P.G.P.
P.retty G.ood P.rivacy

www.stordito.it

A cosa serve la crittografia?

La crittografia serve a:

- cifrare un messaggio di testo o un file affinché solo il destinatario sia in grado di leggerlo (questa funzionalita' in Inglese viene chiamata **ENCRYPT**)
- autenticare il testo inviato dal mittente affinché il destinatario sia certo che il messaggio non è stato alterato (questa funzionalita' in Inglese viene chiamata **SIGN**)
- garantire che l'indirizzo di posta elettronica e la chiave pubblica di una persona appartengono veramente a quella persona (questa funzionalita' in Inglese viene chiamata **TRUST**)

Ogni volta che inviamo una e-mail, essa transita attraverso internet providers che tecnicamente sono in grado di leggerne il contenuto. La crittografia e' quindi nata per rispondere a questi problemi di sicurezza e riservatezza che in alcuni casi sono indispensabili come ad esempio per l'invio di documenti finanziari, strategici, etc

Che cosa e' PGP?

Il tallone d'achille della crittografia classica consiste nel fatto che per cifrare e decifrare un messaggio occorre una password in possesso sia del mittente che del destinatario. Ma queste due persone potrebbero trovarsi a notevole distanza tra di loro o addirittura non conoscersi affatto e pertanto, se non esiste un canale sicuro per scambiarsi la password di cifratura, occorre avvalersi di canali pubblici (telefono, e-mail, chat, posta convenzionale, sms, etc.) attraverso i quali la chiave potrebbe essere intercettata.
Per questo motivo in tempi di guerra fredda un tale di nome Philip Zimmermann invento' un modello di crittografia a doppia chiave che chiamo' PGP (Pretty Good Privacy) e lo rese disponibile su Internet affinche' tutti potessero comunicare protetti dal controllo del governo.
PGP e' un programma che genera automaticamente una coppia di chiavi, una chiamata Pubblica e l'altra chiamata Privata, che sono intimamente legate l'una all'altra attraverso una ulteriore password che scegliamo noi. La chiave segreta non deve mai uscire dal nostro computer, mentre quella pubblica possiamo inviarla a tutti i nostri amici senza paura che ci venga intercettata, anzi e' proprio quello che vogliamo, infatti quando un nostro amico ci inviera' un messaggio cifrandolo usando la nostra chiave pubblica, solo la corrispondente chiave privata sara' in grado di decifrarlo, e quindi soltanto noi poiche' quella chiave privata non e' mai uscita dal nostro computer.
Una chiave pubblica, quindi, potrebbe non essere sicura solo se non si è certi della sua reale appartenenza, cioè solo se temiamo che Carlo ci abbia spedito la sua chiave pubblica spacciandosi per Luca e quindi noi scriviamo a Carlo pensando di stare scrivendo a Luca (si capisce l'estrema rarità del caso descritto.. e comunque e' possibile anche garantire l'appartenenza delle chiavi pubbliche).
Poiche' PGP era un prodotto commerciale, in anni recenti una comunita' di programmatori illuminati ha sviluppato una versione completamente gratuita e open source e l'ha chiamata GPG, per cui e' stata concepito questo manuale.

Riassumendo faccio alcuni esempi di cosa e' possibile fare con GPG:

- io sono in possesso della chiave pubblica di **Mario** e volendo inviargli una mail riservata, effettuo la cifratura del mio messaggio (Comando **ENCRYPT**) usando la SUA chiave pubblica. Solo **Mario**, che ha la corrispondente chiave privata, potra' decodificare la mail
- Viceversa, mi arriva una mail che è stata cifrata sulla base della mia chiave pubblica, io potro' quindi decodificarla (Comando **DECRYPT**) con la mia chiave segreta corrispondente, dove dico corrispondente perché uno può anche avere più coppie di chiavi a suo nome, in genere una per ogni indirizzo di e-mail.

- Voglio inviare a Mario una mail senza cifrarla ma voglio dargli la certezza che sono proprio io ad averla spedita; in tal caso posso usare la mia chiave privata per firmare (Comando **SIGN**) il mio messaggio, e quando Mario lo ricevera' potra' usare la mia chiave pubblica e verificare (Comando **VERIFY**) che il messaggio è stato inviato proprio dal sottoscritto ed inoltre che non è stato in alcun modo alterato da estranei.
- Viceversa, ricevo una mail da Mario che e' stata firmata con la sua chiave privata, e io posso quindi usare la chiave pubblica di Mario per verificare (Comando **VERIFY**) che quella mail e' stata scritta effettivamente da lui e non modificata da nessun altro

Chiaramente le due operazioni di cifratura e firma possono farsi contemporaneamente (Comando ENCRYPT & SIGN) in modo da cifrare il messaggio per Mario cosi' che solo lui possa leggerlo e al contempo garantirgli che l'ho scritto proprio io e nessuno ha potuto modificarlo.

