(nuovo)Partito comunista italiano
Comitato Centrale
Sito: http://www.nuovopci.it
e.mail: lavocenpci40@yahoo.com

Delegazione:
BP3 4, rue Lénine 93451 L'Île St Denis (Francia)
e.mail: delegazionecpnpci@yahoo.it

24 febbraio 2019

Istruzioni per l'uso del programma di criptazione PGP

1. Innanzitutto non lasciarti intimorire e non andare in ansia per ciò che devi imparare a fare!

Inizialmente può sembrare complesso usare PGP: in realtà non lo è. È solo una cosa nuova e, in quanto tale, una cosa da imparare a fare, da apprendere. Come ogni cosa è comprensibile, ma ha sue leggi e suoi procedimenti. Con un po' di esercizio (svolgendo varie volte il procedimento) ciò che ti appare come "complesso" diventerà semplice e, quasi, "meccanico". Se incontrerai dei problemi in corso d'opera, ci scriverai e assieme ne verremo a capo.

Inoltre non devi "andare in ansia" per timore di commettere errori che permetteranno alla polizia politica di leggere i messaggi criptati oppure che le permetteranno di localizzare il Centro clandestino del (n)PCI: se segui i passaggi qui di seguito indicati è infatti quasi impossibile che la polizia politica riesca a leggere i messaggi criptati; per quanto riguarda invece il Centro clandestino del (n)PCI, esso non fa dipendere la sua sicurezza dall'uso che tu farai di queste istruzioni, ma adotta tutta una serie di misure di sicurezza che prescindono da quello che tu farai (se ci pensi sarebbe molto ingenuo far dipendere la propria sicurezza dall'azione di principianti della sicurezza informatica!). Stai tranquillo/a, quindi, e dedicati a seguire con attenzione le istruzioni.

In queste istruzioni abbiamo cercato di fissare in modo chiaro e accessibile a tutti, i passaggi da svolgere per usare PGP. Se però tu trovi che un passaggio è "oscuro", segnalacelo.

2. Il meccanismo di funzionamento di PGP

In estrema sintesi questo è il funzionamento del programma di criptazione PGP: ci sono due corrispondenti; ognuno ha una sua "coppia di chiavi" (una privata e una pubblica) creata da lui usando il programma PGP; i due corrispondenti si scambiano le rispettive chiavi pubbliche. Ognuno di essi cripta con la chiave pubblica dell'altro ogni messaggio che gli invia: dalla criptazione risulta un file che solo l'altro è in grado di leggere (perché solo lui dispone della propria chiave privata, indispensabile per leggere il file criptato).

3. Un accorgimento

L'ideale è usare due computer: un computer che si collega ad internet per ritirare e inviare via mail i messaggi criptati con PGP e un computer che non si collega mai ad internet, in cui istallare il programma PGP e da usare per scrivere le lettere, criptarle e per decriptare le lettere ricevute.

In seconda battuta, se non si hanno due computer, bisogna che quando il computer lo si usa per scrivere, criptare o per decriptare le lettere ricevute sia scollegato da internet durante l'uso. Questo metodo è quello meno sicuro: nel computer la polizia politica può infatti inserire via internet un "virus spia" che copia (registra) l'attività svolta sul computer anche

quando è scollegato da internet e, una volta riattivata la connessione ad internet, trasmette a chi lo utilizza le informazioni che ha registrato.

Per prendere contatto con noi attraverso PGP non bisogna attendere necessariamente di avere due computer: l'importante seguire il procedimento indicato e avere un buon antivirus sul computer.

4. Per scaricare il programma PGP

Il file per installare il programma PGP (detto anche "Kleopatra") si trova al seguente indirizzo internet: http://www.gpg4win.org/download.html Quando apri la pagina del sito, clicca sulla finestra "Download Gpg4win 3.1.5". Così facendo si apre una nuova pagina, in cui ti viene chiesto di effettuare un pagamento o di fare una donazione: clicca su $0 e poi su "Download". Dopo questo passaggio scarichi e istalli sul tuo computer il programma come fai normalmente con qualsiasi altro programma.

