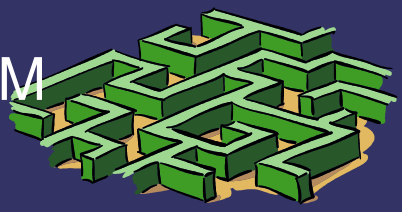
INFO FREE FLOW CREW & LABORATORIO OCCUPATO CRASH!
presentano:

SECURITY HANDSHAKE – Oltre la Paranoia Informatica

SICUREZZA, CRITTOGRAFIA ED ANTISPAM PER LA POSTA ELETTRONICA



24 Ottobre 2008

Trovate i software necessari per questo seminario a:

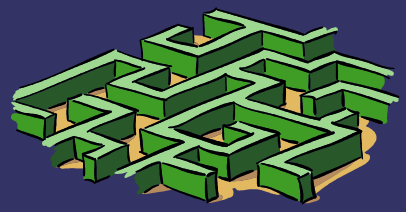
http://www.mozillaitalia.it/thunderbird/

http://www.gnupg.org/

http://enigmail.mozdev.org/

http://oss.codepoet.no/revelation/

http://www.keepassx.org/

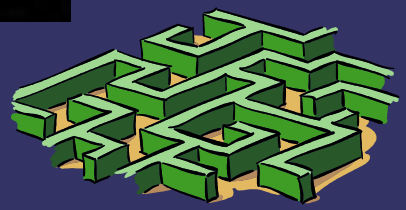


Sicurezza?

Noi di Info Free Flow e del laboratorio Occupato Crash siamo per la sicurezza.

=

????



Sicurezza?

Un esempio da cui partire:

- Sistema di intercettazione britannico recentemente pubblicizzato anche dai media nazionali.

QUALSIASI TIPO DI COMUNICAZIONE IN QUALSIASI MOMENTO POTRÀ ESSERE INTERCETTATA ED ARCHIVIATA IN ENORMI DATABASE.

Incubo totalitario?
Distopia orwelliana?

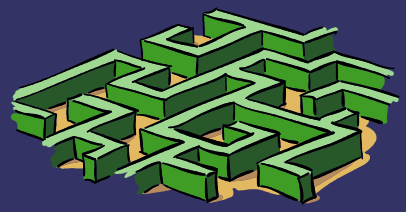
Sicurezza?

NO!

Strumento democratico a salvaguardia dei diritti e della “sicurezza” dei cittadini

<< Dopo l'11 settembre la polizia ed i servizi segreti stanno " dando la caccia ai siti jihadisti" (sic!). Non possiamo più controllare "i criminali" o le sole le categorie a rischio. Non abbiamo tempo. Quindi per semplificare questo gravoso ma indispensabile (per la vostra sicurezza) compito controlleremo tutti voi. Tutto questo per evitare un altro 11 settembre.

Ma non temete: chi non ha nulla da nascondere
non ha nulla da temere. >>



Sorveglianza

Informazione

V

Paura

V

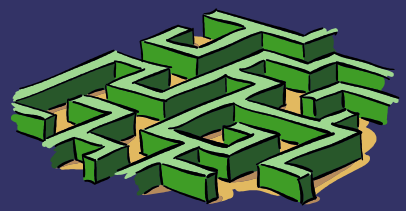
Allarme sicurezza

V

Sorveglianza

V

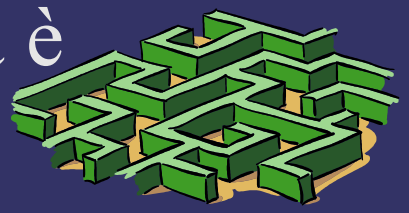
Controllo sociale



Sicurezza?

L'informazione mediatica da una lettura distorta della realtà, creando mostri sociali e “uomini neri” pronti a rapinarti, stuprarti, truffarti, picchiarti, drogarti, terrorizzarti ecc ecc ecc. Essi sono ad ogni angolo, in ogni strada ed in ogni piazza.

Limitarsi a denunciare questa dinamica è **semplicemente idiota ed ingenuo**

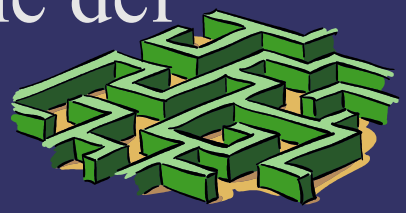


Sicurezza?

"La lotta di classe la facciamo anche noi!"

GianMaria Volonté/Bizanti in "Sbatti il mostro in prima pagina"

Non esiste alcun narratore imparziale.
L'informazione è un processo di soggettivazione dei fatti (input) che produce una narrazione del reale subordinata ad interessi ed obiettivi specifici (output)

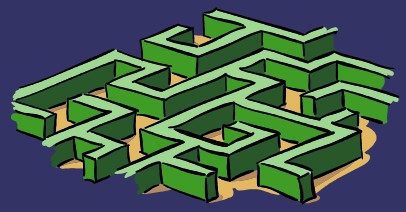


Sicurezza?

Oggi l'obiettivo è la creazione costante di
PAURA

- La paura è un'emozione governata dall'istinto, che ha come obiettivo la sopravvivenza dell'individuo ad una presunta situazione di pericolo.

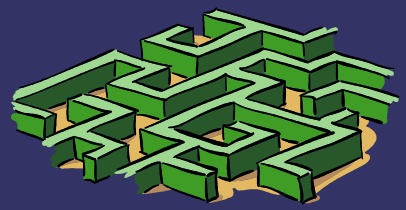
- La paura può essere indotta.



Sicurezza ?

Paura distillata quotidianamente:

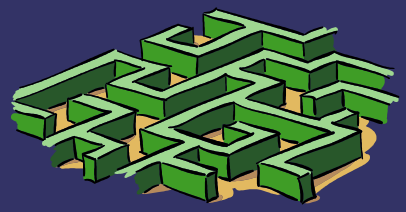
- Insinua un onnipresente sospetto
- Distrugge reti e solidarietà sociale
- Fomenta odio, razzismo, xenofobia, sessismo, paura di ciò che è diverso
- Nega le diversità nell'affermazione di una presunta "normalità"



Sicurezza?

Obiettivi ultimi:

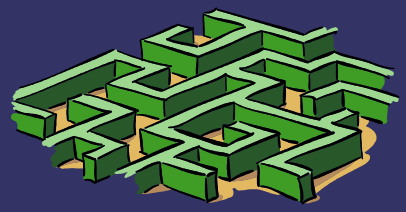
- Smantellamento dell'idea di comunità
- Distruggere con la paura qualsiasi forma di lettura critica del reale (individuale o costruita collettivamente) e di partecipazione sociale e politica
- Giustificare e legittimare misure repressive e leggi sempre più liberticide.



Sicurezza?

Risultato:

- I militari nelle strade
- La militarizzazione delle piazze delle strade
- Il controllo di massa su intere zone e quartieri metropolitani grazie ai sistemi di videosorveglianza
- I lager per migranti
- Le impronte digitali elettroniche ed i sistemi di controllo biometrico

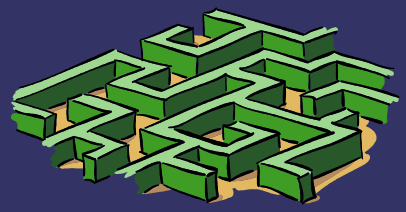


Sicurezza?

Ma tutto questo non viene semplicemente imposto dall'alto.

Il cittadino/l'individuo stesso lo richiede e lo legittima in un contesto che appare sempre più hobbesiano (homo homini lupus) pensando sia una via d'uscita al terrore che vive quotidianamente.

Così decidiamo di barattare la tranquillità persa con IL CONTROLLO SOCIALE

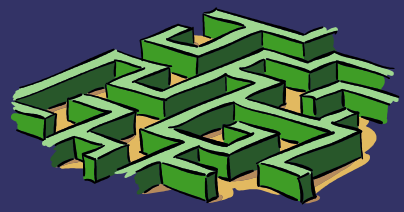


Sicurezza?

E la precarietà?
Essa gioca un ruolo ambivalente in questo contesto:

- Da una parte genera paura per la condizione a cui costringe (affitto , istruzione, lavoro) --> La paura di non arrivare a fine mese.

- Da una parte è strumento di controllo, una necessità a cui si è aggrappati ed a cui è sempre più difficile ribellarsi perché si ha paura di non riuscire a sopravvivere

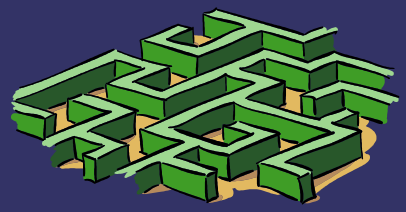


Sicurezza?

E in rete?

Internet è stata forse il campo di sperimentazione della nostra epoca rispetto alla dinamica appena descritta.

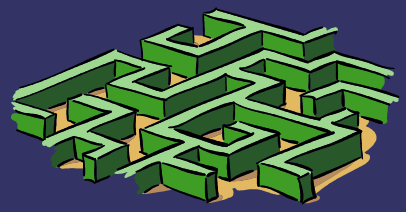
- Gli hacker malefici che imperversano on – line
- Le truffe informatiche, il phishing
- I forum jihadisti
- I pirati del P2P
- E un altro mucchio di baggianate di cui abbiamo PAURA!



Sicurezza?

Risultato:

- L'introduzione di massicci sistemi di sorveglianza delle nostre comunicazioni
- Il costante tracciamento e profilazione delle nostre attività in rete per controllare e rendere monetizzare le nostre comunicazioni
- La progressiva perdita del diritto ad una comunicazione libera



Sicurezza?

