PGP Versione Freeware

@ Pretty Good Privacy @

per Windows 95, Windows 98, Windows NT,
Windows 2000 & Windows Millennium

Manuale Utente

NOTE:

Questo manuale tratta le funzioni piu' utilizzate di PGP. Alcune caratteristiche sono solo accennate. Queste possono anche non essere presenti nella versione Freeware ma solo nella versione a pagamento. Per ulteriori informazioni vedere la documentazione allegata alla propria versione di PGP.

by amc

Caratteristiche principali di PGP

PGP mette a disposizione numerose opzioni per aiutarvi a rendere sicure le vostre e-mail, files e comunicazioni utilizzando un sistema di codifica/decodifica e un sistema di autenticazione.
Ecco cosa potete fare con PGP:

- **Cifrare/Firmare e Decifrare/Verificare la firma.**

Con i plug-ins di PGP potete accedere alle funzioni di PGP dall' interno delle vostre applicazioni.

- **Creare e amministrare le chiavi.**

Usando l' utility PGPkeys e' possibile creare, visualizzare, amministrare la propria coppia di chiavi come pure le chiavi pubbliche degli altri utenti di PGP.

- **Creare files autodecodificanti (SDAs) protetti da password.**

E' possibile creare files autodecodificanti in modo che tutti coloro in possesso della password possano leggerli. Questa caratteristica e' utile per inviare files codificati a coloro che non hanno installato PGP sul loro computer.

- **Eliminare in modo definitivo files, cartelle.**

Con l'utility PGPWipe e' possibile eliminare in modo definitivo files e cartelle senza lasciarne frammenti sparsi sull' hard disk. Con l' utility PGP Free Space Wiper e' possibile eliminare in modo capillare eventuali tracce rimaste di file precedentemente cancellati.dal vostro hard disk.

Primi passi per l' uso di PGP

- **Crea la chiave pubblica e la chiave privata.**

Dopo l' installazione occorre creare una coppia di chiavi: la chiave pubblica e la chiave privata.
E' possibile creare la coppia di chiavi durante l' installazione di PGP oppure successivamente in qualsiasi momento utilizzando l' utility PGPkeys.
La coppia di chiavi e' necessaria per:

- cifrare informazioni
- decifrare informazioni
- firmare informazioni (email o file)
- verificare l' autenticita' di una firma

- **Scambiare la chiave pubblica con quella di altri utenti di PGP**

Dopo aver creato la coppia di chiavi e' possibile iniziare a comunicare in modo sicuro con altri utenti.
Per fare questo e' necessario scambiarsi le rispettive chiavi pubbliche.
La chiave pubblica e' formata da un file di testo quindi e' estremamente semplice inviarla ad altri.
Ad esempio inserirla in un messaggio email o in un file oppure inserirla in un server pubblico direttamente in rete in modo che chiunque possa recuperarla.

- **Convalidare una chiave pubblica**

Ottenuta la chiave pubblica di un' altra persona, occorre inserire questa chiave in un apposito elenco chiamato " keyring" contenente la lista di tutte le chiavi pubbliche di altri utenti in nostro possesso. E' possibile controllare che questa chiave pubblica non sia stata manomessa e che appartenga effettivamente a una certa persona.
Questa verifica si puo' effettuare confrontando l ' impronta digitale della chiave in nostro possesso con l' impronta digitale della chiave originale.
Per maggiori dettagli vedi "Verifica dell' autenticita' di una chiave".
Quando si e' certi di possedere una chiave pubblica valida, e' possibile contrassegnarla come chiave "sicura".
In aggiunta si puo' attribuire a questa chiave pubblica un livello di affidabilita' piu' o meno alto (Trust level o livello di fiducia).
Per maggiori informazioni vedi "Verifica dell' autenticita' di una chiave".

- **Rendi sicure le tue email e files**

Dopo aver creato la tua coppia di chiavi e aver scambiato con altri la tua chiave pubblica, si puo' iniziare a cifrare, firmare, decifrare e verificare le email e i files.
Per effettuare queste operazioni e' sufficiente selezionare il file o il messaggio email da rendere sicuro e scegliere l' operazione desiderata (Encrypt, Sign, Decrypt, o Verify) dal menu di PGP.
Il menu di PGP e' disponibile direttamente all' interno delle applicazioni piu' usate come Outlook.

- **Eliminare files.**

E' possibile eliminare definitivamente e rendere irrecuperabile un file dal nostro hard disk con l'opzione Wipe.