Quale software e' necessario?

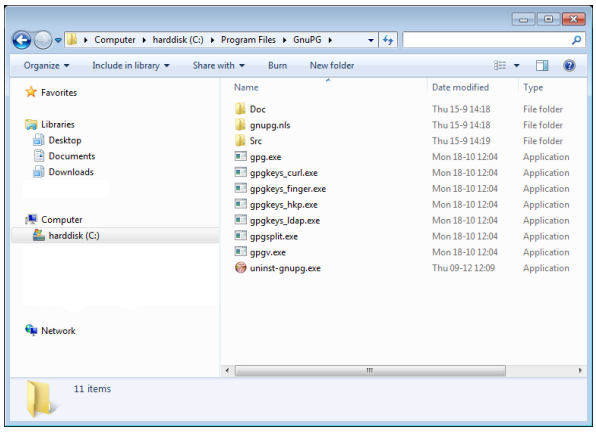
GPG e' di per se un programma a riga di comando, cioe' molto difficile da usare da chi non e' un esperto di computer. Per questo motivo sono nati dei programmi interfaccia (chiamati in inglese "Front End") i quali permettono di usare GPG attraverso una comoda finestra per Windows.
Potete scaricare le versioni installabili di GPG e di svariati Front End dal sito di GPG stesso che e' http://www.gnupg.org tuttavia per installare tali programmi dovete avere diritti da amministratore sul vostro computer. Per questo motivo ho scritto questa guida basandomi sulle versioni portatili (cioe' che non richiedono installazione) di GPG e di Cryptophane (un Front End che io trovo semplice e ben fatto) e che ho reso disponili in un file compresso che potete scaricare da questo link: http://www.stordito.it/software/programmi_per_crittografia.zip

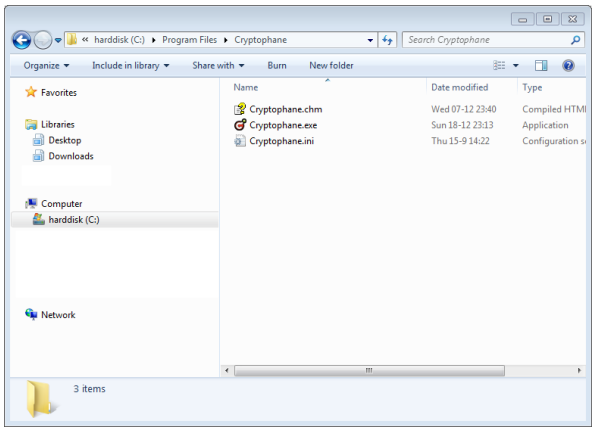
Come lo installiamo?

Una volta scaricato il file compresso dal link sopra, dovete solo decomprimerlo dentro la cartella **C:/Program Files** (in caso vogliate scegliere una cartella diversa e' necessario modificare il file **cryptophane.ini** e indicare il corretto percorso).

Alla fine della operazione vi troverete due nuove sottocartelle al suo interno cosi' nominate:

C:/Program Files
/GnuPG
/Cryptophane



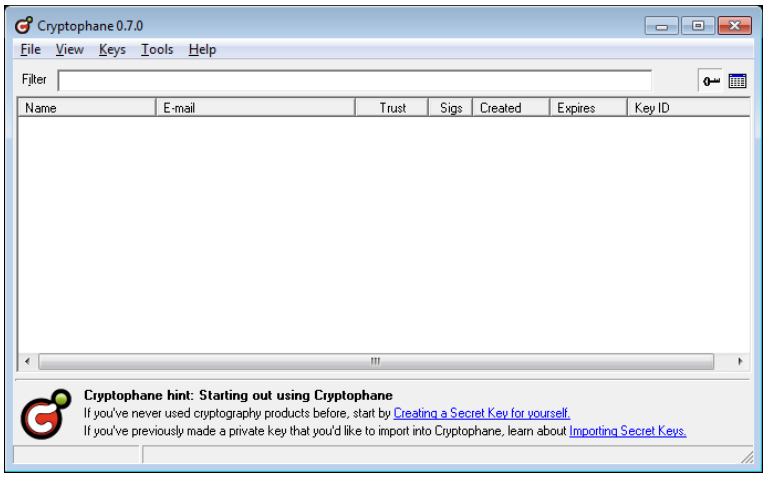


La prima cartella la ignoriamo, e nella seconda clicchiamo il tasto destro del mouse su **Cryptophane.exe** e nel menu contestuale che compare. scegliamo "**Invia a**" e quindi "**Desktop (crea collegamento)**" in modo da trovarci sul desktop di Windows l'icona del programma Cryptophane.

