

# Crittografia Digitale

Perche' chi vende la propria liberta' per briciole di momentanea sicurezza non merita ne l'una ne l'altra

allanon

Grayhats

30 Ottobre 2010 / Workshop Taormina

# Outline

- 1 **Introduzione**
  - Cosa e'?
  - Perche' usarlo?
- 2 **Panoramica sugli algoritmi di cifratura**
  - Algoritmi a chiave simmetrica
  - Algoritmi a chiave pubblica
- 3 **Esempi d'uso quotidiano**
  - GnuPG
  - Email
  - Messagistica istantanea
  - Storage dati

# Outline

## 1 Introduzione

- Cosa e'?
- Perche' usarlo?

## 2 Panoramica sugli algoritmi di cifratura

- Algoritmi a chiave simmetrica
- Algoritmi a chiave pubblica

## 3 Esempi d'uso quotidiano

- GnuPG
- Email
- Messagistica istantanea
- Storage dati

# Impariamo alcuni termini

## Crittografia

Deriva dall'unione di due parole che in greco antico significano **parole segrete**

## Crittoanalisi

lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che e' di solito richiesta per effettuare l'operazione

## Crittologia

Lo studio della crittografia e della crittanalisi si chiama comunemente crittologia.

# Outline

## 1 Introduzione

- Cosa e'?
- Perche' usarlo?

## 2 Panoramica sugli algoritmi di cifratura

- Algoritmi a chiave simmetrica
- Algoritmi a chiave pubblica

## 3 Esempi d'uso quotidiano

- GnuPG
- Email
- Messagistica istantanea
- Storage dati

# Internet e' un canale di trasmissione insicuro

## Ambito accademico

In origine le reti di computer venivano utilizzate da ricercatori universitari per inviare e ricevere email.

Non c'era una reale esigenza di comunicazione privata e protetta

## Oggi

Milioni di persone utilizzano la grande rete per comunicazioni private.

I protocolli alla base di Internet non sono cambiati, trasmettono in chiaro dati sensibili.

## Workaround

Se il mezzo di comunicazione e' insicuro, l'unica soluzione possibile e' rendere sicuro il messaggio da inviare

# Problem derivanti dall'uso di un canale insicuro

- segretezza
- integrità'
- autenticazione
- non-ripudio



# Non sono mica il presidente . . .

. . . che deve proteggere importanti informazioni di stato.

## Quelli che . . .

- . . . pensano che le loro conversazioni private non abbiano valore.
- . . . pensano che chi non ha nulla da nascondere non abbia bisogno di privacy.
- . . . pensano che se Qualcuno controllasse **l'informazione**, si vivrebbe in modo piu' sicuro.

# Non sarete il presidente ma vi intercettano lo stesso!

## Quelli che ...

- ... vivono di pubblicita', di marketing, e per farlo necessitano di informazioni sui target commerciali.
- ... vivono di attivita' ai margini della legge, e per farlo necessitano di informazioni sulle vittime.
- ... vivono vendendo le informazioni sui target commerciali piu' papabili.
- ... vivono fornendo soluzioni per la raccolta di tali informazioni.

# Ok, non siete il Presidente, ma...

vi intercettano lo stesso! Cosa fa lo stato Italiano per difendere i propri cittadini?

un po' di hijacking qua e la' non ha mai ucciso nessuno

Il governo Italiano, e' il piu grande hijacker d'Europa. Chiaramente e' un reato, a livello europeo, e l'Italia paga ogni anno una multa. Ma se ne infischia e continua a pagare.

## Definizione - hijacking

tecnica che consiste nel modificare opportunamente dei pacchetti dei protocolli TCP/IP al fine di dirottare i collegamenti ai propri siti e prenderne il controllo.

## Chiaramente ... per il vostro bene!

Lo Stato Italiano non e' il Male, e non lo fa per Cattiveria. Lo fa per Interesse, cioe' per garantire un discreto giro d'affari ai siti italiani per le scommesse.

