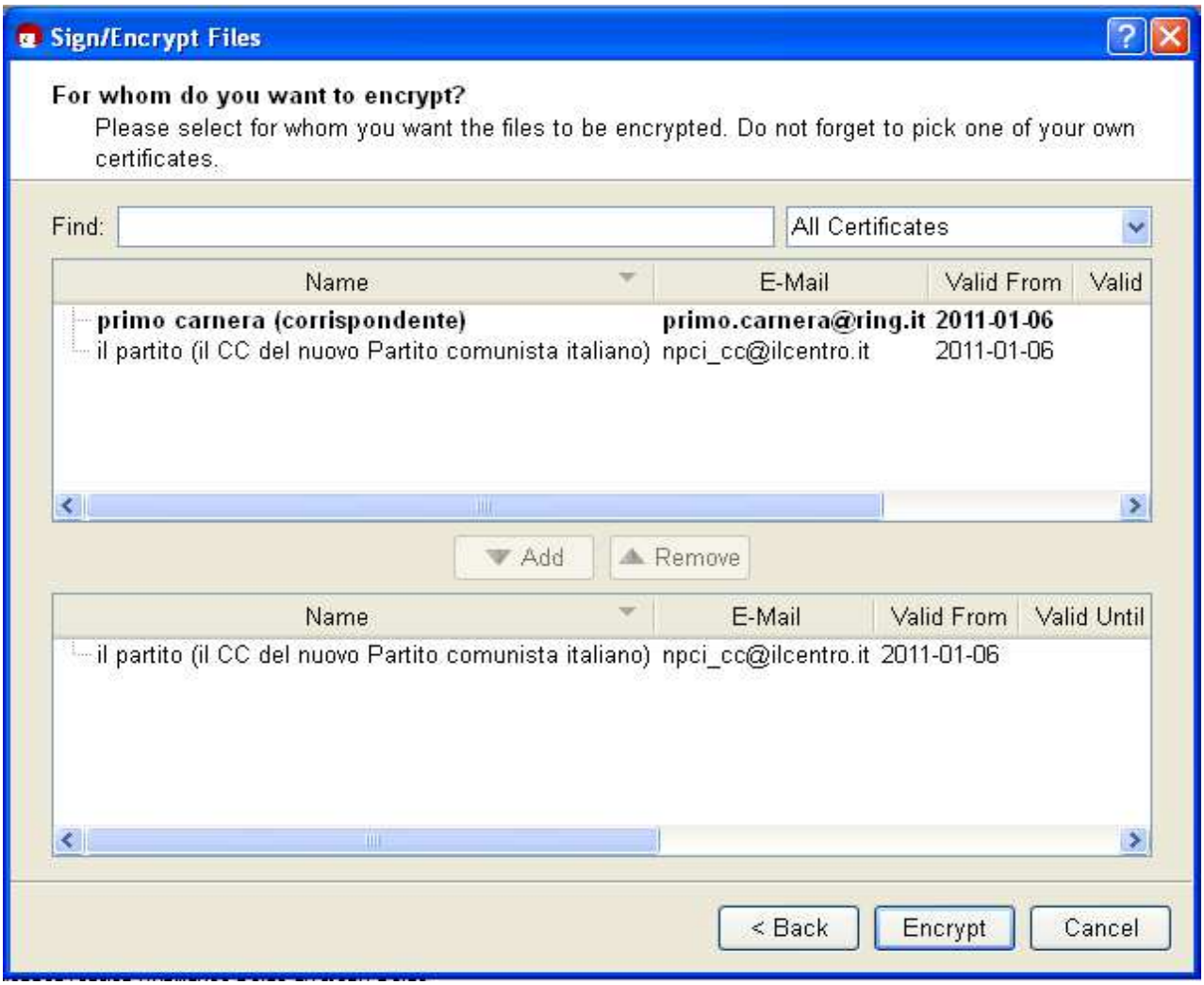
10 Si apre la finestra *Sign/Encrypt Files*, mostrata nell'immagine che segue. In alto, sotto la voce *Selected file:*, è mostrato il file da criptare che avete selezionato. Per il resto, fate in modo che le impostazioni corrispondano all'immagine che segue. In particolare **Encrypt** deve essere attivo (pallino vistato).



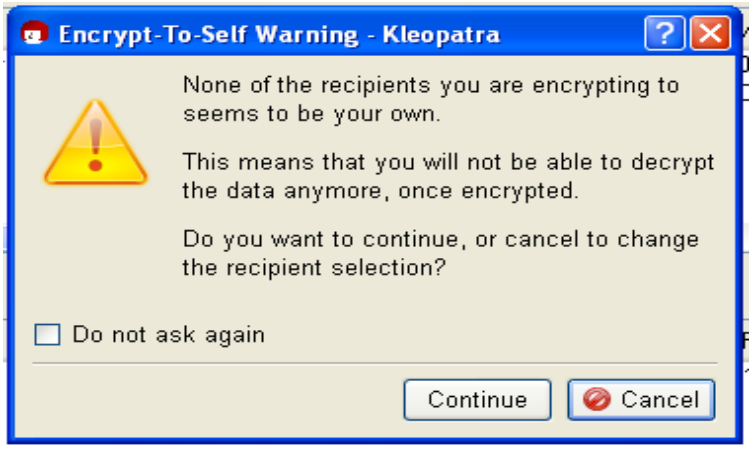
11. Fate click, su **Next >**. La finestra *Sign/Encrypt Files* cambia aspetto, come mostrato nell'immagine che segue. Evidenziate la voce **il partito …** (che corrisponde alla chiave pubblica del Partito) e fate click su **Add**.



Dopo aver fatto click su **Add**, nell'area in basso della finestra *Sign/Encrypt Files*, appare la voce selezionata come mostra l'immagine che segue.

