A.L.R.Pennasilico

# Paranoia is a virtue.

9 Marzo 2007

## Guida alla sopravvivenza della propria privacy.

**mayhem@recursiva.org**
GPG Key ID B88FE057

# $ whois mayhem

**Security Evangelist @ Alba S.T.**

**Member / Board of Directors**:

AIP, AIPSI, CLUSIT, HPP, ILS, IT-ISAC, LUGVR, OPSI, Metro Olografix, No1984.org, OpenBeer/OpenGeeks, Recursiva.org, Sikurezza.org, Spippolatori, VoIPSA.



http://www.recursiva.org/
mayhem@recursiva.org

# Privacy



http://www.recursiva.org/
mayhem@recursiva.org

# Privacy

1890:

"il diritto di essere lasciati soli"

*Warren & Brandeis*



http://www.recursiva.org/
mayhem@recursiva.org

# Privacy

1890:

"il diritto di essere lasciati soli"

*Warren & Brandeis*

2005:

**"il diritto a chiedere di se stessi"**

*Lisi*



http://www.recursiva.org/
mayhem@recursiva.org

# DLGs 196/03



http://www.recursiva.org/
mayhem@recursiva.org

# DLGs 196/03

Esiste in Italia una legge che dovrebbe tutelare la nostra riservatezza.

# DLGs 196/03

Esiste in Italia una legge che dovrebbe tutelare la nostra riservatezza.

**Ma la tutela della nostra privacy non può essere demandata a nessuno.**



http://www.recursiva.org/
mayhem@recursiva.org

# Le informazioni...

“C'è una guerra là fuori, amico mio. Una guerra mondiale. E non ha la minima importanza chi ha più pallottole, ha importanza chi controlla le informazioni. Ciò che si vede, si sente, come lavoriamo, cosa pensiamo, si basa tutto sull'informazione!”

*Cosmo, da I signori della truffa*



http://www.recursiva.org/
mayhem@recursiva.org

# ... ed i computer

I nostri computer, le nostre comunicazioni, traboccano di informazioni che vorremmo non diventassero di pubblico dominio, o fossero conosciute da persone che non hanno alcun diritto di conoscerle.



http://www.recursiva.org/
mayhem@recursiva.org

# Domande ...



http://www.recursiva.org/
mayhem@recursiva.org

# Domande ...

Vogliamo proteggerci?



http://www.recursiva.org/
mayhem@recursiva.org

# Domande ...

Vogliamo proteggerci?

Quali strumenti abbiamo a disposizione per proteggere cosa?



http://www.recursiva.org/
mayhem@recursiva.org

# Domande ...

Vogliamo proteggerci?

Quali strumenti abbiamo a disposizione per proteggere cosa?

Che garanzie ci offrono questi strumenti?



http://www.recursiva.org/
mayhem@recursiva.org

# ... e risposte ...



http://www.recursiva.org/
mayhem@recursiva.org

# ... e risposte ...

La crittografia ci permette di garantire non solo la confidenzialità dei nostri dati, ma anche la loro integrità.

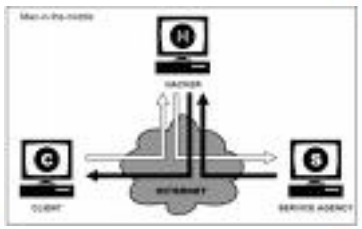
# ... e risposte ...

La crittografia ci permette di garantire non solo la confidenzialità dei nostri dati, ma anche la loro integrità.

L'utilizzo di strumenti OpenSource ci permette di essere certi delle funzionalità degli strumenti scelti.

# Comunicare con gli altri

Inviare una mail, fare una telefonata, non garantisce in alcun modo né che la conversazione resti riservata, né che il nostro interlocutore riceva l'informazione inviata da noi.



# Crittografia e servizi

L'utilizzo della crittografia a livello di servizio è da più parti implementata e consigliata, anche a livello commerciale o governativo.