# Tutti intercettati, a prescindere

## Data Retention

I ministri europei della Giustizia e la Commissione Europea vogliono conservare tutti i dati relativi al traffico telefonico e di Internet di tutti i 450 milioni di cittadini europei.

Lo Stato Italiano fu tra i primi artefici della manovra, che è tutt'ora in vigore, in Italia, dopo mille proroghe. Il famoso decreto milleproroghe di ogni anno . . .

eppure. . .

neanche, e soprattutto, la classe politica, vuole essere intercettata. . .  
Perché dovremmo essere intercettati noi?

# Libertà o sicurezza?

## Benjamin Franklin

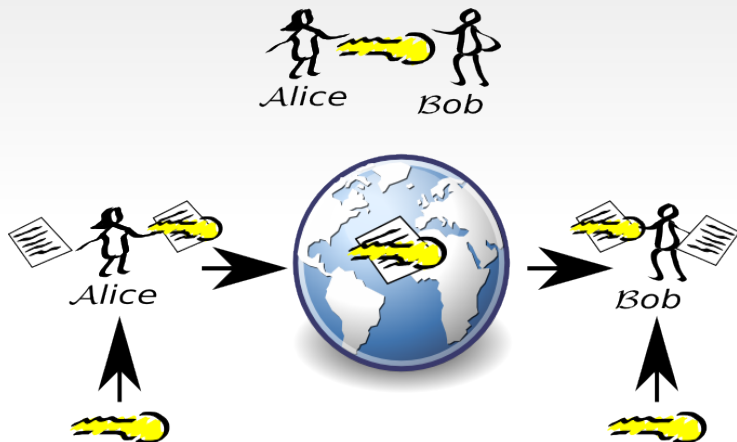
Chi è pronto a dar via le proprie libertà fondamentali per comprarsi briciole di temporanea sicurezza non merita né la libertà né la sicurezza.

# Outline

- 1 **Introduzione**
  - Cosa e'?
  - Perche' usarlo?
- 2 **Panoramica sugli algoritmi di cifratura**
  - **Algoritmi a chiave simmetrica**
  - Algoritmi a chiave pubblica
- 3 **Esempi d'uso quotidiano**
  - GnuPG
  - Email
  - Messagistica istantanea
  - Storage dati

# Algoritmi a chiave simmetrica

- Unica chiave, utilizzata sia per cifrare che per decifrare
- la distribuzione delle chiavi e' il punto debole di tale algoritmo



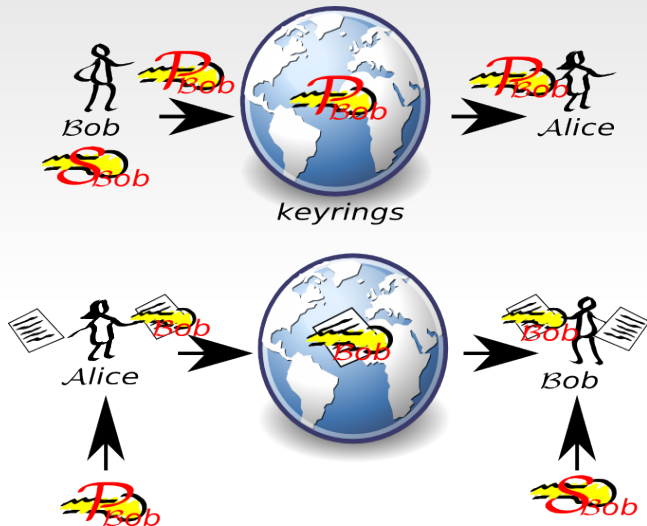
# Outline

- 1 **Introduzione**
  - Cosa e'?
  - Perche' usarlo?
- 2 **Panoramica sugli algoritmi di cifratura**
  - Algoritmi a chiave simmetrica
  - **Algoritmi a chiave pubblica**
- 3 **Esempi d'uso quotidiano**
  - GnuPG
  - Email
  - Messagistica istantanea
  - Storage dati

# Algoritmi a chiave pubblica

- Due chiavi, una per cifrare messaggi diretti solo a voi, e una per decifrare i messaggi cifrati per voi.
- La chiave per cifrare puo' essere pubblica, anzi e' consigliabile pubblicarla online negli appositi keyrings.  
Perche' chiunque deve poter scrivere un messaggio confidenziale diretto a voi.
- La chiave per decifrare deve essere conservata in modo accurato, affinche' solo voi possiate decifrare un messaggio scritto con la vostra chiave pubblica.

