# Formulario semplificato per l'uso della posta elettronica in modo cifrato e semplice.

**Per inviare e ricevere messaggi di posta in tutta sicurezza in un ambiente insicuro.**

**Guida per i sistemi Windows**
**(Compatibile con altri sistemi)**

Edizioni: tramaci.org

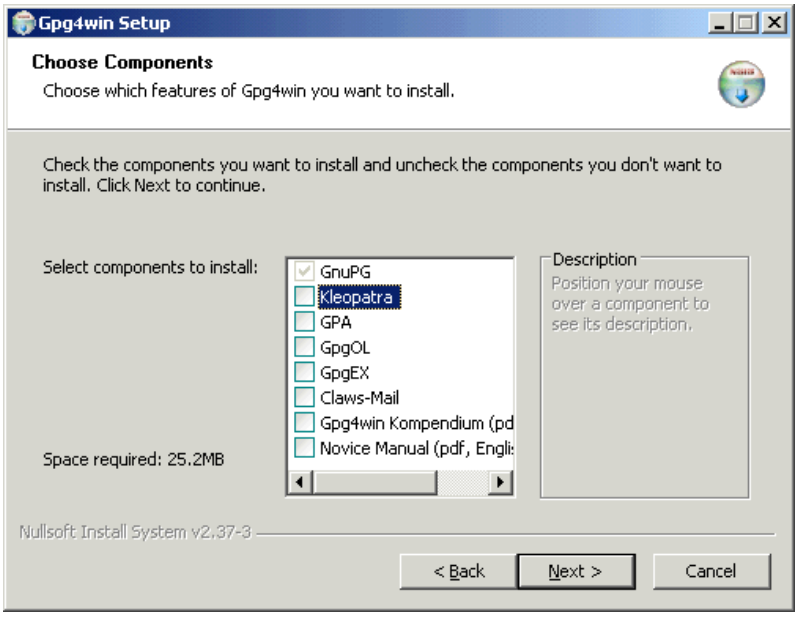
Come prima cosa occorre procurarsi i programmi da utilizzare:

- Mozilla Thunderbird (Posta elettronica)
  http://www.mozilla.org/it/thunderbird/

- GnuPG (Crittografia)
  http://ftp.gpg4win.org/gpg4win-2.0.0.exe
  (Altri sistemi operativi)
  http://www.gnupg.org/download/index.en.html#auto-ref-3

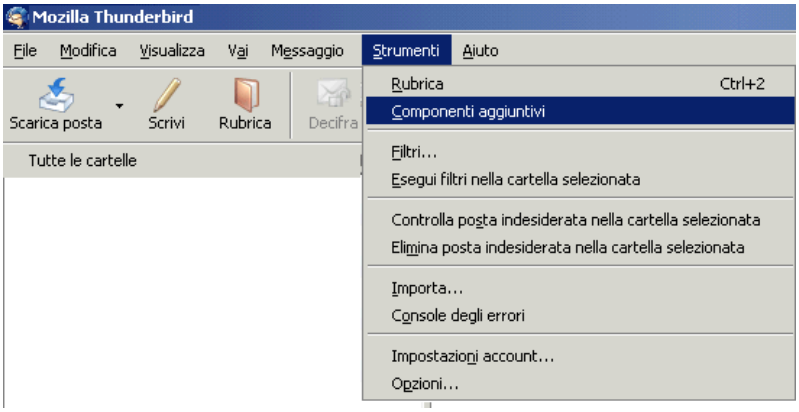
- Enigmail (Componente aggiuntivo per thunderbird)
  http://www.enigmail.net/home/index.php
  (Questo sito permette il download di un file con estensione .xpi)

Il primo programma da installare è Thunderbird, dopo l'installazione facendolo avviare configura il tuo account di posta.