Permette di aumentare la sicurezza dell'infrastruttura di rete.



http://www.recursiva.org/
mayhem@recursiva.org

# SSL

http -> https

pop3 -> pop3s

imap -> imaps

smtp -> smtps

telnet -> **ssh**

ftp -> **s**ftp

Utilizzare SSL permette in primis di proteggere il nome utente e la password utilizzati per accedere al servizio da eventuali attacker.



http://www.recursiva.org/
mayhem@recursiva.org

# Internet Service Provider



http://www.recursiva.org/
mayhem@recursiva.org

# Internet Service Provider

Proteggere da occhi indiscreti le nostre comunicazioni è un buon inizio.



http://www.recursiva.org/
mayhem@recursiva.org

# Internet Service Provider

Proteggere da occhi indiscreti le nostre comunicazioni è un buon inizio.

Ma le informazioni dove si trovano? Chi può accedervi? In che modo?

# Paranoia



http://www.recursiva.org/
mayhem@recursiva.org

# Paranoia

Vogliamo essere **tecnicamente certi** che nessuno possa accedere alle nostre informazioni, se non autorizzato da noi stessi.

# Paranoia

Vogliamo essere **tecnicamente certi** che nessuno possa accedere alle nostre informazioni, se non autorizzato da noi stessi.

**La nostra sicurezza deve essere demandata esclusivamente a noi.**

# Unethical laws

Questo approccio viene spesso ignorato, sconsigliato o addirittura vietato.

Utilizzarlo significa vanificare alcuni controlli previsti dalle leggi di molte nazioni. Tutto questo senza infrangere, **per ora**, nessuna legge.



http://www.recursiva.org/
mayhem@recursiva.org

“Chi non ha nulla da nascondere,
non ha nulla da temere”



http://www.recursiva.org/
mayhem@recursiva.org

**“Chi non ha nulla da nascondere, non ha nulla da temere”**

***Adolf Hitler, 1936***



http://www.recursiva.org/
mayhem@recursiva.org

# Ho il diritto di scegliere se inviare una cartolina o una lettera

# GNU Privacy Guard

GPG è uno dei programmi più usati per proteggere le proprie e-mail.

Utilizza uno standard molto diffuso (RFC2440), è OpenSource, gratuito e multipiattaforma.

E' compatibile con moltissimi client di posta.




http://www.recursiva.org/
mayhem@recursiva.org

# to sign

GPG permette di “firmare” le mail così da rendere il destinatario certo di due fattori:

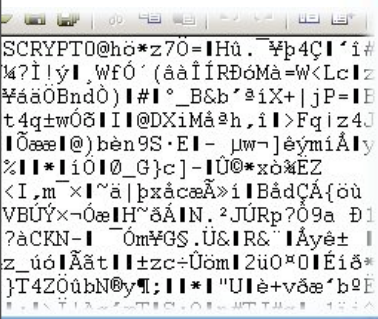
**sono davvero io il mittente e**

**nessuno ha modificato il contenuto**

Alessio Pennasilico

# to crypt

L'encryption è lo strumento che permette di essere certi che solo il destinatario ed il mittente sono (e saranno) in grado di leggere il contenuto di quel messaggio e-mail.






http://www.recursiva.org/
mayhem@recursiva.org

# Crittografia asimmetrica

Scambiare una password tra due persone, magari sconosciute, in modo sicuro, è un problema.

Per questo GPG lavora tramite l'utilizzo di due diverse chiavi:

- **la mia chiave pubblica**

- **la mia chiave privata**



http://www.recursiva.org/
mayhem@recursiva.org

# Chiave pubblica

Liberamente disponibile su Internet, su siti web e keyserver, viene usata dagli altri per verificare la mia firma e/o per criptare i messaggi diretti a me.



http://www.recursiva.org/
mayhem@recursiva.org

# Chiave privata

Mi è più cara della mia stessa vita, la ho solo io e ne sono l'unico gelosissimo ed attentissimo custode.