# Schema riassuntivo - caso ideale

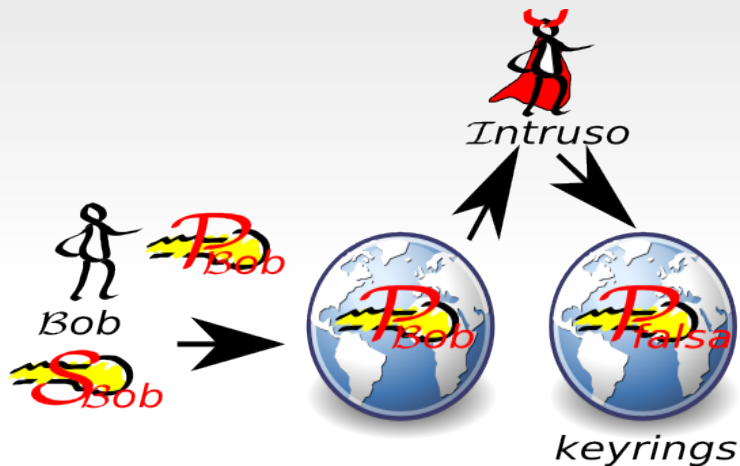


# Problema!

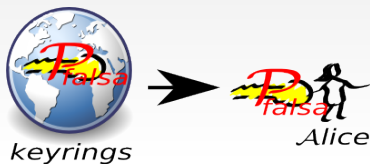
## Problema di identità

Come fa Alice a sapere che quella è davvero la Chiave Pubblica di Bob??

# L'intruso intercetta e si sostituisce a Bob



# Alice viene ingannata



# Comunicazione compromessa



# Verifica della chiave pubblica

## Fingerprint

E' **l'impronta digitale** associata alla chiave.

Consiste in una sequenza di lettere che puo' essere dettata anche dettata a voce, per telefono.

- Dopo aver verificato che il fingerprint corrisponda, Alice puo' **firmare** come affidabile la chiave pubblica di Blob e ripubblicarla nei keyrings.
- Tutti i keyrings sapranno che Alice ha verificato la chiave pubblica di Bob, come appartenente a Bob.

# Ring of Trust

- Reiterando il processo di verifica e firma delle chiavi verificate si crea il **Ring of Trust**.
- La bontà dell'anello della fiducia dipende dall'affidabilità delle persone. Chi firma a caso verrà tacciato come inaffidabile e le sue firme non avranno valore.
- Quando una chiave pubblica colleziona un buon numero di firme affidabili, essa è ragionevolmente una chiave pubblica affidabile.

# Esempio

- un gruppo di amici decide di utilizzare la crittografia per le loro conversazioni.
- Ognuno di loro genera la coppia di chiavi.
- Verificano e firmano reciprocamente le chiavi pubbliche.
- Tali chiavi pubbliche possono quindi essere, ragionevolmente, accettate da qualunque nuovo amico che decida di aggiungersi in seguito.

# Avviso!

- Accettare una chiave, sebbene in modo ragionevole, non vuol dire firmarla
- la firma di una chiave dovrebbe avvenire solo dopo l'avvenuta verifica.
- Pena l'essere classificato come inaffidabile.

