

# Cripto libretto

Unit hacklab - unit@paranoici.org

1 Aprile 2019

## Contents

<b>1</b>	<b>Per una corretta igiene digitale</b>	<b>3</b>
<b>2</b>	<b>Usiamo software libero e a sorgente aperta</b>	<b>3</b>
<b>3</b>	<b>Una buona password</b>	<b>3</b>
3.1	Non usare la stessa password . . . . .	4
3.2	Il password manager . . . . .	4
3.3	La passphrase . . . . .	5
3.4	Doppia autenticazione . . . . .	5
<b>4</b>	<b>Accecare la telecamera del portatile</b>	<b>6</b>
<b>5</b>	<b>Navigazione consapevole</b>	<b>6</b>
<b>6</b>	<b>Navigazione anonima</b>	<b>7</b>
<b>7</b>	<b>Navigazione paranoica</b>	<b>8</b>
<b>8</b>	<b>Usare un sistema operativo libero</b>	<b>9</b>
8.1	Scaricare e installare una distribuzione GNU/Linux . . . . .	9
<b>9</b>	<b>GnuPG, la crittografia pesante a doppia chiave</b>	<b>11</b>
9.1	Installazione . . . . .	12
9.2	Configurazione e creazione delle chiavi . . . . .	12
9.3	Uso . . . . .	12

9.4	Verifica . . . . .	13
9.5	Fingerprint, revoca e backup . . . . .	13
10	Un lucchetto alla penna Usb	13
11	Verificare l'integrità di un software scaricato	14
12	Cancellare i metadati da un file	15
13	Condividere un documento in maniera anonima	15
14	Nascondere un messaggio in una foto	16
15	Collegarsi a un pc usando ssh con scambio di chiavi	17
16	Self hosting con Nextcloud	18
17	Mettere un software in scatola	18
18	Comunicazione sicura dal telefonino	19
19	Backup incrementale sicuro e remoto con duplicity	19
20	Risorse	20
21	Consigli	21
22	Storia	21



unit hacklab, Milano 2019

- Automazione usando make

Il sorgente è disponibile:

<https://git.abbiamoundominio.org/unit/criptolibretto>

Licenza Copyleft

*Libertà di distribuire e modificare con la stessa licenza*

Shoutz: crudo, dan, putro.

## 1 Per una corretta igiene digitale

Usiamo il termine: “igiene digitale” perché ci sembra che esistano elementi di base dell’uso delle reti e dei dispositivi che sono l’equivalente del lavarsi i denti. Quando viene presentato un problema e al suggerimento di una eventuale soluzione viene risposto: “ma questa è sbatta” è il segnale che il problema era un altro. Ok non RTFM, ma almeno la parte di come non prendere la scossa è meglio leggerla. Crediamo nell’alfabetizzazione informatica e che si debba studiare la grammatica della questione tecnica, non perché tutti debbano essere programmatori, ma perché nessuno sia schiavo.

## 2 Usiamo software libero e a sorgente aperta

Perché il software ha degli aspetti sociali e non ci si può fidare di ciò che non è libero.

<https://gnu.org/philosophy/free-sw.it.html>

Usiamo un sistema operativo GNU/Linux.

Il quale esiste in infinite versioni, chiamate distribuzioni. Consiste in un insieme di software per formare un sistema operativo, tra cui la collezione di software libero GNU con licenza libera GPL, il Kernel chiamato Linux e in alcuni casi, ad esempio per i driver della scheda wifi per alcuni portatili, dei pezzi di software non-libero necessari al funzionamento.

Si dice software libero quello che è studiabile, riproducibile e modificabile. Perché sia studiabile bisogna che il codice sorgente sia disponibile, perché sia riproducibile e modificabile bisogna che la licenza d’uso lo permetta. Il software chiamato solamente *open* permette lo studio, ma non è automatico che permetta anche la copia e la modifica.

## 3 Una buona password

Usare delle password *forti*, che contengano sia lettere minuscolo e maiuscole che numeri e anche altri caratteri come questi: `!@&%#)(*_:?`

### 3.1 Non usare la stessa password

Un conto è la password che si usa per sbloccare il proprio Pc, la quale non viaggia in internet, un altro sono le password che si usano per utilizzare dei servizi online di terze parti.