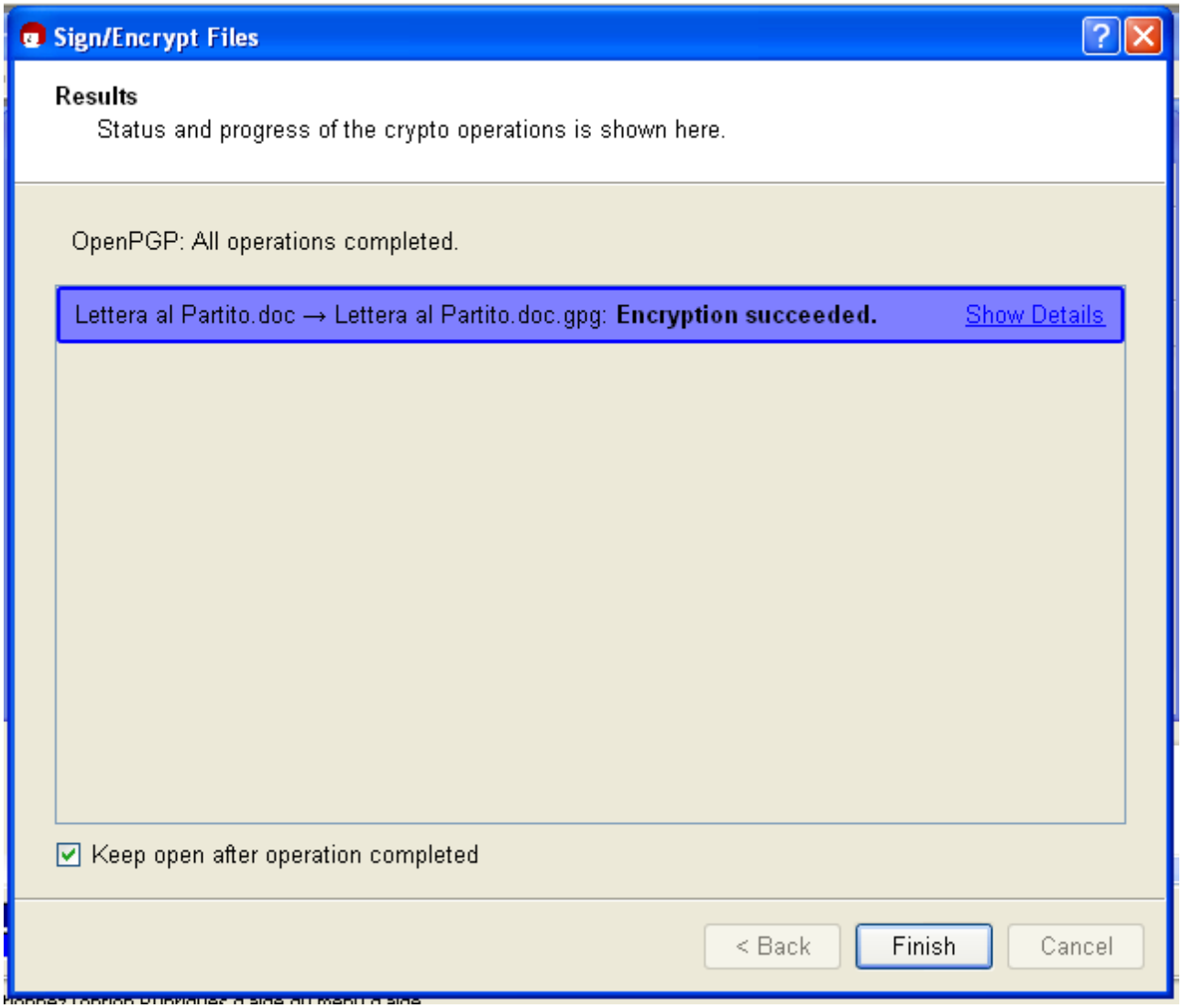


12. State bene attenti che qui è richiesta la chiave pubblica del corrispondente a cui volete inviare il messaggio criptato e non la vostra. Fate click su **Encrypt**. Vi appare, vedi l'immagine che segue, un messaggio di avvertimento che vi avvisa del fatto che il file che criptate non potrà essere decriptato con la chiave che state usando. **Notate Bene** che poiché state usando **la chiave pubblica del Partito**, solo il Partito, che è in possesso anche **della propria chiave privata**, può decriptare il messaggio. Voi stessi, se cancellate l'originale, non potrete più recuperare il suo contenuto. Quindi ricordatevi di non cancellare il file originale. Per conservare i propri file protetti dagli spioni, criptateli come indicato al capitolo 8. di queste istruzioni.

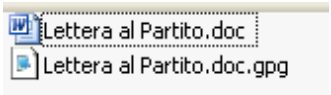


Fate click su **Continue**.

13. Inizia il processo di criptazione. Alla fine nella finestra compare il messaggio mostrato nell'immagine che segue. "Encryption succeeded", indica che l'operazione è riuscita.



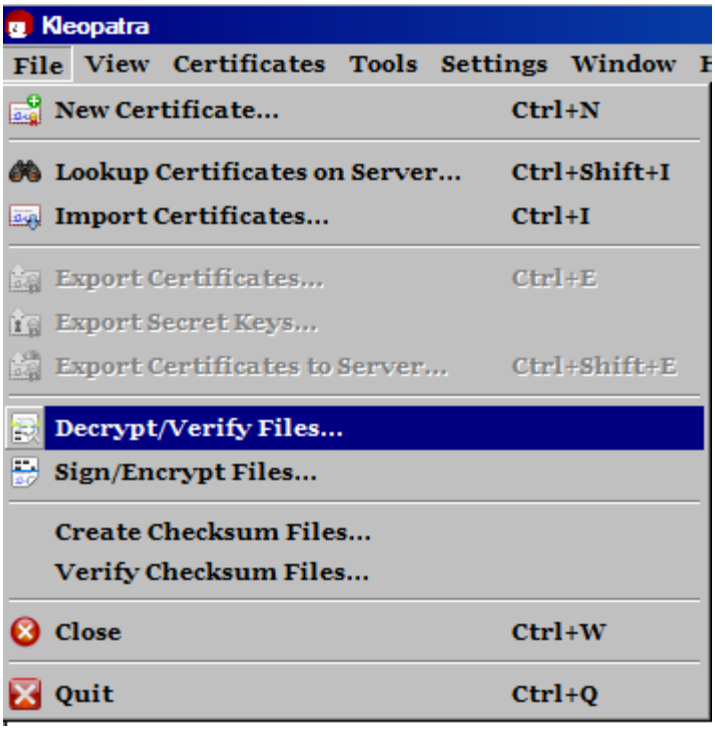
14. Fate click su **Finish**: la finestra si chiude. Aprite la cartella in cui è contenuto il file "Lettera al Partito.doc": lì troverete anche il file "Lettera al Partito.doc.gpg", come mostra l'immagine che segue. Quest'ultimo è il file criptato che potete ora inviare allegandolo ad un messaggio email in chiaro al Partito. Inviatelo da una casella webmail**(4)** creata apposta, usando possibilmente TOR**(5)** alle caselle ufficiali del Partito. Se volete subito una risposta riservata dal Partito ricordatevi che dovete inviare un file compresso e poi criptato con Kleopatra nel modo sopra descritto, che deve contenere la vostra chiave pubblica e il messaggio per il Partito.



7. Decriptare i file ricevuti

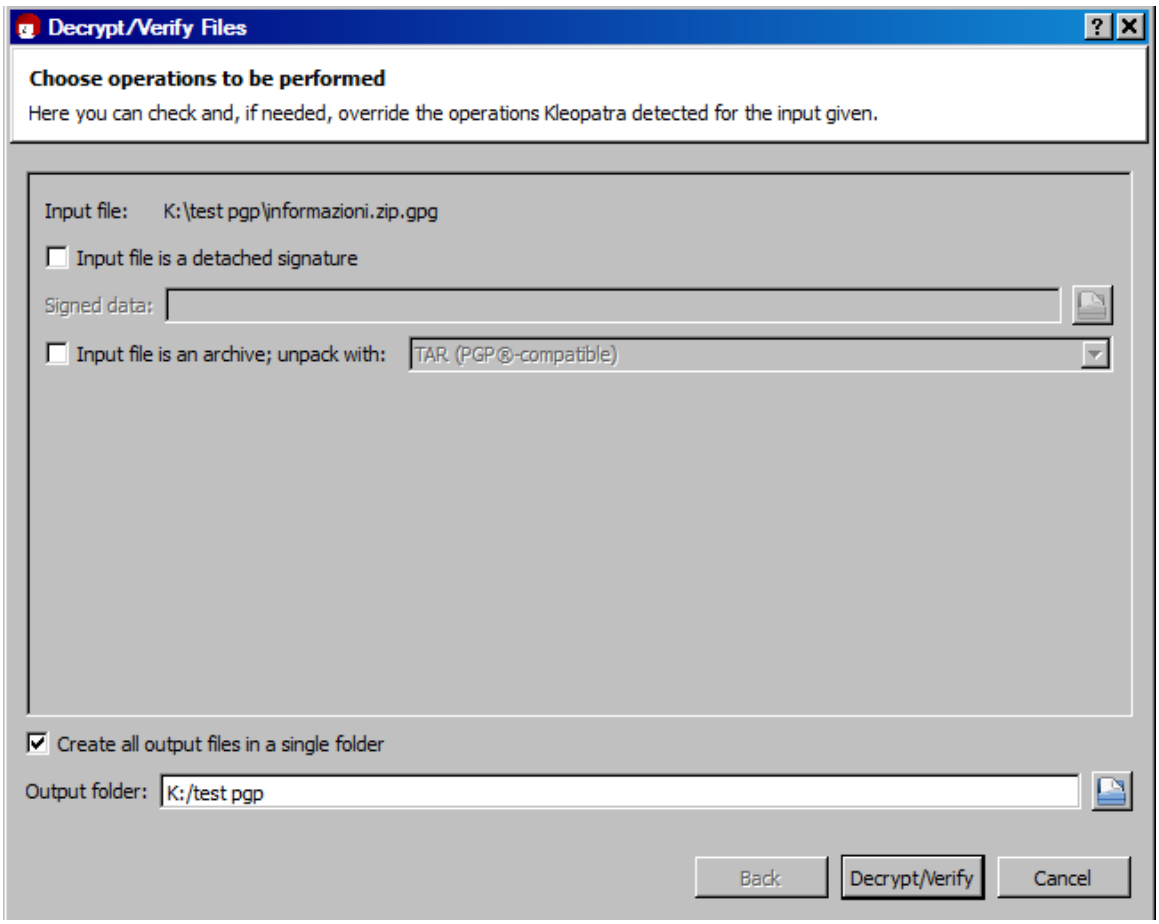
1. Il Partito o un altro corrispondente vi invia il file come allegato ad un messaggio email in chiaro alla vostra casella. Lo scaricate su una chiavetta USB o su un disco esterno. **Solo dopo esservi scollegati da internet** potrete decriptare il file PGP che il Partito o un altro corrispondente vi ha inviato. Nell'esempio che segue il Partito vi ha inviato il file "informazioni.zip.gpg".