# Outline

- 1 **Introduzione**
  - Cosa e'?
  - Perche' usarlo?
- 2 **Panoramica sugli algoritmi di cifratura**
  - Algoritmi a chiave simmetrica
  - Algoritmi a chiave pubblica
- 3 **Esempi d'uso quotidiano**
  - **GnuPG**
  - Email
  - Messagistica istantanea
  - Storage dati

# GnuPG

- GnuPG è una libera e completa implementazione dello standard OpenPGP definito dal documento RFC4880.
- Se' un programma multiplatforma.
- E' installato di default sulle maggiori distribuzioni GNU/Linux.
- Permette le operazioni di cifratura/decifratura/firma sul file.
- Un sistema di gestione delle chiavi molto versatile e integrato nei keyrings.
- Programma a linea di comando che si integra molto bene in vari ambienti di lavoro e interfacce grafiche



# Outline

- 1 **Introduzione**
  - Cosa e'?
  - Perche' usarlo?
- 2 **Panoramica sugli algoritmi di cifratura**
  - Algoritmi a chiave simmetrica
  - Algoritmi a chiave pubblica
- 3 **Esempi d'uso quotidiano**
  - GnuPG
  - **Email**
  - Messagistica istantanea
  - Storage dati

# Inviemo email cifrate

- Visto che già esiste GnuPG, e che funziona bene, non c'è bisogno di reinventare l'acqua calda.
- Si tratta di utilizzare GnuPG, e quindi tutto il ring of trust costruito attorno ad esso, nei più diffusi programmi per invio/ricezione delle email.
- Molti programmi includono già una interfaccia per GnuPG, in molti altri è possibile installare un plugin.

# Firefox e FireGPG

- FireGPG e' una interfaccia per GnuPG.
- E' un plugin per Firefox.
- Permette l'uso di GnuPG su browser
- gmail, yahoo, etc etc ...

# Firefox e FireGPG

The screenshot shows a Firefox browser window with the address bar displaying "Posta Alaimo.org - Scrivi messaggio - allanon@alaimo.org - Iceweasel". The browser's menu bar includes "File", "Modifica", "Visualizza", "Cronologia", "Segnalibri", "Strumenti", and "Aiuto". The "Strumenti" menu is open, showing various utility options. The "FireGPG" option is highlighted, and its sub-menu is displayed, containing the following items:

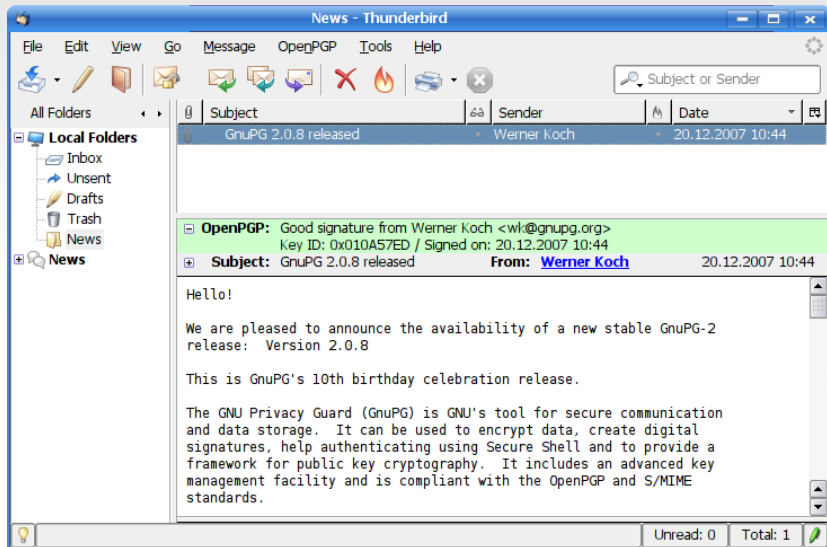
- Firma (Clearsign)
- Firma (a capo automatico)
- Firma
- Controlla Firma
- Cripta
- Criptazione simmetrica
- Firma e Cripta
- Decripta
- Importa
- Esporta

The background interface shows an email composition screen with fields for "A:", "Oggetto:", and "Allega un file". The "Oggetto:" field contains the text "Inserisci: invito". The "Allega un file" button is visible, and the "Invia" button is highlighted. The left sidebar shows navigation links like "Posta in arrivo", "Speciali", "Posta inviata", and "Bozze".