Il servizi online sono detti SaaS (software as a service), si tratta di software, come Facebook o Google Drive, che non sono installati sul Pc ma che sono accessibili solamente online, in forma di servizio.

Non usare mai la stessa password per diversi servizi online. Quando il servizio sarà compromesso, la password diventerà pubblica ed è meglio che non coinvolga tutto il tuo ecosistema. Per ogni servizio, una diversa password.

I servizi sono tanti ed è difficile ricordare a memoria tante password diverse, per questo è consigliabile l'utilizzo di un password manager.

### 3.2 Il password manager

Usando un password manager non c'è bisogno che la password facile da ricordare e potremo usare delle password forti.

KeePassXC è un software per la gestione di password che offre un luogo sicuro dove scriverle, ma non bisogna dimenticare la sua password di sblocco. In questo caso è bene usare una *passphrase*.

<https://keepassxc.org>

```
apt-get install keepassxc
```

Per usare un password manager si sceglierà una frase di sblocco e il nome del documento che contiene i dati crittografati da salvare sul disco del Pc. Quel piccolo file è un database e bisogna averne un backup, ma visto che è un file crittato inutilizzabile per chi non conosce la frase di sblocco, non è difficile salvare una copia anche solo in una penna Usb.

<https://cryptpad.fr>

**Prism-break** fornisce un elenco di strumenti per liberarsi dai programmi globali di sorveglianza

<https://prism-break.org/it>

Questa è una lista parziale: esistono altri progetti con la stessa attitudine di rifiuto di far diventare un business la difesa della privacy e si basano su donazioni volontarie. Diffidate da chi vuole vendervi un prodotto per la vostra difesa.

## 21 Consigli

Il computer non ha un cervello, usa il tuo.

Non fidarti troppo di chi ti dà consigli.

## 22 Storia

Il criptolibretto nasce dentro Unit hacklab per avere un pieghevole da distribuire come promemoria e appunti al cryptoparty organizzato in Macao a Milano il 15 aprile 2018. Continua con l'intento di essere un sintetico supporto aggiornato perché la causa della libertà nel 21esimo secolo è inestricabilmente connessa alla resistenza alla sorveglianza elettronica.

Il metodo (DIY) per la creazione del libretto può essere utilizzato da singole o gruppi per fare e pubblicare autoproduzioni. Nel caso, fatecelo sapere!

Questo (cripto) libretto è stato scritto e impaginato usando software libero (LaTeX)

- Scrittura usando sintassi markdown
- Collaborazione usando git
- Conversione in pdf usando pandoc
- Conversione in PostScript con ghostscript
- Foliazione (signature) effettuata con psbook
- Scala delle pagine da A4 ad A5 usando psnup

*Downloads*, sul pc chiamato *pc*, nella directory *backup* dell'utilizzatore con lo stesso nome, in questo esempio chiamato *tu*.

Nei giorni successivi usare stesso comando per eseguire un backup incrementale

```
duplicity --use-agent --encrypt-sign-key [Key-ID] \  
--exclude ~/Downloads $HOME/ sftp://tu@pc//home/tu/backup
```

Verificare il backup

```
duplicity verify -v9 sftp://tu@pc//home/tu/backup /home/tu
```

Recuperare il backup nella cartella *recupero*

```
mkdir recupero  
duplicity sftp://tu@pc//home/tu/backup /home/tu/recupero
```

Esiste un front-end grafico di duplicity, chiamato *Deja Dup*

```
apt-get install duplicity deja-dup
```

## 20 Risorse

**Autistici/Inventati** offre ad attivisti, gruppi e collettivi piattaforme per una comunicazione più libera e strumenti digitali per l'autodifesa della privacy, come per esempio email, blog, mailing list, instant messaging e altro.

<https://www.autistici.org>

**Disroot** offre una serie di soluzioni alternative ed open source a servizi commerciali, tra cui: email, cloud, forum, pad, calc, privatebin, polls e altro.