   Quando vi siete scollegati da internet, avviate Kleopatra e dal menu *File* selezionate la voce **Decrypt/Verify Files...**, come mostrato nell'immagine che segue.

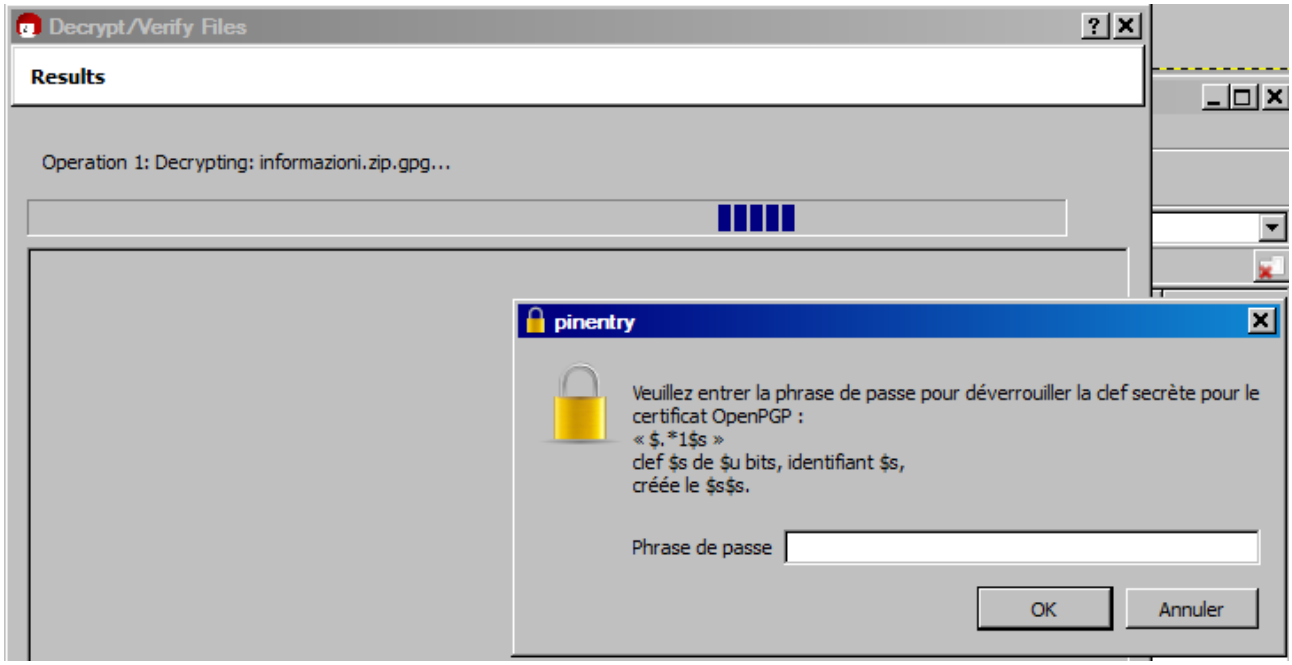


2. Si apre la finestra *Select One or More Files to Decrypt and/or Verify*. È una finestra come quelle per aprire i file. Navigate fino alla chiavetta USB o disco esterno dove avete registrato il file ricevuto da Partito. Nell'esempio il file inviato dal Partito a voi si chiama "informazioni.zip.gpg".

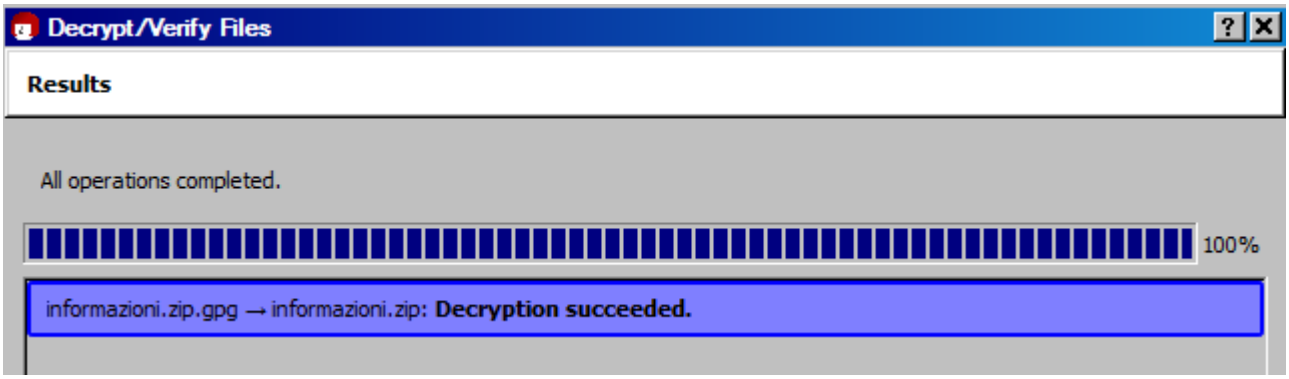
   Selezionatelo e fate click sul bottone "Open" o "Apri" (il nome del bottone dipende dal sistema operativo che state impiegando). Si apre la finestra *Decrypt/Verify Files*. (vedi immagine che segue)



3. Per decriptare il file, fate click sul bottone **Decrypt/Verify**. Appare la finestra *pinentry*, vedi immagine che segue. Nel campo di testo dovete inserire la password che avete usato quando avete creato la vostra coppia di chiavi privata e pubblica (vedi capitolo 3. di queste istruzioni). Poi fate click sul pulsante **OK**.



Se tutto ha ben funzionato, la finestra *Decrypt/Verify Files* vi presenterà il messaggio “Decryption succeeded”.