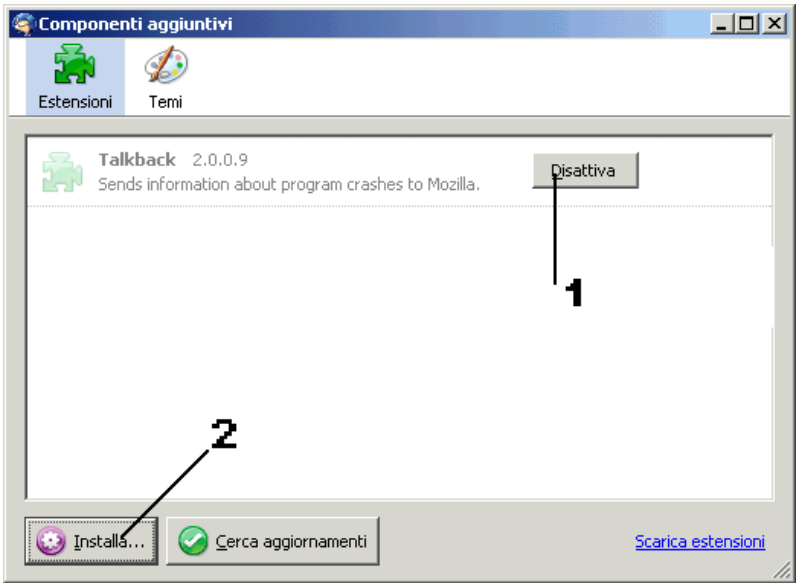



Poi occorre installare GnuPG. Quando fai partire il programma di installazione scegli solo GnuPG e scarta tutti gli altri sotto programmi che non saranno utilizzati.

Quando hai finito di installare GnuPG, fai partire thunderbird per i passaggi successivi.

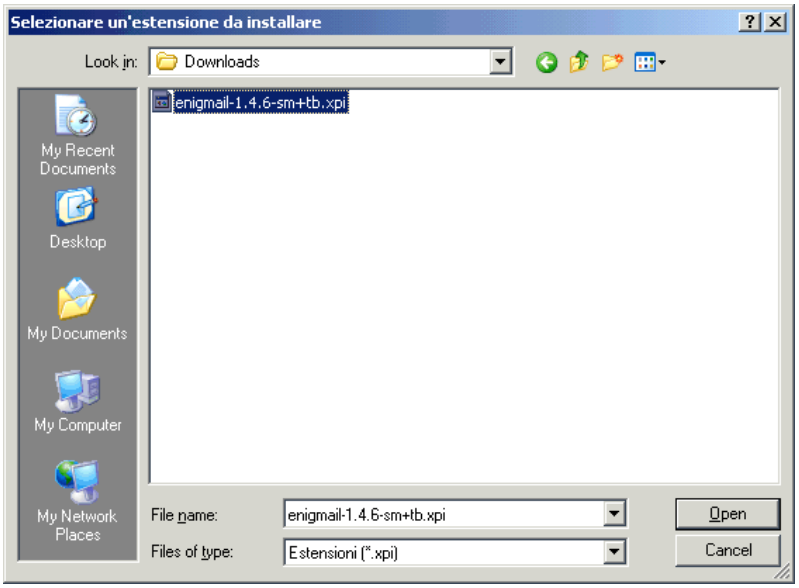



Su Thunderbird dal menù "Strumenti" scegli "Componenti Aggiuntivi"




Si aprirà una finestra simile a questa.

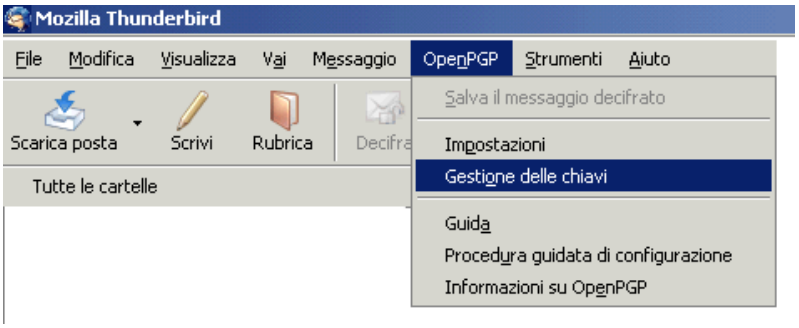
1) Primo passo: Disattivare gli altri componenti aggiuntivi come per esempio: TalkBack, Flash, Java, ecc...
2) Cliccare sul tasto "installa"




A questo punto sarà necessario indicare il file di installazione di ENIGMAIL.