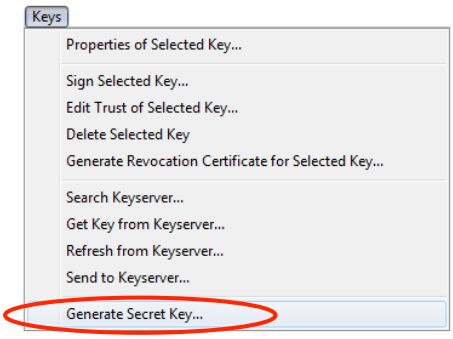
A questo punto e' fatta, ci basta doppio cliccare sull'icona sopra e saremo pronti al prossimo paragrafo!

Come generiamo la nostra coppia di chiavi?

È decisamente la cosa fondamentale, o no? ... quindi lanciate **Cryptophane** e vi troverete davanti la finestra sottostante:



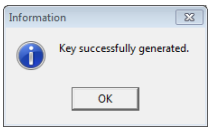
La finestra centrale elenca le chiavi pubbliche e private e quindi e' vuota perche' lo abbiamo appena installato.
Andiamo allora nel menu **Keys** e scegliamo **Generate secret keys** come mostrato qui sotto:



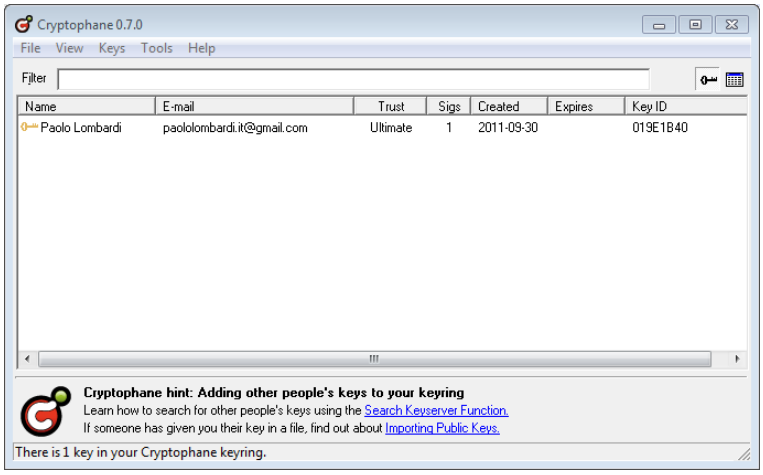
Si aprira' la finesta sottostante in cui ci viene richiesto **Nome Cognome** e l'indirizzo **E-Mail** a cui tale chiave corrispondera'. Nota bene che tali informazioni saranno "incorporate" nelle chiavi generate, pertanto dovete fare una coppia di chiavi per ogni indirizzo e-mail dove desiderate ricevere o scrivere messaggi crittografati.

Nella stessa finestra dovete scegliere la "passphrase" che rappresenta una ulteriore sicurezza al sistema della doppia chiave. Nota bene che se la dimenticate, sara' per sempre irrecuperabile tutta la posta crittografata che avete inviato e ricevuto.

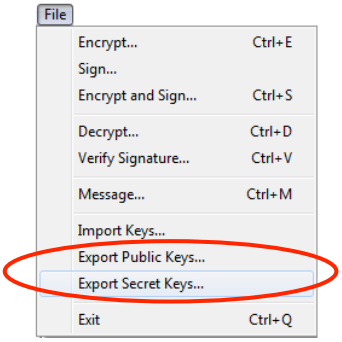
Siamo pronti, e finalmente potete premere il pulsante **Generate**



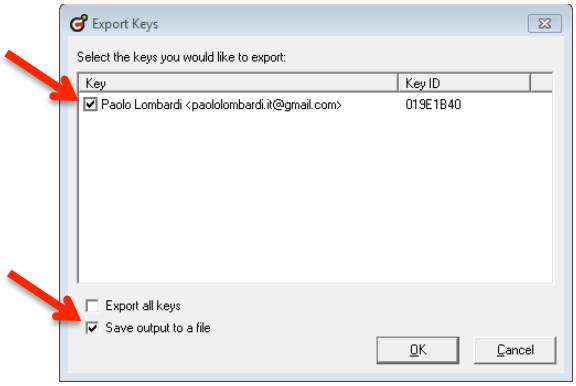
Ed ecco che nella finestra principale di Cryptophane comparira' elencata la nostra prima chiave



Ora la prima cosa da fare e' una copia di sicurezza delle nostra coppia di chiavi, su un memory stick esterno.
In questo modo, se mai un giorno cambiassimo il computer, o dovesse rompersi l'hard disk, noi avremo sempre modo di recuperare la coppia delle nostre chiavi.
Nota che se perdete la vostra chiave segreta, non potreste più decifrare alcun messaggio crittografato con la corrispondente chiave pubblica, la quale invece è ancora viva e vegeta e in mano ai vostri corrispondenti. In un tale scenario dovreste generare una nuova coppia di chiavi, inviare ai vostri corrispondenti la vostra nuova chiave pubblica, e comunque non potrete piu' leggere tutta la posta crittografata ricevuta e inviata fino a quel momento, per questo e' importante fare una copia di sicurezza.
Per esportare la nostra chiave segreta, e' sufficiente andare nel menu **file** e scegliere **Export Secret keys** come mostrato qui:

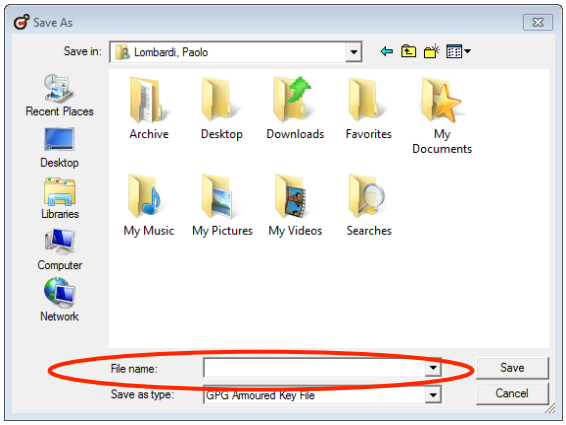


Si aprira' una finestra dove selezionare la chiave segreta che volete esportare (in questo caso ce ne e' una sola che abbiamo precedentemente generato e quindi selezioniamo lei)

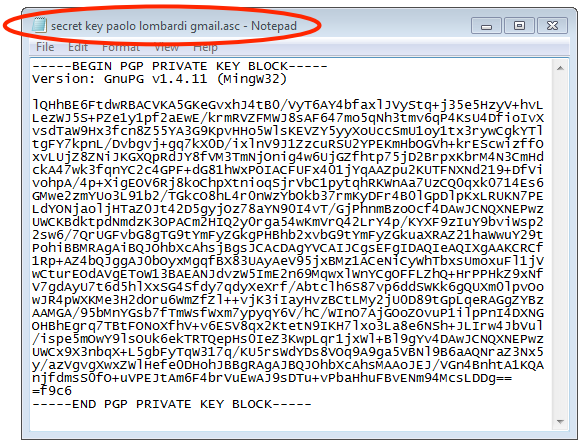


Ci accertiamo che sia selezionato "**Save output to file**" e poi clicchiamo su OK.

Si aprira' la finestra sottostante in cui possiamo scegliere sia il nome che la posizione del file di testo che conterra' la nostra chiave segreta.



Come nome del file, consiglio di cominciare con "secret key" che vi ricorda quale tipo di chiave state esportando, per poi seguire con il vostro nome e quindi un testo che vi faccia capire a quale indirizzo e-mail tale chiave si riferisca. Nel mio esempio, digitero' "**secret key paolo lombardi gmail**" e poi clicchero' su **Save**
Cryptophane salva di default files con estensione .ASC che sono automaticamente aperti con Cryptophane stesso.
Un file .ASC e' un file di testo, per cui potete anche scrivere direttamente l'estensione .TXT quando scegliete il nome del file nella maschera sopra. Se aprite con Blocconote il file appena generato, vedrete i caratteri che compongono la vostra chiave segreta:

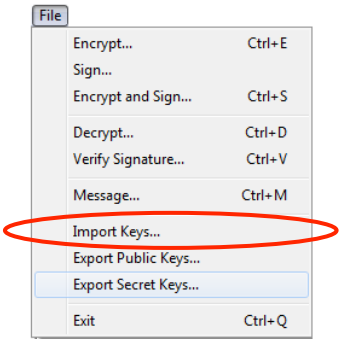


Questa intera procedura va chiaramente ripetuta anche per la chiave pubblica. Dal menu **file** di Crypthophane sceglierete **Export public keys** e quindi selezionerete dall'elenco quale chiave pubblica volete esportare, e poi sceglierete posizione e nome del file, che nel mio esempio questa volta sara' "**public key paolo lombardi gmail**", e anche stavolta se aprirete il file esportato con Blocconote, visualizzerete una finestra piena di caratteri, come potete vedere sotto:

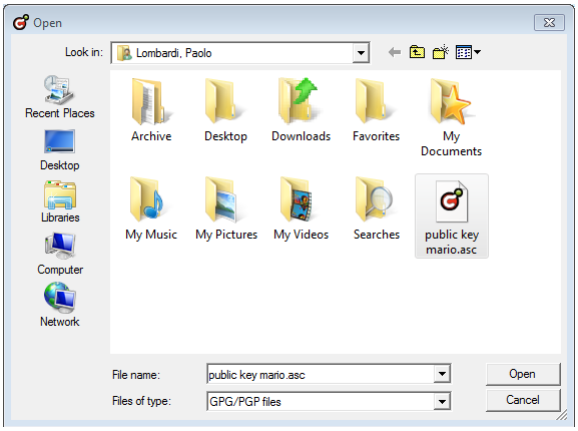
A questo punto potete trasferire su un memory stick esterno la coppia di chiavi che avete appena salvato per sicurezza, e potete anche inviare via mail ai vostri corrispondenti il file relativo alla chiave pubblica, perche' solo da quel momento loro potranno finalmente inviarvi messaggi e file crittografati.