<https://www.disroot.org>

**Riseup** fornisce caselle di posta, mailing list e siti web a persone impegnate per un cambiamento sociale libertario. Altri servizi: pad, share (pastebin, imagebin), VPN, jabber, Crabgrass

<https://www.riseup.net>

**Cryptpad** fornisce una suite di strumenti di collaborazione crittati: Crypt-Drive, Rich text, Code, Presentation, Poll, Kanban, Whiteboard, Todo. Il software è open-source e disponibile per il self-hosting.

## 3.3 La passphrase

Nel caso del password manager, invece che una password, si può usare una passphrase. Invece che una parola, una frase compresa di spazi, più forte ma anche più facile da ricordare. Gli esempi che seguono contengono sia maiuscole che numeri che caratteri strani. Sono lunghe ed efficaci, ma difficili da dimenticare.

Una passphrase, o frase di sblocco, è una password con gli spazi. Facile da ricordare. per esempio:

Nel Mezzo Del Cammin Di Nostra Vita 42!

99 #Luft,Ballons#

È semplice trovare una frase di una poesia, prosa o canzone che si ricordi, aggiungere le maiuscole, qualche numero, un punto e virgola e voilà.

## 3.4 Doppia autenticazione

L'autenticazione si basa tradizionalmente su un massimo di tre elementi possibili:

- Qualcosa che so
- Qualcosa che ho
- Qualcosa che sono

Il primo caso comprende password e PIN, il secondo le chiavi o la carta bancomat, il terzo è la biometrica come l'impronta digitale o il riconoscimento facciale.

Il concetto di doppia (o tripla) autenticazione si basa sull'utilizzare più di un elemento in contemporanea, come nel caso di un prelievo con bancomat che usa sia PIN (qualcosa che so) che la carta (qualcosa che ho).

Se il servizio lo prevede è bene abilitare la doppia autenticazione, ad esempio Autistici.org permette la doppia autenticazione tramite OTP (One Time Password). I servizi istituzionali o commerciali spesso usano il numero telefonico come elemento di verifica inviando un codice temporaneo via SMS.

Autistici.org permette anche di creare delle password uniche da usare per un determinato scopo, come ad esempio per la email sul telefonino. Nel caso venga compromessa, quella password non ha altro utilizzo.

## 4 Accecare la telecamera del portatile

Attaccare un pezzo di scotch nero da elettricista sulla telecamera del portatile. Il fatto che non si accenda la lucina non significa che sia spenta.

## 5 Navigazione consapevole

Usiamo Firefox.

La gestione dei containers, dei profili e degli add-ons ci permettono di creare ambienti isolati

**Multi-account-containers** è un componente aggiuntivo (add-on) per creare schede contenitore (tab) e compartimentare le preferenze del sito, le sessioni registrate e i dati di tracciamento. Un sito non avrà dunque accesso ai dati (cookies) delle altre tab aperte. Questo permette di separare il lavoro dalla navigazione personale.

I **profili** sono sessioni diverse del browser, usare un diverso profilo è come aprire un nuovo browser. Si possono usare scrivendo nella finestra di navigazione:

```
about:profiles
```

e creare un nuovo profilo.

**Add-ons:**

- Multi-account-containers: per compartimentare le sessioni di navigazione
- https-everywhere: preferisce https a http
- Ghostly: blocca i tracker della nostra navigazione
- No-Script: blocca gli script
- Ublock origin: blocca la pubblicità

**Motori di ricerca:**

Mettere in scatola firefox, in modo che lo script di un sito non possa accedere al disco. Notare che non sarà possibile caricare una foto dal disco alla rete, perché firefox non potrà accedere al disco

```
firejail firefox
```

Ad esempio mettere in scatola vlc ed impedirgli di collegarsi in rete

```
firejail --net=none vlc
```

<https://firejail.wordpress.com>

## 18 Comunicazione sicura dal telefonino

Premessa: consideriamo che gli smartphone sono insicuri per definizione.