Menu di Avvio

E' possibile avviare la maggior parte delle utility (PGPkeys, PGPtools, PGPtray, PGPnet, PGPDocumentation) tramite lo Start menu dalla barra delle applicazioni.

PGPtools

Se si sta utilizzando una applicazione email o un programma che non supporta i plug-ins, e' possibile utilizzare ugualmente tutte le funzioni di PGP direttamente da PGPtools.
Avviare PGPtools dall'icona sulla barra delle applicazioni oppure tramite **Start—>Programs—>PGP—>PGPtools.**
Se si desidera cifrare, decifrare, firmare o verificare un qualsiasi file, e' sufficiente selezionare il testo e trascinarlo su uno dei pulsanti di PGPtool.
Si puo' anche aprire un file o il contenuto degli appunti tramite uno dei pulsanti di PGPtools.
Dopo aver decodificato un file, verra' aperta una finestra con l' opzione **Save As** e PGP creera' un nuovo file in chiaro con l'estensione **.TXT** Il file criptato avra' l'estensione **.TXT.PGP**

PGP all' interno di applicazioni email

NOTA: PGP Freeware non supporta il plug-in per Lotus Notes.
PGP Freeware contiene “plugs in” per le applicazioni email piu' popolari. Mediante questi plug-in si possono effettuare quasi tutte le operazini di PGP mentre si sta scrivendo o leggendo una e-mail.
Se state utilizzando una applicazione email che non supporta i plug-in potete cifrare/decifrare i messaggi semplicemente utilizzando le utilities di PGP.
PGP ha plug-ins per le seguenti applicazioni email:
• Qualcomm Eudora
• Microsoft Exchange
• Microsoft Outlook
• Microsoft Outlook Express
• Lotus Notes
Quando i plug-in di PGP sono installati, verranno visualizzati i pulsanti **Encrypt e Sign** nella barra degli strumenti del programma che si sta utilizzando. Cliccando semplicemente su queste icone e' possibile cifrare/decifrare/firmare e verificare una firma.

PGP con Windows Explorer

E' possibile cifrare/decifrare e verificare files come documenti di Word processing, spreadsheets e video clips direttamente da Windows Explorer.
Per accedere a queste funzioni da Windows Explorer selezionare il file desiderato e quindi apparira' nel menu **File** l' opzione PGP.

PGPtray

NOTA: Potete accedere alle principali funzioni di PGP cliccando sull' icona del lucchetto grigio in basso a destra sulla barra delle applicazioni. Se non vedete questa icona, la troverete su **Start—>Programs—>PGP—>PGPtray**
NOTA: La grafica dell' icona PGtray rivela anche se l' utility PGPnet (utility per rendere sicura una rete privata) e' installata (lucchetto su simbolo rete) oppure installata ma non attiva (lucchetto su simbolo rete con X rossa).
Se PGPnet non e' installato apparira' solo il lucchetto grigio.

Usare gli appunti

Se si sta usando una applicazione che non supporta il plug-ins di PGP si possono effetuare tutte le operazioni di PGP tramite gli appunti di Windows.
Ad esempio per cifrare o firmare un testo, copiarlo negli appunti con CTRL+C, aprire PGPtools e cliccare sul pulsante desiderato, quindi effettuata l' operazione incollarlo con CTRL+V nell' applicazione.

Usare le scorciatoie

Esistono numerose scorciatoie per lavorare con PGP. Ad esempio in PGPkeys, dopo aver selezionato una chiave, e' possibile accedere a tutte le funzioni premendo il tasto destro del mouse anziche' utilizzare la barra dei menu'.
Oppure si puo' aggiungere una chiave a PGPkeys semplicemente trascinandovela sopra.
Si possono anche creare dei tasti scorciatoia personalizzati.

Il concetto di “chiave”

PGP realizzato nel 1991 da Phil Zimmerman, usa il sistema di crittografia a chiave pubblica.Ogni utente genera tramite il programma PGP una coppia di chiavi: la **chiave pubblica** e **la chiave privata**.

La **chiave pubblica** viene comunicata a tutti coloro che vogliono comunicare confidenzialmente con noi, mentre occorre mantenere segreta la propria **chiave privata**.

La procedura da adottare per la codifica e decodifica dei messaggi (o un file) e' la seguente:

> supponendo di voler spedire una mail confidenziale occorre eseguire una operazione di codifica (tramite PGP) sul messaggio da inviare utilizzando la chiave pubblica del destinatario.
>
> Il destinatario, ricevuto il messaggio cifrato, puo' provvedere alla decodifica del messaggio (con PGP) utilizzando per questa operazione la propria chiave privata.

