

## Pillole di autodifesa digitale

come tutelare la propria riservatezza con un seminario  
bellissimo, pratico e indolore

Cryptoparty

## Introduzione

Cifratura a chiave pubblica

GPG (on win:( )

Mail

Instant messaging : chat

Anonimato online

Files encryption

# CIOTOFLOW

**\*\* Ciotoflow \*\* - <http://flow.ciotoni.net> -**

- Mercoledì 18.00 ca aula p2

# CryptoParty

- Gran parte delle informazioni sulla nostra vita passa attraverso un computer (chat, mail, etc)
- I nostri dati passano per decine di dispositivi (potenzialmente malevoli) prima di arrivare a destinazione
- Facilità di analisi, immagazzinamento, e intercettazione dei nostri dati (quasi sempre sensibili)
- Molto spesso accettiamo nelle policy superficialmente che la destinazione analizzi,utilizzi e venda! i nostri dati

# CryptoParty

- Gran parte delle informazioni sulla nostra vita passa attraverso un computer (chat, mail, etc)
- I nostri dati passano per decine di dispositivi (potenzialmente malevoli) prima di arrivare a destinazione
- Facilità di analisi, immagazzinamento, e intercettazione dei nostri dati (quasi sempre sensibili)
- Molto spesso accettiamo nelle policy superficialmente che la destinazione analizzi,utilizzi e venda! i nostri dati

# CryptoParty

- Gran parte delle informazioni sulla nostra vita passa attraverso un computer (chat, mail, etc)
- I nostri dati passano per decine di dispositivi (potenzialmente malevoli) prima di arrivare a destinazione
- Facilità di analisi, immagazzinamento, e intercettazione dei nostri dati (quasi sempre sensibili)
- Molto spesso accettiamo nelle policy superficialmente che la destinazione analizzi,utilizzi e venda! i nostri dati

# CryptoParty

- Gran parte delle informazioni sulla nostra vita passa attraverso un computer (chat, mail, etc)
- I nostri dati passano per decine di dispositivi (potenzialmente malevoli) prima di arrivare a destinazione
- Facilità di analisi, immagazzinamento, e intercettazione dei nostri dati (quasi sempre sensibili)
- Molto spesso accettiamo nelle policy superficialmente che la destinazione analizzi,utilizzi e venda! i nostri dati

# Cryptoparty

- gli strumenti non sono solo per pochi nerd eletti
- più pratica possibile
- banchetti per approfondimenti/sperimentazioni/installazioni
- domande/risposte

# Cryptoparty

- gli strumenti non sono solo per pochi nerd eletti
- più pratica possibile
- banchetti per approfondimenti/sperimentazioni/installazioni
- domande/risposte



# Cryptoparty

- gli strumenti non sono solo per pochi nerd eletti
- più pratica possibile
- banchetti per approfondimenti/sperimentazioni/installazioni
- domande/risposte

# Cryptoparty

- gli strumenti non sono solo per pochi nerd eletti
- più pratica possibile
- banchetti per approfondimenti/sperimentazioni/installazioni
- domande/risposte

## Di cosa parleremo

- 1 Introduzione
- 2 Cifratura a chiave pubblica
- 3 GPG (on win:( )
- 4 Mail
- 5 Instant messaging : chat
- 6 Anonimato online
- 7 Files encryption

# Crittografia

Rendere illeggibile il contenuto di un informazione a chi non è autorizzato

cryptoparty!!

# Crittografia

Rendere illeggibile il contenuto di un informazione a chi non è autorizzato

cryptoparty!!

# Crittografia

Rendere illeggibile il contenuto di un informazione a chi non è autorizzato

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

```
Version: GnuPG v1.4.12 (GNU/Linux)
```

```
hQIOA7vElRJR89J3EAf/VKtmXc6FnWmAre225nRN8NZRvJM1UZ0  
57/Uy0xkiqOGv2nsg5e41eGHBx2qZoIMkSBKgVU1o4I+XwalZVb  
Jpk4R/1Blj5ExaqkXJqjBwf5Zl01gNXpYDmM+gyFrWB2mk9ZVNP  
0/J9r3qySYrrw9k2L5QzJytAuvIZwmddqryUyaUemSzLMPV6eGP
```

```
P9+waOz1S6YZyKNQAPjWthhxiLDziTV178tUIQITEw==  
=OEvO
```

```
-----END PGP MESSAGE-----
```

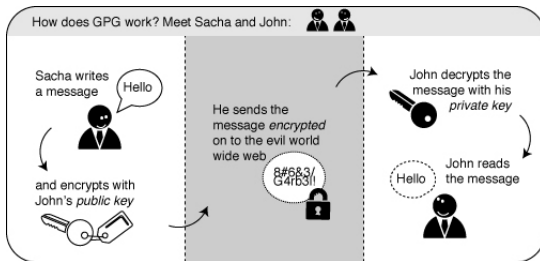
## Coppia chiavi!

- !Coppia di chiavi! -
  - Coppia di file su un computer
  - Una pubblica e una privata

## Coppia chiavi!

- !Coppia di chiavi! -
  - Coppia di file su un computer
  - Una pubblica e una privata





- Se qualcuno vuole inviarmi informazioni cifrate ha bisogno della mia chiave pubblica
- Se voglio inviare informazioni cifrate ho bisogno della sua chiave pubblica

## Diffusione delle chiavi pubbliche

Quindi basta distribuire le chiavi pubbliche  
Come??

- Fisicamente (es. chiavette usb)
- Per email
- Archivi online dedicati allo scopo (key server)
- Alcuni programmi (es. pidgin+otr) si occupano trasparentemente della diffusione della chiave pubblica

## Di cosa parleremo

- 1 Introduzione
- 2 Cifratura a chiave pubblica
- 3 GPG (on win:( )
- 4 Mail
- 5 Instant messaging : chat
- 6 Anonimato online
- 7 Files encryption

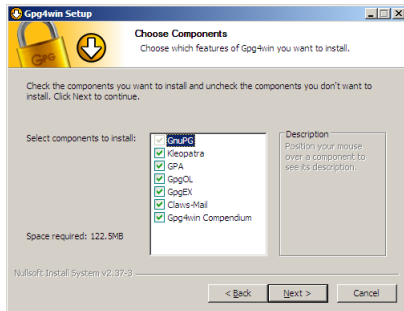
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# GPG4WIN

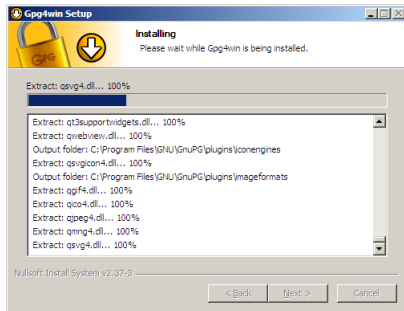
<http://gpg4win.org/>



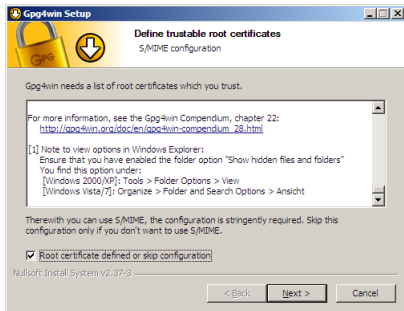
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption



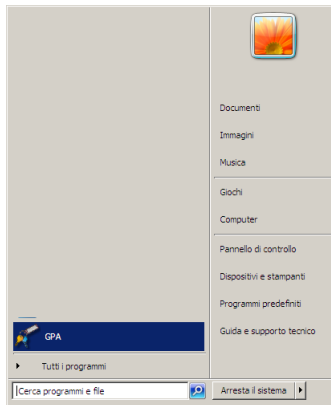
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption





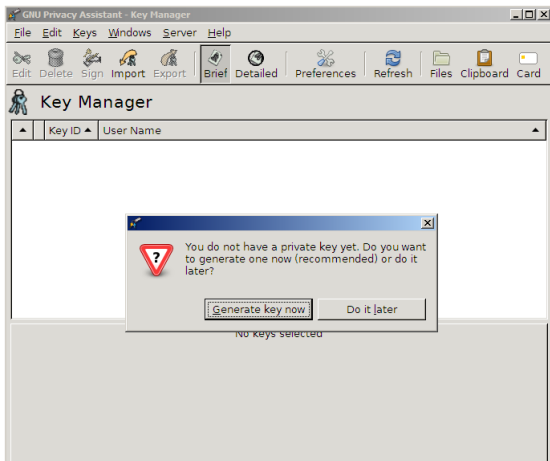
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Manager delle chiavi



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# CREARE UNA NUOVA COPPIA DI CHIAVI



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# CREARE UNA NUOVA COPPIA DI CHIAVI



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# CREARE UNA NUOVA COPPIA DI CHIAVI



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# CREARE UNA NUOVA COPPIA DI CHIAVI



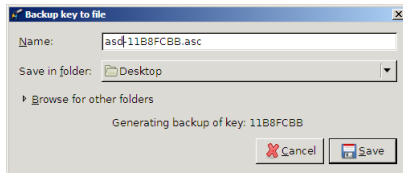
## CREARE UNA NUOVA COPPIA DI CHIAVI

Proteggere la chiave privata con una parola d'ordine

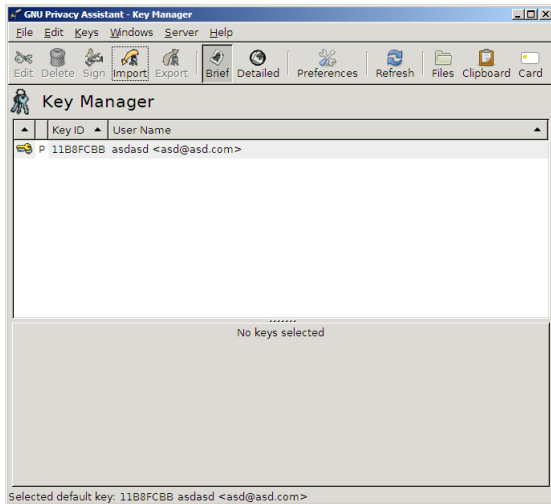


Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# CREARE UNA COPIA DI BACKUP DELLA PROPRIA CHIAVE



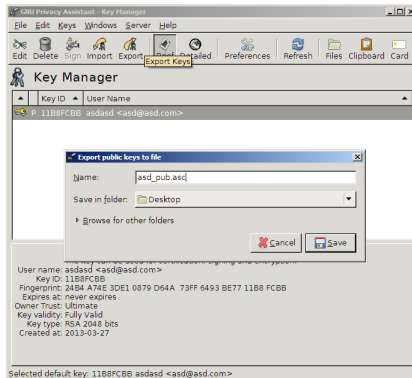
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption





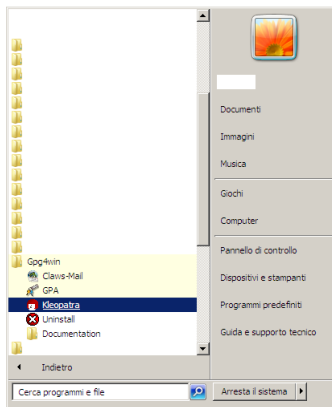
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# ESPORTARE CHIAVE PUBBLICA SU FILE



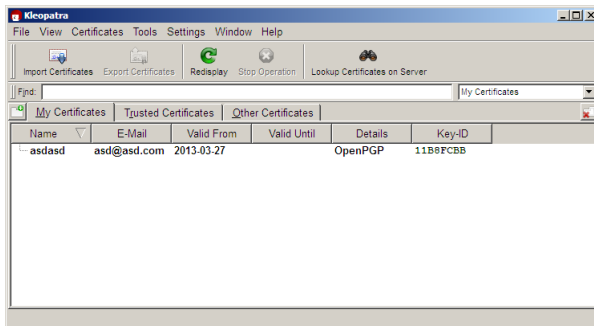
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# USARE KLEOPATRA PER CIFRARE FILE



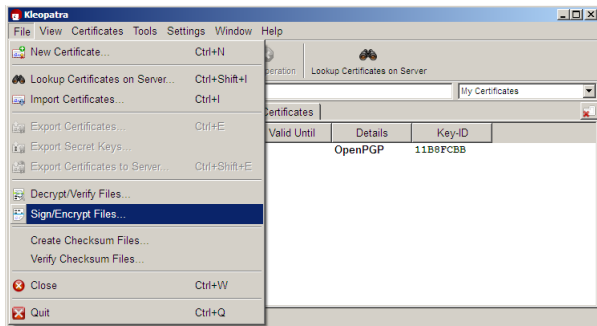
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# USARE KLEOPATRA PER CIFRARE FILE



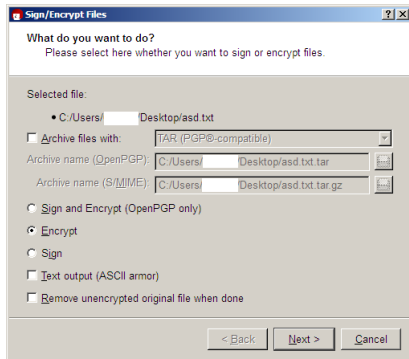
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# USARE KLEOPATRA PER CIFRARE FILE