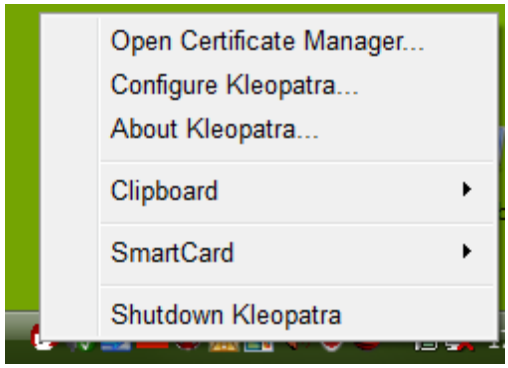
4. Notate bene che Kleopatra riconosce automaticamente la chiave con cui è stato criptato il messaggio, quindi non è necessario indicarla. Se il messaggio è criptato con una chiave pubblica diversa dalla vostra, Kleopatra vi segnala subito che il file non è decriptabile. Se tutto ha ben funzionato, nella stessa cartella in cui era contenuto il file “informazioni.zip.gpg”, ora c’è il file non criptato: “informazioni.zip”, il quale può contenere più file. Quando dovete inviare più file comprimeteli sempre in un unico file compresso: è il metodo più pratico. Date anche un nome di fantasia o neutro che non dia indicazioni sul mittente o sul contenuto del file compresso. Ora tocca a voi rispondere criptando la vostra risposta con la chiave pubblica del Partito o di un altro corrispondente.

8. Criptare i propri file per conservarli protetti dagli spioni.

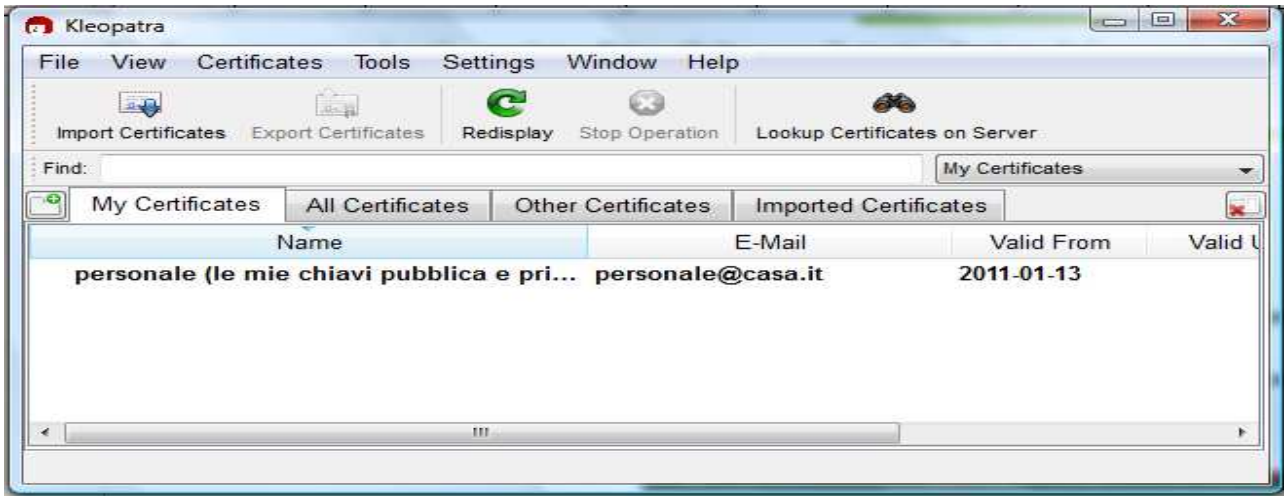
1. È possibile usare il sistema PGP per conservare i documenti riservati sul computer o sulle chiavette USB o su dischi esterni.

   Avviate Kleopatra, fate click sull'icona mostrata nell'immagine che segue.

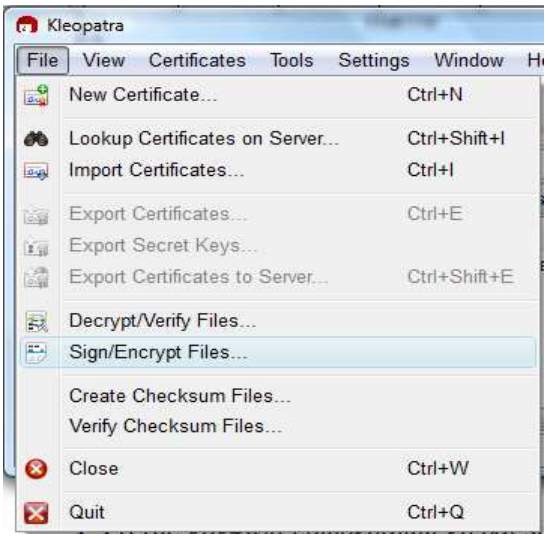
   Se il programma è già avviato, fate click con il tasto destro del mouse sull'icona in basso a destra nella barra di Windows e scegliete la voce: **Open Certificate Manager**.



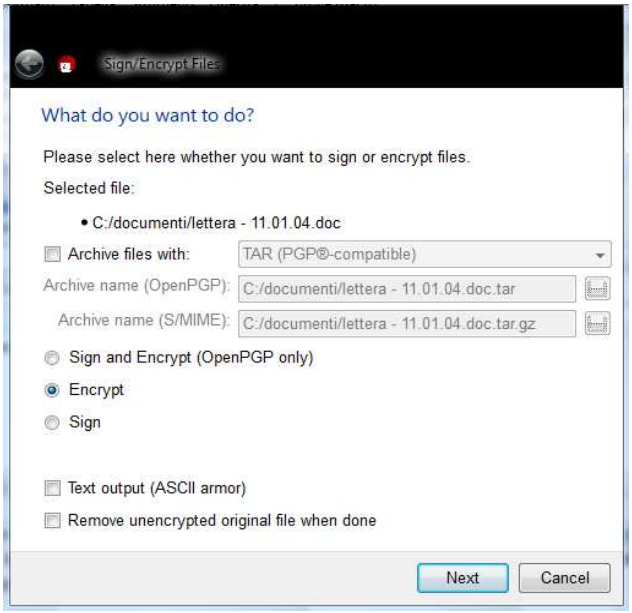
2. Si apre la finestra di Kleopatra mostrata nell'immagine che segue.



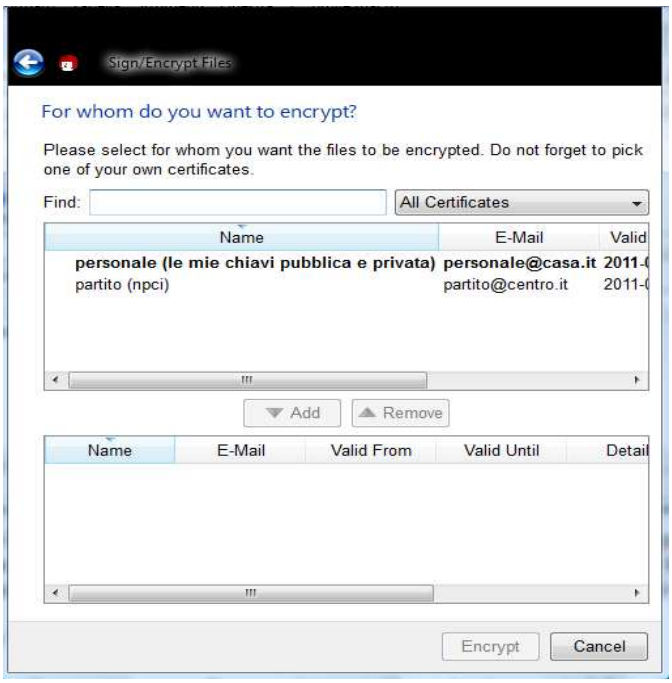
3. Dal menu *File* selezionate la voce **Sign/Encrypt Files...** , come mostrato nell'immagine che segue.