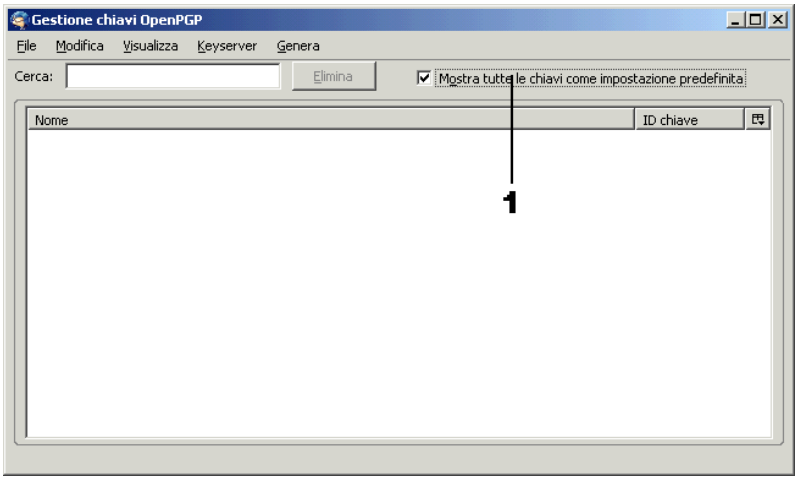
Questa operazione installerà Enigmail come componente aggiuntivo per thunderbird. Dopo l'installazione su thunderbird ci saranno dei nuovi menù e funzioni.

In alcune versioni di thunderbird potrebbe essere necessario riavviare (chiudere e riaprire) il programma per attivare le nuove funzioni.



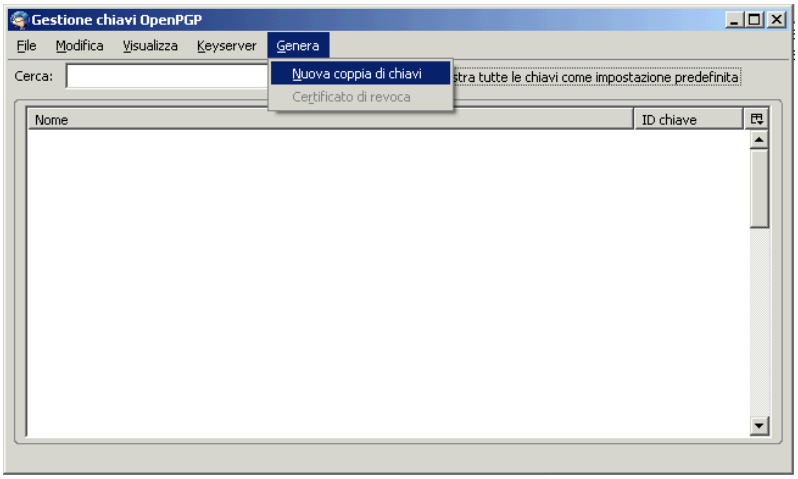

Questa operazione la dovrai fare solo la prima volta per poter creare una chiave cifrata per poter inviare e ricevere messaggi criptati.

Scegli il nuovo menù "OpenPGP" e quindi l'opzione "Gestione delle chiavi".