La uso per firmare i messaggi che invio ed è l'unica a poter decriptare i messaggi inviatimi dagli altri, criptati con la mia chiave pubblica.



http://www.recursiva.org/
mayhem@recursiva.org

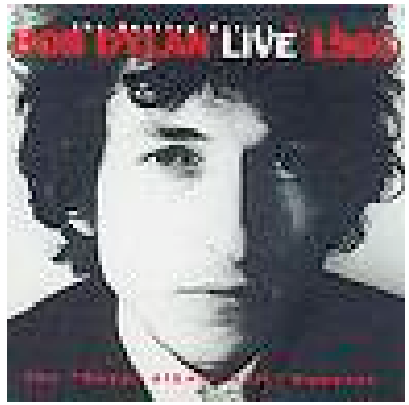
# Alice and Bob - sign

# Alice and Bob - sign



http://www.recursiva.org/
mayhem@recursiva.org

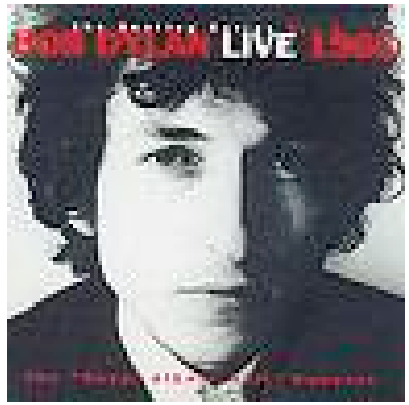
# Alice and Bob - sign






http://www.recursiva.org/
mayhem@recursiva.org

# Alice and Bob - sign



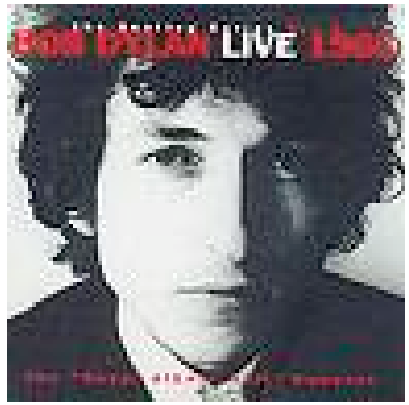

Chiave privata di Alice



http://www.recursiva.org/
mayhem@recursiva.org

# Alice and Bob - sign

sign




Chiave privata di Alice

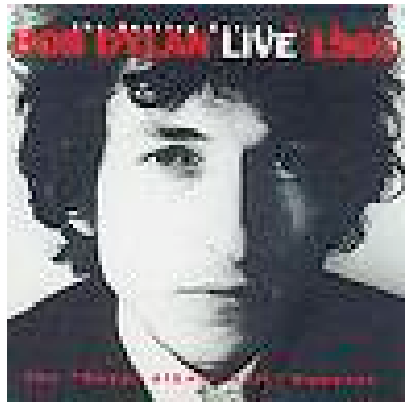


http://www.recursiva.org/
mayhem@recursiva.org

# Alice and Bob - sign

Chiave pubblica di Alice

sign



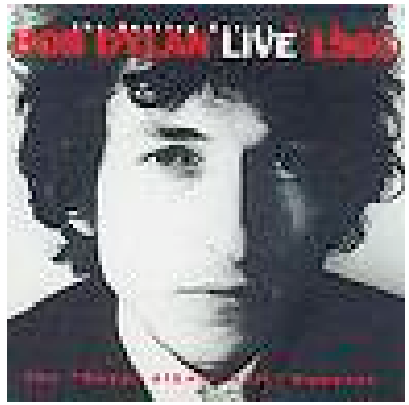

Chiave privata di Alice



http://www.recursiva.org/
mayhem@recursiva.org

# Alice and Bob - crypt

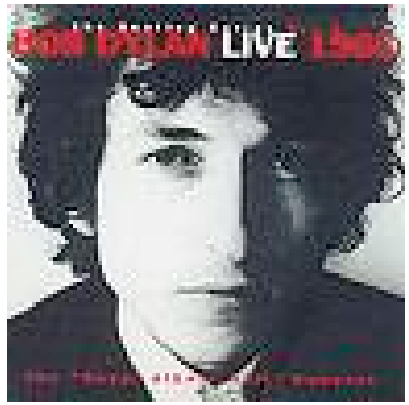
# Alice and Bob - crypt






http://www.recursiva.org/
mayhem@recursiva.org

# Alice and Bob - crypt

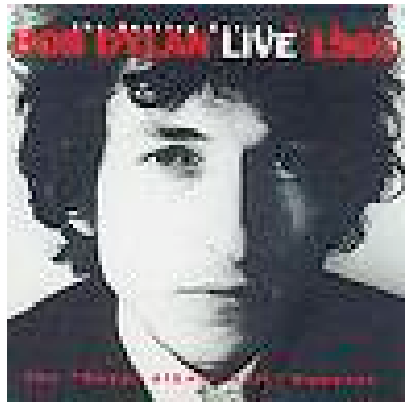





http://www.recursiva.org/
mayhem@recursiva.org

# Alice and Bob - crypt

Chiave pubblica di Alice

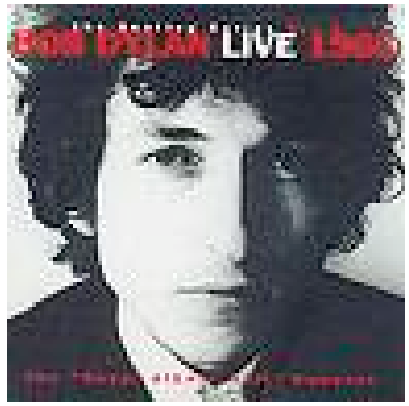





http://www.recursiva.org/
mayhem@recursiva.org

# Alice and Bob - crypt

Chiave pubblica di Alice



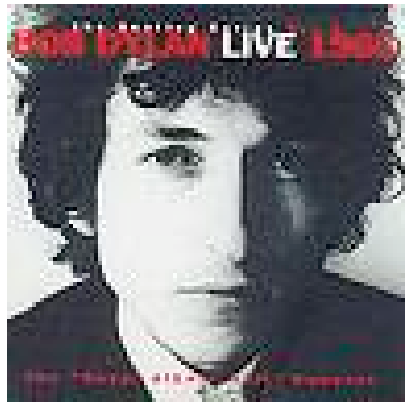

crypt



http://www.recursiva.org/
mayhem@recursiva.org

# Alice and Bob - crypt

Chiave pubblica di Alice




crypt