- **Signal.org** è una app per comunicare privatamente
- **Conversations.im** è una app per comunicare privatamente con protocollo federato
- **lineageos.org** è un sistema operativo per telefonini basato su Android

Il progetto **Privacy matters on my phone** affronta il discorso privacy su smartphone per livelli. Ricordiamo qui che Conversation è disponibile dal repository <https://f-droid.org> e Signal da <https://signal.org/android/apk/>.

<https://unit.abbiandominio.org/pmomp>

## 19 Backup incrementale sicuro e remoto con duplicity

Usando duplicity, ssh e gpg si può crittografare un backup e conservarlo in modo sicuro su un pc remoto. Attenzione a conservare a parte una copia della chiave gpg che serve per il recupero

```
apt-get install duplicity
```

In questo esempio avviene un backup della Home, con scambio chiavi ssh, definendo la chiave gpg da usare per la cifratura, con esclusione della cartella

## 16 Self hosting con Nextcloud

Per avere una copia di riserva dei propri dati, sincronizzare una rubrica e un calendario con un dispositivo mobile e condividere documenti non è obbligatorio usare i servizi commerciali, i quali non sono gratuiti, ma costano in libertà. Quando i nostri dati vengono sparpagliati e utilizzati come risorse per creare profitto, subiamo un danno all'integrità del nostro *mio* digitale. Self hosting significa gestire autonomamente uno spazio digitale. Si può fare in gruppo e collettivizzare le risorse e i costi. È meno facile che usare i servizi commerciali.. ma no, è il paragone che non regge. La guida per fare un orto verticale non deve giustificarsi dicendo che è meno facile che andare al supermercato.

Installare e configurare Nextcloud (con mariadb, apache2, php7, ufw e fail2ban) su una VPS o un Pc, con già Debian 9

```
apt-get install curl
```

```
curl -sSL https://raw.githubusercontent.com/ \
nextcloud/nextcloudpi/master/install.sh | bash
```

Conservare le password e seguire le info di post installazione

<https://github.com/nextcloud/nextcloudpi/wiki>

Se si ha un (sub)dominio a disposizione si può ottenere da LetsEncrypt un certificato SSL

```
ncp-config
```

Configurare nextcloud creando gli utilizzatori e attivare calendario, rubrica e quel che serve.

## 17 Mettere un software in scatola

Per mettere un software dentro una scatola (sandbox) usare firejail. Utile per far girare un software del quale non ci si fida, limitandolo in un ambiente chiuso dal quale non potrà uscire, per evitare che faccia danni al sistema

```
apt-get install firejail
```

Il modello di internet commerciale si basa sulla raccolta dati degli utilizzatori, come ad esempio il famoso motore di ricerca Google, il quale appartiene alla ditta Alphabet. È possibile fare ricerche in rete usando motori di ricerca orientati alla privacy e migliorare il controllo sui propri dati evitando la profilazione e limitando la filter bubble.

- <https://duckduckgo.com>
- <https://www.startpage.com>
- <https://lite.qwant.com>
- <https://www.searx.me>

### Navigazione privata

Aprendo dal Menu di Firefox:

File -> Nuova finestra privata

si accede a una finestra di navigazione che non terrà memoria della navigazione. Questa pratica è utile nel caso si utilizzi un computer in prestito. Nasconde la storia di navigazione su quel Pc, ma non la rende anonima al gestore d'accesso o ai siti che vengono visitati.

## 6 Navigazione anonima

Tor, **The Onion Router** è un protocollo per l'anonimizzazione del traffico web. Scaricare, installare e usare il programma Tor browser bundle per navigare in rete anonimamente.

<https://torproject.org>

Attenzione alla presunzione di sicurezza. Anche dopo aver installato Tor è necessario tenersi aggiornati. L'intimità nella comunicazione è un processo in corso, non un risultato. Ricordare che la crittografia si vede, cioè anche se la navigazione o un messaggio è nascosto e non è leggibile, si vedrà che è stato nascosto, come si vede quando viene usato Tor.