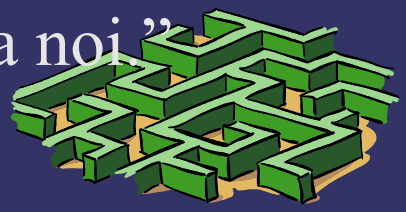
A proposito di sicurezza in rete:

Trusted networking

(tratto da HAX N°6)

"In nome della sicurezza e della qualità del servizio, internet sarà canalizzata nell'alveo di fiumi di comunicazioni contingentati, precostituiti e sorvegliati."

"Il Web 2.0, inoltre, si muove nella direzione de Trusted Networking. Reti sicure per transazioni sicure. Il prezzo della sicurezza è sempre la libertà personale. Sempre . Per convincerci a rinunciare alla libertà personale, il primo è quello di farci sentire insicuri. Internet è pericoloso. Ci sono gli hackerz. Ci sono i virus. Ti fregano la carta di credito. Tranquillo, stiamo studiando una nuova internet dove sarai sicuro e felice, senza problemi. Basta che ti affidi con fiducia a noi."



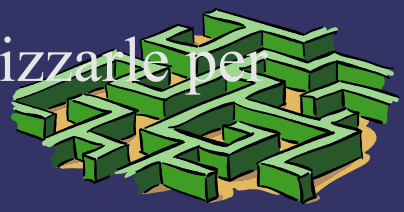
Sicurezza?

Un ultimo appunto:

Sicurezza e sorveglianza sono business miliardari.

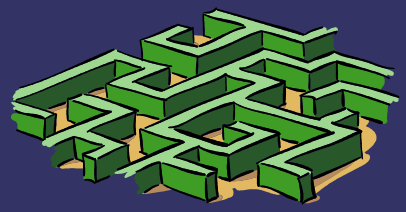
- Software antivirus e per la sicurezza dal costo proibitivo.
- L'utilizzo di software e sistemi operativi dal codice sorgente chiuso spacciati per sicuri.
- Il trusted computing
- Sistemi operativi che mandano di continuo informazioni personali alla “casa madre” a insaputa dell'utente.
- I social network commerciali

Qualcuno accumula informazioni su di noi, pronto ad utilizzarle per affinare le ricerche di mercato oppure quelle di polizia.



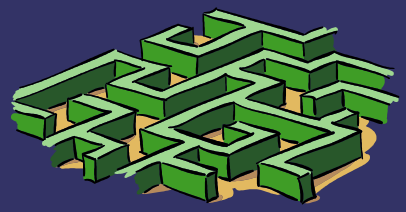
Conclusione

Se ancora non è chiaro stiamo imparando che la sorveglianza può essere invadente, e rappresentare un attentato alla nostra libertà infinitamente maggiore delle minacce che ci fanno passare davanti agli occhi.



Sicurezza?

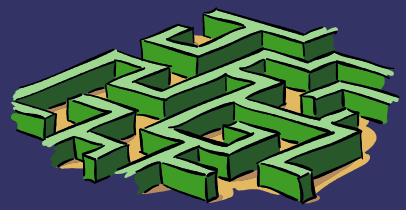
Noi di Info Free Flow e del Laboratorio Occupato
Crash siamo per la sicurezza



SICUREZZA!

Abbiamo paura:

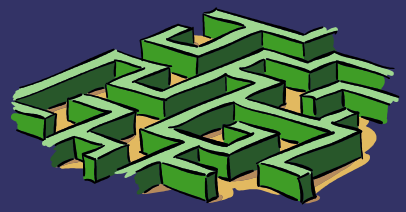
- Della precarietà che affligge ogni aspetto della nostra esistenza
- Del razzismo, dell'omofobia, del sessismo e dei continui rigurgiti neo fascisti
- La continua erosione dei nostri diritti in tutti i settori sociali
- Il controllo sociale esteso e pervasivo



Sicurezza!

La nostra sicurezza

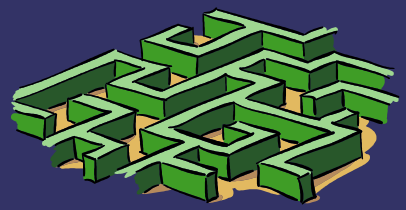
- Il rafforzamento delle reti sociali
- Rendere viva ed attraversata la città grazie alla pratica dell'occupazione
- L'autogestione delle nostre esistenze
- Riuscire a soddisfare con pratiche collettive i nostri bisogni e desideri.



Sicurezza!

E in rete?

- L'autogestione delle nostre informazioni
- La libera condivisione di saperi e conoscenze
- La possibilità di utilizzare software liberi
- La creazione di comunità on – line
- La difesa della nostra privacy

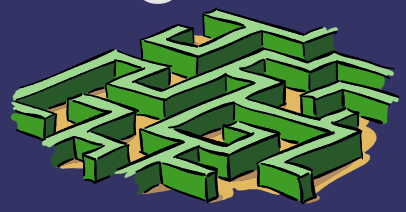


Tipologie di sorveglianza

a)***Log delle sessioni di navigazione su internet da parte dei provider*** con Decreto Pisanu/Legge 155/2005

- Per aver accesso alla rete dai luoghi pubblici (internet point o università) è necessario disporre di un documento con cui verranno potenzialmente correlate le nostre attività in rete.

- I provider sono obbligati per legge a tenere i log delle attività degli utenti per 30 mesi.



Salvataggio delle informazioni diffuse dagli utenti di internet durante la navigazione (Log) da parte dei provider [Decreto Pisanu, convertito nella Legge 155/2005 http://www.parlamento.it/leggi/05155l.htm]

Art. 6.

Nuove norme sui dati del traffico telefonico e telematico

1. A decorrere dalla data di entrata in vigore del presente decreto e fino al 31 dicembre 2007 e' sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni, e limitatamente alle informazioni che consentono la tracciabilità degli accessi, *nonche', qualora disponibili,* dei servizi, debbono essere conservati fino a quella data dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'art. 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del presente decreto-legge, salvo l'esercizio dell'azione penale per i reati comunque perseguibili. 2. All'articolo 55, comma 7, del decreto legislativo 1° agosto 2003, n. 259, le parole *«al momento* dell'attivazione del servizio.» sono sostituite dalle seguenti: «prima dell'attivazione del servizio, al momento della consegna o messa a disposizione della occorrente scheda elettronica (S.I.M.). Le predette imprese adottano tutte le necessarie misure affinche' venga garantita l'acquisizione dei dati anagrafici riportati su un documento di identità, nonche' del tipo, del numero e della riproduzione del documento presentato dall'acquirente, ed assicurano il corretto trattamento dei dati acquisiti.».

3. All'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole «al traffico telefonico», sono inserite le parole: «, inclusi quelli concernenti le chiamate senza risposta,»;

b) al comma 1, sono aggiunte in fine le parole: «, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per sei mesi»;

c) al comma 2, dopo le parole: «al traffico telefonico», sono inserite le seguenti: «, inclusi quelli concernenti le chiamate senza risposta,»

d) al comma 2, dopo le parole: «per ulteriori ventiquattro mesi», sono inserite le seguenti: «e quelli relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati per ulteriori sei mesi»;

e) al comma 3, le parole: «giudice su istanza del pubblico ministero o» sono sostituite dalle seguenti: «pubblico ministero anche su istanza»;

f) dopo il comma 4, e' inserito il seguente:

«4-bis. Nei casi di urgenza, quando vi e' fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che e' comunicato immediatamente e comunque non oltre ventiquattro ore al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non viene convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati.».

4. Con regolamento adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Presidente del Consiglio dei Ministri, di concerto con i Ministri interessati, *sentito il Garante per la protezione dei dati personali,* sono definiti le modalità ed i tempi di attuazione della previsione di cui al comma 3, lettere *a), b), c)* e *d), del presente articolo* anche in relazione alla determinazione e allocazione dei relativi costi, con esclusione, comunque, di oneri per il bilancio dello Stato.

I dati relativi al traffico sono i dati sottoposti a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione. La Direttiva 2002/58/CE definisce i dati relativi al traffico come i dati concernenti l'instradamento, la durata, il tempo o il volume di una comunicazione, il protocollo usato, l'ubicazione dell'apparecchio terminale di chi invia o riceve, la rete sulla quale la comunicazione si origina o termina, nonché i dati inerenti l'inizio, la fine o la durata di un collegamento.

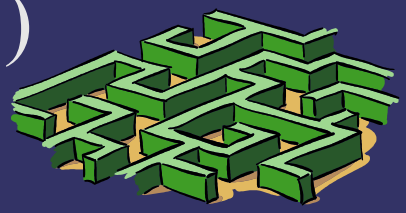
Tipologie di sorveglianza

b) ***Data Mining.*** Monitoraggio a fini pubblicitari e commerciali di:

- Attività degli utenti
- Controllo di profili
- Network di utenza
- Risorse condivise e contenuti fruiti in rete: tramite l'incrocio di questi dati in un primo momento "amorfi", il data mining attribuisce loro un senso

Basato su due principi:

- Concetto di esternalità di rete (economico)
- Coda lunga (matematico)



Tipologie di sorveglianza

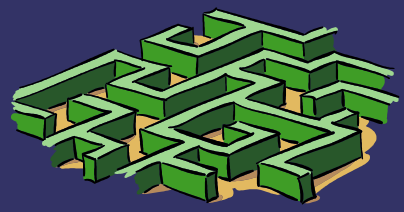
- Esternalità di rete: un bene o un servizio assume un valore tanto più grande quanto maggiore è il numero dei consumatori che lo utilizzano.