Chiave privata di Alice



http://www.recursiva.org/
mayhem@recursiva.org

# Autenticità della chiave

L'unico problema che resta è sapere con certezza che la chiave con ID B88FE057 è davvero la mia.

Per questa ragione si firmano le chiavi pubbliche altrui la cui appartenenza è certa *(keysigning party)*.



http://www.recursiva.org/
mayhem@recursiva.org

# Conclusioni

Si consiglia di usare un client di posta “sicuro”, meglio se OS, ad esempio Thunderbird, anch’esso gratuito e multipiattaforma, che supporta GPG.

E’ inoltre opportuno crittografare ogni e-mail e non solo quelle importanti.



http://www.recursiva.org/
mayhem@recursiva.org

# Comunicazioni e dati



http://www.recursiva.org/
mayhem@recursiva.org

# Comunicazioni e dati

Con GPG ho messo al sicuro il contenuto della mia posta.



http://www.recursiva.org/
mayhem@recursiva.org

# Comunicazioni e dati

Con GPG ho messo al sicuro il contenuto della mia posta.

Cosa posso fare per i file che conservo sul mio computer?



http://www.recursiva.org/
mayhem@recursiva.org

# Comunicazioni e dati

Con GPG ho messo al sicuro il contenuto della mia posta.

Cosa posso fare per i file che conservo sul mio computer?

Come evitare che un furto o uno smarrimento del mio laptop si trasformi in disclosure dei miei dati?



http://www.recursiva.org/
mayhem@recursiva.org

# TrueCrypt

Truecrypt è un programma OS, gratuito e multipiattaforma.

Permette di creare volumi o partizioni criptate a cui solo il proprietario può accedere grazie ad una password, ad un certificato o entrambi.