Come utilizziamo le chiavi pubbliche dei nostri amici?

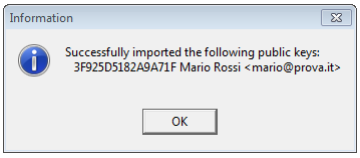
Cosi' come noi invieremo ai nostri amici la chiave pubblica che ci siamo appena preparati al paragrafo precedente, anche loro faranno la stessa cosa! Immaginiamo che il nostro amico Mario ci abbia inviato una mail con allegata la sua chiave pubblica nel file "**public key mario.asc**". Come prima cosa noi salveremo il file sul nostro disco, e poi per poter utilizzare la chiave per crittografare messaggi, dovremo importarla dentro Cryptophane. L'importazione e' un processo molto simile alla esportazione, infatti bastera' andare nel menu **file** e scegliere **Import keys** come mostrato:



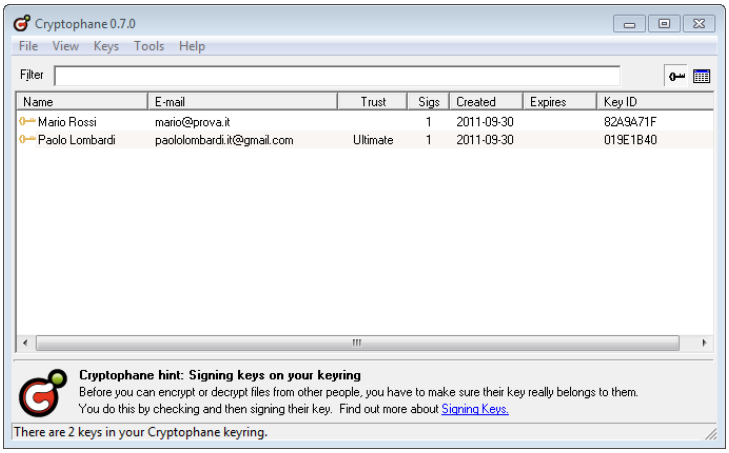
Si aprira' una ulteriore finestra in cui dovete localizzare il file della chiave pubblica che vi ha spedito Mario.



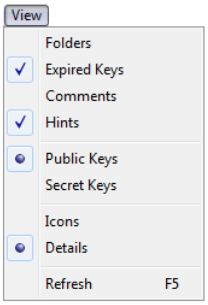
A questo punto vi bastera' selezionare il file e cliccare su Open per importare la chiave:



Notate che nei dettagli della chiave leggiamo anche l'indirizzo email di Mario per il quale la chiave e' stata creata.
Ora troveremo elencata la nuova chiave di Mario tra le chiavi pubbliche disponibili in Cryptophane.

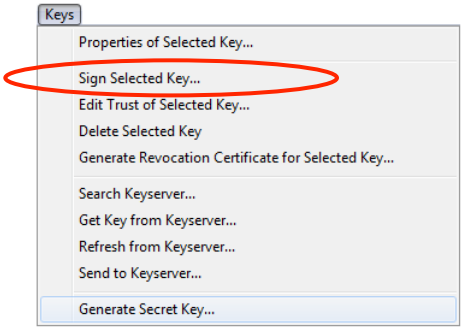


Anche noi siamo elencati nella lista delle chiavi pubbliche perche'anche noi siamo dei possibili destinatari di messaggi di posta crittografata. In parole semplici, quando noi crittograferemo un messaggio, dobbiamo scegliere quali chiavi pubbliche utilizzare perche' solo le corrispondenti chiavi private potranno decodificare il messaggio; ne viene che se codifichiamo un messaggio per Mario usando solo la sua chiave pubblica, una volta codificato noi stessi non saremo piu' in grado di decodificarlo indietro! Per permettere questo, dovremo codificare il messaggio per Mario usando sia la sua chiave pubblica che la nostra. Per questo motivo la nostra chiave pubblica e' presente nell'elenco delle chiavi pubbliche installate in Cryptophane che e' infatti l'elenco delle chiavi per le quali noi possiamo codificare un messaggio.
Nota che per visualizzare le nostre chiavi segrete installate in Cryptophane (chiaramente una per ciascun indirizzo email per cui abbiamo creato una coppia di chiavi), e' sufficiente andare nel menu **View** e scegliere **Secret Keys**.