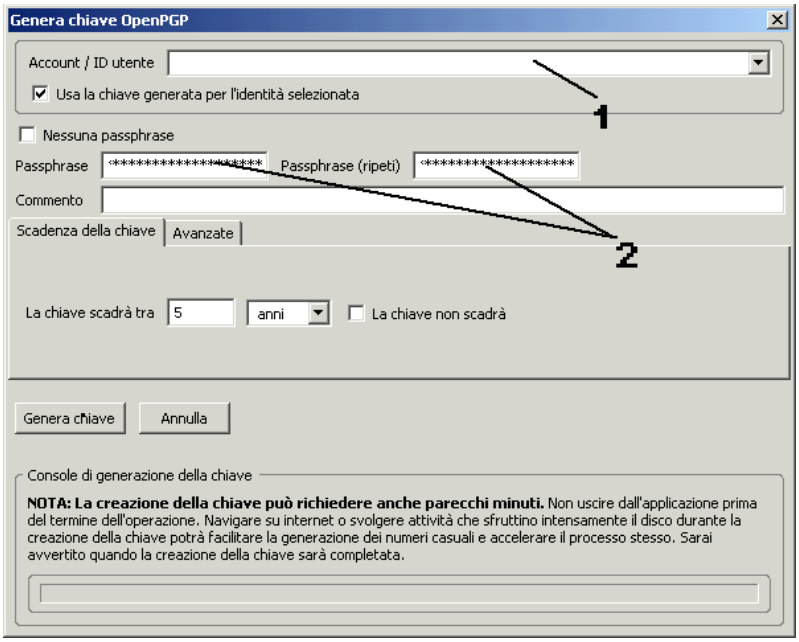

Si aprirà questa finestra che serve per gestire le tue chiavi criptate e quelle dei tuoi contatti.

1) Ricordati di attivare questa casella altrimenti potresti non vedere tutte le chiavi.




La prima cosa da fare è creare la propria coppia di chiavi. Quindi dal menù "Genera" scegli "Nuova coppia di chiavi".

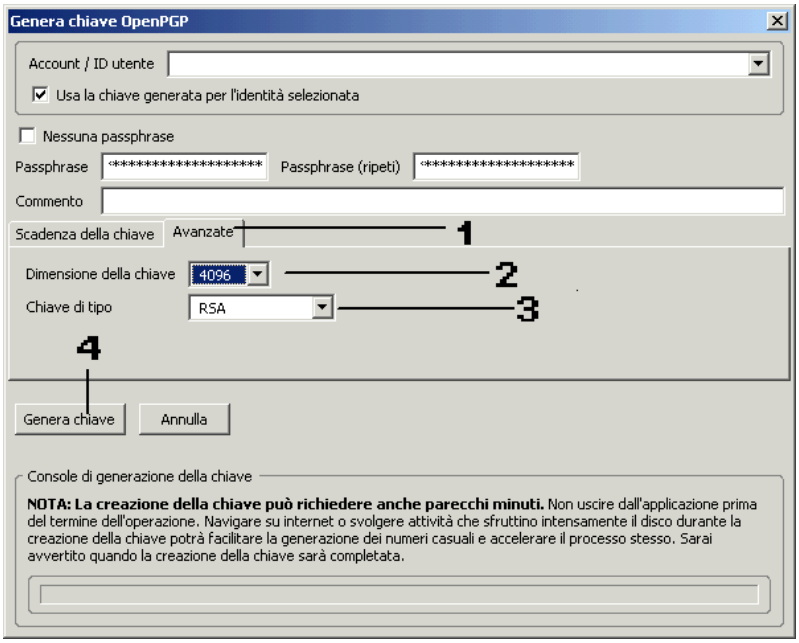
La tua chiave sarà associata al tuo indirizzo mail. La chiave è in realtà divisa in due parti: una pubblica che condividerai con i tuoi amici e possibilmente con i keyserver, l'altra privata che terrai al sicuro e non la condividerai con nessuno.




Si aprirà una finestra come questa.

1) Scegli l'indirizzo mail a cui associare la tua chiave. (Se qui non trovi il tuo indirizzo di posta allora vuol dire che devi ancora configurarlo).
2) Devi inserire la passphrase:
   Si tratta di una frase che sarà la password per poter usare la tua chiave. Deve essere lunga e non devi dimenticarla.

Non cliccare subito su "Genera chiave", facciamone una più forte del solito.