In questo caso parliamo di servizi di comunicazione come

-***I motori di ricerca*** (Google, Yahoo, ecc)

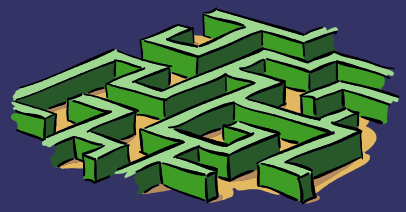
-***I social network*** (Myspace, Youtube, Flickr ecc)

-***Le webmail*** (Gmail)



Tipologie di sorveglianza

•La coda lunga: gli eventi poco frequenti o di bassa ampiezza – la coda lunga, rappresentata dalla porzione gialla della curva – possono cumulativamente superare in numero o in importanza la porzione iniziale della curva, di modo che presi tutti insieme rappresentano la maggioranza



Tipologie di sorveglianza

E allora? Come si combinano questi 2 elementi?

Passaggio da
→ pubblicità di massa spersonalizzata
→ pubblicità individuale personalizzata

Grazie alla profilazione (elaborazione di un profilo) delle attività (sopratutto quelle marginali) di milioni di internauti i motori di ricerca o i social network propongono delle pubblicità ad hoc, MIRATE, basate sui vostri gusti e sulle vostre preferenze specifiche.

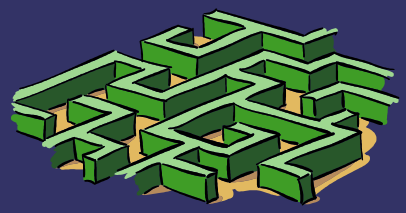
Tipologie di sorveglianza

RISULTATO:

- Gli inserzionisti sono felici, comprano spazi pubblicitari sapendo che grazie alla sorveglianza messa in atto sul network dei motori di ricerca il loro messaggio arriverà con molta più probabilità a chi è interessato.

- Google guadagna miliardi grazie alle vostre attività in rete. Anzi vive di quelle.

Questa è l'architrave portante del sistema economico del "***web 2.0***"



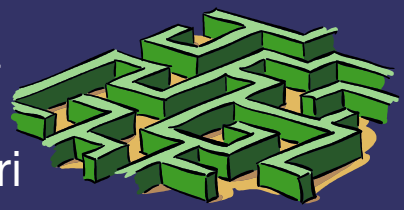
Tipologie di sorveglianza

Data Mining: Monitoraggio a fini di pubblicitari, ma anche di controllo, di profili, network di utenza, attività, risorse condivise, contenuti fruiti in rete:
[Dalla Privacy Policy di Google: http://www.google.it/privacy.html]

Utilizzi

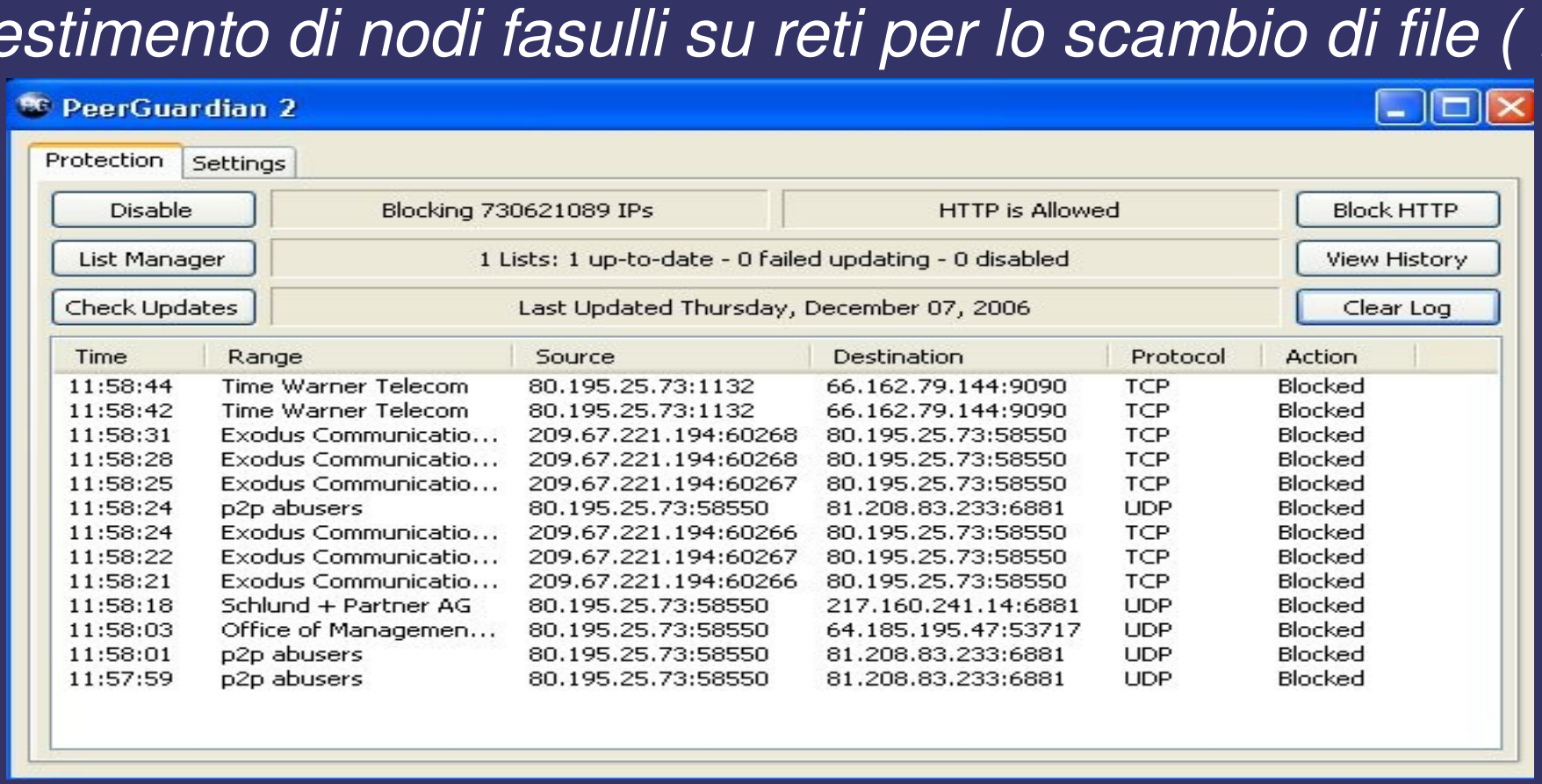
- Possiamo usare i dati personali per fornire i servizi che avete chiesto, ivi inclusa la visualizzazione di contenuti personalizzati e della pubblicità.
- Possiamo anche usare i dati personali ai fini di controllo, ricerca ed analisi per gestire e migliorare le tecnologie ed i servizi di Google.
- Possiamo condividere dati aggregati non personali con terze parti esterne a Google.
- Quando ci serviamo di terzi per farci aiutare nel trattamento dei vostri dati personali, chiediamo a tali terzi di rispettare le nostre Norme sulla privacy e qualunque misura di riservatezza e sicurezza necessaria.
- Possiamo anche condividere le informazioni con terzi in alcuni casi particolari, come in caso di procedimenti legali, evitare la frode o danni imminenti, e garantire la sicurezza del nostro network e dei nostri servizi.
- Google tratta i dati personali sui suoi server situati negli Stati Uniti ed in altri paesi. In alcuni casi i vostri dati personali vengono trattati su un server che si trova al di fuori del vostro paese..
- Per saperne di più cliccate su Leggi piu nel testo completo delle norme sulla privacy.

Il processo di ***Data Mining*** stabilisce delle correlazioni tra questi dati, in un primo momento amorfi, attribuendogli un “senso”:
- da un lato, costruendo un profilo-utente incrociando i dati che questo rilascia usando più servizi
- dall'altro, con l'individuazione di preferenze aggregate (es. I brani più popolari su LastFm)



Tipologie di sorveglianza

c) *Allestimento di nodi fasulli su reti per lo scambio di file (P2P)*



Lo scopo di tali nodi fasulli è quello di minare la fiducia degli utenti nel meccanismo P2P:

- Fornendo falsi risultati
- Mettendo in condivisione file contraffatti e potenziali esecutori di codice malevolo
- Rallentando lo scambio P2P in genere
- Tracciando l'attività degli utenti e mettere in atto sanzioni penali e salatissime multe
- Minando il sistema di fiducia che sta alla base della condivisione P2P

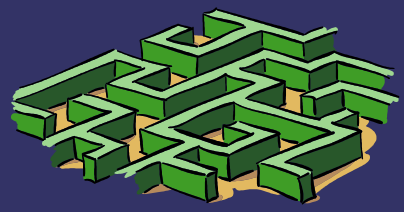
Tipologie di sorveglianza

d) *Sequestro di Siti+Siti Civetta+Filtraggio Istituzionale per Categorie*

- A volte si manifesta in modo illegale: nell'agosto 2008 la Guardia di Finanza, bloccato l'accesso al sito thepiratebay.org Alcuni provider (Fastweb) al posto di inserirvi come da prassi un banner che testimoniasse l'avvenuto blocco, ne redirigeva gli utenti sul sito dei fonografici inglesi, i quali a loro volta potevano curiosare nei profili di chi metteva file in condivisione.

- Caso analogo per Marijuana.it.

- A Palazzo Paleotti l'UNIBO opera un filtraggio categorizzato di determinati siti internet.



LIVELLI DI SICUREZZA NELLA POSTA ELETTRONICA

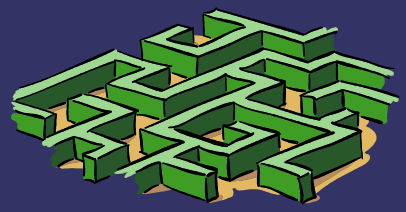
- ***Scelta dei servizi di posta:*** utilizzare quelli autogestiti come Autistici/Inventati; i servizi commerciali (gmail, yahoo, tiscali, libero, ecc. praticano il Data Mining)

- ***Trasporto del Messaggio:*** usare ***SSL*** (protocollo di cifratura dati) e controllo dell'autenticità

- ***Accesso alla Posta:*** occorre formulare una BUONA ***password***

- ***Contenuto del Messaggio:*** si può (deve) cifrare con ***GPG***

- ***Origine del Messaggio:*** si nasconde con il *remailer* (***Mixmaster, Mixminion***) – non verrà trattato in questo corso



SSL

Secure Socket Layer

(livello di connessione sicura)

- Protocollo proposto dalla Netscape Communications Corporation.