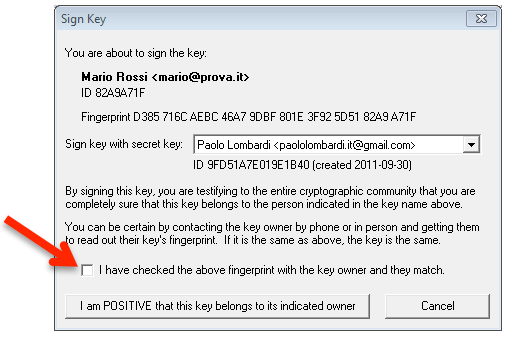


Come garantiamo una chiave?

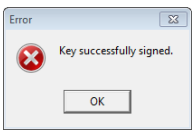
Ora che abbiamo ricevuto e installato la chiave pubblica di Mario, dobbiamo garantire a Cryptophane che quella chiave e' proprio quella di Mario. Questa procedura che si chiama "Trust" consiste in pochi semplici passaggi: nella finestra principale di Cryptophane fate un click sulla chiave pubblica di Mario in modo che sia evidenziata, poi dal menu **Keys** scegliete **Sign Selected Key**.



Si aprira' una finestra in cui vi viene chiesto di garantire che il Fingerprint (spiego piu' avanti nel manuale il perche' di questa richiesta) della chiave pubblica di Mario e' proprio di Mario, e una volta attivato il segno di spunta nel box "**I have checked the above fingerprint...**" dovete semplicemente cliccare sul pulsante **I am Positive** e poi inserire la vostra passphrase**.**

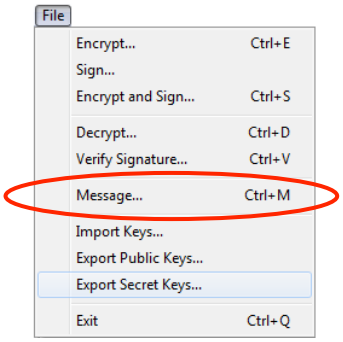


Si aprira' una finestra di conferma che tuttavia, per via di un baco del programma, mostra l'icona e il titolo di errore.

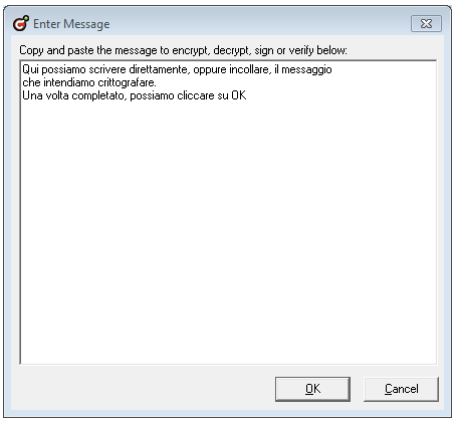


Come crittografiamo una mail?

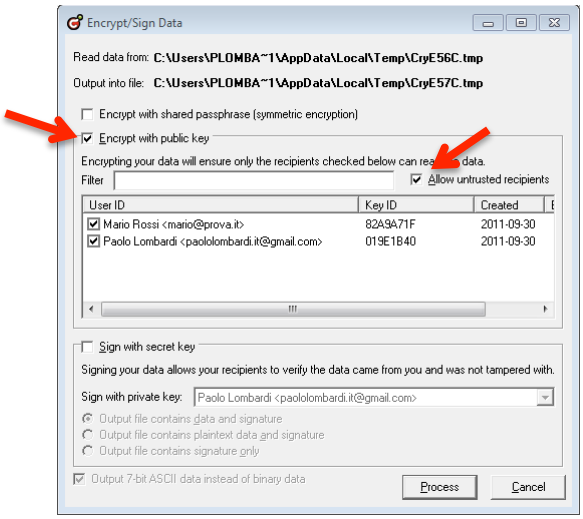
Supponiamo che vogliate scrivere un messaggio crittografato per Mario. Dal menu **File** di Cryptophane, scegliete **Message**



Si aprira' una finestra in cui potete scrivere direttamente o incollare il vostro messaggio. Osservate che il testo qui non e' formattabile cioe' grassetto, corsivo, dimensione del carattere, font, colore del carattere, etc. sono tutte caratteristiche che vanno perse. In caso vogliate inviare un testo formattato, allora dovete scriverlo in Word, ad esempio, salvare tale testo come un file, e quindi inviare il file come allegato crittografato in un modo che vedremo a seguire. Ora voglio mostrarvi come inviare un semplice testo.