Oltre che per codificare i messaggi, PGP puo' essere utilizzato per apporre ad un documento (E-Mail, File) la propria firma digitale che dimostra incontestabilmente l' autenticita' del messagio.

> La procedura di autenticazione di un documento da inviare avviene utilizzando la propria chiave privata e l' opzione **SIGN Now** oppure **SIGN on send** di PGP.
>
> La procedura di controllo delle firme allegate ai messaggi ricevuti avviene uttilizzando la chiave pubblica del mittente e l' opzione **Verify** di PGP.

Crea una coppia di chiavi

Prima di poter utilizzare PGP occorre essere in possesso di una coppia di chiavi.
1. Se e' la prima volta che si usa PGP occorre crearle. Si possono creare durante l' installazione di PGP oppure in qualsiasi momento andando sull' utility **PGPkey —> Keys —> New key**
NOTA: se si e' gia' in posssesso di una coppia di chiavi si puo' impostare in qualsiasi momento la cartella dove si trova la coppia di chiavi dall' utility **PGPkey —> Edit —> Option —> Files**
IMPORTANTE: e' opportuno non possedere piu' di **una** coppia di chiavi per non creare confusione tra chi deve spedirvi un file codificato.
2.. Dopo aver cliccato su **New key** si aprira' la finestra dell' utilita' **PGP key Generation Wizard** che guidera' passo passo alla creazione delle due chiavi.
3. Cliccando su **Next apparira'** una nuova finestra in cui e' presente un pulsante **Expert** tramite il quale si possono definire parametri avanzati per la creazione delle chiavi. (Vedi piu' avanti).

4. Si puo' tralasciare **Expert** e premere **Next** quindi inserire il proprio nome e indirizzo email.
Non e' necessario inserire nome e indirizzo email veritieri. In ogni caso se questi dati sono esatti sara' piu' facile identificare la vostra chiave pubblica negli archivi e se anche l 'indirizzo e-mail e' quello giusto, i plug-in di PGP riconosceranno automaticamente la vostra chiave.
5. Nel box della **Passphrase** inserire una frase o stringa di caratteri o parole che serviranno per farvi accedere alla vostra chiave privata. Per confermare premere il tasto TAB per passare alla riga successiva e reinserire la Passphrase scelta.
Per evitare che occhi indiscreti possano leggere la vostra Passphrase mentre la digitate, i caratteri che scrivete non sono visibili. Se siete sicuri che nessuno vi sta osservando eliminare la spunta nella casella **Hide Typing** e potrete cosi' vedere cio' che state digitando.
NOTA: Per una Passphrase sicura bisogna che contenga parole composte, spazi, numeri e segni di punteggiatura. In ogni caso cercate di avere una Passphrase che solo voi riuscite a ricordare facilmente e ricordate che un carattere minuscolo e' considerato diverso dallo stesso carattere scritto in maiuscolo. Se la Passphrase e' lunga e complessa e' piu' sicura ma sara' anche piu' difficile da ricordare e da scrivere.

6. Cliccare **Next** per iniziare il processo di generazione delle chiavi. Il movimento del mouse e le battute di tasti a caso generano dei valori casuali che PGP usa per generare le chiavi. Se queste informazioni casuali sono insufficienti PGP aprira' una finestra di avviso.

7. Cliccare **Finish** e PGP memorizzera' automaticamente le due chiavi nell' elenco delle chiavi pubbliche e private pubring.pkr e secring.skr

l **Per generare una coppia di chiavi con l' opzione Expert:**
Come detto piu' sopra, durante la fase di creazione delle chiavi e' possibile premere il tasto **Expert** per definire il tipo di chiave, la lunghezza, e anche la data di scadenza e di validita'.

Scegliere **Diffie-Hellman/DSS** per utilizzare propieta' avanzate delle chiavi come il multiple encryption, l' Additional Decryption o l' aggiunta di foto nella chiave.
Attualmente anche le chiavi di tipo **RSA** supportano tutte le funzioni di **Diffie-Helman/DSS** a differenza delle versioni piu' datate e delle chiavi **RSA Legacy**

Cliccare **Next** e nel box **Key Size** inserire la dimensione della chiave che puo' essere 1024 to 4096 bits per Diffie-Hellman/DSS e 1024 to 2048 per chiavi di tipo RSA. La sicurezza aumenta con la dimensione della chiave ma contemporaneamente aumenta il tempo necessario per le operazioni di cifratura.