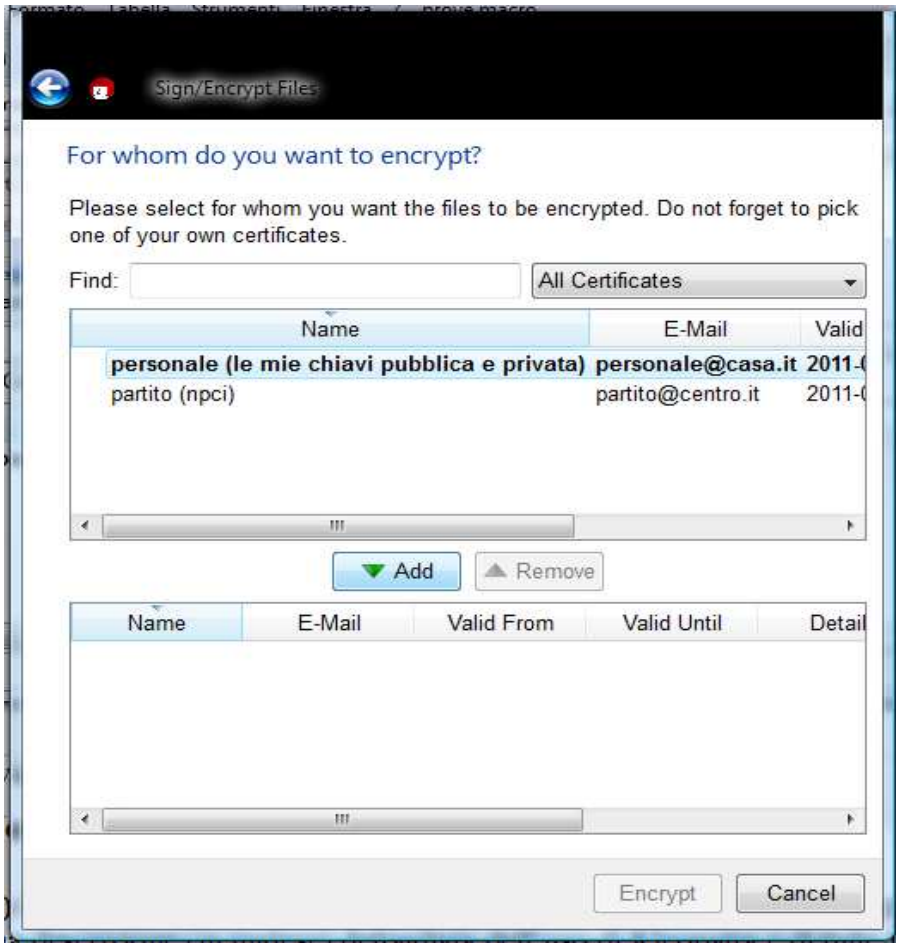
4. Si apre la finestra standard di sistema per la scelta del file (non mostrata): selezionate il file da criptare e fate click su **Apri**. Si apre la finestra mostrata nell'immagine che segue. In alto è mostrato il file selezionato per la criptazione "lettera – 11.01.04.doc". Fate in modo che **Encrypt** sia attivo (il pallino a sinistra deve essere vistato). Fate click su **Next**.



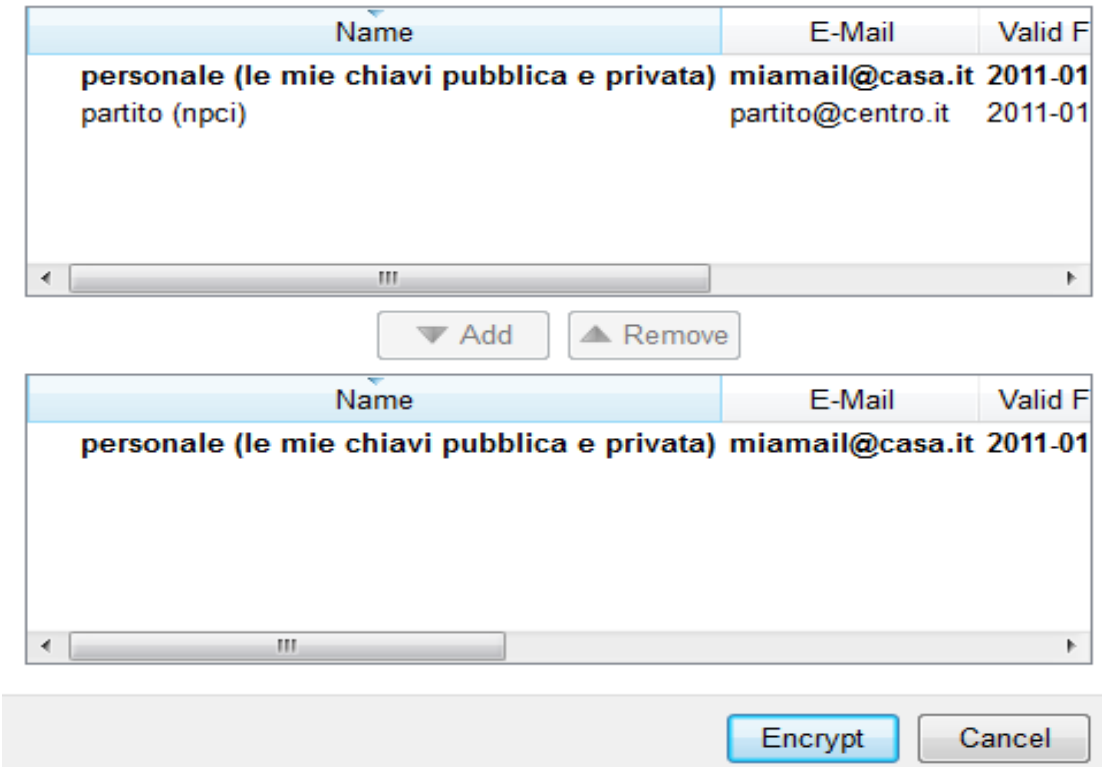
5. Notate bene che fin qui la procedura è uguale a quella descritta al capitolo **6. Criptare e inviare un messaggio al Partito o a un altro corrispondente**, fatto salvo che in questo caso non dovete usare una chiave pubblica di un altro corrispondente, ma usare **la vostra chiave privata**. Usando **la vostra chiave privata**, voi avrete la possibilità di decriptare il documento che volete conservare in modo riservato. Dopo aver fatto click su **Next** nella finestra mostrata nell'immagine precedente, appare la finestra mostrata nell'immagine che segue. Per criptare il file dovete scegliere **la vostra chiave privata**. Nell'esempio si chiama **personale ...** e **non** quella di un altro corrispondente Nell'immagine che segue notate che Kleopatra indica in grassetto la vostra chiave privata. Per esempio nell'immagine che segue è mostrato che Kleopatra ha a disposizione anche "la chiave pubblica del Partito**" (**partito (npci) ...**)**. Le chiavi pubbliche di altri corrispondenti sono mostrate non in grassetto.