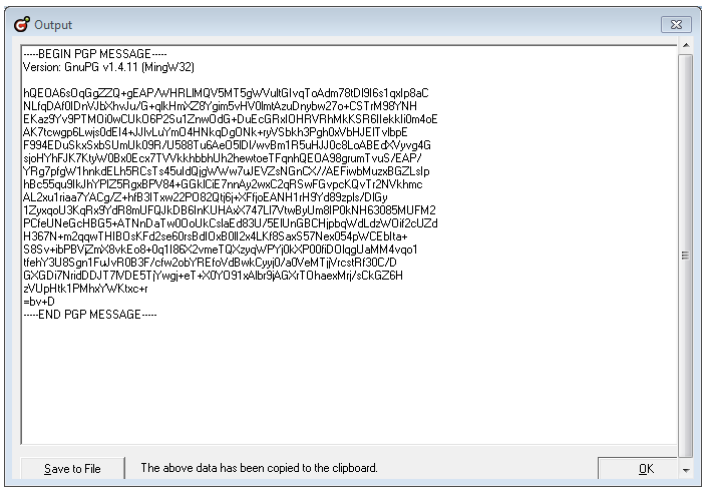


Una volta scritto o incollato il testo che volete inviare a Mario, cliccate su Ok e si aprira' una finestra in cui dovrete selezionare le chiavi pubbliche per le quali volete crittografare il messaggio, e chiaramente avrete a disposizione le sole chiavi elencate precedentemente nella finestra di Cryptophane.



Selezionate la chiave di Mario e la vostra chiave (altrimenti, come gia' spiegato, non potrete piu' decodificare indietro il messaggio che avete voi stessi inviato!) e poi cliccate su Ok.
In caso non abbiate garantito la chiave pubblica di Mario oppure non vogliate farlo, allora dovete sempre tenere abilitato il segno di spunta "**Allow Untrusted Recipients**".

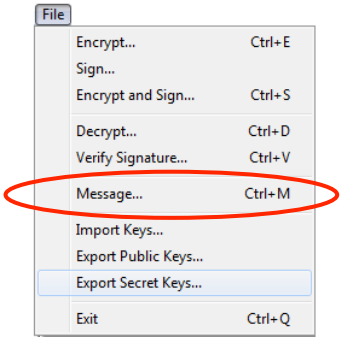
La finestra dove avete scritto il messaggio,ora conterra' la sua versione crittografata che voi potete copiare e incollare in una mail per Mario oppure potete salvare su file cliccando sul pulsante **Save to File** e quindi inviare il file in allegato a Mario.



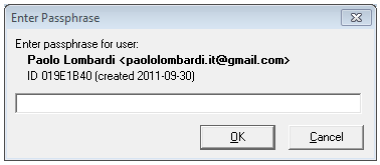
Nota che per crittografare un file anziche' una messaggio di testo, la procedura e' molto simile, semplicemente dovete cliccare sul comando **Encrypt** nel menu **File** di Cryptophane.

Come decrittografiamo una mail?

Supponiamo che abbiate ricevuto una email da Mario in cui una parte del testo sia un messaggio crittografato. Innanzitutto selezionate tutto il testo crittografato e copiatelo negli appunti (CTRL+C) poi dal menu **File** di Cryptophane, scegliete **Message**



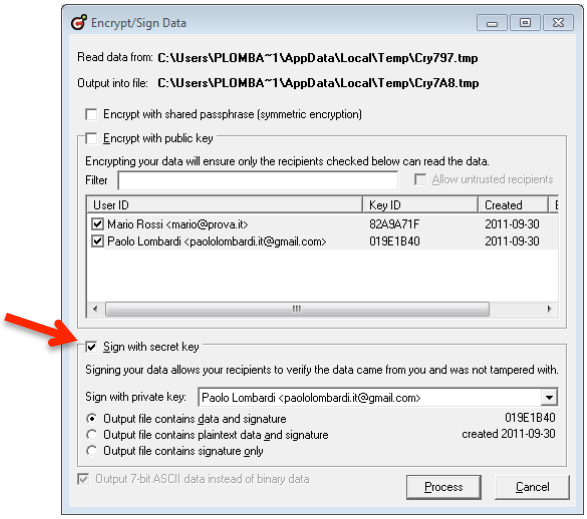
Si aprira' una finestra in cui potete incollare (CTRL+V) il testo crittografato da Mario, e quindi premendo Ok vi verra' richiesta di inserire la passphrase della vostra chiave pubblica:



Se inserite la passphrase correttamente, la finestra precedente ora conterra' il messaggio di Mario perfettamente leggibile. Nota che per decrittografare un file anziche' una messaggio di testo, la procedura e' molto simile, semplicemente dovete cliccare sul comando **Decrypt** nel menu **File** di Cryptophane.

Come autentichiamo una mail?

La procedura per firmare una mail e' molto simile a quella per crittografarla, cambia solo dove mettiamo il segno di spunta nella finestra di scelta delle chiavi pubbliche.