Impostare eventualmente anche la data di scadenza della chiave. Di solito la scadenza viene inserita solo in casi particolari ma normalmente le chiavi personali non hanno scadenza.

Creare la passphrase

Per una serie di ragioni riguardo la sicurezza, non si consiglia di scegliere una parola singola bensi' una frase (passphrase). Una singola parola e' soggetta ad essere facilmente scoperta facendo semplicemente dei tentativi a caso.
Comunque e' possibile aumentare la sicurezza anche di una singola parola scrivendola combinando lettere maiuscole con lettere minuscole e inserendo anche spazi, numeri e segni di punteggiatura. Ad esempio se si sceglie una parola come **mongolfiera,** la passphrase potrebbe essere: **1.MonGoLFieRa,9**

Modificare una coppia di chiavi

Dopo aver creato la coppia di chiavi, e' possibile apportarvi delle modifiche:
- aggiunger una foto alla chiave pubblica
- aggiungere una subkey
- aggiungere un nuovo nome utente
- aggiungere un nuovo indirizzo email
- modificare la passphrase
- ecc.

- **Cosa posso fare se dimentico la passphrase o perdo la mia chiave?**

Se perdi la tua chiave privata o dimentichi la passphrase non potrai piu' decodificare i messaggi a te indirizzati.
Esiste una possibilita' di recupero della chiave se hai adottato l' opzione di recupero su server (solo per le versioni di PGP abilitate)

Inserire una chiave pubblica in una email

1. Apri PGP keys.
2. Seleziona la tua coppia di chiavi (key pair) quindi dal menu Edit clicca su Copia.
3. Apri l' editor che utilizzi per scrivere il messaggio e incolla nel punto desiderato la chiave con **Paste**.

In alcune applicazione come Outlook e' sufficiente selezionare la chiave e trascinarla all' interno del messaggio.

Inserire la chiave pubblica in un file

Ci sono tre metodi per esportare una chiave tramite un file:
• Seleziona l' icona della tua Key Pair quindi dal menu Keys seleziona Export. Inserisci quindi il nome col quale vuoi che venga memorizzata.
• Trascina l' icona che rappresenta la tua coppia di chiavi dentro una cartella.
• Seleziona l' icona della tua coppia di chiavi quidi dal menu Edit scegli Copy quindi la puoi incollare all' interno di un qualsiasi documento di testo.

Ottenere una chiave pubblica di altri

La procedure e' semplice in quanto la key pubblica e' un blocco di testo e come tale si puo' trattare con diversi metodi:
• Prendi la chiave da un server
• Aggiungi una chiave direttamente da un messaggio email.
• Importa la chiave da un file

Verifica l' autenticita' di una chiave

Il metodo piu' sicuro per scambiarsi una chiave pubblica e' passarla con un floppy disk.
Poiche' questo metodo e' di difficile attuazione e nella maggior parte dei casi si utilizza lo scambio via email, e' importante verificare che la chiave appartenga effettivamente a quella persona. PGP mette a disposizione alcuni strumenti per fare questa verifica.

- **Verifica con l' impronta digitale**

Si puo' controllare che la chiave pubblica appartenga veramente a una persona confrontando l' impronta digitale (che e' una serie di nomi o numeri esadecimali generati al momento della creazione della chiave) con l' impronta della chiave originale.
1. Apri PGPkeys e seleziona la chiave pubblica da verificare.
2. Seleziona Properties dal menu Keys
3. Confronta l' impronta digitale (a scelta una serie di nomi o numeri esadecimali) con l' impronta digitale della chiave originale.

L' impronta digitale della chiave originale occorre ottenerla tramite un canale sicuro.
Ad esempio se si e' ottenuto la chiave tramite email, si puo' confrontare l' impronta con quella della chiave presente su un server sicuro, oppure si puo' chiamare telefonicamente il proprietario della chiave.