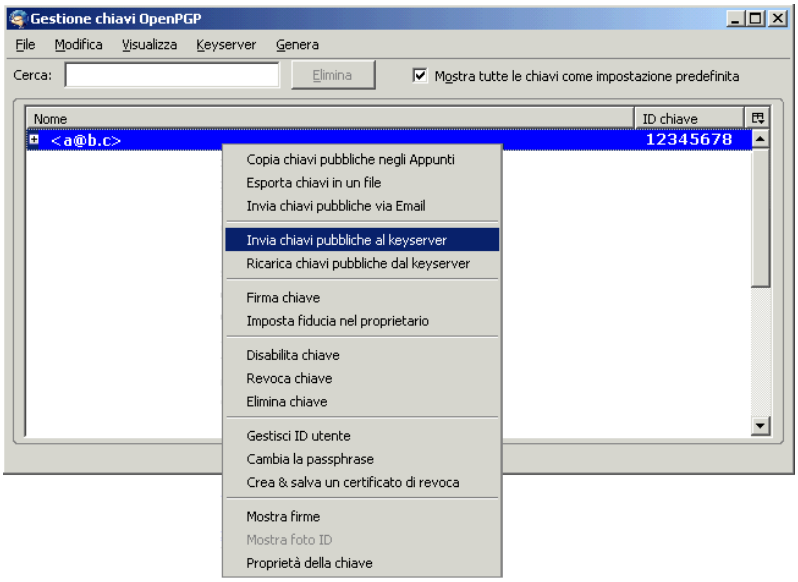



1) Clicca sulla scripta "Avanzate".
2) Come dimensione della chiave scegli 4096.
3) Puoi scegliere l'algoritmo di cifratura. (Con DSA & El Gamal sarà molto più lento).

Alla fine clicca su "Genera chiave".

A questo punto puoi fare altro per diversi minuti perchè per generare la chiave ci vorrà del tempo...

É consigliabile fare altre attività per aumentare la casualità nella generazione delle chiavi. Per esempio potresti cercare sul tuo computer un file che non c'è così da creare attività sui dischi e facilitare la generazione di chiavi più casuali possibile.




Dopo aver creato la propria chiave, cliccando con il tasto destro del mouse nelle lista delle chiavi, invia la tua chiave pubblica al keyserver e via email agli altri tuoi contatti.

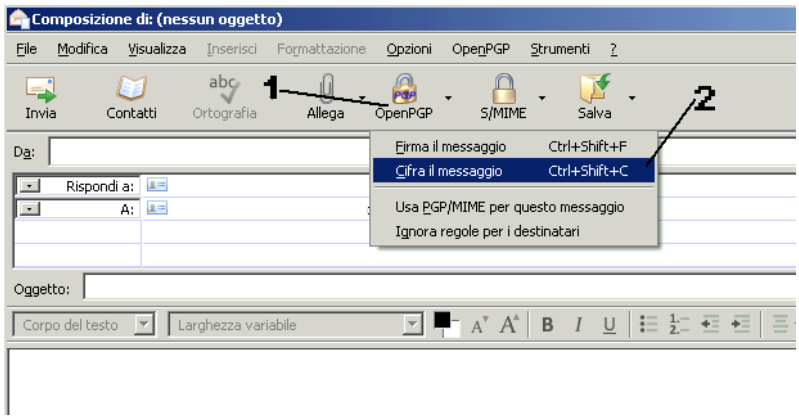
Scambiandovi le chiavi pubbliche potrete comunicare in modo cifrato.

D'ora in poi quando scrivi un messaggio basterà specificare che è criptato, enigmail userà la chiave che tu hai generato e si occuperà di usare quella del destinatari dei tuoi messaggi.

Se ti manca la chiave di qualcuno, da questa finestra puoi scegliere sul menù "Keyserver" l'opzione "Ricerca chiavi". Inserendo l'indirizzo di posta se presente saranno visualizzate le chiavi.