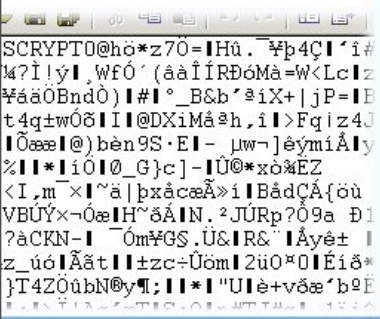
TRUECRYPT



http://www.recursiva.org/
mayhem@recursiva.org

# Deniable encryption

Dato un volume di TC è impossibile dire, anche a fronte di una attenta analisi, se quel volume sia criptato o meno.






http://www.recursiva.org/
mayhem@recursiva.org

# Steganografia

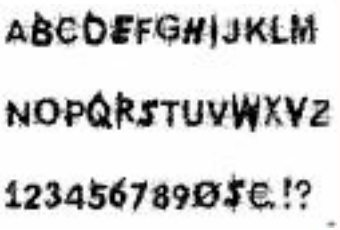
E’ possibile nascondere un volume di TC dentro un altro.

Il risultato è avere due password/ certificati:

# Password policy

E' necessario scegliere una saggia politica di gestione delle chiavi ed una robusta policy per la scelta delle password.

Non usiamo password banali, riconducibili a noi o utilizzate in altri contesti.






http://www.recursiva.org/
mayhem@recursiva.org

# Il problema delle chiavi

Lascereste le chiavi di casa nascoste in giardino?

La riservatezza della chiave è il presupposto fondamentale per l'efficacia di questi strumenti.

# Dispositivi USB

Per questa ragione conservare i file delle chiavi su un supporto rimovibile potrebbe essere una saggia decisione.

Non va trascurata l'esigenza di conservare una copia di backup della chiave in un luogo sicuro.



http://www.recursiva.org/
mayhem@recursiva.org

# Le telefonate

Tutte le considerazioni fatte per la posta valgono anche per le telefonate.

Essere rintracciati od intercettati è fattibile e succede molto più spesso di quanto si pensi.

# GSM/analog

Utilizzare la linea di casa può permettere anche a sconosciuti di “ascoltare” le nostre conversazioni in molti casi.

Nel caso dei telefoni GSM è quasi sempre necessario che siano le forze dell’ordine ad interfacciarsi con il nostro operatore.



http://www.recursiva.org/
mayhem@recursiva.org

# VoIP, una soluzione

Il Voice over IP, telefonare attraverso Internet, ci permette di riprendere possesso del mezzo di telecomunicazione.

Nulla mi vieta di avere un centralino VoIP a casa e di utilizzarlo per parlare con le persone di cui ho fiducia, anche gratuitamente.




http://www.recursiva.org/
mayhem@recursiva.org

# Skype

Skype protegge con la crittografia tutte le comunicazioni.

Tuttavia non conosciamo il funzionamento del programma, chi lo può controllare.

Le nostre informazioni sono conservate su un server di cui non abbiamo alcun controllo.




http://www.recursiva.org/
mayhem@recursiva.org

# Soluzione: la solita!

Appoggiarsi a strumenti OS di cui conosciamo il funzionamento *(es. OpenWengo).*

Utilizzare carrier di cui abbiamo fiducia e che permettono di utilizzare tecnologie aperte e messe in sicurezza *(es. SIP con TLS ed SRTP).*

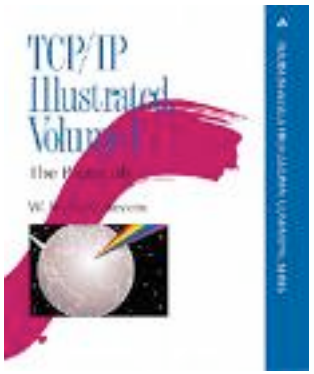


http://www.recursiva.org/
mayhem@recursiva.org

# Indirizzo IP

Quando siamo in rete il nostro computer viene identificato da un numero, un indirizzo univoco.

Anche se l'indirizzo IP può cambiare nel tempo, sul nostro computer restano diverse informazioni sui siti visitati *(es. cookies)*.






http://www.recursiva.org/
mayhem@recursiva.org

# Log

Tramite l'indirizzo IP è possibile tenere traccia dei siti visitati da un particolare computer/persona, del loro contenuto.