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

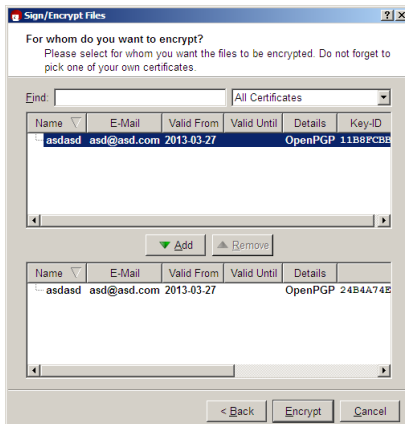
# USARE KLEOPATRA PER CIFRARE FILE



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

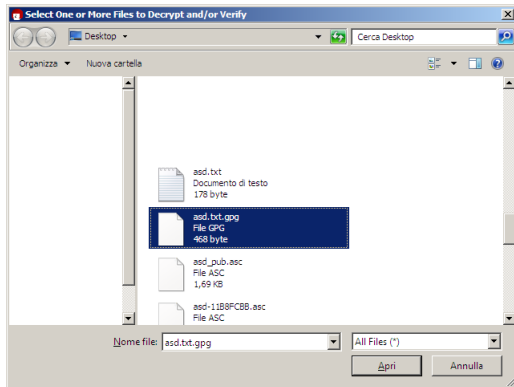
# USARE KLEOPATRA PER CIFRARE FILE

Per chi vogliamo cifrare il file???



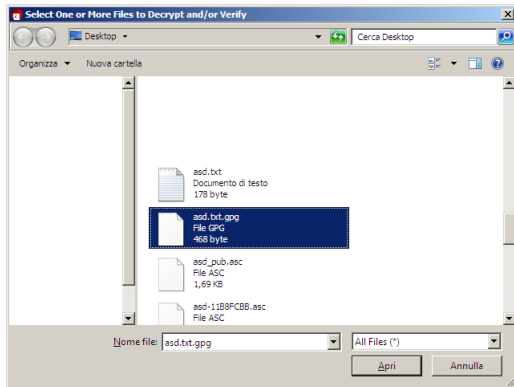
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# USARE KLEOPATRA PER CIFRARE FILE



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# USARE KLEOPATRA PER CIFRARE FILE





# Mail



## Thunderbird

- Programma (client) per leggere la posta non dal browser
- Strumenti integrati per cifrare le email
- Permette di leggere le email anche offline

# Mail



## Thunderbird

- Programma (client) per leggere la posta non dal browser
- Strumenti integrati per cifrare le email
- Permette di leggere le email anche offline

# Mail



## Thunderbird

- Programma (client) per leggere la posta non dal browser
- Strumenti integrati per cifrare le email
- Permette di leggere le email anche offline

# ENIGMAIL

## Enigmail

- estensione di Thunderbird per rendere facile e indolore la cifratura delle nostre mail
- gestisce chiavi, cifratura e firma delle nostre email

# ENIGMAIL

## Enigmail

- estensione di Thunderbird per rendere facile e indolore la cifratura delle nostre mail
- gestisce chiavi, cifratura e firma delle nostre email

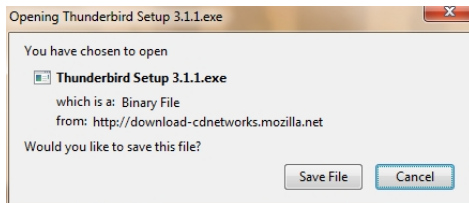
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installare Thunderbird

The screenshot shows the Mozilla Thunderbird 3.1 download page. At the top, there is a navigation bar with the following links: Thunderbird, Add-ons, Support, Community, and About. The main heading is "Thunderbird 3.1" with the subtext "Now with tabs, better search, and email archiving. It's easy to upgrade to Thunderbird 3.1". Below this, there is a "Free Download" button with a download icon and the text "3.1.1 for Windows, English (US) (6.4MB)". To the right of the main heading, there are links for "Thunderbird", "Features", "Release Notes", and "Other Systems & Languages". The background of the page features a stylized city skyline at sunset.

Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installare Thunderbird



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

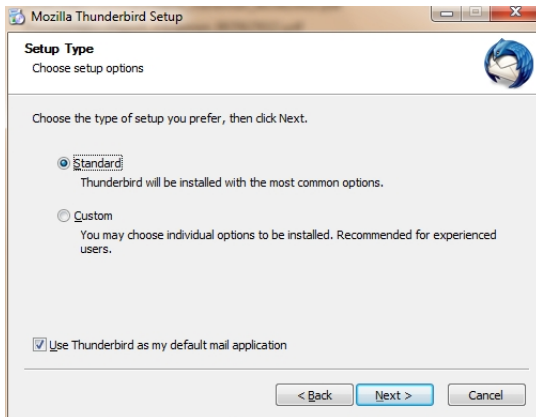
# Installare Thunderbird





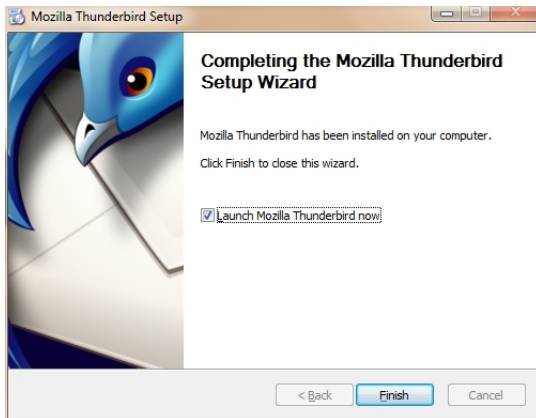
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installare Thunderbird



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

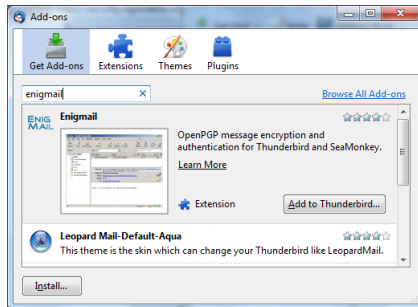
# Installare Thunderbird



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

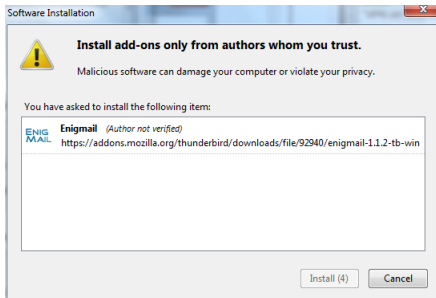
# Installare Enigmail

## Enigmail



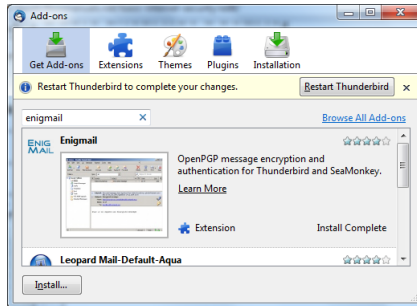
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installare Enigmail



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installare Enigmail



# Configurare Enigmail



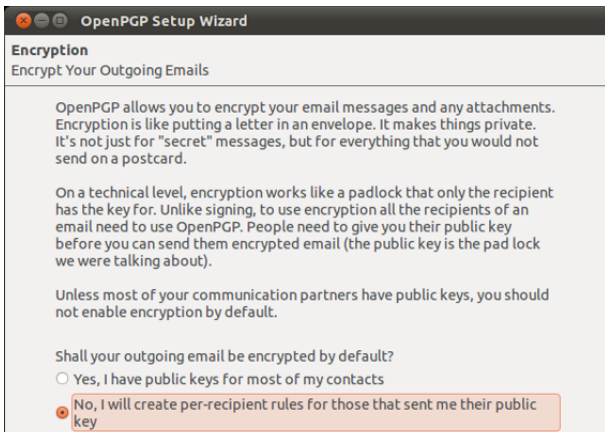
## Configurare Enigmail

Vuoi firmare tutte le email???