# Thunderbird e Enigmail

- Enigmail e' una interfaccia per GnuPG.
- E' un plugin per Thunderbird che e' un diffuso client per la posta elettronica
- Permette l'uso di GnuPG su client locale.

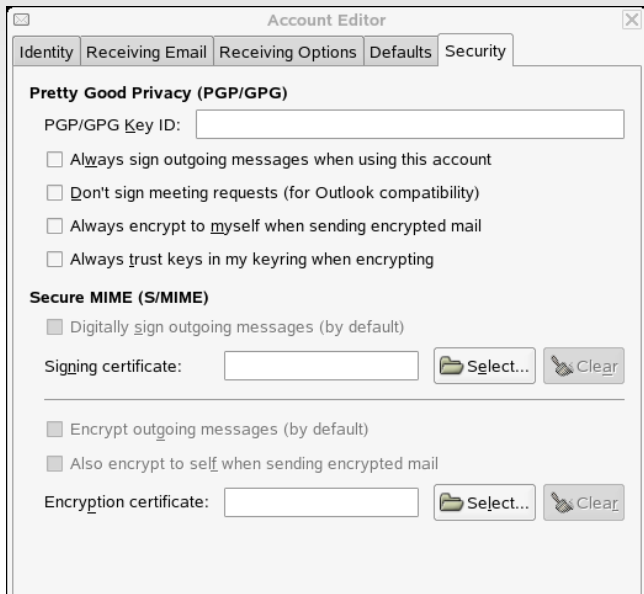
# Thunderbird e Enigmail



# Evolution

- Evolution e' un diffuso client per la posta elettronica
- Gia' incluso e integrato nell'ambiente GNOME
- Supporta nativamente l'uso di GnuPG per la posta elettronica

# Evolution



# Outline

- 1 **Introduzione**
  - Cosa e'?
  - Perche' usarlo?
- 2 **Panoramica sugli algoritmi di cifratura**
  - Algoritmi a chiave simmetrica
  - Algoritmi a chiave pubblica
- 3 **Esempi d'uso quotidiano**
  - GnuPG
  - Email
  - **Messagistica istantanea**
  - Storage dati

# OTR plugin

- Pidgin e' un programma di messagistica istantanea multiplatforma e multiprotocollo
- OTR (Off the Records) e' un plugin che permette l'autenticazione e cifratura dei messaggi.

# OTR plugin

The image shows two overlapping windows from a messaging application. The left window, titled "Plugin", lists several installed plugins. The "Off-the-Record Messagin..." plugin is selected and highlighted. Below the list, there are buttons for "Configura il plugin" and "Chiudi". A file size of "30,5 kB" is visible at the bottom of this window. The right window, titled "Off-the-Record Messaging", is the configuration dialog for the selected plugin. It has tabs for "Config" and "Known fingerprints". The "Config" tab is active, showing sections for "My private keys", "Default OTR Settings", and "OTR UI Options".

**Plugin**

Abilitato Nome

- Mystatusbox (Show Statu...**  
Hide/Show the per-account st...
- Notifica messaggi 2.7.3**  
Fornisce diversi modi per noti...
- Notifiche di libnotify 0.14**  
Visualizza le notifiche median...
- Off-the-Record Messagin...**  
Provides private and secure c...
- Schedule 2.6.3**  
Schedule reminders at speci...
- Scoperta servizi XMPP 2....**  
Permette di sfogliare e regist...