5. Per creare la tua "coppia di chiavi" PGP

Una volta installato il programma sul computer, scollega il computer da internet (o, meglio ancora, istalla il programma PGP sul computer che non colleghi mai ad internet) e procedi con la creazione della tua "coppia di chiavi" PGP. Indichiamo in dettaglio i passaggi che devi svolgere:

1. Entra in Kleopatra, cliccando sull'icona (volto stilizzato di una donna con i capelli rossi a caschetto);
2. Vai su "File";
3. Clicca su "Nuova coppia di chiavi";
4. Clicca su "Crea un nuova coppia di chiavi personali OpenPGP";
5. Inserisci un nome e un indirizzo mail di fantasia nel riquadro "Inserimento dati" (ad es. Giovanni, giovanni2019@riseup.net); dopo questo, restando sulla stessa pagina, vai su "Impostazioni avanzate"; qui togli il segno di visto su "Valida" in modo da disattivare la scadenza del programma e farlo durare più a lungo. Poi premi "ok": così ritorni nel riquadro "Inserimento dati", dove clicchi su "Successivo";
6. Accedi così alla pagina "Ricontrolla i parametri" e clicca su "Crea";
7. Appare un riquadro con un lucchetto, dove devi inserire la password che intendi utilizzare per usare le tue chiavi PGP nella corrispondenza con noi (più complicata è, meglio è: ad es. combina circa 40 lettere e cifre, possono essere anche parole intervallate da numeri). A questo punto appare un riquadro con scritto: "Coppia di chiavi creata correttamente" (se il programma non accetta la password, ripeti l'operazione). Hai creato la tua "coppia di chiavi" PGP!
8. Sempre nel riquadro "Coppia di chiavi creata correttamente" appare la voce "Fai una copia di sicurezza delle tue chiavi" (in modo da farti un doppione): clicca su di essa. Si apre così il riquadro "Esporta certificato segreto - Kleopatra": sul lato destro di "File in uscita" trovi una icona rettangolare; clicca su questa icona rettangolare, inserisci il nome che vuoi dare al file (un nome qualsiasi, ad es. "Federico Verdi") e seleziona dove intendi salvare questo file (ad esempio "Desktop"), procedi quindi cliccando su "Salva";
9. A questo punto ti ritrovi in "Esporta certificato segreto - Kleopatra" e premi "OK"; appare una finestra con il lucchetto; inserisci la password che hai precedentemente creato per utilizzare le tue chiavi PGP (v. il precedente punto 7);
10. Ti appare "Chiave segreta esportata correttamente", premi quindi "Ok" e poi "Fine";

11. A questo punto sul dekstop compare il file "Federico Verdi.pgp" (è il doppione della tua "coppia di chiavi" PGP). Copialo su una chiavetta USB, che devi conservare in un luogo sicuro. Cancella dal dekstop il file "Federico Verdi.pgp" con un programma di cancellazione sicura (ad es. Eraser).
Sintetizzando: con questo procedimento hai creato sia la tua "coppia di chiavi" PGP, che il suo doppione.

6. Per rendere la tua chiave pubblica PGP un file a se stante (in modo da inviarla a noi)

1. Clicca sull'icona di Kleopatra (volto stilizzato di una donna con i capelli rossi a caschetto); trovi scritto il nome che hai dato al file contenente la tua chiave PGP (v. punto 5 del capitolo precedente, ad es. Giovanni, giovanni2019@riseup.net);
2. Con la freccia del mouse vai su questo nome (ad es. ad es. Giovanni, giovanni2019@riseup.net), clicca su di esso con il tasto destro del mouse e poi premi "esporta": appare un'icona con scritto "esporta certificati" e nella voce "file" troverai un nome incomprensibile che finisce con ".asc". Cambi il nome del file incomprensibile (l'ideale è dargli un nome che ti fa ricordare che è la tua chiave pubblica: ad es. "rossa pubblica") lasciando però alla fine ".asc" e lo salvi. *Questo file che termina con ".asc" è la tua chiave pubblica, che devi inviare a noi in modo da permetterci di scriverti messaggi criptati e, dunque, leggibili solo da te.*