- Garantisce confidenzialità e affidabilità delle comunicazioni su Internet.

- Protegge da intrusioni, modifiche falsificazioni.

- Essenziale per:

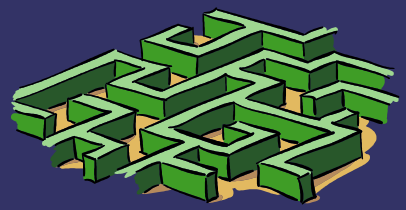
E-commerce, trading on-line, internet banking, e-mail privata, etc...




- Un po' di nomi:

HTTPS vs HTTP, POPs vs POP, SMTPs vs SMTP, IMAP vs IMAPS

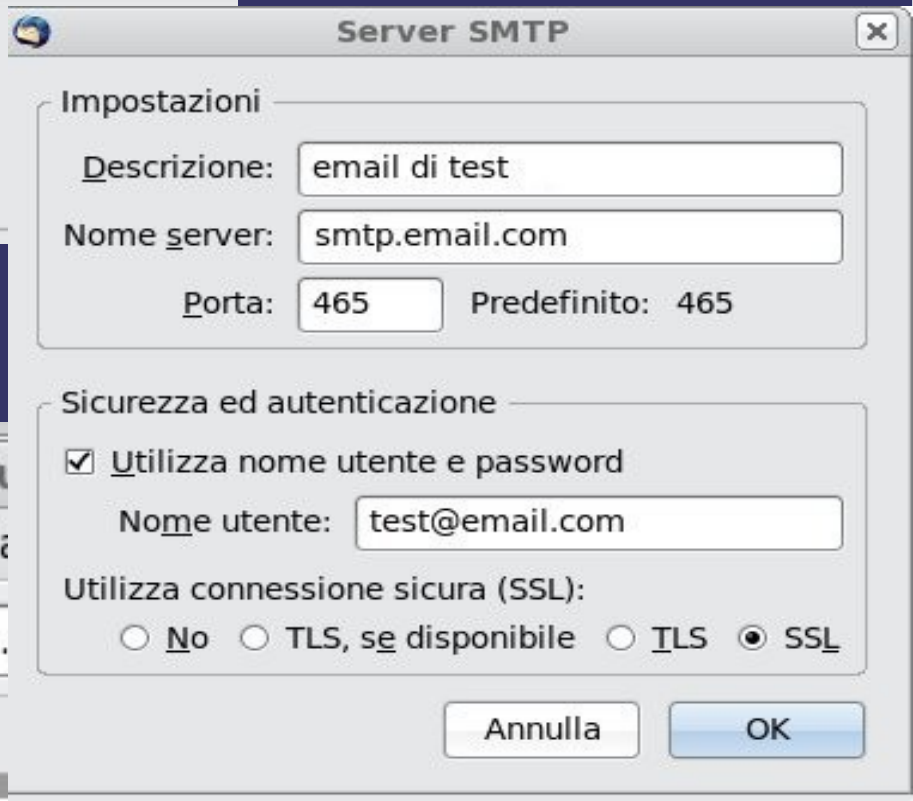
- HyperText Transport Protocol
- Post Office Protocol
- Simple Mail Transfer Protocol
- Internet Message Access Protocol



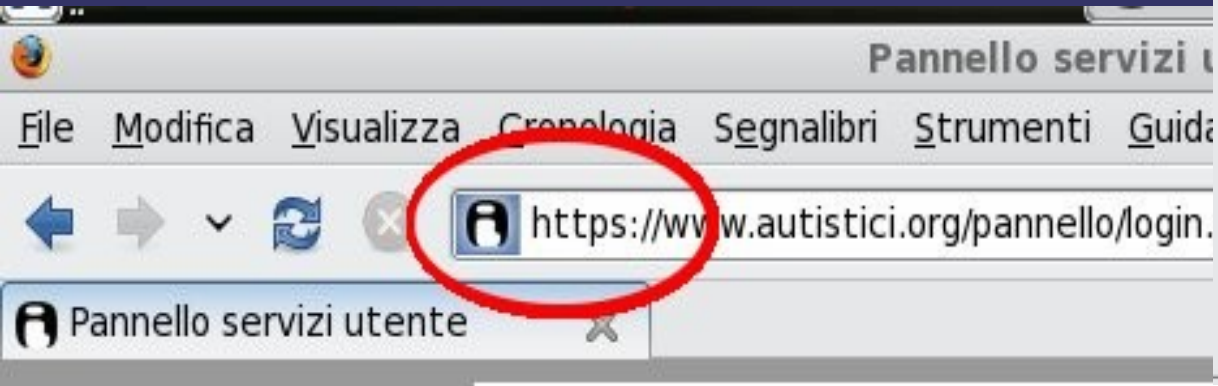
Come riconoscere se si sta usando una connessione sicura?

Thunderbird: Modifica -> Impostazioni Account -> Impostazioni server

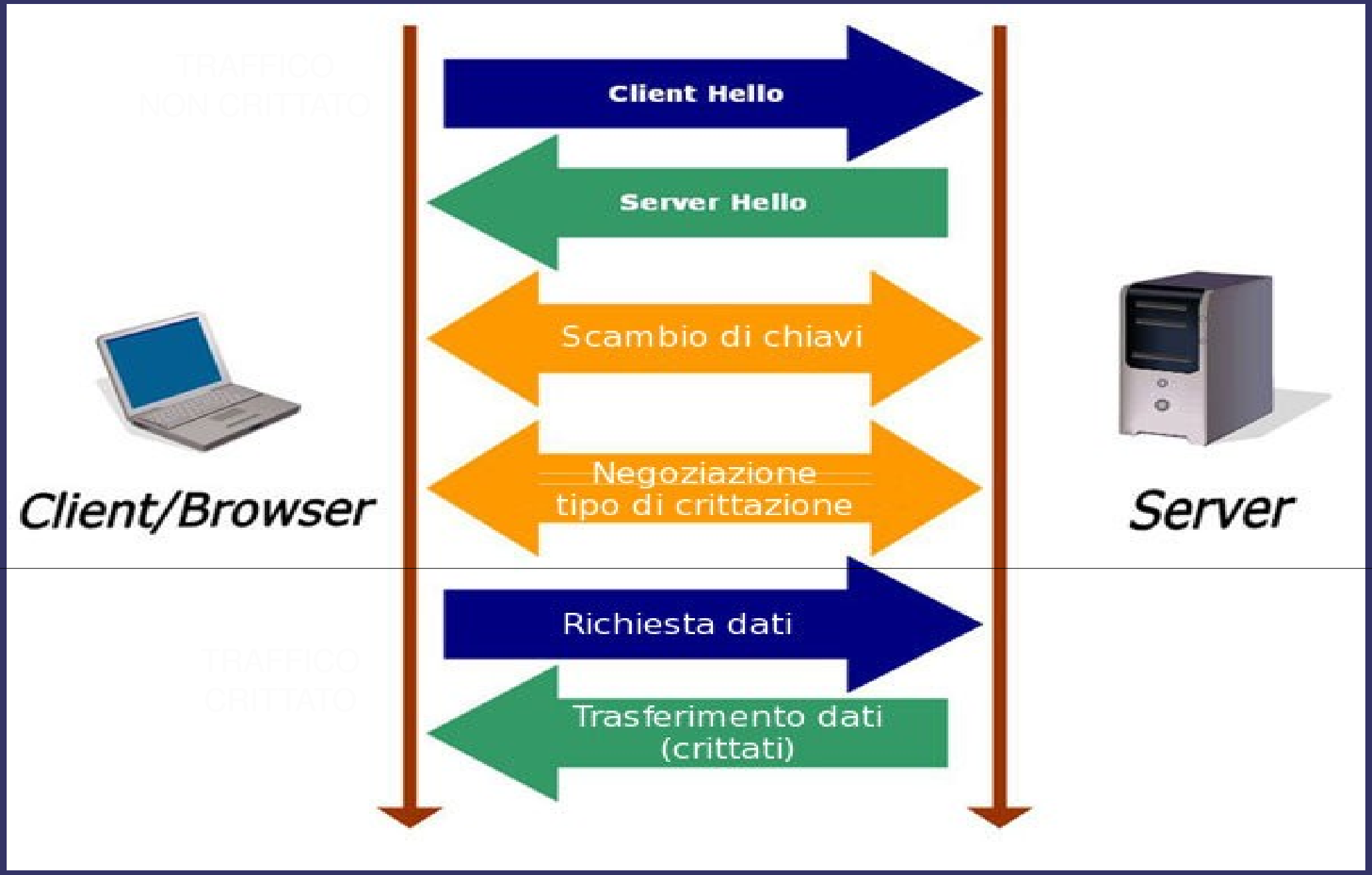
Thunderbird:
Modifica ->
Impostazioni Account ->
Server in uscita



Firefox: accertarsi che l'indirizzo inizi per https (s=SSL)