## Configurare Enigmail

Vuoi cifrare tutte le email???





Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Configurare Enigmail

**OpenPGP Setup Wizard**

### Create Key

Create A Key To Sign And Encrypt Email

You need to have a 'key pair' to sign and encrypt email, or to read emails that are encrypted. A key pair has two keys, one public and one private.

You need to give your public key to everyone in your contact list who will want to verify your signature, or to encrypt email to you. Meanwhile, you need to keep your private key secret. You must not give it away, or leave it unprotected. It can read all the email people encrypt and send to you. It can also encrypt email in your name. Because it's secret, it's protected by a passphrase.

Account / User ID:  
Johnny Cash <maildemo@greenhost.nl> - maildemo@greenhost.nl

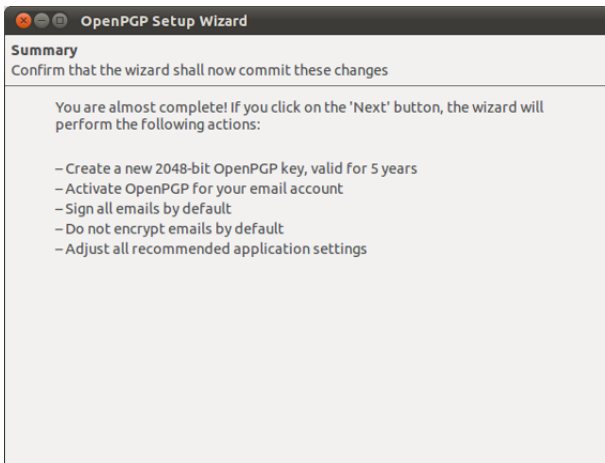
Passphrase

Please confirm your passphrase by typing it again

Navigation icons: back, forward, home, search, refresh.

Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
**Mail**  
Instant messaging : chat  
Anonimato online  
Files encryption

# Configurare Enigmail



Introduzione

Cifratura a chiave pubblica

GPG (on win:( )

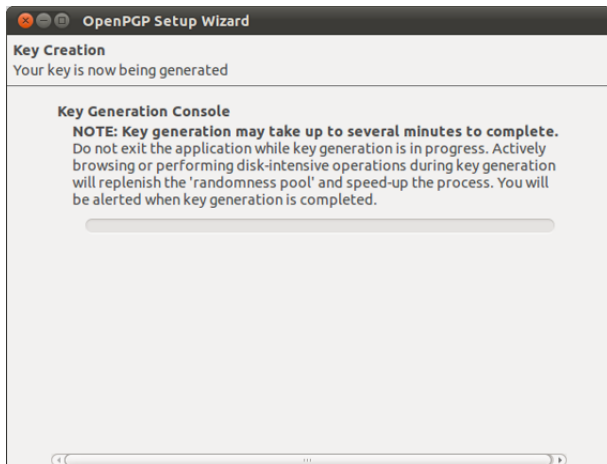
Mail

Instant messaging : chat

Anonimato online

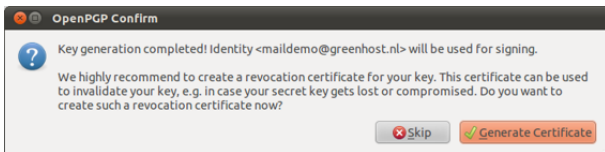
Files encryption

# Configurare Enigmail



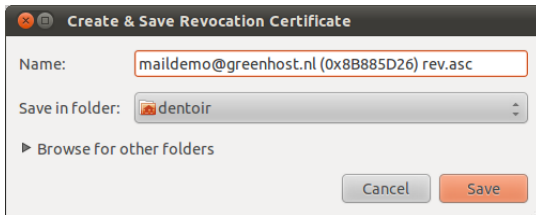
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Configurare Enigmail

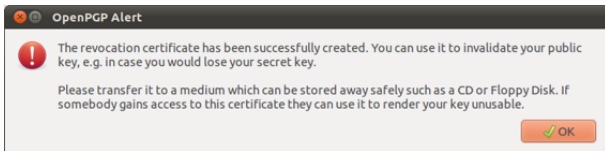


Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

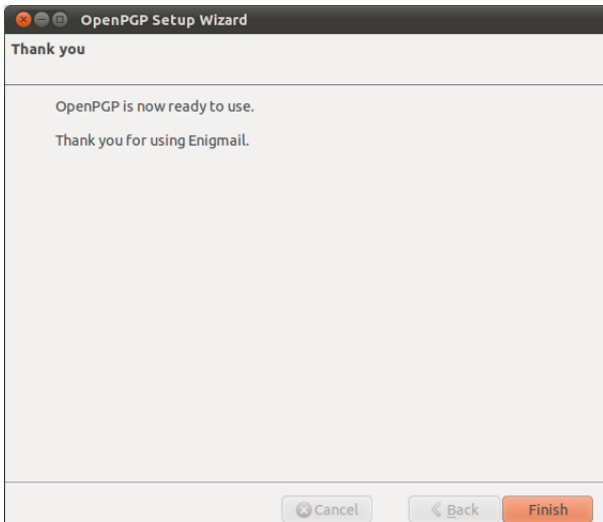
## Configurare Enigmail



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

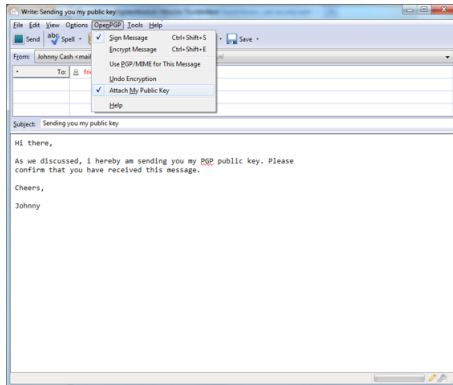


Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
**Mail**  
Instant messaging : chat  
Anonimato online  
Files encryption