**Una volta generata la tua coppia di chiavi non sarà più necessario ripetere questi passaggi fatti fino ad adesso. Conserva la tua chiave privata al sicuro. Non rivelare mail la tua passphrase. Se per qualche malaugurato motivo qualcuno dovesse entrare in possesso della tua chiave, revocala e fanne un'altra.**

La finestra "gestione delle chiavi" è sempre raggiungibile dalla finestra principale di Thunderbird al menù "OpenPGP"

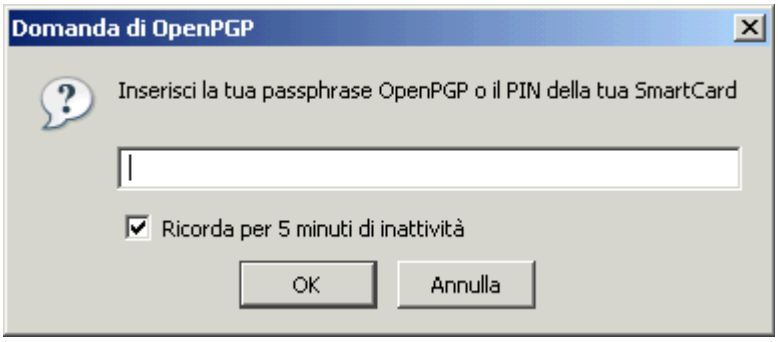



Per inviare un messaggio cifrato basta scegliere dalla finestra di composizione del messaggio:

1) Bottone "OpenPGP"
2) Cifra il messaggio

Il resto sarà automatizzato, tu devi solo scrivere il messaggio come sempre.

Durante l'invio del messaggio potrebbe apparire per un secondo un insieme di caratteri strani, quella è la cifratura automatica del messaggio.




Per ricevere un messaggio cifrato basta riceverlo normalmente, l'unica cosa diversa è che Thunderbird ti chiederà la tua passphrase per decifrare il messaggio.

(La stessa che è stata messa quando hai fatto generare la chiave).

**Ricordati di scambiare le chiavi pubbliche con i tuoi contatti prima di leggere o scrivere messaggi. Una volta ottenute le chiavi non sarà più necessario scambiarle perchè saranno già salvate nel tuo programma di posta. Accertati sempre che le chiavi siano quelle giuste controlla l'ID della chiave ed il fingerprint prima di accettarle come valide.** Se per qualche motivo, avendo già le chiavi di un tuo contatto mail capitasse che la chiave non corrisponda oppure la firma risulti alterata, comincia a dubitare.

Questi sistemi consentono di scambiarsi messaggi di posta elettronica tranquillamente in ambienti insicuri. **Ricorda che le uniche parti dei messaggi che non sono criptate sono il Subject (l'oggetto), il mittente ed il destinatario. Se invii messaggi con allegati anche il nome del file può essere visibile. Per inviare allegati in sicurezza invia tutto come PGP MIME (il programma di posta dovrebbe chiedertelo automaticamente).** Con quest'ultimo metodo il messaggio e gli allegati saranno cifrati ed inviati come una unica cosa senza possibilità di distinguere gli allegati dal messaggio da parte di malintenzionati.

I keyserver detengono le chiavi pubbliche, inviando la tua chiave puoi permettere a chiunque di comunicare con te usando le mail cifrate. Se invece non vuoi che si sappia troppo in giro che stai usando quella chiave allora inviala solo direttamente ai tuoi amici. Puoi scegliere di firmare le chiavi di chi conosci  e gli altri possono fare la stessa cosa con te. Ogni firma garantirà che quelle persone sanno che quella è proprio la tua chiave. Tuttavia eviterei di firmare e/o farsi firmare la chiave, perchè analizzando le firme delle chiavi si può risalire alla cerchia di amici e conoscenti che condividono i contatti, stile facebook. Quindi eviterei di firmare le chiavi.