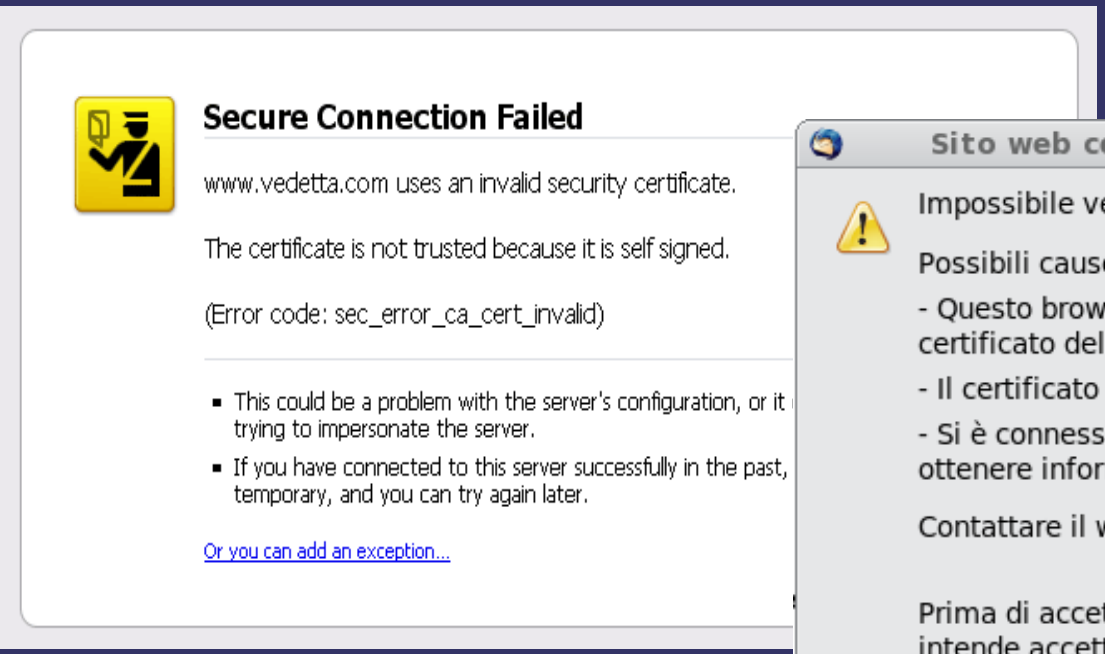
Funzionamento SSL (in parole povere)



Certificati “autoprodotti” o prodotti/verificati/certificati da qualche autorità!

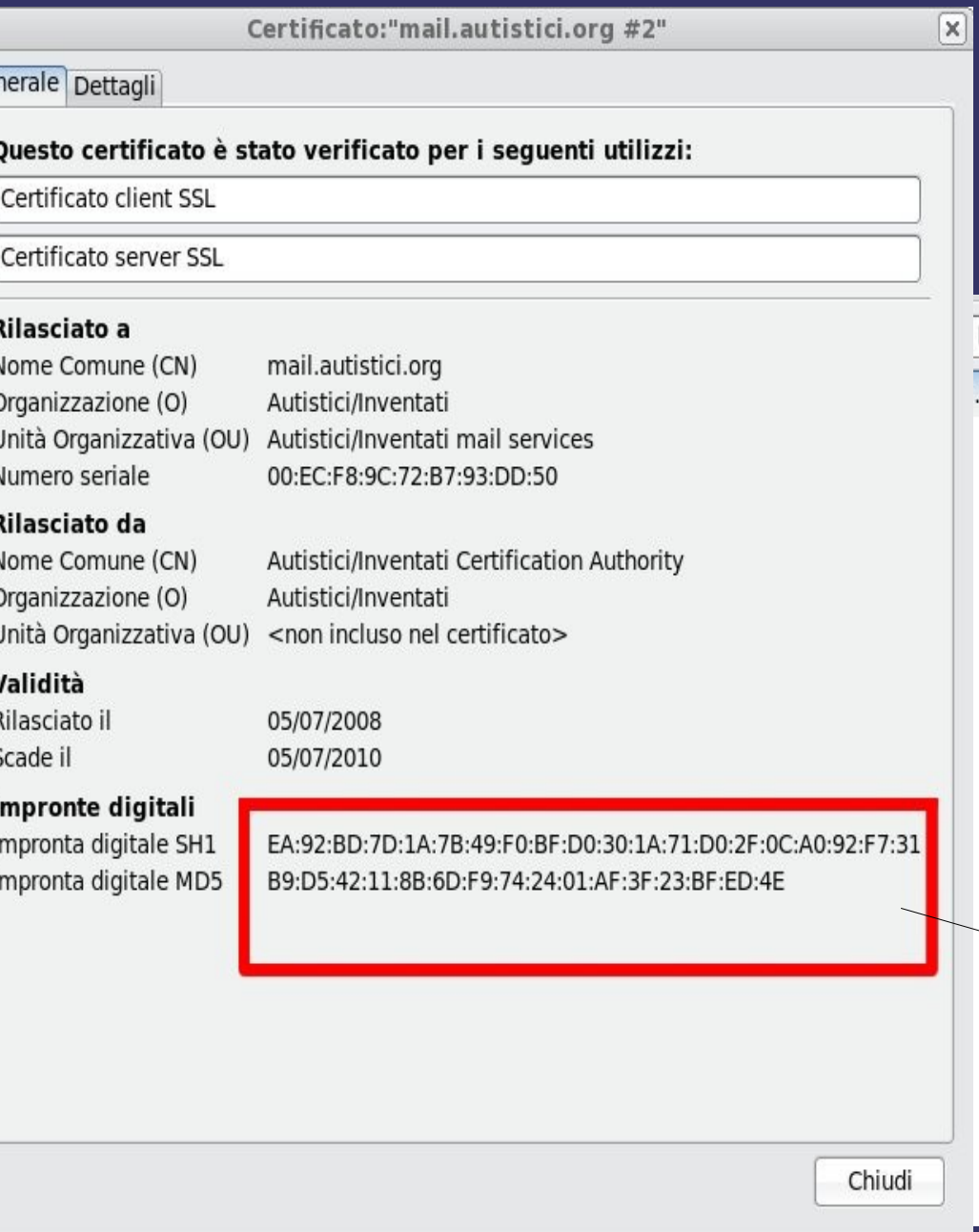
La CA è un ente di terza parte (trusted third party), pubblico o privato, abilitato a rilasciare un certificato digitale tramite procedura di certificazione che segue standard internazionali e conforme alla normativa europea e nazionale in materia.

Alcune CA: VerySign, RSA Inc, etc.
Esempi di certificato autoprodotto

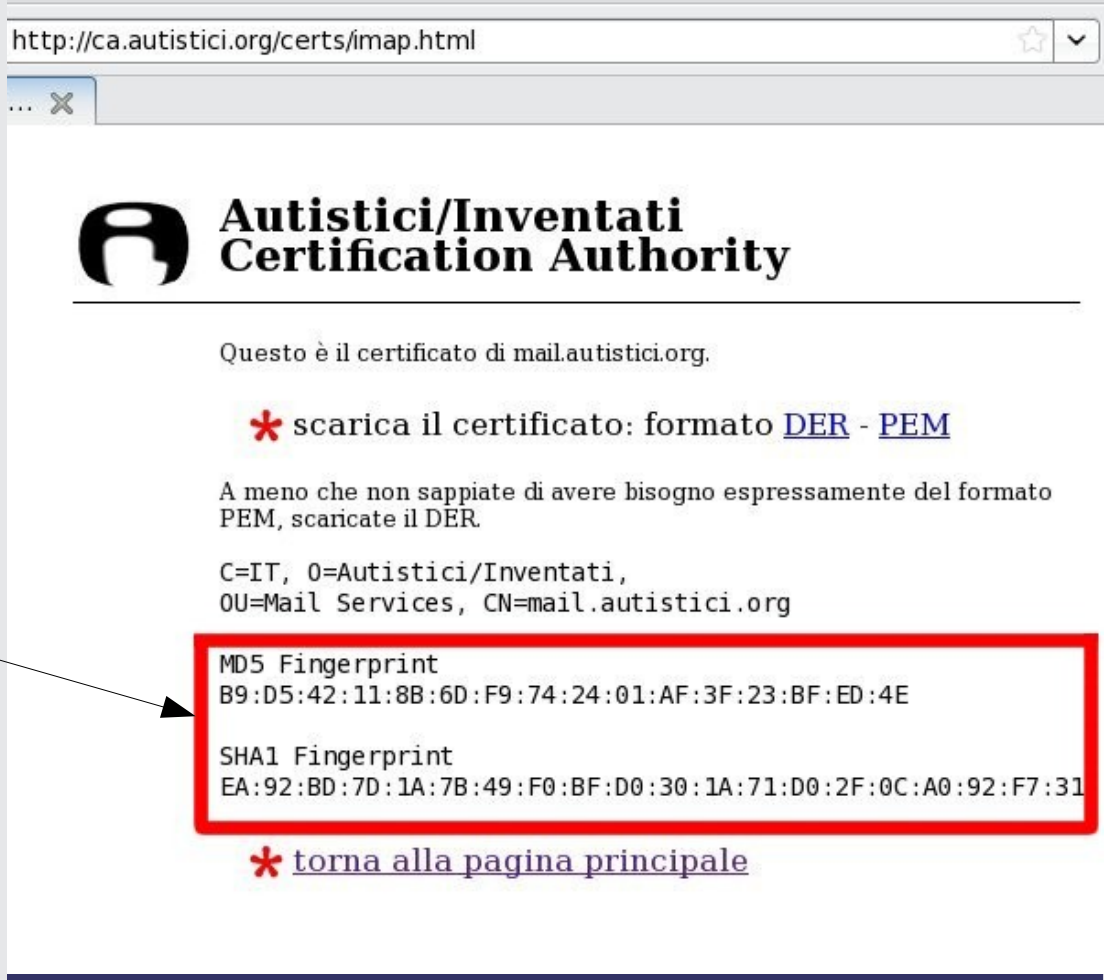


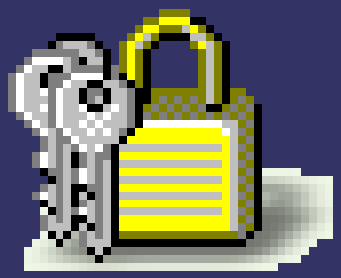
Controllare la bontà del certificato di autistici

Thunderbird: Modifica -> Preferenze -> Avanzate -> Certificati -> Mostra certificati

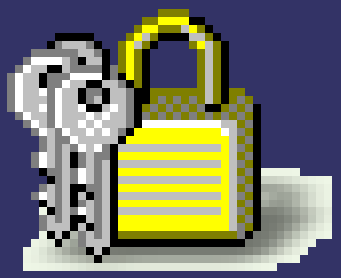


http://ca.autistici.org





Conclusioni SSL

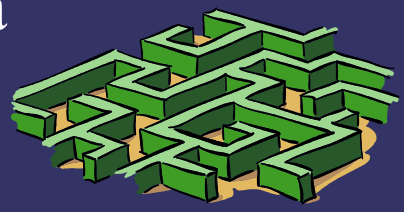


- Sarebbe meglio NON usare i protocolli con chiavi troppo corte! (disabilitarli nel proprio programma di posta/navigazione)

- Non effettuare connessioni con sistemi anonimi perché si rischia che la propria password venga estorta !!! (anonimo = senza certificato, senza nessuna autorità che garantisca,senza un controllo dell'md5 / sha1 del certificato)

- Controllare per la propria privacy i certificati che non sono rilasciati dalle CA!