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

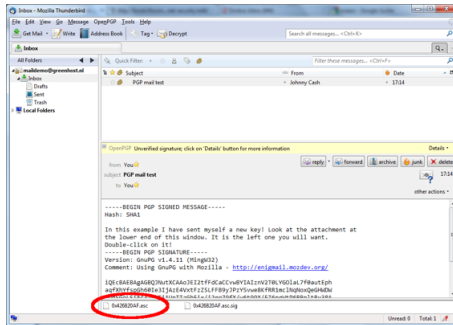
## Spedire la chiave pubblica



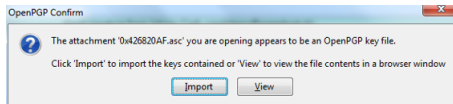


Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

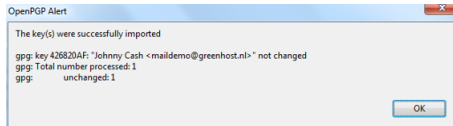
## Ricevere e importare una chiave pubblica



## Ricevere e importare una chiave pubblica

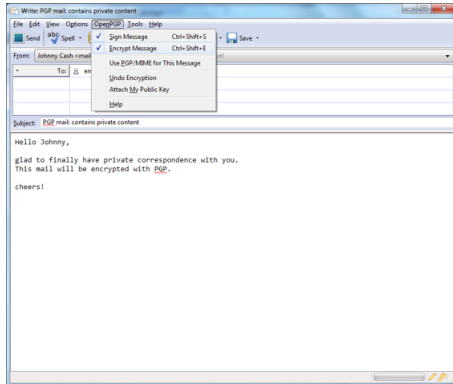


## Ricevere e importare una chiave pubblica



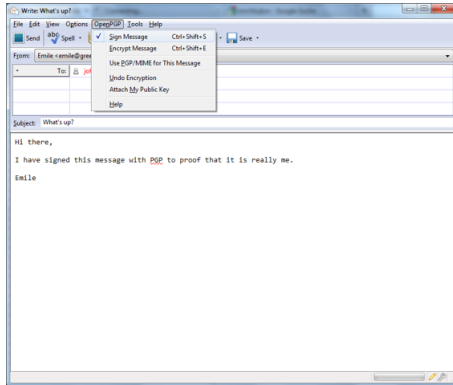
Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

## Spedire un email cifrata



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

## Spedire un email firmata



## Pidgin

- Client di messaggistica multiprotocollo - multiaccount (gmail, facebook, ICQ) - Multiplatforma (va bene anche per winzozz)

# OTR

## OTR “off-the-record”

- Ci permette di avere delle conversazioni private
- Si basa sul paradigma della cifratura a chiave pubblica

# OTR

## OTR “off-the-record”

- Ci permette di avere delle conversazioni private
- Si basa sul paradigma della cifratura a chiave pubblica



# PIDGIN-OTR

## Pidgin + OTR

- Pidgin può essere facilmente esteso per utilizzare OTR
- OTR su tutti i protocolli supportati da pidgin
- Diffusione delle chiavi pubbliche “automatica”

# PIDGIN-OTR

## Pidgin + OTR

- Pidgin può essere facilmente esteso per utilizzare OTR
- OTR su tutti i protocolli supportati da pidgin
- Diffusione delle chiavi pubbliche “automatica”

# PIDGIN-OTR

## Pidgin + OTR

- Pidgin può essere facilmente esteso per utilizzare OTR
- OTR su tutti i protocolli supportati da pidgin
- Diffusione delle chiavi pubbliche “automatica”

# PIDGIN-OTR

## Pidgin + OTR

- Pidgin può essere facilmente esteso per utilizzare OTR
- OTR su tutti i protocolli supportati da pidgin
- Diffusione delle chiavi pubbliche “automatica”

Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installazione/Configurazione

Winz:

pidgin: [www.pidgin.im](http://www.pidgin.im)



The screenshot shows the Pidgin website homepage. At the top left is the Pidgin logo, a purple penguin. Below it is a navigation menu with links for DOWNLOAD, PLUGINS, HELP, ABOUT, NEWS, and DEVELOPMENT. The main content area features a large 'pidgin 2.10.7' logo. Below the logo is a 'Download Now' button with a green arrow and the text 'SOURCEFORGE - Trusted For Open Source'. To the right of the download button is a smaller penguin icon and the text '2.10.7 for Windows - Samples.com'. To the right of the main content is a section titled 'IM all your friends in one place' with a sub-header 'Pidgin is an easy to use and free chat client used by millions. Connect to AIM, MSN, Yahoo, and more chat networks all at once.' Below this is a list of supported chat networks: AIM, Bonjour, Gadu-Gadu, Google Talk, Groupwise, ICQ, IRC, MSN, MXit, MySpaceIM, SILC, SIMPLE, Sametime, XMPP, and Zephyr. A 'Learn More' button is located at the bottom right of this section. At the bottom of the page, there is a paragraph of text: 'Pidgin 2.10.7 contains some security updates for users of MXit, Sametime, and anyone connected to a public network (unencrypted Wi-Fi, universities, offices, etc). It also contains updated SSL certificates to fix...'



# Installazione/Configurazione

Winz:

pidgin-otr: otr.cypherpunks.ca -> win32\_installer

The screenshot shows a web browser window displaying the website [www.cypherpunks.ca/otr/index.php#downloads](http://www.cypherpunks.ca/otr/index.php#downloads). The page content includes a security notice about a remote attacker and a recommendation to upgrade to pidgin-otr version 3.2.1. Below the notice, there are three download sections: 'OTR library and toolkit', 'OTR plugin for Pidgin', and 'OTR localhost AIM proxy'. The 'OTR localhost AIM proxy' section has a red-bordered warning box stating 'This software is no longer supported. Please use an IM client with native support for OTR.' The 'OTR plugin for Pidgin' section lists links for 'README', 'Source code (4.0.0)', 'Compressed tarball (sig)', and 'Windows (4.0.0-1)', with a note that the Windows package is a 'Win32 installer for pidgin 2.x (sig)'. The 'OTR library and toolkit' section lists links for 'README', 'UPGRADING from version 3.2.x', and 'Source code (4.0.0)', with a note that the source code is a 'Compressed tarball (sig)' and that users may need to make changes for win32.

remote attacker to cause arbitrary code to be executed on the user's machine.

The flaw is in pidgin-otr, not in libotr. Other applications that use libotr are not affected.

CVE-2012-2369 has been assigned to this issue.

Please upgrade to [pidgin-otr version 3.2.1](#) immediately.

Users of pidgin-otr packages in Linux and \*BSD distributions should see updated packages shortly.

[More News...](#)

## Downloads

### OTR library and toolkit

This is the portable OTR Messaging Library, as well as the toolkit to help you forge messages. You need this library in order to use the other OTR software on this page. (Note that some binary packages, particularly Windows, do not have a separate library package, but just include the library and toolkit in the packages below.) The current version is 4.0.0.