E' possibile tenere traccia anche delle persone con cui si scambiano mail.

# Profiling

E’ possibile quindi tracciare un profilo dei nostri gusti, delle nostre abitudini, idee... anche da un punto di vista sessuale, politico, religioso, persino di eventuali malattie.



http://www.recursiva.org/
mayhem@recursiva.org

# Anonimato

Per tutte queste ragioni è spesso preferibile, se non addirittura necessario essere in grado di poter utilizzare Internet in modo anonimo, senza poter mettere in grado un sito o un motore di ricerca di risalire a noi.

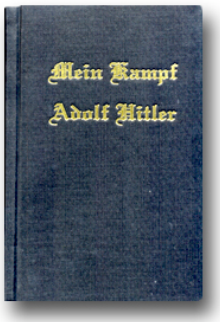


http://www.recursiva.org/
mayhem@recursiva.org

# Basta con i falsi slogan!

**“Chi non ha nulla da nascondere, non ha nulla da temere”**

***Adolf Hitler, 1936***

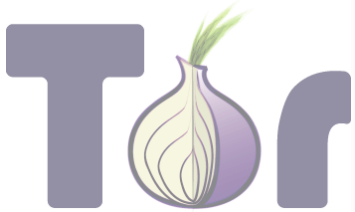





http://www.recursiva.org/
mayhem@recursiva.org

# Tor

“Tor ha serve a proteggere contro l'analisi del traffico, una forma di sorveglianza della rete che minaccia la privacy e l'anonimato personale, i rapporti d'affari e le attività confidenziali, la sicurezza dello stato. Con Tor le comunicazioni vengono indirizzate attraverso una rete distribuita di server, chiamati onion router, che proteggono l'utente dalla profilazione dei siti web, o da intercettazioni locali che, controllando il traffico dei dati, possono capire quali siti vengono visitati.”





http://www.recursiva.org/
mayhem@recursiva.org

# Vidalia

E’ possibile installare Vidalia per avere una interfaccia grafica semplice dalla quale gestire il proprio server Tor.

Vidalia, come Tor, è gratuito ed OpenSource, nonchè multipiattaforma.

# TorPark

TorPark, purtroppo solo per windows, permette di non utilizzare il nostro disco fisso per la navigazione, ma una chiave USB sulla quale si trovano Tor e Firefox.

Alla rimozione della chiavetta non resterà alcuna traccia dei siti da noi visitati sul computer utilizzato.




http://www.recursiva.org/
mayhem@recursiva.org

# Anonymous remailer

Per poter inviare una mail anonima non basta cambiare il mittente nel programma di posta.

E' necessario appoggiarsi a server che utilizzano sistemi conosciuti e consolidati di gestione dell'anonimato del messaggio, magari mettendone in catena diversi *(es. Mixminion).*



http://www.recursiva.org/
mayhem@recursiva.org

# OpenSource

Tutti i programmi mostrati funzionano su diversi sistemi operativi.

Se la riservatezza è tra i nostri obiettivi forse dovremmo valutare di affidarci a programmi il cui funzionamento è documentato, conosciuto e verificabile.




http://www.recursiva.org/
mayhem@recursiva.org

# Paranoia is a virtue



http://www.recursiva.org/
mayhem@recursiva.org

# Bibliografia


http://www.gnupg.org/

http://www.ietf.org/rfc/rfc2440.txt

http://www.truecrypt.org/

http://sourceforge.net/projects/truecrypt/

http://tor.eff.org/index.html.it

http://vidalia-project.net/

http://www.torrify.com/software_torpark.html

http://kaostour.autistici.org/2005/materiali/kaostour-slides/kaostour-2005.html


# Domande?

Queste slide sono disponibili su:
http://www.recursiva.org

Per domande o approfondimenti:
mayhem@recursiva.org

# Domande?

## Grazie per l'attenzione!

Queste slide sono disponibili su:
http://www.recursiva.org

Per domande o approfondimenti:
mayhem@recursiva.org