▶ **Dettagli sul plugin**

Configura il plugin Chiudi

30,5 kB

**Off-the-Record Messaging**

Config Known fingerprints

My private keys

Key for account:

Fingerprint: 542F637E 38E45049 8AA4DC0B 76A9BBB8 661D8158

Generate

Default OTR Settings

- Enable private messaging
- Automatically initiate private messaging
- Require private messaging
- Don't log OTR conversations

OTR UI Options

- Show OTR button in toolbar

Chiudi

# Outline

- 1 Introduzione
  - Cosa e'?
  - Perche' usarlo?
- 2 Panoramica sugli algoritmi di cifratura
  - Algoritmi a chiave simmetrica
  - Algoritmi a chiave pubblica
- 3 Esempi d'uso quotidiano
  - GnuPG
  - Email
  - Messagistica istantanea
  - **Storage dati**

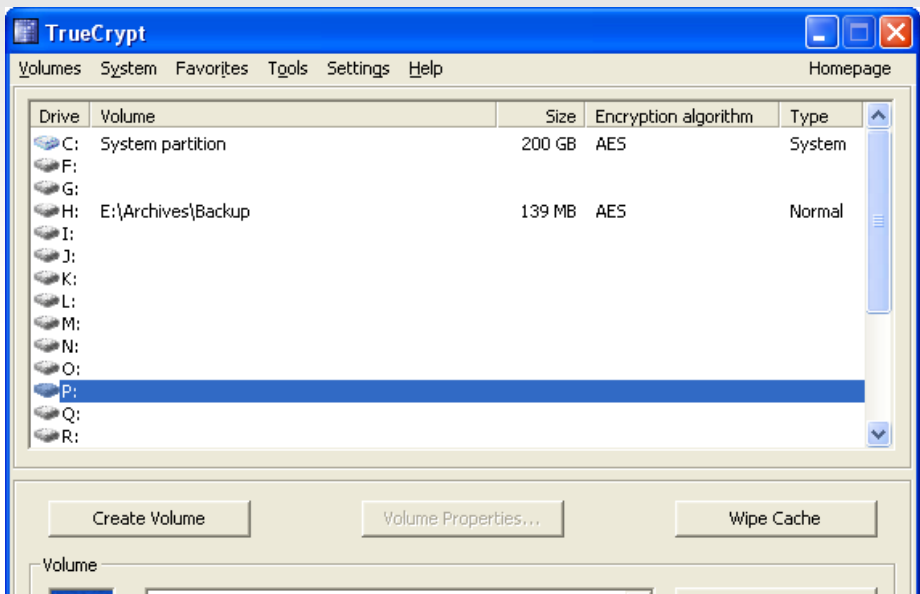
# Ora tocca ai nostri file in locale

- Oggi l'accesso al mondo digitale e' diventato flessibile (notebook netbook, dischi esterni . . . )
- Nel caso di utilizzo di tali dispositivi in ambito professionale e' d'obbligo cifrare interi dischi o partizioni . . .
- . . . ma, essendo la crittografia molto a buon mercato, possiamo usarla anche per contesti molto piu' rilassanti.

# Truecrypt

- Multiplatforma
- Cifrare una intera partizione o disco.
- Ovviamente anche le penne usb e i dischi esterni!
- Include anche un sistema per nascondere partizioni cifrate (Steganografia)
- Molto oneroso il backup, in quando bisogna copiare l'intero blocco cifrato della partizione, o del disco
- Impossibile il backup incrementale

# Truecrypt



The screenshot shows the TrueCrypt application window. The title bar reads "TrueCrypt" and includes standard window controls. The menu bar contains "Volumes", "System", "Favorites", "Tools", "Settings", "Help", and "Homepage". The main area displays a table of encrypted volumes:

Drive	Volume	Size	Encryption algorithm	Type
C:	System partition	200 GB	AES	System
F:				
G:				
H:	E:\Archives\Backup	139 MB	AES	Normal
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				
Q:				
R:				

Below the table, there are three buttons: "Create Volume", "Volume Properties...", and "Wipe Cache". At the bottom left, there is a "Volume" label and a partially visible input field.

# Cryptokeeper e encfs

- Non e' multiattaforma
- Usato in ambienti linux
- Piu' flessibile rispetto Truecrypt
- Permette la cifratura **on fly** di file e cartelle di file
- Puo' essere usato in sinergia con programmi di backup incrementali, in quanto i file sono cifrati singolarmente.

# Vediamoli meglio

## Encfs

Programma a riga di comando

## Cryptkeeper

Interfaccia grafica

# Cryptokeeper