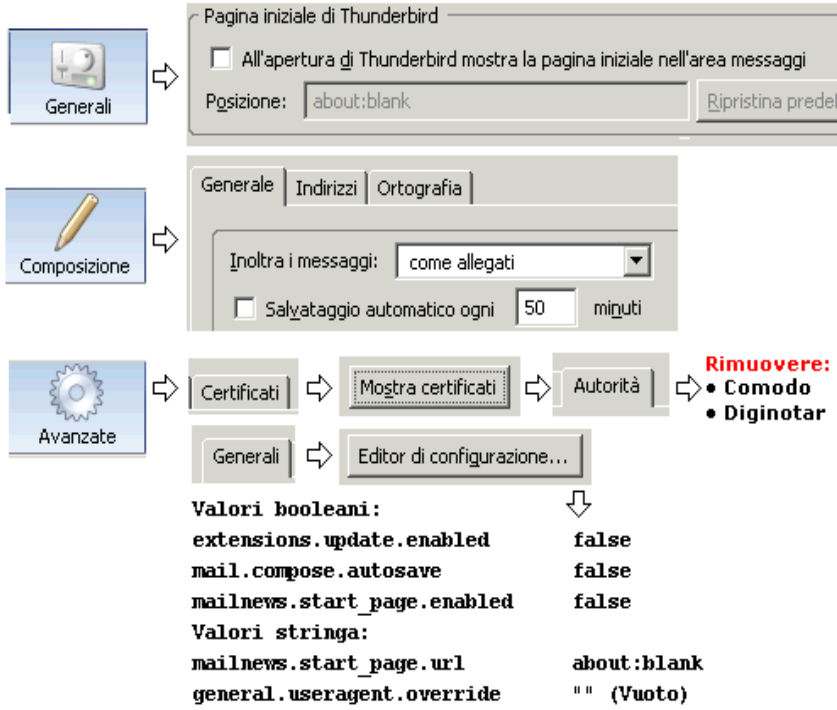
Usa la posta criptata sempre, per ogni tipo di messaggio, che si tratti di mettersi d'accordo per una pizza o che si tratti delle password per l'accesso root ad un server condiviso. Non ha importanza, l'uso costante delle email cifrate impedisce di sapere quali sono i messaggi sensibili, dove magari in essi ci sono importanti configurazioni dei server oppure password per l'accesso di piattaforme condivise o perché no, messaggi d'amore ;).

Ricordati che la tua chiave privata con la passphrase è l'unica cosa che può tradurre tutti i messaggi criptati che sono stati ricevuti da te.
Una buona pratica è **eliminare sempre i messaggi cifrati già letti,** in modo da evitare compromissioni future.

**Ricorda che per natura del sistema di posta, ogni messaggio passa da un server SMTP all'altro per un sacco di punti prima di arrivare al destinatario e non si sa mai se i tuoi messaggi sono letti da apparati pubblicitari o da malintenzionati che potrebbero connettersi alla tua rete Wi-Fi di casa. Con le email cifrate eviti qualunque problema di questi problemi e puoi comunicare in privato anche se qualcuno tenta di leggerti la posta.** I messaggi cifrati senza avere la chiave di traduzione sono solo un insieme di caratteri strani che praticamente non possono essere tradotti.

**.: Ciliegina sulla torta :.**

Queste operazioni non sono richieste, tuttavia sono la ciliegina sulla torta se vuoi fare le cose un pò meglio:
Queste impostazioni sono raggiungibili da Thunderbird, menù "Strumenti", quindi "Opzioni":
Questa immagine è riassuntiva di tutte le operazioni:




Pagina iniziale di Thunderbird: nessuna (about:blank)

- Plugin non richiesti (eccetto enigmail) disattiviati:
  Java, Flash, etc... Solo Enigmail.
- Elimina il salvataggio automatico è rischioso e "palloso" se usi GPG quando scrivi messaggi impegnativi in molto tempo.
- Certificati: Eliminare le seguenti autorità:
  Commodo e Diginotar, perchè non sono attendibili.
- Editor di configurazione:
  Aggiungi la variabile "general.useragent.ovverride" con valore stringa vuoto.
  Questo impedisce a Thunderbird di inviare informazioni nelle email relative al tuo sistema operativo ed a Engmail stesso.
- Manda un messaggio di posta a te stesso, visualizza tutti gli header e scopri se il tuo server di posta da informazioni sul tuo indirizzo IP, oppure se thunderbird è configurato per non inviare informazioni sul tuo sistema operativo.