La firma (in inglese **Signature**) di un messaggio di testo e' un blocco di caratteri speciali che viene aggiunto in fondo al messaggio il quale resta perfettamente leggibile (per questo si dice "firma in chiaro").
Tale blocco di caratteri speciali viene calcolato da Cryptophane in funzione della nostra chiave segreta e dei caratteri che compongono il messaggio originale. In caso anche un solo carattere del messaggio originale cambiasse, anche un solo spazio venisse aggiunto, Cryptophane calcolerebbe un blocco di caratteri speciali diverso dal precedente.
Quando uno riceve un messaggio autenticato (o firmato), Cryptophane non fa altro che verificare la corrispondenza biunivoca tra messaggio originale e caratteri speciali e ci garantisce che tale messaggio non e' stato alterato in alcun modo.
Un esempio di messaggio "firmato in chiaro" con PGP potrebbe essere il seguente:

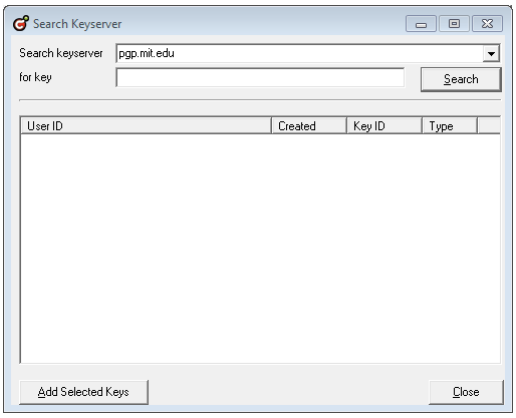
```
-----BEGIN PGP SIGNED MESSAGE-----

Ciao Mario,
Ho firmato questo messaggio cosi' puoi verificare che l'ho scritto io e
non e' stato modificato da nessuno!
Ti saluto!
Paolo

-----BEGIN PGP SIGNATURE-----
iQA/AwUBNr84La1N2hTAk0JyEQIIFQCgi7JsVwZ/5TAZK/9cWGxu/uUWOBcAmwTA
pTIY3wiNKqPWMflTir+yzyz+ =kxr6
-----END PGP SIGNATURE-----
```

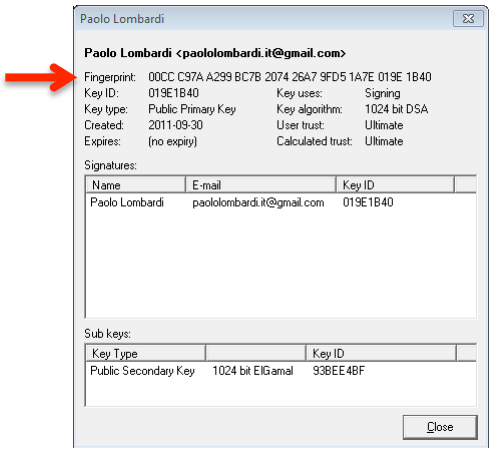
Cosa sono i Keyservers?

I keyservers sono dei database di chiavi pubbliche accessibili a tutti al fine di aggiungere la propria chiave o di trovare quella di un utente. Sono come una sorta di pagine gialle delle chiavi pubbliche dove chiunque può andare e cercare la chiave pubblica di Mario Rossi e, a patto che il signor Rossi l'abbia spedita al keyserver precedentemente.
Inviare la propria chiave a un keyserver e'molto semplice, e' sufficiente cliccare su "**Send to keyserver**" dal menù **Keys** di Cryptophane. Con altrettanta semplicita' e' possibile cercare la chiave pubblica di un utente, incollo senza spiegarla la finestra che compare selezionando "**Search keyserver**" sempre dal menu **Key**



Che cosa e' il Fingerprint di una chiave?

Il fingerprint e' una sequenza di 32 cifre ricavate dalla chiave pubblica e che la identifica in modo univoco.
Doppiocliccando su una chiave nella finestra principale di Cryptophane, si apre una finestra che mostra le proprieta' della chiave stessa, tra cui il fingerprint.
Incollo a seguire un esempio di tale finestra delle proprieta':



A cosa serve il fingerprint?
Serve perche' quando Mario ci ha spedito via mail la sua chiave pubblica e noi l'abbiamo aggiunta al nostro Cryptophane, ancora non siamo sicuri che sia la chiave effettivamente di Mario perche' qualcuno avrebbe potuto sostituire la chiave allegata alla mail di Mario lungo il tragitto (abbiamo gia' detto che la posta elettronica e' intrinsecamente insicura).
Per fare questa verifica ci bastera' telefonare a Mario e chiedergli il fingerprint della sua chiave, in modo che se coincide con quello della chiave che abbiamo ricevuto via mail, allora siamo certi che quella e' veramente la sua chiave, e possiamo cosi' alzare il livello di Trust come visto precedentemente in questo manuale.