- Controllare ogni volta che si inseriscono dati “sensibili” (user/pass/carta di credito etc) che la comunicazione avvenga in SSL.

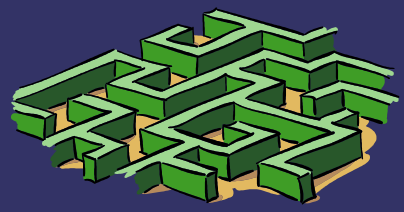


Formulazione di una cattiva Password:

- Pochi caratteri, con dati facili da reperire/capire

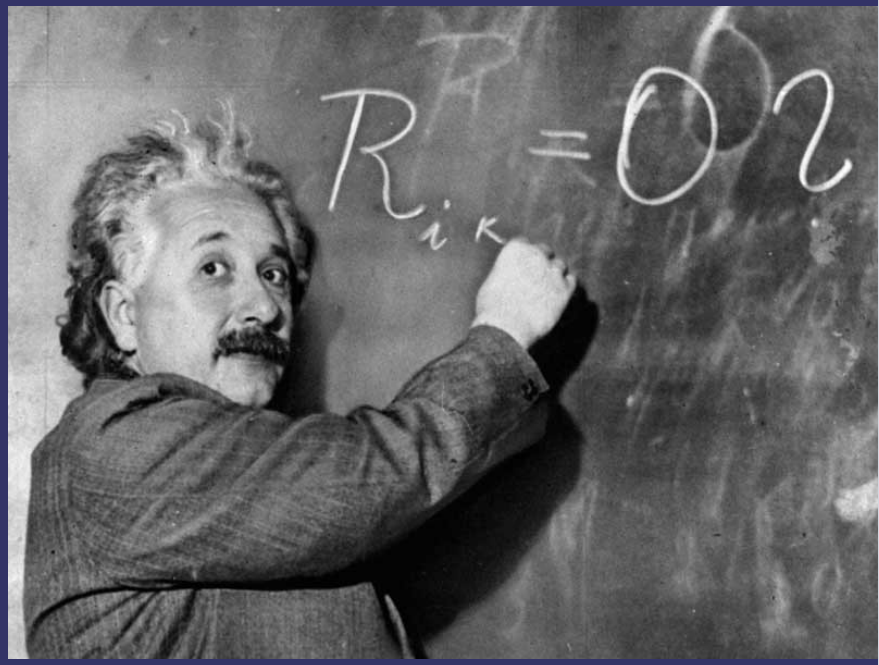
Es: data di nascita,nome/ cognome, il tuo cane

- parole associabili a te: crash, intifada77 etc...

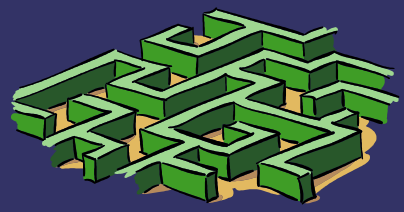


Formulazione di una buona Password:

- Più di 8 caratteri alfabetici/ numerici/simboli (Es: #@!|$ %&1aEfOiU - sono tutti USA-BILI)
- sfruttare i caratteri maiuscoli/ minuscoli (Es: r1v0luZ10n3... ma non basta!)

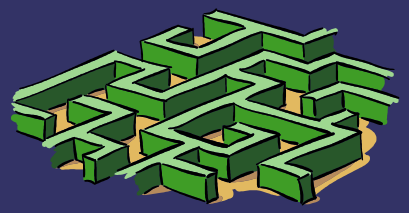


- Non impostare come password una parola che si possa trovare in dizionario (o un nome proprio)!



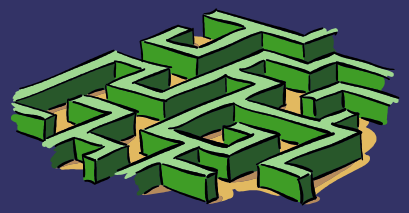
Gatto, sì o no?

- Se sì, non impostare una domanda la cui risposta possa essere intuita!
  Es. Qual'è il sistema operativo più soggetto a V.i-rus, I.ntrusioni, S.pyware, T.rojan, A.dware? = NO
- Se no, occorre ricordarsi la password a memoria

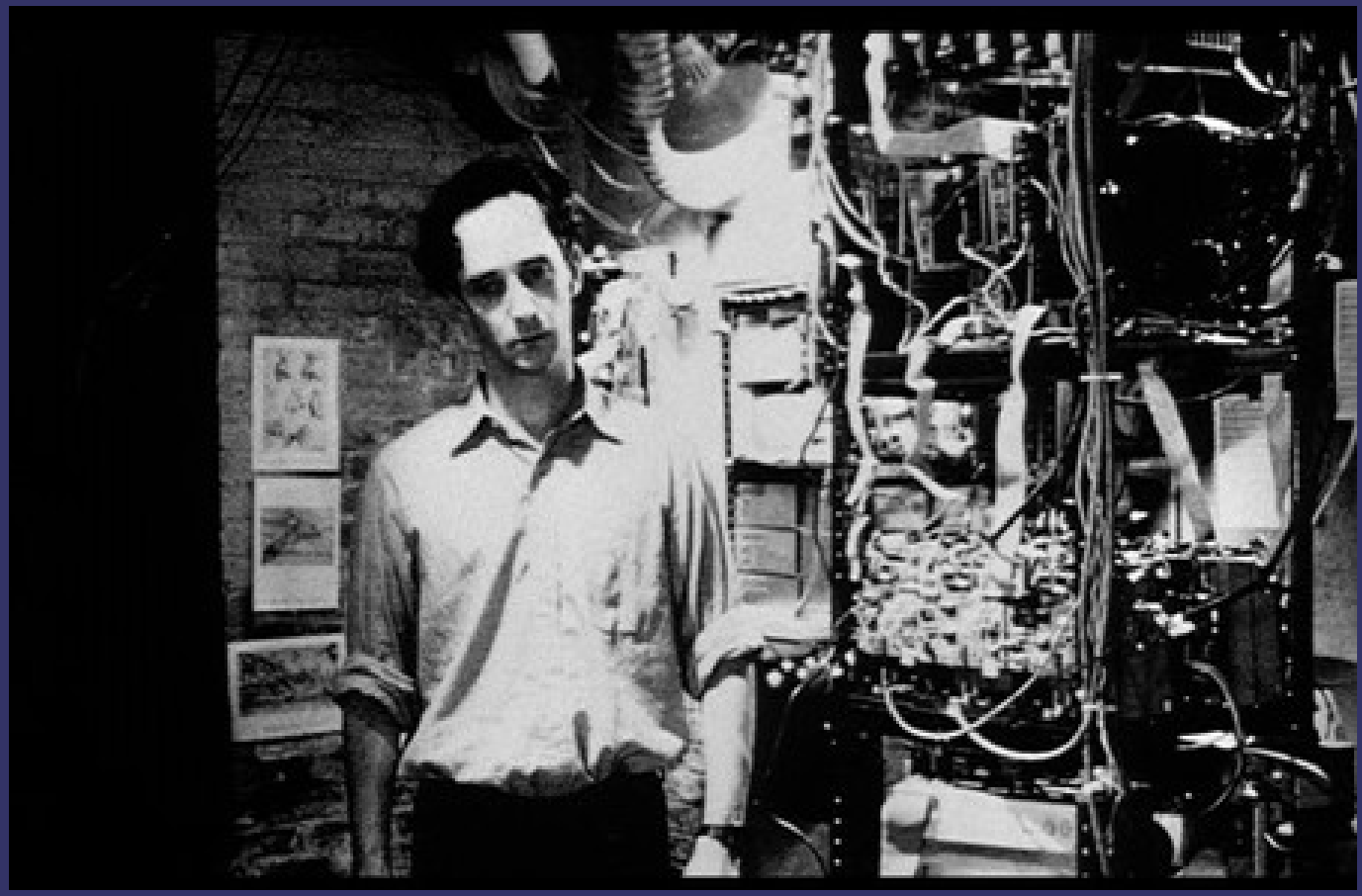


Portachiavi - Livello Persona Normale

Impostare la Master Password su Thunderbird
(Thunderbird →Modifica → Preferenze
→ Privacy → Usa una password
principale per cifrare le password
memorizzate)

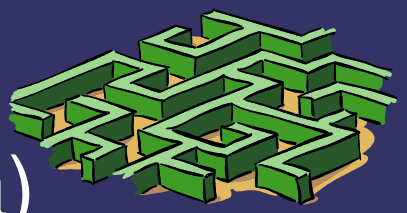


Portachiavi – Livello Malato/Paranoide



- ***Revelation*** (GNU/Linux)
- ***KeePassX*** (multipiattaforma)

L'utilizzo di questi programmi è intuitivo
(seguire i consigli per le password qui sopra)

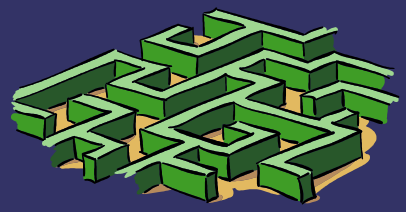


Finora abbiamo visto:

- ***SSL*** per il trasporto dei messaggi (ovvero come creare un tunnel cifrato e sicuro in cui far transitare le nostre informazioni in rete).