Convalidare una Chiave Pubblica

La **validita'** e la **fiducia** (Trust) che si attribuiscono a una chiave pubblica presente nel proprio Key ring, sono due concetti di vitale importanza per l' uso di PGP.
Il sospetto che potrebbe sorgere a un utente che riceve una chiave pubblica da un Keyserver e' che la chiave ricevuta non

appartenga effettivamente alla persona a cui si desidera scrivere.
Cio' implica che non ci si puo' fidare nemmeno della firma digitale di quell' utente.
Infatti la garanzia di autenticita' di una firma digitale si ha solo avendo la certezza che la chiave pubblica che la verifica matematicamente appartiene al suo ufficiale proprietario.
E' possibile che un utente malintenzionato sostituisca la chiave pubblica di un utente con una chiave pubblica creata appositamente per intercettare le comunicazioni.
Per evitare che simili casi si verifichino, si puo' far apporre una firma digitale alla chiave pubblica da un ente o persona della quale entrambe le parti si fidano.
Nel caso di PGP si parla di una **misura di fiducia** associata alle firme apposte da altre persone sulla chiave pubblica; se le firme sono di persone di nostra fiducia, esse ci garantiscono dell' autenticita' della chiave pubblica e quindi della firma digitale che abbiamo verificato.
Poiche' la sequenza delle firme non e' organizzata secondo alcuna gerarchia formale, ma ha valore in funzione delle singole firme, si crea una rete di fiducia nota come **Web of Trust.**

In breve, se siete assolutamente sicuri di essere in possesso di una chiave pubblica autentica di un' altra persona, potete firmare e quindi convalidare questa chiave.
Firmando e quindi autenticando la chiave pubblica di questa persona, certificate l' autenticita' e la provenienza di questa chiave.
Quando create una vostra nuova chiave, questa viene automaticamente convalidata con la vostra firma digitale.
Quando convalidate una chiave con la vostra firma, per default questa viene convalidata solo sulla vostra lista (Key ring) e la convalida che le attribuite, a meno che non si spunta la casella **Allow signature to be exported,** non viene esportata, cioe' se inviate questa chiave a un vostro amico, questa chiave per lui dovra' essere ancora convalidata.

Certificare una chiave pubblica

1. Aprire PGP Keys e selezionare la chiave desiderata.
2. Aprire il menu Keys e selezionare Sign. Si aprira' una finestra con la chiave e la relativa impronta digitale.
3. Spuntare la casella **Allow signature to be Exported** per esportare eventualmente questa chiave con la vostra convalida.

Selezionare **More Choices** per attivare altre opzioni::
- **Non-exportable.** Per convalidare questa chiave ma non permettere di esportare la vostra certificazione.
- **Exportable.** Permette anche l' esportazione della vostra certificazione. L' effetto e' lo stesso della spunta della casella **Allow signature to be exported**
- **Durata della convalida**

Se non avete alcuna possibilita' di verificare l 'autenticita' di una chiave pubblica ma dovete fidarvi della convalida effettuata da un' altra persona, potete assegnarle un livello di fiducia a vostra discrezione (Trust Level).
Infatti, dopo aver certificato la firma come sopra, viene abilitata la barra Trust in cui muovendo il cursore potete modificare il livello di affidabilita'.
Barra vuota: chiave non valida o non affidabile.
Barra evidenziata a meta': chiave poco affidabile oppure utente che l' ha convalidata poco affidabile.
Barra totalmente evidenziata: chiave (o utente) valida (o affidabile)
Barra zigrinata: la propria chiave che per convenzione e' valida e affidabile. Anche la propria chiave in ogni caso deve essere convalidata come sopra.

Aggiungere una foto alla propria chiave

NOTA: Questa caratteristica e' disponibile per le chiavi di tipo Diffie-Hellman/DSS e RSA keys ma non per quelle di tipo RSA Legacy keys.

1. Aprire PGPkeys, selezionare la vostra coppia di chiavi quindi cliccare su **Add Photo** nel **Keys** menu. Si aprira' la relativa finestra.
2. Trascinare o incollare la propria foto nel box **Add Photo** dialog box oppure sceglierla tramite **Select File**.

NOTA: La fotografia puo' essere anche essere importata dagli appunti e deve essere di tipo .JPG o .BMP .
Per una buona qualita' dell' immagine, questa deve essere in formato 120x144 pixel prima di inserirla.
In caso contrario sara' PGP che portera' l' immagine a questa risoluzione ma il risultato potra' non essere soddisfacente.

3. Cliccare su **OK** e apparira' il box per inserire la **Passphrase**.
4. Inserire la Passphrase e premere **OK.**
La fotografia sara' aggiunta alla chiave e visualizzata in una finestra delle proprieta'.
IMPORTANTE: ogni volta che effettuate delle modifiche alle vostre chiavi ricordatevi di effettuare l' aggiornamento anche sul server in rete per renderle disponibili a tutti.

- **Sostituire la foto nella chiave**

1. Aprire PGPkeys e selezionare la foto elencata sotto la chiave.
2. Cliccare su **Delete** nel menu **Edit** .
3. Aggiungere una nuova foto seguendo la procedura sopra descritta.