[i](#) [README](#)

[i](#) [UPGRADING](#) from version 3.2.x

Source code (4.0.0)

[Compressed tarball \(sig\)](#)

[Note that if you're compiling from source on win32, you may need to make [this](#)

### OTR plugin for Pidgin

This is a plugin for Pidgin 2.x which implements Off-the-Record Messaging over any IM network Pidgin supports. The current version is 4.0.0.

[i](#) [README](#)

Source code (4.0.0)

[Compressed tarball \(sig\)](#)

**Windows (4.0.0-1)**

[Win32 installer for pidgin 2.x \(sig\)](#)

### OTR localhost AIM proxy

This software is no longer supported. Please use an IM client with native support for OTR.

This is a localhost proxy you can use with almost any AIM client in order to participate in Off-the-Record conversations. The current version is 0.3.1, which means it's still a long way from done. Read the README file carefully. Some things it's still missing:

- \* Username/password authentication to the proxy
- \* Having the proxy be able to use outgoing proxies itself
- \* Support for protocols other than AIM/ICQ

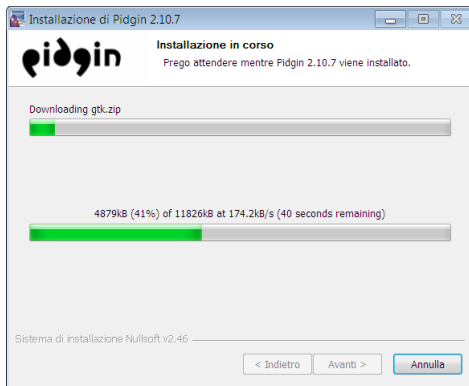
## Installazione/Configurazione

GNU/Linux:

ppp Utilizzare il gestore di pacchetti della propria distribuzione

Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installazione/Configurazione

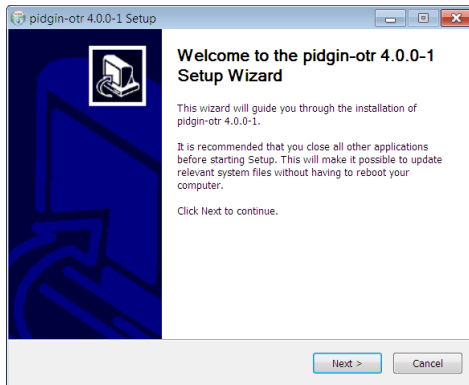




Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installazione/Configurazione

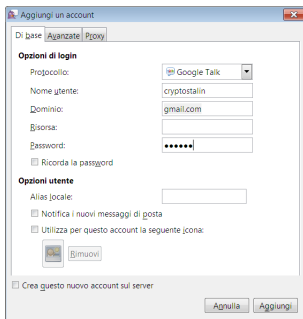
## Installare pidgin-otr



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

## Installazione/Configurazione

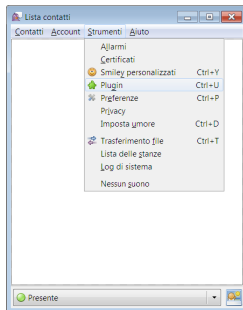
### Configurare un account su gmail



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

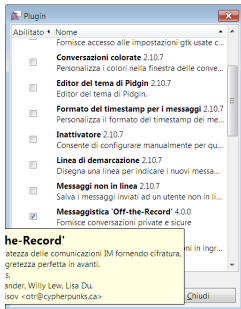
# Installazione/Configurazione

## Abilitazione del plugin



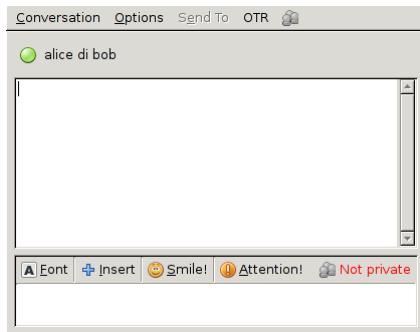
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Installazione/Configurazione



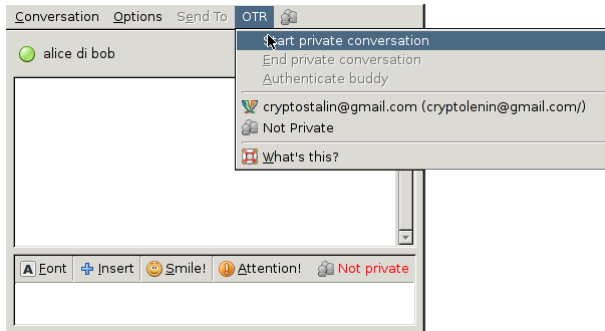
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# Chat NON privata



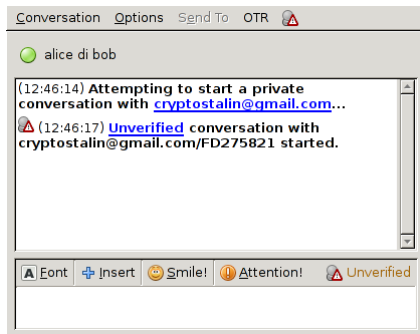
Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# INIZIARE UNA CHAT PRIVATA



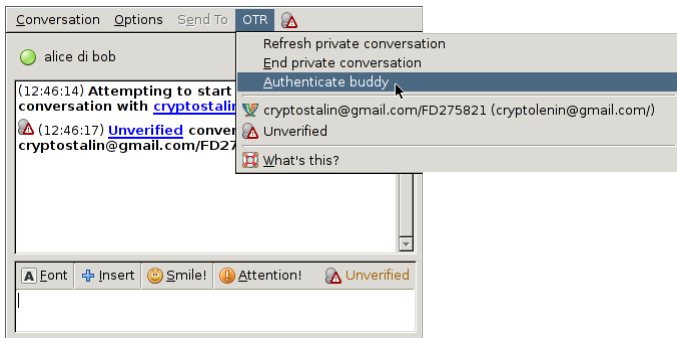
Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# CHAT NON VERIFICATA



# AUTENTICARE UN CONTATTO

La **prima** volta autenticate i vostri contatti!





Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# AUTENTICAZIONE

## Autenticazione con domanda segretissima



 **Authenticate cryptostalin@gmail.com**

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

How would you like to authenticate your buddy?  
Question and answer

*To authenticate using a question, pick a question whose answer is known only to you and your buddy. Enter this question and this answer, then wait for your buddy to enter the answer too. If the answers don't match, then you may be talking to an imposter.*

Enter question here:  
A ru.. ?