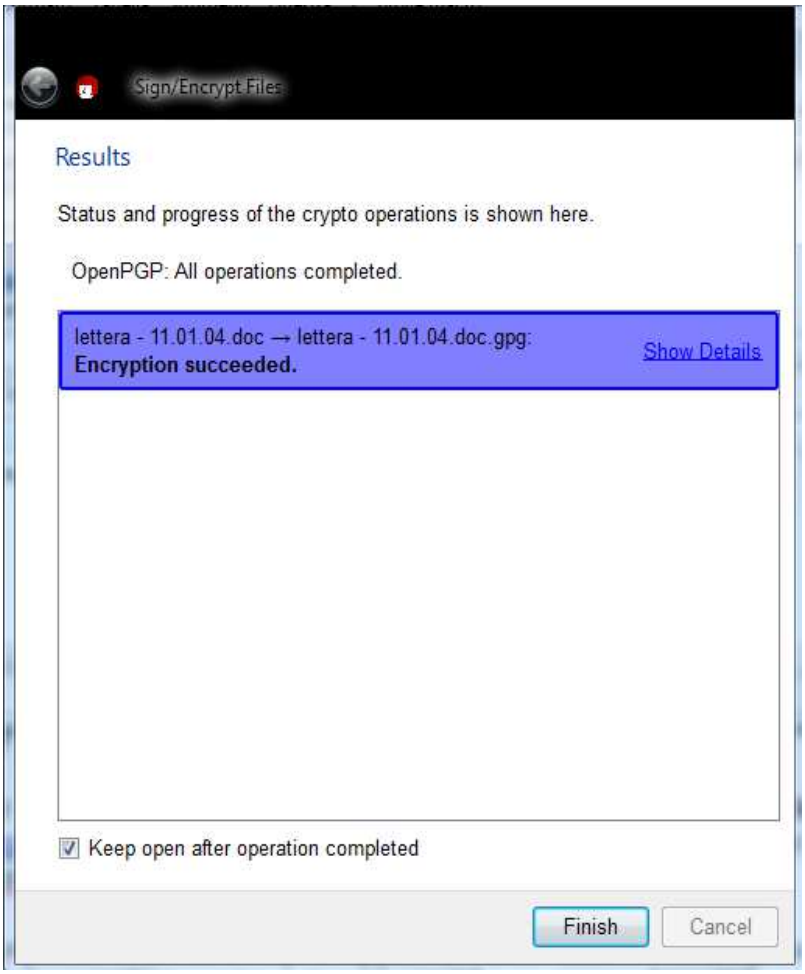
6. Evidenziate la vostra chiave privata (nell'esempio: **personale …**) e fate click su **Add**, come mostrato nell'immagine che segue.



7. La chiave **personale …**, appare nella parte bassa della finestra come mostra l'immagine che segue. Fate click su **Encrypt**.



8. La procedura di criptazione si avvia. Alla fine dell'operazione, la finestra vi appare come mostrato nell'immagine che segue. Il messaggio **Encryption succeeded** vi conferma che l'operazione è riuscita. Notate che rispetto alla criptazione con una chiave pubblica di un altro corrispondente, descritta al capitolo 6. di queste istruzioni, non viene mostrato il messaggio che vi avverte che il file criptato non può più essere decriptato. Infatti voi **state usando la vostra chiave privata** e quindi l'operazione di decriptazione è possibile.



9. Fate click su **Finish** per chiudere la finestra. Nella cartella in cui è contenuto il file che avete criptato, trovate oltre al file originale anche il file criptato con il metodo PGP. Il file si chiama "lettera – 11.01.04.doc.gpg" ed è anche compresso: nell'esempio da 287 Kb è diventato di 98 Kb. È inutile comprimerlo di nuovo.

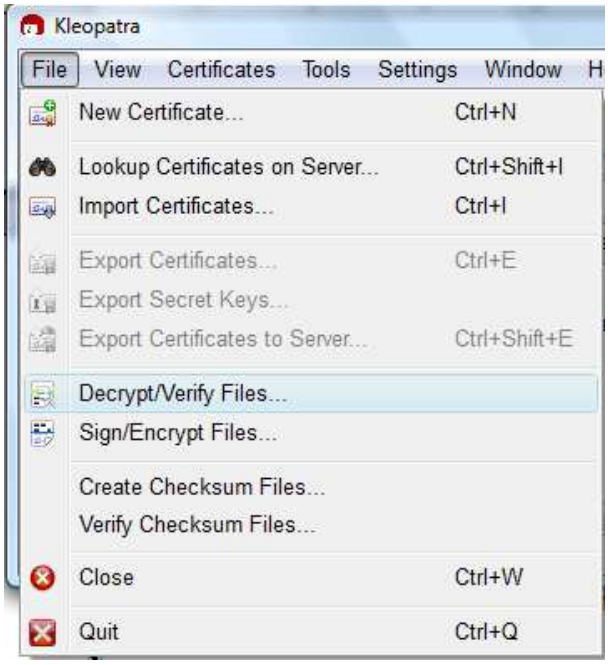
lettera - 11.01.04.doc	13/01/2011 18:51	Documento di Mi...	287 K
lettera - 11.01.04.doc.gpg	13/01/2011 18:40	Fichier GPG	98 K

10. A questo punto vi domanderete: ma se per caso qualcuno mette le mani sul computer, avendo Kleopatra nella sua memoria la mia coppia di chiavi, non può decriptare tutti i miei documenti riservati?

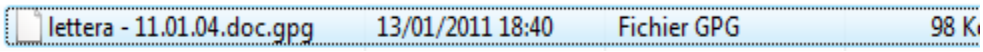
    Prima di tutto è necessario tenere i file criptati su una chiavetta o disco esterno in modo che se uno spione ve la sequestra o ruba non ha a disposizione la vostra chiave privata, la cui copia di sicurezza deve essere conservata su un supporto differente da quello che contiene i dati.

    In secondo luogo non può farlo, perché come vedremo nella procedura di decriptazione dei vostri documenti riservati, descritta di seguito, Kleopatra vi chiederà la password che voi avete inserito quando avete creato la **vostra coppia di chiavi** (procedura descritta nel capitolo 3. di queste istruzioni). Per questo è importante inserire sempre una password adeguata**(3)** quando create le vostre chiavi.

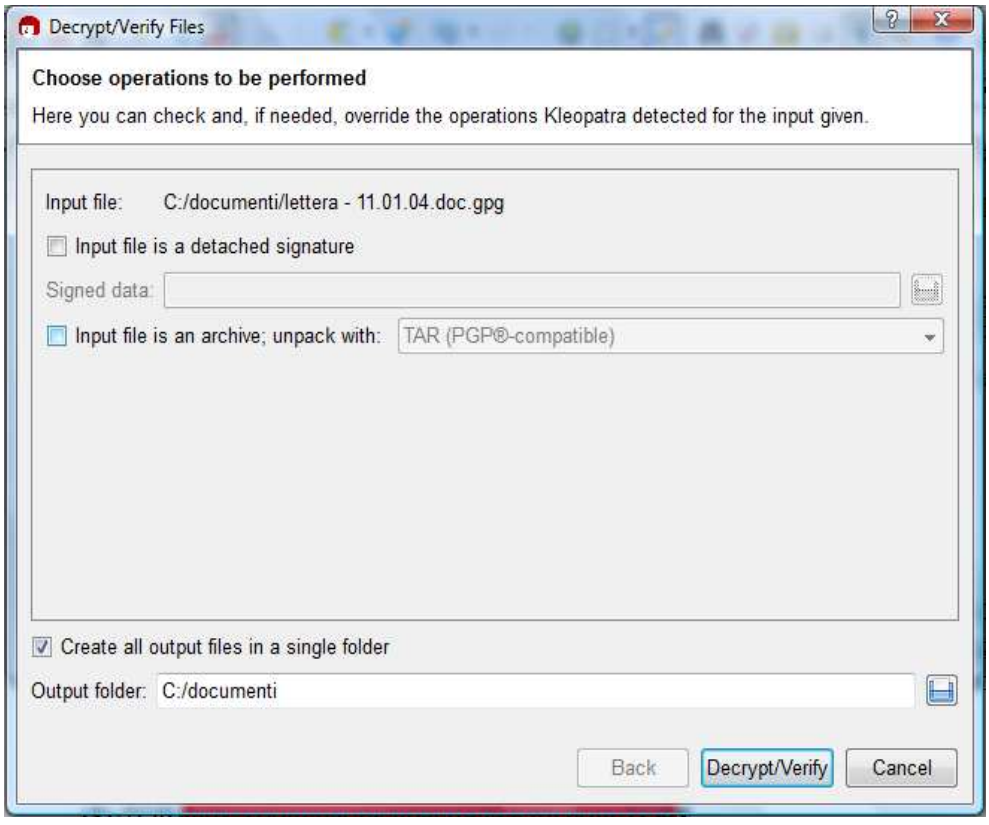
11. Prima di cancellare l'originale in modo sicuro**(6)**, controllate se il processo di decriptazione funziona. Per farlo spostate il file originale "lettera – 11.01.04.doc" o il file PGP "lettera – 11.01.04.doc.gpg" in una cartella differente.
    Avviate Kleopatra e dal menu *File* scegliete la voce **Decrypt/Verify Files...**.