Aggiornamento delle chiavi sul key server

Se avete cambiato indirizzo email oppure avete effettuato delle modifiche alla vostra chiave, occorre aggiornare anche il server con la nuova chiave.
L' aggiornamento (aggiunta di ID, firme, foto) di una chiave e' una operazione semplice che si esegue con l' opzione update del menu server.
Se pero' l'aggiornamento consiste nel cancellare ID e firme associati alla vostra chiave pubblica, occorre tenere presente che i server pubblici permettono solamente l' aggiunta di nuove informazioni al proprio data base e non permettono **mai** di cancellare un user name o firma associati alla vostra chiave.
Un modo per effettuare questa operazione e' quello di appoggiarsi **unicamente** ad un server LDAP, inoltre occorre che questo server sia configurato in modo da accettare questo comando.
Ammesso di avere a disposizione un server LDAP e che questo sia abilitato a effettuare questa operazione, la procedura da effettuare e' la seguente:
1. Aprire PGPkeys
2. Connettersi al server LDAP e cercare la chiave
3. Trovata la chiave premere il tasto destro e quindi Delete. La chiave verra' cancellata dal server dopo aver inserito la Passphrase.
4. Aggiornare la chiave togliendo gli ID e le firme
5. Inviare la chiave aggiornata al server LDAP
A questo punto se il server LDAP e' configurato in modo da sincronizzarsi automaticamente, tutte le modifiche apportate alla vostra chiave verranno effettuate anche sugli altri server pubblici.

Per fare in modo che una certa chiave memorizzata sul server non venga piu' utilizzata esiste un sistema piu' semplice e cioe' occorre utilizzare l'opzione di Revoca.

Revoca di una chiave

Se per un qualsiasi motivo decidete di non utilizzare piu' una vostra coppia di chiavi, potete revocarne la validita' e inserirla nel server in modo che tutti gli utenti possano sapere che questa chiave non e' piu' valida.
1. Aprire PGPkey e selezionare la chiave da revocare.
2. Selezionare **Revoke** dal menu **Keys**. Si aprira' una finestra e cliccare **OK** .
3. Si aprira' una finestra in cui inserire la **Passphrase,** quindi cliccare su **OK**.
Una chiave revocata cioe' non piu' valida e' contrassegnata con una X rossa.
4. Inviare la chiave revocata sul server.

ATTENZIONE: coloro che sono in possesso della vostra chiave pubblica possono a loro volta inviarla su di un server.
Quindi puo' capitare che se avete cancellato una vostra chiave da un server questa puo' riapparire.
E' consigliabile controllare a distanza di tempo che la chiave sia cancellata o revocata definitivamente.

Usare PGP con ICQ

PGP permette di scambiarsi messaggi codificati tramite ICQ in modo semplice utilizzando plug-ins.
E' possibile codificare i messaggi prima di inviarli su Internet e quindi decodificarli e verificarli automaticamente all' arrivo subito dopo averli aperti.
Quando il plug-in per ICQ e' installato nel sistema, verra' visualizzato il simbolo del lucchetto e il tasto **Send** nella finestra di invio messaggi.

- **Scambiare la chiave pubblica via ICQ**

IMPORTANTE: ICQ permette di inviare messaggi di lunghezza illimitata a utente online. Tuttavia se l' utente e' offline, la lunghezza massima del messaggio non puo' superare i 450 caratteri. Poiche' i messaggi codificati possono superare questa lunghezza, si raccomanda di inviare la chiave pubblica e i messaggi codificati solo a utenti online.
1. Fare Doppi Click sul nome della persona a cui si vuole inviare la nostra chiave pubblica.
2. A questo punto si puo' anche scrivere un messaggio normalmente.
3. Cliccare su **Send Key.** La chiave verra' associata al vostro numero personale di ICQ e quindi inviata insieme al messaggio.

NOTA: In questo caso il testo inviato non e' ancora codificato.

- **Aggiungere la chiave ricevuta con ICQ al proprio Keyring:**

1. Aprire il messaggio che contiene la chiave.
2. Selezionare la chiave e cliccare su **Import** per aggiungerla alla propria lista di chiavi.

- **Inviare un messaggio codificato con ICQ:**

1. Comporre normalmente il messaggio.

NOTA: La formattazione del testo viene persa in fase di decodifica.
3. Cliccare sull' icona del lucchetto (nella finestra di scrittura messaggio di ICQ). Il messaggio viene criptato.
4. Cliccare su **Send**.