Enter secret answer here (case sensitive):  
\_\_\_\_\_

 Help       Cancel      Authenticate

Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# AUTENTICAZIONE

## Autenticazione con password segretissima



 **Authenticate cryptostalin@gmail.com**

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

How would you like to authenticate your buddy?  
Shared secret

*To authenticate, pick a secret known only to you and your buddy. Enter this secret, then wait for your buddy to enter it too. If the secrets don't match, then you may be talking to an imposter.*

Enter secret here:  
|lasuperpassword|

 Help       Cancel      Authenticate

# AUTENTICAZIONE

Autenticazione con verifica manuale delle fingerprint (numeri unici per ogni chiave!)



 **Authenticate cryptostalin@gmail.com**

Authenticating a buddy helps ensure that the person you are talking to is who he or she claims to be.

How would you like to authenticate your buddy?  
Manual fingerprint verification

*To verify the fingerprint, contact your buddy via some other authenticated channel, such as the telephone or GPG-signed email. Each of you should tell your fingerprint to the other. If everything matches up, you should indicate in the above dialog that you **have** verified the fingerprint.*

Fingerprint for you, cryptolenin@gmail.com/ (XMPP):  
04C84F51 AD22E608 9F5F7935 3397398E FC678DD0

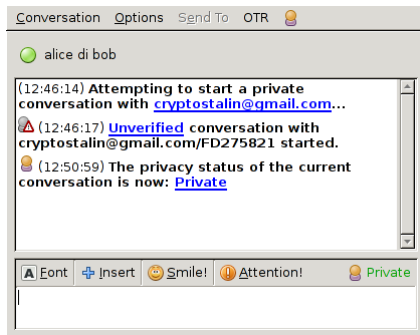
Purported fingerprint for cryptostalin@gmail.com:  
2FB1B0D3 72D056C8 61E4417A AAC1B823 79BFDC4A

verified that this is in fact the correct fingerprint for cryptostalin@gmail.com.

Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# CHAT PRIVATA

bla bla privato



## Perche'???

- **Tracciamento pubblicitario, profilazione**
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

## Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

## Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

## Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)



## Perche'???

- Tracciamento pubblicitario, profilazione
- Tutela della libertà di espressione
- Divulgazione sicura di informazioni che potrebbero metterci in pericolo
- Riservatezza
- Aggiramento della censura (es: PirateBay, Iran, China)

## Browser

- Lascia un sacco di informazioni su chi siamo
- Se configurato male è molto ad-friendly
- Banchetti per configurazione più sicura e anonima di firefox

# TOR

Tor:

- Invece di raggiungere direttamente un sito veniamo “rimbalzati” tra vari computer della rete TOR
- I computer che ci rimbalzano non possono sapere la nostra reale destinazione, nè la nostra reale provenienza

# TOR

Tor:

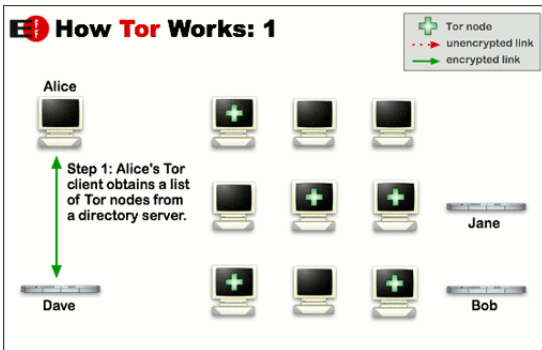
- Invece di raggiungere direttamente un sito veniamo “rimbalzati” tra vari computer della rete TOR
- I computer che ci rimbalzano non possono sapere la nostra reale destinazione, nè la nostra reale provenienza

# TOR

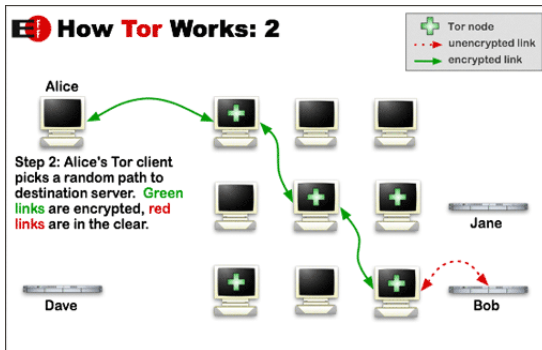
Tor:

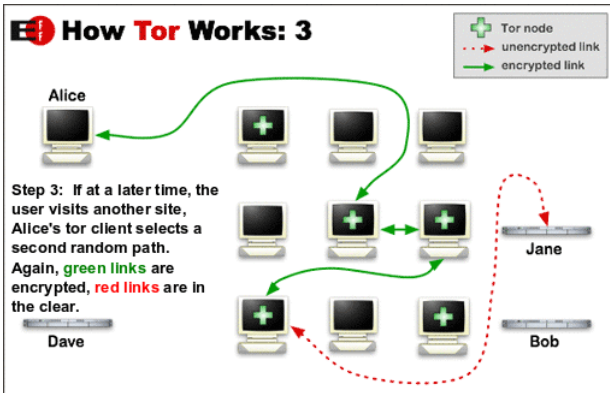
- Invece di raggiungere direttamente un sito veniamo “rimbalzati” tra vari computer della rete TOR
- I computer che ci rimbalzano non possono sapere la nostra reale destinazione, nè la nostra reale provenienza

Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:() )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption







## Niente paura: Tor Bundle

### Tor bundle

- realizzata per rendere più accessibile e sicuro l'utilizzo della rete TOR
- basata su firefox (Free software, multiplatforma)

## Niente paura: Tor Bundle

### Tor bundle

- realizzata per rendere più accessibile e sicuro l'utilizzo della rete TOR
- basata su firefox (Free software, multiplatforma)

## Niente paura: Tor Bundle

### Tor bundle

- realizzata per rendere più accessibile e sicuro l'utilizzo della rete TOR
- basata su firefox (Free software, multiplatforma)

# CIFRATURA FILE

Perche'???

- Furti
- Sequestri
- Manomissioni

# CIFRATURA FILE

## Metodi

- **cifrare solo file sensibili**
  - scomodo per molti file
  - non nasconde il nome, la dimensione, il numero di file, e altre informazioni
- contenitori cifrati
- cifratura totale del sistema (LUKS)

# CIFRATURA FILE

## Metodi

- cifrare solo file sensibili
  - scomodo per molti file
  - non nasconde il nome, la dimensione, il numero di file, e altre informazioni
- contenitori cifrati
- cifratura totale del sistema (LUKS)

# CIFRATURA FILE

## Metodi

- cifrare solo file sensibili
  - scomodo per molti file
  - non nasconde il nome, la dimensione, il numero di file, e altre informazioni
- contenitori cifrati
- cifratura totale del sistema (LUKS)

# CIFRATURA FILE

## Metodi

- cifrare solo file sensibili
  - scomodo per molti file
  - non nasconde il nome, la dimensione, il numero di file, e altre informazioni
- contenitori cifrati
- cifratura totale del sistema (LUKS)