## 7 Navigazione paranoica

**Tails** è un sistema operativo smemorato e incognito. Si avvia da penna Usb con un sistema GNU/Linux già configurato per la navigazione anonima e provvede al cambio automatico cambio del *MAC address*, l'identificativo univoco assegnato all'interfaccia di rete. Una volta spento non ricorda nulla di quello che è successo. È anche possibile attivare una modalità persistente, che ora non ci interessa. Tails usa Tor di default e permette di usare un qualunque computer senza doverci installare nulla né lasciarvi tracce dell'utilizzo. Utile in viaggio in zone di guerra. Decidi tu in che zona vivi.

Installare Tails su una penna Usb di almeno 16GB scaricando l'immagine dal sito. Seguire la procedura di verifica dell'immagine. Sia usando l'add-on di verifica Tails per Firefox, che verificando la firma digitale OpenPGP.

L'installazione di Tails si basa sulla *rete di fiducia*. Ad esempio se conosci qualcun\* che lo usa, è possibile usare la sua penna Usb per installare Tails su un'altra penna Usb senza collegarsi in rete.

Inserire in un Pc entrambe le penne Usb

Avviare il Pc, se serve indicando nel BIOS di avviare da penna Usb

Menu > Strumenti di sistema > Tails installer

Usare Tails

Avviare il Pc dalla penna Usb con Tails

Attenzione alla presunzione di sicurezza. È necessario tenersi aggiornati. L'intimità delle comunicazioni in rete è un faticoso processo, non un risultato. Ricordare che la crittografia si vede: anche se la navigazione o un messaggio è crittato e non è leggibile, si vede che è crittato, come si vede che viene usato Tor. Ad esempio se in una stanza dove ci sono poche persone qualcuno usa Tor, il sorvegliante non farà fatica a scoprire chi è andando per esclusione, anche senza poter sapere dove sta navigando.

<https://tails.boum.org/index.it.html>

Se si desidera inserire un lungo testo, o addirittura una foto in una foto, accorrerà usare un contenitore capiente.

Per sapere quante informazioni posso inserire in foto-delle-vacanze.jpg

```
steghide info foto-delle-vacanze.jpg
```

## 15 Collegarsi a un pc usando ssh con scambio di chiavi

Nella crittografia asimmetrica quando si usa una passphrase per sbloccare una chiave, la decrittazione avviene in locale, perciò la passphrase non viaggia per internet. Questa viene chiamata cifratura *end to end* ed è più sicura.

Creare la coppia di chiavi per collegarsi al pc

```
ssh-keygen -b 8192 -t rsa -f chiave
```

Caricare sul pc la chiave pubblica e rinominarla in ~/.ssh/authorized\_keys con i giusti permessi

```
cat chiave.pub | ssh tu@pc "mkdir -p ~/.ssh && \
chmod 700 ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

Avviare ssh-agent e usare la chiave privata

```
eval 'ssh-agent' ; ssh-add chiave
```

Collegarsi al pc

*“tu” è il nome utilizzatore e “pc” è il nome o l'indirizzo IP della macchina remota*

```
ssh tu@pc
```

Dopo verifica sarà possibile disabilitare sul pc l'accesso ssh via password specificando *PasswordAuthentication no* in */etc/ssh/sshd\_config*

Per comunicare un breve messaggio, è possibile usare il servizio protected text. Accedendovi tramite Tor. Il quale permette di scrivere un messaggio sul web protetto da password.

<https://www.protectedtext.com/>

Sarà stato concordato precedentemente con il corrispondente l'indirizzo e la password, e basterà comunicare, magari con una telefonata, che il file è disponibile. Oppure avrò già concordato giorno e ora della condivisione perché sono Mata Hari. Se la condivisione non avviene al momento concordato il corrispondente capisce che qualcosa è andato storto e che deve scappare immediatamente.

*Nota: se si sta facendo qualcosa di così delicato quanto il Blog del Narco, storico blog di denuncia del narcotraffico messicano, consigliamo di studiare molto e bene, di chiedere aiuto, rivedere il film: Notorious di Alfred Hitchcock, ma soprattutto ricordare che non è solo una questione tecnica.*

## 14 Nascondere un messaggio in una foto

La crittografia nasconde un messaggio, ma il file crittografato è visibile, anche se non leggibile. Un esempio: se metto la mano davanti alla bocca mentre telefono, chi mi osserva non può leggere le mie labbra, ma vede che sto tenendo la mano davanti alla bocca e capisce che sto nascondendo qualcosa.

Nascondere un messaggio in una foto, come anche in un video, serve a nascondere un messaggio crittato allo scopo di poterne negare l'esistenza e si chiama *steganografia*. Il suo scopo è far passare messaggi riservati senza che il controllo se ne accorga.