Ora vedremo:

- ***GPG*** (***GNU Privacy Guard*** - Algoritmo per la cifratura con chiave pubblica dei dati, open source) per cifrare il contenuto stesso dei messaggi. Perché Open Source? Se non posso leggere il codice sorgente, non so cosa possa fare il programma



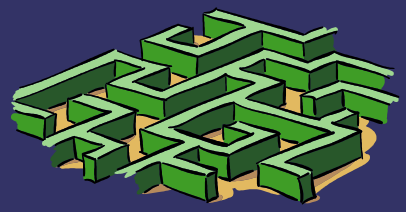
NOTA BENE:

Crittografia: Nasconde il testo di un messaggio

Crittanalisi: Cerca di risalire al testo di un messaggio crittografato individuandone la chiave

Anonimato: Oscura il mittente del messaggio

Steganografia: Cela un messaggio dentro ad un altro di tipo diverso (solo il destinatario sa che c'è un messaggio e che è stato inviato)



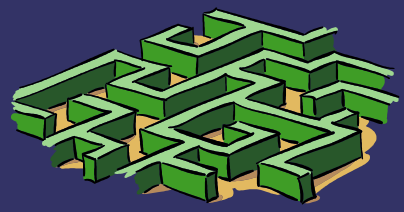
TESTO E CIFRATURA

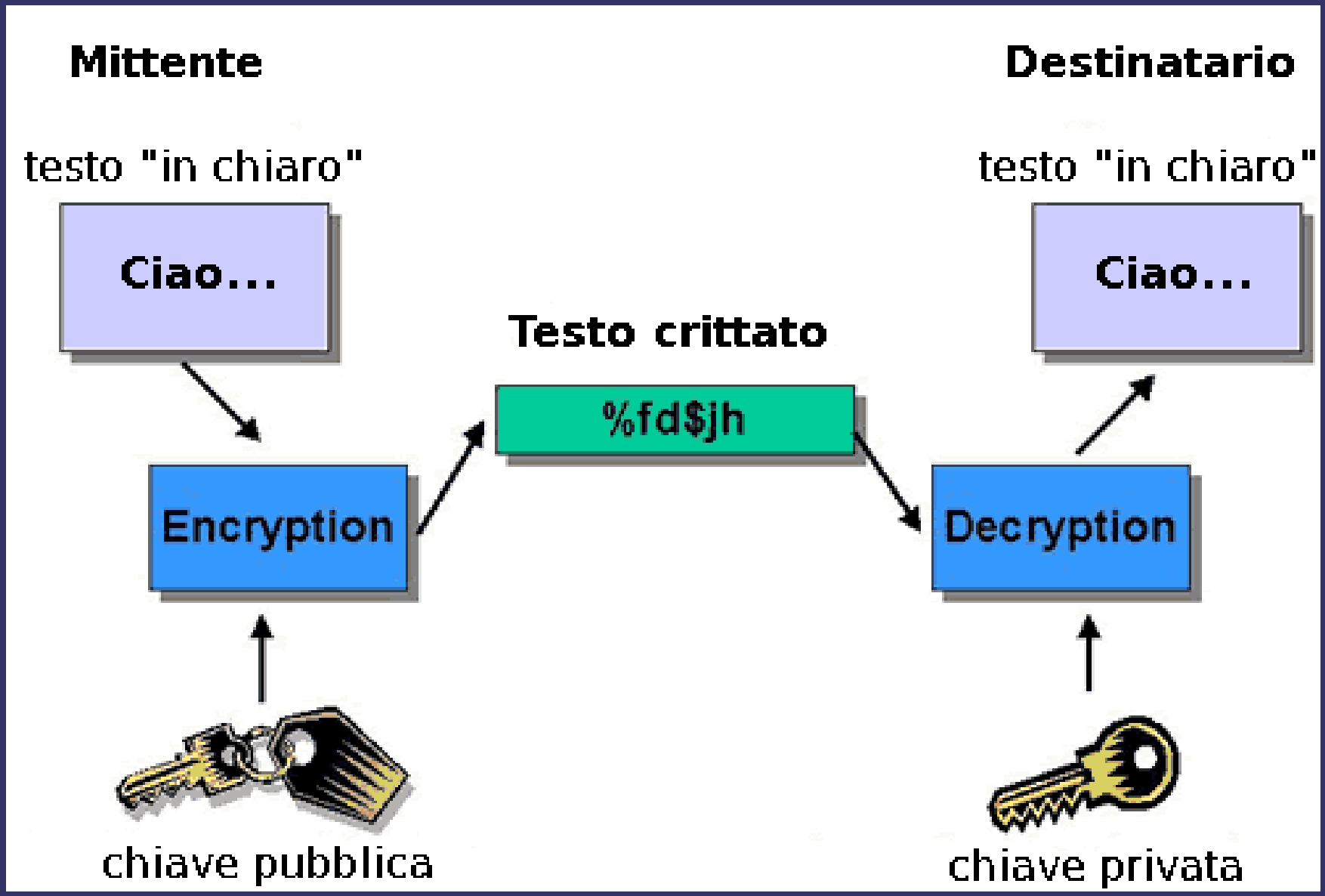
Testo in chiaro (cleartext) :
un dato che possiamo leggere e capire senza l'ausilio di nessun mezzo particolarmente speciale

Cifratura (encryption) :
un qualsiasi metodo che ci permette di nascondere un testo in chiaro modificandone la sostanza.

Testo cifrato (cypertext):
il naturale risultato, illeggibile, di una cifratura.

Decifratura (decryption) :
un qualsiasi metodo che ci permette di riottenere il testo in chiaro da un testo cifrato

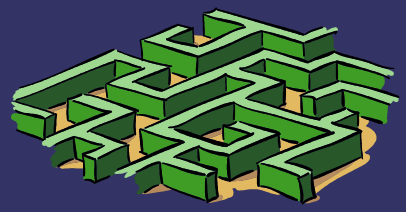



Mittente
Destinatario
testo "in chiaro"
testo "in chiaro"
Ciao...
Ciao...
Testo crittato
%fd$jh
Encryption
Decryption
chiave pubblica
chiave privata

Due passaggi nella crittografia:

- cifrare il contenuto della mail

- firmare la mail con chiave digitale per accertare l'identità del mittente



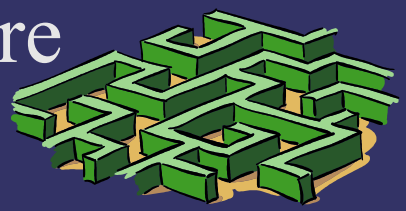
Crittografia Simmetrica

<u>Il Cifrario di Cesare:</u>

Indietro non si torna
Joejfusp opo tj upsob

Chiave = Ogni lettera del messaggio in chiaro viene sostituta nel messaggio cifrato con quella che la segue nell'alfabeto

- E' un sistema debole: il mittente ed il destinatario devono mettersi d'accordo su una chiave da usare
- Chiunque intercetti questa chiave potrà decrittare tutti i messaggi
- Deve esserci un canale di trasmissione sicuro



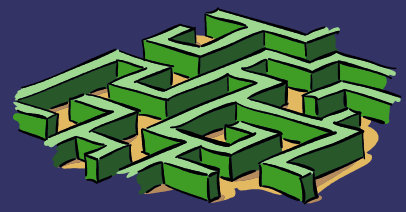
Scalzone & Piperno (Crittografia a Chiave Pubblica)

- Scalzone e Piperno vanno in fonderia e creano due lucchetti con le rispettive chiavi

- Scalzone invia per posta il proprio lucchetto a Piperno

- Piperno scrive il messaggio e lo mette in una scatola che chiude con il lucchetto di Scalzone, ed invia la scatola a Scalzone

- Il postino non può aprire la scatola, la porta a Scalzone che ha la chiave del lucchetto, apre il pacco e legge il messaggio



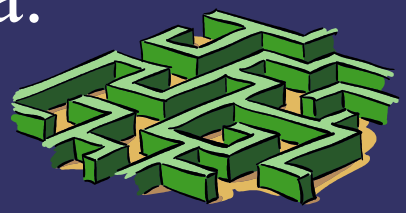
GENERIAMO UNA COPPIA DI CHIAVI (va fatto solo una volta):

Thunderbird → OpenPGP → Gestione delle Chiavi → Genera

- ***Privata:*** personale, da tenere nascosta (su partizione criptata o chiave USB per i paranoici) e protetta da una password; serve per decrittare i messaggi e per firmarli.

- ***Pubblica:*** può essere distribuita liberamente, serve per criptare i messaggi e per verificare la firma elettronica.

Che caratteristiche hanno?