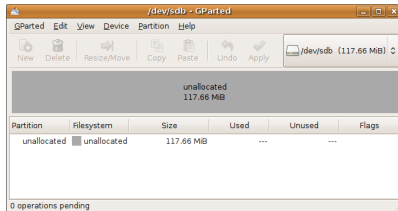


- Nella fase di installazione alcuni sistemi GNU Linux facilitano molto
- Luks + dm crypt (facile in fase di installazione)

Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# TRUECRYPT

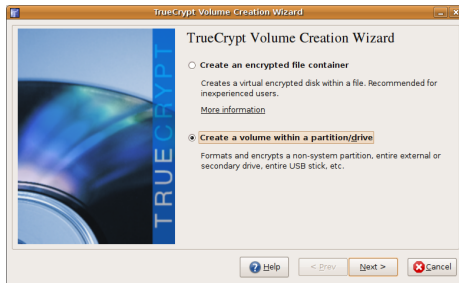
Creiamo la partizione da cifrare nel nostro device (tipo una penna usb) con gparted



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:( )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# TRUECRYPT

Selezioniamo di creare una partizione cifrata



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:)  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# TRUECRYPT

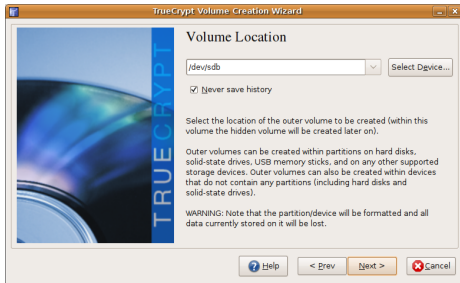
Scegliamo di creare un volume nascosto



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# TRUECRYPT

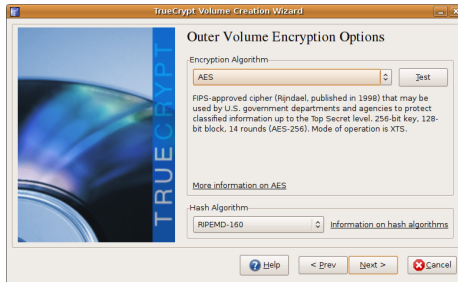
Specifichiamo il device del nostro supporto (nel nostro caso la penna e' vista come /dev/sdb) **ATTENZIONE: Assicuriamoci di non sbagliare il nome del device**



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# TRUECRYPT

Scegliamo l'algoritmo con cui cifreremo il contenitore del nostro volume nascosto. AES va bene come scelta di default.



Introduzione  
Cifratura a chiave pubblica  
GPG (on win:() )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# TRUECRYPT

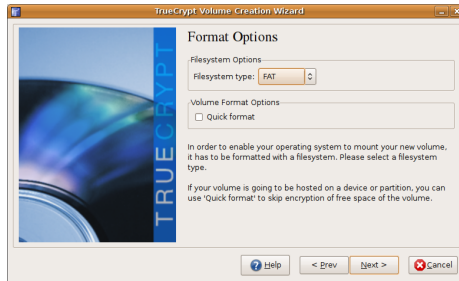
Impostiamo una password per aprire il contenitore del volume nascosto.



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

# TRUECRYPT

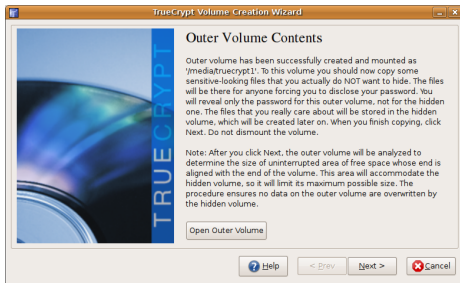
Scegliamo il filesystem per la nostra partizione





# TRUECRYPT

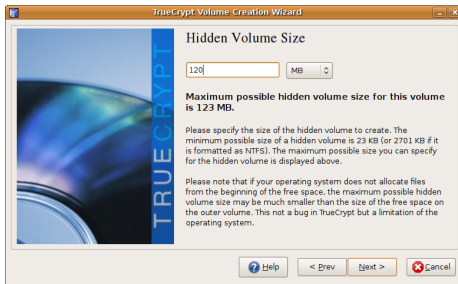
Adesso copiamo dei files nel contenitore. **ATTENZIONE:** I files copiati qui non dovranno essere dati sensibili e non dovremo copiare nuovi files altrimenti rischiamo di sovrascrivere il contenitore nascosto sottostante.



Introduzione  
Cifratura a chiave pubblica  
GPG (on win: )  
Mail  
Instant messaging : chat  
Anonimato online  
Files encryption

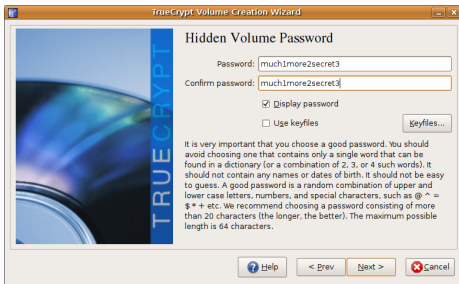
# TRUECRYPT

Scegliamo la dimensione della partizione nascosta.  
**ATTENZIONE:** la dimensione non potrà essere maggiore/uguale alla dimensione del contenitore.



# TRUECRYPT

Scegliamo la password con la quale aprire la partizione nascosta: **ATTENZIONE**: la password dovrà essere **ROBUSTA** e **DIVERSA** dalla password del contenitore creato prima.



## Sicurezza assoluta non esiste

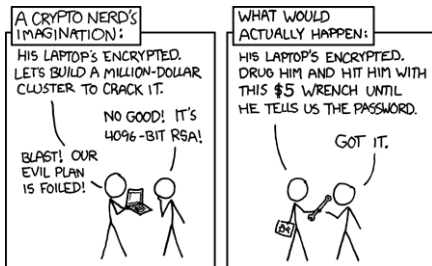
- Questi strumenti sono “sicuri” MA:
  - Il nostro computer è un’insieme di molti software, e tutti questi potrebbero essere utilizzati per aggirare la sicurezza
  - I programmi sono scritti da esseri umani, errori nel software sono utilizzati per aggirare la sicurezza

## Sicurezza assoluta non esiste

- Questi strumenti sono “sicuri” MA:
  - Il nostro computer è un’insieme di molti software, e tutti questi potrebbero essere utilizzati per aggirare la sicurezza
  - I programmi sono scritti da esseri umani, errori nel software sono utilizzati per aggirare la sicurezza

## Sicurezza assoluta non esiste

- Questi strumenti sono “sicuri” MA:
  - Il nostro computer è un’insieme di molti software, e tutti questi potrebbero essere utilizzati per aggirare la sicurezza
  - I programmi sono scritti da esseri umani, errori nel software sono utilizzati per aggirare la sicurezza



## Allora che si fa??

- Importanza dell'utilizzo di software libero
- codice aperto == controllato dalla comunità