```
apt-get install steghide
```

Nascondere il testo del Segreto della pizza all'interno di una foto. Verrà chiesto di inserire una password.

```
steghide embed -ef segreto-della-pizza.txt -cf foto.jpg
```

Rivelare il testo

```
steghide extract -sf foto.jpg
```

## 8 Usare un sistema operativo libero

Usiamo GNU: software libero o almeno a sorgente aperta, il quale viene raccolto e assemblato assieme al kernel Linux per formare un sistema operativo in quella che viene chiamata distribuzione. Ogni distro ha il suo perché. Noi ne elenchiamo tre:

- Linux Mint: <https://linuxmint.com>

Un desktop familiare. Semplice da usare e da installare. La nonna e il nonno lo usano e non hanno mai chiamato per fare domande. Intuitivo per chi proviene da Windows o da Macintosh. È una buona scelta per lo smanettone che può permettersi un sistema operativo che richiede abbastanza risorse e che desidera stare in contatto con i suoi vicini, usando e facendo usare un sistema completo, ma compatibile anche dai meno tecnicamente inclinat\*. Può avviarsi direttamente da Cd o da Usb (live). Preferisce un computer moderno con almeno 4Gb di Ram. Basata su Debian e Ubuntu.

- Bunsenlabs: <https://www.bunsenlabs.org>

Minimale, leggera e funzionale. Buona sia per un pc moderno che non. Erede della distro Crunchbang. Usandola si imparano cose utili. Live. Basata su Debian.

- Debian: <https://www.debian.org>

Il sistema operativo universale. Può fare sia da desktop che da server. Sapendo già cosa si vuole e come ottenerla è la miglior cosa. La sua versatilità comporta qualche piccolo lavoro di customizzazione dopo l'installazione.

### 8.1 Scaricare e installare una distribuzione GNU/Linux

Individuare e scaricare l'immagine del sistema operativo prescelto. Per un comune computer moderno usare la versione amd64. Verificare la checksum e masterizzare l'immagine su Cd, Dvd o penna Usb. In questo esempio viene copiato Debian su penna Usb.

Inserire la Usb e scoprire dove è stata montata

```
ls -l /dev/disk/by-id/*usb*
```

Nell'esempio che segue è in /dev/sdb, copiarvi Debian:

*il contenuto della penna sarà cancellato*

```
dd if=debian-9.8.0-amd64-netinst.iso of=/dev/sdb bs=4M; sync
```

Riavviare il Pc dalla penna Usb tenendo premuto **F12**

*Se il Pc non avvia automaticamente dalla penna, entrare nel Bios e scegliere Usb come dispositivo d'avvio. A seconda del modello tenere premuto all'avvio uno di questi tasti: ESC, DEL, F1, F2, F8, F10. Una volta nel Bios, editare l'ordine di avvio mettendo per prima la penna Usb.*

Nella procedura di installazione si verrà guidati a scegliere la lingua da usare, la zona geografica, il nome del Pc, la rete e la creazione dell'utilizzatore. Durante la partizione guidata formattare l'intero disco senza complicazioni. In conclusione installare Grub bootloader nel Master Boot Record.

*Il disco del Pc verrà formattato e cancellato, non ci saranno altri sistemi operativi oltre a GNU/Linux Debian. È possibile effettuare al momento dell'installazione scelte diverse per casi particolari*

*È possibile durante l'installazione crittografare l'intero disco e in questo caso si dovrà mettere una passphrase ad ogni avvio, in aggiunta alla password di login. Consigliabile per un portatile, in caso venga smarrito non ci si dovrà preoccupare della perdita dei dati. Ricordare che senza la passphase non è possibile accedere al disco.*

### 8.1.1 Migrare la posta di Thunderbird da *quel sistema* a GNU/Linux

Prima di cominciare fare un backup zippando la cartella di Thunderbird,

Poi compattare le cartelle di Thunderbird

Thunderbird: Menu > File > Compact Folders

Infine copiare il profilo da un pc all'altro. Il profilo si trova, a seconda per Gnu/Linux, MacOSX, WindowsXp, Windows7, in:

```
/home/tu/.thunderbird/[nome profilo]
/Users/tu/Library/Thunderbird/Profiles/[nome profilo]
C:\Documents and Settings\tu\Application Data\Thunderbird\Profiles
```

## 12 Cancellare i metadati da un file

Il software grafico **MAT** permette di cancellare i metadati di un file. Ad esempio una foto digitale contiene i metadati con quale apparecchio è stato usato e le coordinate GPS di dove. Tails contiene MAT.

```
apt-get install mat
```

Avviare MAT > Trascinare nella finestra il file da pulire

## 13 Condividere un documento in maniera anonima

Per condividere un documento in maniera anonima utilizzare Onionshare. Si consiglia di usarlo attraverso Tails con la sua interfaccia grafica. Onionshare avvia un servizio nella rete Tor, la quale è una *darknet*, ossia una rete che usa un protocollo diversi dalla rete tradizionale, oltre che naturalmente una *deepnet*, cioè una rete non indicizzata dai motori di ricerca. Dopo aver trascinato nella finestrella il documento da condividere, OnionShare fornirà un indirizzo onion. Il corrispondente, usando Tor, potrà recarsi a quell'indirizzo e scaricare il file. Importante: è il computer stesso a fare da server e non vengono coinvolti servizi di terze parti, dunque il file non sarà più condiviso una volta chiuso Onionshare o spento il computer. Onionshare fornisce un utile avviso quando il documento è stato scaricato.

Avviare il Pc da Tails

Avviare OnionShare > Trascinare nella finestra il file

Cliccare: Inizio condivisione

Copiare l'indirizzo e comunicarlo al corrispondente

Potrò comunicare l'indirizzo al mio corrispondente ad esempio inviando una email o un messaggio, anche crittato usando gpg. Chiunque conosca l'indirizzo potrà scaricare il file, ma lo scopo potrebbe essere la sua diffusione proteggendo l'anonimato e non la sua segretezza.

*Durante la configurazione la penna verrà formattata e sarà sempre necessario usare VeraCrypt per montarla e accedere al contenuto.*

<https://veracrypt.fr>

## 11 Verificare l'integrità di un software scaricato

Nell'usare del software per la comunicazione privata si deve poter essere sicuri che il software non sia stato compromesso da terze parti.

Per questo alcuni software sono distribuiti accompagnati dal risultato della somma di controllo (checksum) oppure da una firma digitale a lato (.sig) e la sua fingerprint.

Verificare che la stringa alfanumerica univoca (hash) che risulta applicando l'algoritmo sha256 coincida con quella pubblicata

```
openssl sha256 debian-9.6.0-amd64-netinst.iso
c51d84019c3637ae9d12aa6658ea8c613860c776bd84c6a71eaaf765a0dd60fe
```

Verificare una firma

```
gpg --import VeraCrypt_PGP_public_key.asc
key 821ACD02680D16DE: public key "VeraCrypt Team" imported
(è stato troncato ciò che non interessa all'esempio)
```

```
gpg --fingerprint VeraCrypt
5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE
(coincide con la fingerprint pubblicata sul sito?)
```

```
gpg --verify veracrypt-1.23-setup.tar.bz2.sig
Good signature from "VeraCrypt Team"
(Bene. Il warning indica solo che non ho firmato la chiave)
```

*Non è necessario firmare una chiave per usarla. Firmarla serve a ricordare (e nel caso si usi il web of trust, a dichiararlo al mondo) che ci si fida di quella chiave. È giusto farlo dopo averla verificata con una telefonata. P.S. non chiamare al telefono Debian, tantomeno all'ora di cena.*

C:\Users\tu\AppData\Roaming\Thunderbird\Profiles\[nome profilo]

In caso di problema, far partire thunderbird con profile manager e sistemare:

```
thunderbird -profilemanager
```

Se il problema persiste:

Chiudere e riaprire.

Controllare i permessi.

Verificare il path in ./thunderbird/profiles.ini

nel mac era: Path=Profiles/76gighirz.default

su debian è: Path=76gighirz.default

Cancellare questi files, che comunque si rigenerano da soli

```
compreg.dat
extensions.cache
extensions.ini
extensions.rdf
pluginreg.dat
```

## 9 GnuPG, la crittografia pesante a doppia chiave

Gnu Privacy Guard <https://gnupg.org> è la versione libera del software di crittografia asimmetrica Pgp, Pretty Good Privacy.

Si usa per cifrare, cioè per nascondere il contenuto di un messaggio. E per firmare, cioè per autenticare un messaggio. Dunque anche per decifrare e per verificare una firma.

Il suo scopo è permettere una comunicazione sicura tra persone che non si sono incontrate di persona e frustrare chi intercetta i messaggi ma non ha la chiave per decifrarli.

## 9.1 Installazione

Si può usare da terminale o con la grafica, in entrambi i casi si vorrà integrarne l'uso con l'email, dunque `gpg+mutt` o `gpg+enigmail+thunderbird`.

Installare GnuPG, il client di posta grafica e il suo plugin (che può gestire Gpg fin dalla creazione delle chiavi)

```
apt-get install gnupg thunderbird enigmail
```

## 9.2 Configurazione e creazione delle chiavi

```
gpg --gen-key
```

oppure

```
Aprire thunderbird > enigmail
```

Creare la coppia di chiavi, indicando una email, assegnando una passphrase e specificando una scadenza. Otterremo una chiave pubblica (pubkey) e una chiave privata (privkey). La privkey viene conservata privatamente, la pubkey viene divulgata liberamente.

## 9.3 Uso

- Si usa la propria privkey per firmare un documento o una email
- Si usa la pubkey di qualcun\* per verificare la sua firma al messaggio
- Si divulga la propria pubkey perché il nostro corrispondente possa scriverci segretamente
- Si ottiene la pubkey del nostro corrispondente per scrivergli segretamente
- Si usa la propria privkey per decifrare un messaggio a noi indirizzato
- Si usa la pubkey di qualcun\* per cifrare un messaggio ad ess\* destinato

Solitamente si invia un messaggio segreto sia cifrandolo che firmandolo ed è ragionevole aspettarsi di ricevere dei messaggi segreti firmati, ma quando non si vuole nascondere il contenuto ma solo avere la certezza di stare dialogando con la persona giusta, si firma solo.

*La crittografia a doppia chiave è semplice, ma non è facile. Usarla nel quotidiano permette di sperimentare e capire attraverso la pratica. Trovare un corrispondente*

Una guida con infografiche: <https://emailselfdefense.fsf.org/it>

## 9.4 Verifica

Ogni coppia di chiavi ha una fingerprint che la identifica univocamente. È buona pratica, prima di inserire la chiave nella nostra rete di fiducia, chiedere alla persona con cui voglio corrispondere di leggere al telefono la sua fingerprint per verificare che corrisponda con quella della pubkey che ci siamo scambiati\*. E viceversa. Gpg è una rete sociale.

## 9.5 Fingerprint, revoca e backup

Ottenere la fingerprint di una chiave

```
gpg --fingerprint [email o Key-ID]
```

È meglio creare subito un certificato di revoca delle chiavi

```
gpg -o ~/.gnupg/RevocaCertificato.asc --gen-revoke [fingerprint]
```

Fare un backup della cartella nascosta .gnupg da conservare altrove con cura

```
tar -zcpf ~/backup-gnupg.tar.gz ~/.gnupg
```

*È possibile usare una penna Usb cifrata con VeraCrypt per contenere il backup di gpg e altri dati importanti come le mailbox.*

## 10 Un lucchetto alla penna Usb

VeraCrypt è un software che permette di proteggere con una passphrase una penna Usb. Utile per trasportare dei documenti in viaggio senza preoccuparsi di perderla.