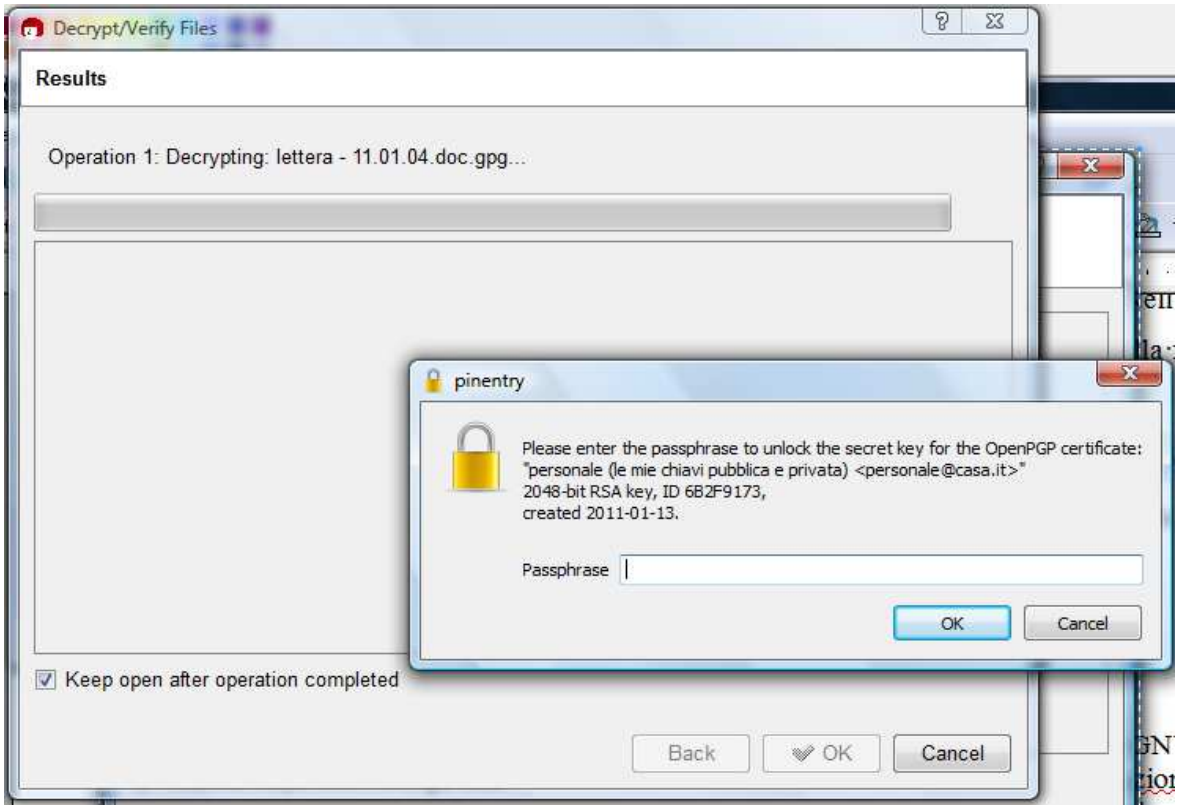
12. Si apre la finestra di sistema da cui scegliere il documento da decriptare. Selezionate il file criptato: "lettera – 11.01.04.doc.gpg" (il file di cui vogliamo verificare che il processo di decriptazione funzioni). Nell'immagine che segue è mostrato un particolare della finestra di sistema per l'apertura dei documenti.



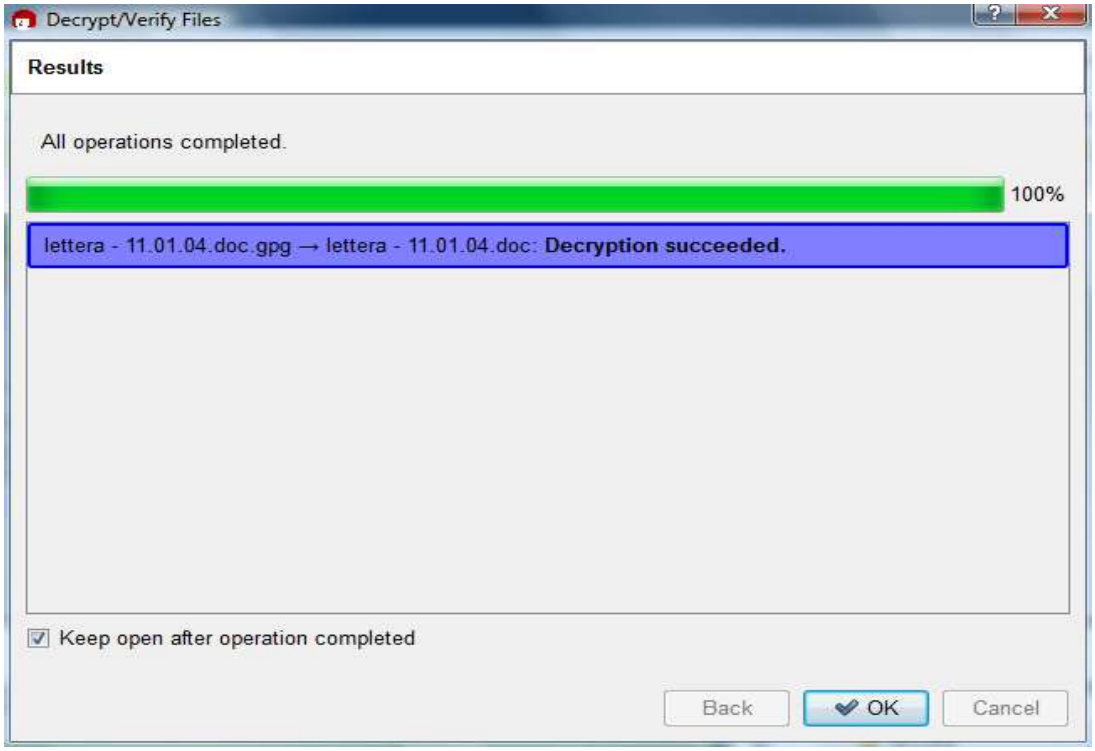
    Se fate click su **Apri**, nella finestra di sistema (non mostrata), appare la finestra *Decrypt/Verify Files* mostrata nell'immagine che segue. Fate click su **Decrypt/Verify**.



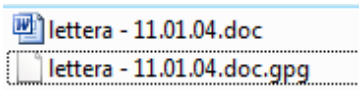
13. La finestra cambia di aspetto, inoltre si apre la finestra *pinentry***(7)**, come mostrato nell'immagine che segue, in cui dovete inserire la stessa password che avete utilizzato per creare la vostra coppia di chiavi privata e pubblica (vedi capitolo 3. di queste istruzioni). Dopo aver inserito la password nella finestra *pinentry* fate click su **OK**.