7. Per scrivere a noi

Per scrivere a noi innanzitutto devi fare le seguenti operazioni preliminari:
- ricordati di usare un computer scollegato da internet per scrivere la lettera che vuoi inviarci (o, meglio ancora, usa un computer che non connetti mai ad internet e in cui hai installato anche il programma Kleopatra);
- devi avere a disposizione il file con la chiave pubblica PGP del (n)PCI (reperibile sul nostro sito internet: http://www.nuovopci.it/PGP/chiave_pubblica_PGP_(n)PCI.asc)
- dopo aver scritto la lettera per noi, entri in Kleopatra (cliccando sul volto stilizzato di una donna con i capelli rossi a caschetto), premi su "Importa" (si trova sotto "Strumenti"); si apre la finestra "Seleziona file certificato". Usando il mouse clicchi quindi sul file con la chiave pubblica PGP del (n)PCI (il file della chiave pubblica del (nuovo)PCI si chiama: "chiave_pubblica_PGP_(n)PCI.asc") e poi premi "apri". *A questo punto la chiave pubblica PGP del (n)PCI è registrata nel tuo Kleopatra: questo è un tassello fondamentale per poter comunicare con noi in modo criptato.* Nota: la registrazione nel tuo Kleopatra della chiave pubblica PGP del (n)PCI va fatta solo una volta, non occorre ripetere l'operazione ogni volta che vuoi scriverci (la chiave resta infatti registrata sul tuo Kleopatra).

Fatte queste tre operazioni preliminari, procedi con la criptazione della tua lettera per noi. Questi sono i passaggi da fare:
1. Entra in Kleopatra (cliccando sul volto stilizzato di una donna con i capelli rossi a caschetto), clicchi su "Firma/Cifra" (si trova sotto "File"), si apre la pagina "Seleziona uno o più file da cifrare o firmare" e selezioni il file con la tua lettera, poi premi su "apri";
2. A questo punto si apre la pagina "Firma/cifra file - Kleopatra"; dentro questa pagina trovi "Cifra per gli altri": alla destra di "Cifra per gli altri" c'è un rettangolo, tu devi cliccare sul simbolo che si trova dentro questo rettangolo; si apre la finestra "Selezione dei certificati - Kleopatra"; clicca sulla chiave pubblica PGP del (n)PCI e poi premi "Ok";
3. Torni così nella pagina "Firma/cifra file - Kleopatra"; premi su "Firma/cifra"; si apre un'altra finestra e inserisci la password che hai creato per usare le tue chiavi PGP; clicca su "Ok"; si apre la pagina "Risultati" e appare un rettangolo

celeste con scritto “Firma e cifratura riuscite”; clicca su “Fine”. *Se invece l’operazione non riesce (non appare il rettangolo celeste con scritto “Firma e cifratura riuscite”), ripeti l’operazione dall’inizio.*

4. A questo punto appare la tua lettera criptata: ha lo stesso nome del file che hai criptato seguito però da “.gpg” e, inoltre, il file ha il simbolo di un lucchetto. **Questo è il file che devi inviarci, allegandolo a una tua mail.**

Alcuni accorgimenti:

- se vuoi restare completamente anonimo, devi creare una casella mail con TOR e inviarci da essa (connettendoti sempre con TOR) il messaggio criptato con PGP. Se non usi TOR, la polizia politica capirà che tu entri in contatto con noi, ma non sarà in grado di conoscere il contenuto della tua lettera criptata con PGP e il contenuto delle lettere criptate che riceverai da noi. TOR lo puoi scaricare al seguente link: https://www.torproject.org/ . La casella mail puoi crearla facilmente con TOR in uno dei seguenti siti: https://www.netcourrier.com/ - https://www.tutanota.com/ - https://www.autistici.org/

- prima di inviarci la lettera criptata, cambia il nome del file: con il tasto destro del mouse clicca sul file con il simbolo di un lucchetto e dagli un nome che non richiama il contenuto della lettera (ad es. “manifestazione”, “gita”, ecc.), con l’accortezza di lasciare però alla fine del nome del file “.gpg”;

- nella mail che ci invii assieme alla lettera criptata non fare riferimenti al contenuto della lettera criptata, ma parla di altro per confondere le acque, facendo attenzione però a ad essere coerente con il nome che hai dato al file criptato (ad es. se il nome del file criptato è “manifestazione”, nella mail che ci invii tratti di una manifestazione);

- se è la prima volta che ci scrivi, oltre ad allegare alla tua mail la lettera criptata, allega anche la tua chiave pubblica PGP in modo da permetterci di risponderti a nostra volta in modo criptato.

8. Per leggere le nostre lettere criptate:

1. Copia su una chiavetta USB il file criptato che ti abbiamo inviato;

2. Ricordati di scollegare il computer da internet (o, meglio ancora, di usare un computer che non connetti mai ad internet e in cui hai installato Kleopatra);

3. Entri in Kleopatra, premi su “Decifra/Verifica”, selezioni con il mouse il file con la nostra lettera criptata, premi “Apri” e inserisci la tua password. *A questo punto hai la nostra lettera leggibile.*

.