Caratteristiche della Chiave

Indirizzo utente — Indirizzo di posta elettronica con il quale verrà usato il paio di chiavi

Passphrase — Permette lo sblocco e perciò l'uso della chiave privata (decifrare e firmare)

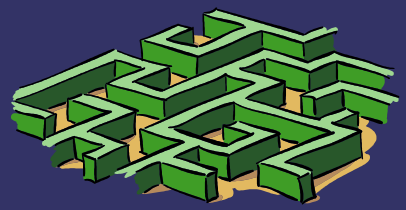
Scadenza della chiave — Numero di giorni oltre il quale la chiave diventerà inutilizzabile

Avanzate - Dimensione della chiave — Impostare a seconda della paranoia personale

Avanzate - Tipo di algoritmo — Va bene il default (DSA and Elgamal)

Fingerprint — Hash della chiave pubblica Identificativo

→ Selezionare “Genera chiave”

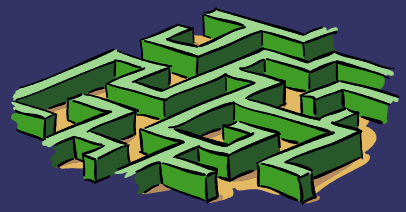


Passphrase

- Ulteriore livello di protezione della posta elettronica: è una parola d'ordine che permette di utilizzare la chiave privata.

- In mancanza di essa, se anche un intruso riuscisse ad impossessarsi della nostra chiave privata, la troverebbe inutilizzabile.

- Valgono sempre i consigli di formulazione delle password illustrati prima.

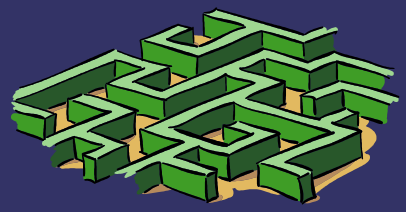


Fingerprint

E' una breve sequenza di byte utilizzata per identificare in maniera univoca una chiave pubblica, allo stesso modo in cui un'impronta digitale caratterizza una persona ben precisa.

Esempio di Fingerprint:

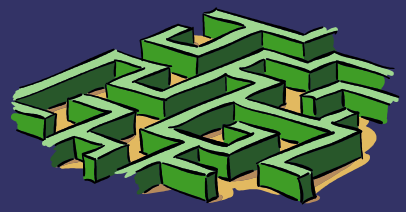
43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8



Inviare una mail firmata e crittata

- Thunderbird → Scrivi → OpenPGP → Spuntare “Firma il messaggio” e “Cifra il messaggio”

- Inserire la password della propria chiave privata e quella del proprio account di posta



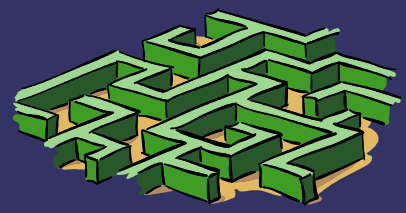
Ulteriori dettagli su queste due chiavi

Man In the Middle e Rete della Fiducia

Tramite tecniche apposite, esiste la possibilità che qualcuno possa contraffare od intercettare la chiave pubblica di una data persona.

Per assicurarsi che la chiave pubblica di una persona con cui voglio comunicare tramite mail criptata sia effettivamente la sua:

- Ci incontriamo di persona e ce la scambiamo (PGP Party)
- Gli telefono e gli chiedo il fingerprint della chiave pubblica
- Mi fido delle firme associate alla sua chiave pubblica: se Scalzone non conosce Negri, ma conosce Piperno che ne ha firmato la chiave pubblica, allora è molto probabile che la chiave appartenga a Negri.



Dove trovare le Chiavi Pubbliche?

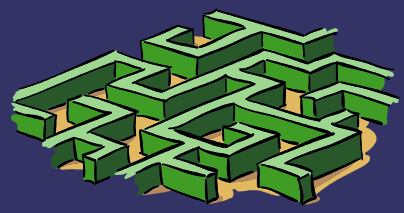
E' possibile caricare e scaricare le proprie chiavi pubbliche e quelle altrui dai ***keyserver***, servizi che offrono anche un motore di ricerca interno.

Per inviare la propria chiave pubblica ad un keyserver:

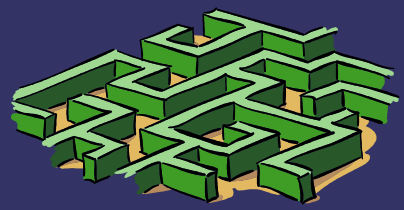
Thunderbird → OpenPGP → Gestione delle Chiavi → [Tasto Destro Mouse sulla chiave da inviare] → Invia chiavi pubbliche al keyserver

Per cercare una chiave pubblica su di un keyserver:

Thunderbird → OpenPGP → Gestione delle Chiavi →Keyserver → Ricerca Chiave



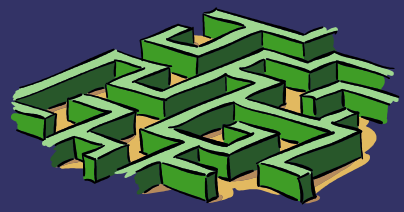
Tre passi da effettuare per avere sempre con sé le proprie mail ed il proprio client di posta elettronica



1) Configurare Thunderbird per scaricare i messaggi di posta sul proprio computer

http://www.autistici.org/it/stuff/user_howto/man_mail/ clients/posta_thunderbird_win_howto.html

E' bene, anche se le caselle di posta di Autistici/Inventati possono offrire spazio teoricamente illimitato, scaricarsi la posta sul proprio computer: ciò libera preziose risorse di spazio dai loro server autogestiti. Inoltre, la posta sul computer può essere protetta da ulteriori strumenti di privacy, come le partizioni criptate.



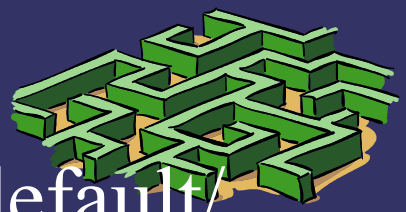
2) Effettuare un backup delle proprie mail, anche per trasferirle su altri supporti (Chiavette USB, hard disk, altri computer)

Operando manualmente, occorre individuare la cartella associata al profilo dell'utente.

Su GNU/Linux:
/[home/].mozilla-thunderbird/xxxxxxxx.default/

Su Windoom:
C:\WINDOWS\Application Data\Mozilla\Thunderbird\Profiles\xxxxxxxx.default\

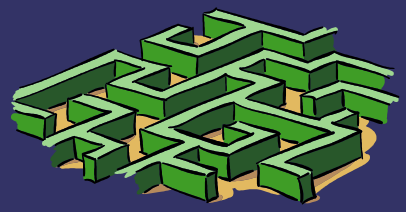
Su MACosX:
/Library/Thunderbird/Profiles/xxxxxxxx.default/



3) Utilizzare applicazioni da chiavetta:

http://portableapps.com/apps/internet/thunderbird_portable

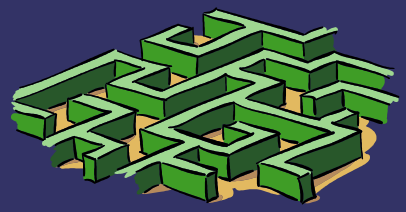
In questo modo vi è la possibilità di portare sempre con sé il proprio client e la propria posta, e di utilizzarli senza problemi anche offline.



Un'ultima raccomandazione...

Limitarsi ad utilizzare GPG per le sole mail “scottanti” richiama l'attenzione e gli sforzi dei crittanalisti su di esse...

...ecco perché un'ulteriore buona abitudine per proteggere la propria privacy è quella di scambiarsi mail cifrate ogniqualvolta ve ne sia la possibilità.

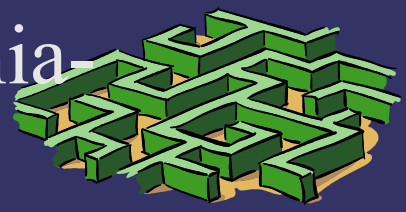


Antispam

- Su Thunderbird è possibile impostare un sistema di filtri per disfarsi delle mail spazzatura:

Thunderbird → Strumenti → Filtri → Nuovo

rendendo facile e veloce cestinare automaticamente mail sgradite in base a mittente, data, parole-chiave, ecc. o più di questi parametri alla volta.

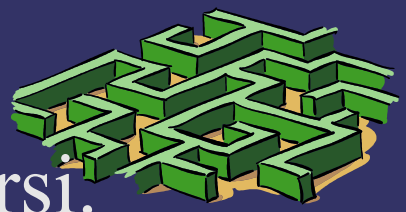


Caselle di Posta Elettronica Temporanee

Gran parte dello spam e della posta indesiderata arrivano alla nostra casella mail a partire da quando ne divulghiamo l'indirizzo in rete, ad esempio richiedendo l'iscrizione a servizi e forum non adeguatamente protetti.
E' possibile effettuare queste operazioni servendosi di una casella di posta temporanea:

http://10minutemail.com/

che rimarrà attiva per 10 minuti,
senza tenere log, per poi autodistruggersi.



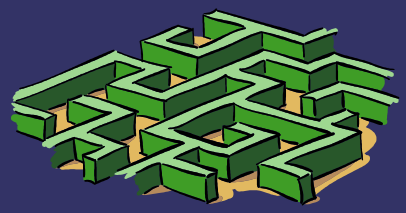
Un piccolo trucchetto finale

Come fare per non far visualizzare le mail
ricevute all'avvio di Thunderbird senza prima immettere la password?
Ecco la soluzione in due passaggi:

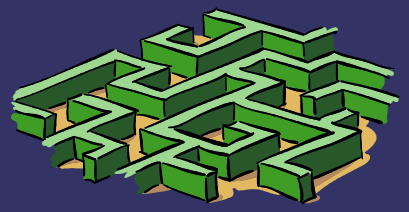
1) Selezionare **Modifica** -> **Preferenze** -> **Avanzate** -> **Editor di configurazione** ->

2) cliccare due volte su
mail.password_protect_local_cache
per cambiare il valore in "**true**"

GAME OVER!!



DOMANDE?



Prossimo Appuntamento: Proteggere la Navigazione ed il P2P

Venerdì 7 Novembre Ore 20.30