14. Alla fine della decriptazione vi viene mostrato un messaggio "Decryption succeeded", che conferma la correttezza del processo, come mostra l'immagine che segue. Fate click su **OK**, la finestra si chiude e uscite dal programma Kleopatra**(9)**.



Nella stessa cartella in cui era contenuto il file criptato ora è presente anche l'originale.



Ora potete cancellate il file originale e il file risultato della prova di decriptazione con un programma per la cancellazione sicura**(6)**: noi vi consigliamo l'uso del programma Eraser**(9)**. Usando Eraser sul computer non vi sarà più traccia leggibile del contenuto del file riservato: resta solo il file criptato.

9. Propagandare e diffondere l'uso di PGP e TOR

Tanto maggiore sarà la diffusione e la conoscenza di TOR e PGP, tanto maggiore sarà la possibilità di comunicare liberamente le proprie idee e di organizzare le proprie iniziative senza l'intralcio della censura che la borghesia imperialista esercita. Il tentativo di censura e spionaggio sulle comunicazioni si estende; di conseguenza la diffusione e la conoscenza dei mezzi per contrastarla non riguarda solo i rivoluzionari, ma praticamente ogni frangia popolare che vuole esercitare delle azioni politiche contro la borghesia imperialista, la Repubblica Pontificia, gli imperialisti USA e altri gruppi imperialisti e agenzie (in particolare le agenzie sioniste) che in Italia tentano di soffocare o controllare tutti i mass media!

Note

(1) Ma, attenzione, senza TOR il gestore della casella email resta individuabile dai controllori di internet. Per non far vedere che tra voi e il Partito c'è una corrispondenza criptata, oltre al PGP, dovete usare TOR (vedi nota 5).

(2) Il file *gpg4win-compendium-en.pdf* si trova nella cartella "C:\Program Files\GNU\GnuPG\share\gpg4win". Contiene una descrizione (in inglese) dettagliata dell'uso di Kleopatra e di tutte le altre funzioni di PGP. Queste nostre istruzioni riguardano solo la criptazione dei messaggi da inviare e dei documenti riservati da conservare.

(3) Per **password adeguata**, intendiamo una password difficilmente individuabile. Per intenderci, una password facilmente identificabile contiene dei riferimenti personali a nomi di figli, zie, animali domestici, pianeti, segni zodiacali, ecc.. Una password adeguata può essere una frase del tipo: "oggi il fornaio ha bruciato le torte" (a meno che voi non siate di professione fornaio!!). Una frase facile da ricordare, ma slegata da ogni riferimento personale. Aggiungete a questa frase un codice di quattro o più cifre come ad esempio 1581. La vostra password potrà essere "oggi1581 il fornaio ha bruciato le torte", oppure "oggi1il5fornaio8ha1bruciato le torte", ma le possibilità sono infinite. In compenso avete una password difficile da individuare e facile da ricordare. Per le cifre potete usare anche un codice che avete già memorizzato: vi semplificherà la vita e sopratutto non dovrete scrivere la password su un foglietto!!!

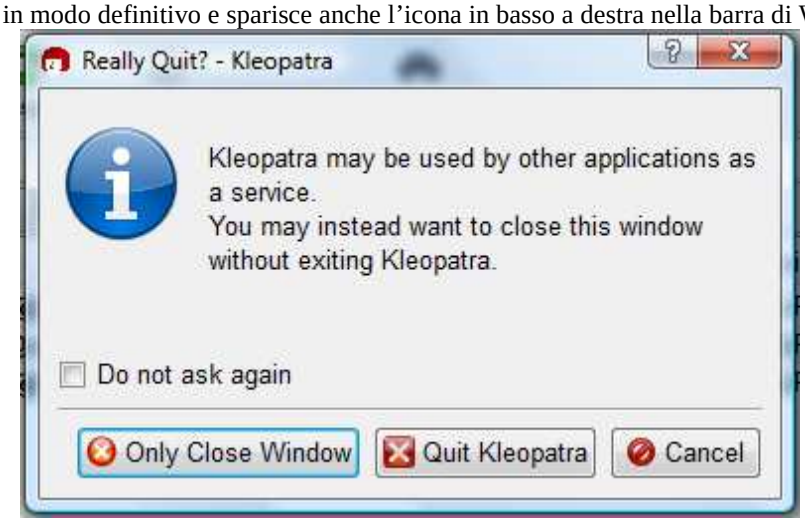
(4) Per **casella web mail intendiamo** una casella consultabile attraverso Firefox, che quindi non lascia traccia della sua attività sul vostro computer. Consultate le istruzioni TOR per Firefox (vedi nota 5), dove vengono descritti i metodi per non lasciare traccia della propria attività internet e di come creare una webmail anonima.

(5) Le istruzioni per usare TOR le trovate al seguente indirizzo internet:
http://www.nuovopci.it/corrisp/risp03.html

(6) Per **cancellazione sicura** si intende l'effettiva cancellazione del file e **non come fanno tutti i sistemi operativi** che eliminano i file solo cancellandone il nome da un indice generale. Quando aprite una cartella, il sistema operativo per mostrarvi il suo contenuto sotto forma di icone, legge l'indice generale che contiene l'elenco di ciò che è contenuto in esso. Quando cancellate un file, il sistema operativo cancella i file solo nell'indice generale, ma non la loro registrazione sul disco!
Una volta che avete gettato nel cestino il file o la cartella e poi svuotato il cestino, è solo l'indice generale che è stato modificato. I dati, ad esempio un testo di word, giace intatto sul disco, ma non è più contenuto nell'indice generale. Il file rimarrà registrato fino a quando non verrà sovrascritto totalmente o parzialmente da un nuovo file. Esistono svariati programmi che leggono tutto il disco e recuperano sia i file interi che quelli parzialmente sovrascritti anche se non sono più elencati nell'indice generale del sistema operativo. Per eliminare definitivamente i file, vi sono dei programmi (vedi nota 9) che sovrascrivono con una serie di caratteri casuali questi file che dimorano intatti o parzialmente sovrascritti. Oltre che sovrascriverli con caratteri casuali, lo fanno più volte, in modo che la traccia magnetica del file precedentemente scritto sparisca completamente; questa è la cancellazione sicura.

(7) Se la finestra *pinentry* non viene mostrata, è perché essa non vi verrà più richiesta durante i successivi 10 minuti da quando inserite la password. Non abbandonate quindi il vostro computer accesso se non sono ancora passati 10 minuti da quando avete inserito la password. Oppure chiudete la sessione di lavoro di Windows se volete lasciare il computer acceso.

(8) Quando si chiude Kleopatra appare la finestra mostrata nell'immagine seguente.
Se pensate di dovervi servire ancora del programma, fate click su **Only Close Window**: si chiude la finestra di Kleopatra, ma rimane l'icona sulla barra di Windows in basso a destra. Da quest'ultima icona potete riaprire Kleopatra. Se invece avete finito tutte le operazioni che avevate in programma, fate click su **Quit Kleopatra**: in questo modo il programma si chiude in modo definitivo e sparisce anche l'icona in basso a destra nella barra di Windows.



(9) Il programma **Eraser** è gratuito ed è scaricabile dal sito http://eraser.heidi.ie/, alla pagina http://eraser.heidi.ie/download.php . Scegliete la versione disponibile alla voce "Stable builds". Nel momento in cui scriviamo, il file più recente è "Eraser 6.0.8.2273.exe".