GnuPG e la Posta Sicura

Simone Kalb
http://www.nodelay.org

Cos'è la crittografia

- La *crittografia* è una tecnica con cui mascherare un messaggio per renderlo illeggibile da chiunque altro non sia il destinatario
- Evita la trasmissione d'informazioni "in chiaro" su un canale di comunicazione.
- Si basa sulla disponibilità di una chiave di lettura da parte degl'interlocutori

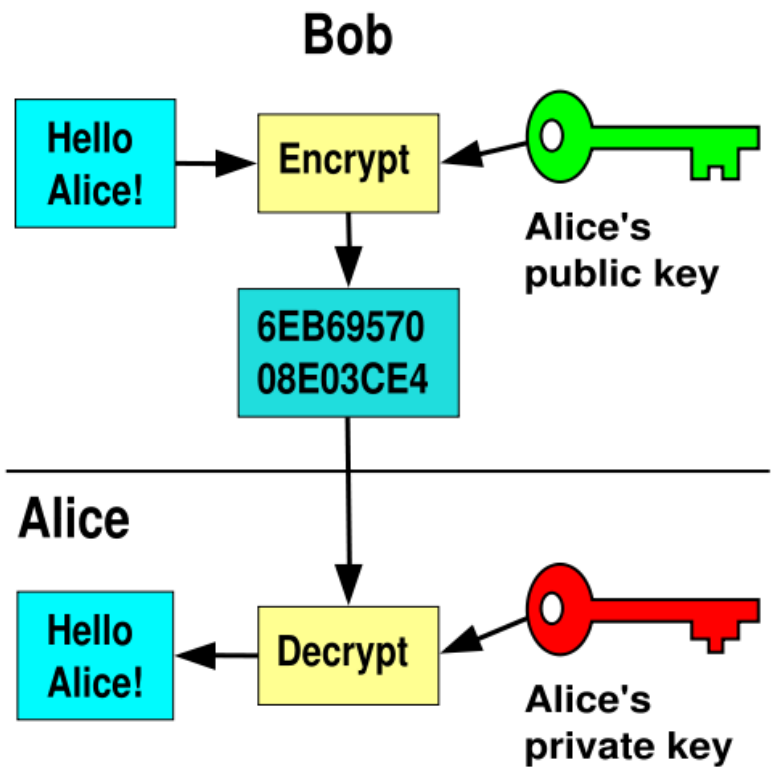
Cenni storici sui codici crittografici

- Il primo fu l' **atbash** di origine ebraica utilizzato anche nella Bibbia, si basa su una sostituzione alfabetica
- Giulio Cesare utilizzava un codice a sostituzione monoalfabetica poi chiamato il *cifrario di Cesare*, appunto
- Leon Battista Alberti, Tritemio, Giovan Battista Bellaso, Vigenère, Kasiski sono i più importanti della storia moderna

La crittografia a chiave simmetrica

- Dopo gli studi di Claude Shannon e Vernam con il suo cifrario..
- Nasce l'OTP una chiave lunga quanto il messaggio ed utilizzabile solo una volta
- Algoritmi a chiave simmetrica con funzioni matematiche non reversibili
- AES, DES, 3DES, potenti ma non sicuri al 100%

La crittografia a chiave asimmetrica



- Alice deve mandare un pacco a Bob
- Alice e Bob si scambiano i lucchetti aperti
- Alice manda il pacco e lo chiude con il lucchetto di Bob
- Bob utilizza la sua chiave per aprire il pacco

GNU Privacy Guard

- GNU Privacy Guard è un'implementazione libera dell'RFC 2440 meglio conosciuto come OpenPGP
- Consente l'utilizzo della crittografia a chiave asimmetrica su sistemi Unix/Linux
- Supporta anche altri S.O. basati su Win32 [4]
- Gestisce le chiavi e elenchi di chiavi pubbliche
- Alternativa libera di PGP (Pretty Good Privacy) di Phil Zimmerman

Cosa me ne faccio di GNUPg?

- GNUPg è un programma molto utile per vari scopi:
  - comunicazioni riservate tra utenti
  - posta elettronica riservata
  - posta elettronica autenticata
  - crittografia su disco

- Noi vedremo il suo utilizzo solo per ciò che concerne la posta elettronica

Come si installa?

- GnuPG è molto semplice da installare ed i pacchetti pre-compilati si trovano per tutte le distribuzioni più diffuse

- Per le distro derivate da Debian, come Ubuntu basta un semplice:

```
$sudo apt-get install gpg
```

- Per la compilazione dai sorgenti il solito:

```
$ ./configure
$ make && sudo make install
```

Creazione delle chiavi

- Per la creazione delle chiavi si agisce da linea di comando:

```
$gpg --gen-key
~
Please select what kind of key you want:
   (1) DSA and Elgamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection? 1
```

- La nostra scelta ricade su DSA/Elgamal

Creazione delle chiavi (2)

- Scegliamo la lunghezza della chiave:

```
DSA keypair will have 1024 bits.
ELG-E keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
```

- Scegliamo anche la sua data di scadenza:

```
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
```

Creazione delle chiavi (3)

- Scegliamo il nostro nome reale e la nostra mail:

```
You need a user ID to identify your key; the software
  constructs the user ID from the Real Name, Comment and
  Email Address in this form:

    "Heinrich Heine (Der Dichter) <
  heinrichh@duesseldorf.de>"

Real name: Zack J.L.

Email address: zack@nodelay.org

Comment:

You selected this USER-ID:

    "Zack J.L. <zack@nodelay.org>"


Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?O
```

Creazione delle chiavi (4)

- Abbiamo quasi finito, manca solo la parola d'ordine:

```
Enter passphrase:

We need to generate a lot of random bytes. It is a good
  idea to perform some other action (type on the
  keyboard, move the mouse, utilize the disks) during
  the prime generation; this gives the random number
  generator a better chance to gain enough entropy.

~~~~~~~~~~

pub   1024D/1137F781 2007-10-14

      Key fingerprint = 6F2B E51A FA3A 9D61 7923  A011
  6EEA B0FE 1137 F781

uid                  Zack J.L. <zack@nodelay.org>

sub   2048g/4C65A345 2007-10-14
```

Generazione della revoca

- Il file di revoca serve per disattivare una chiave prima della sua effettiva scadenza
- È sempre bene creare una revoca, per maggiore sicurezza:

```
$gpg --output revoca.txt --gen-revoke nome@dominio.ext
```

- Questo comando genera un file revoca.txt che contiene le informazioni per la disattivazione
- Per disattivare la firma basta semplicemente importarla col comando:

```
$gpg --import revoca.txt
```

Alcuni utili comandi

- *gpg --list-keys*

  Visualizza la lista di tutte le chiavi installate

- *gpg --remove-secret-keys [--remove-keys] email*

  Rimuove la chiave privata[pubblica] specificata dall'indirizzo di 'email'

- *gpg --output public.asc --export --armor email*

  Esporta la chiave pubblica nel file public.asc

- *gpg -r Nome -sc dati*

  Cripta il file 'dati' con la chiave di Nome, e lo autentica con il nome del creatore

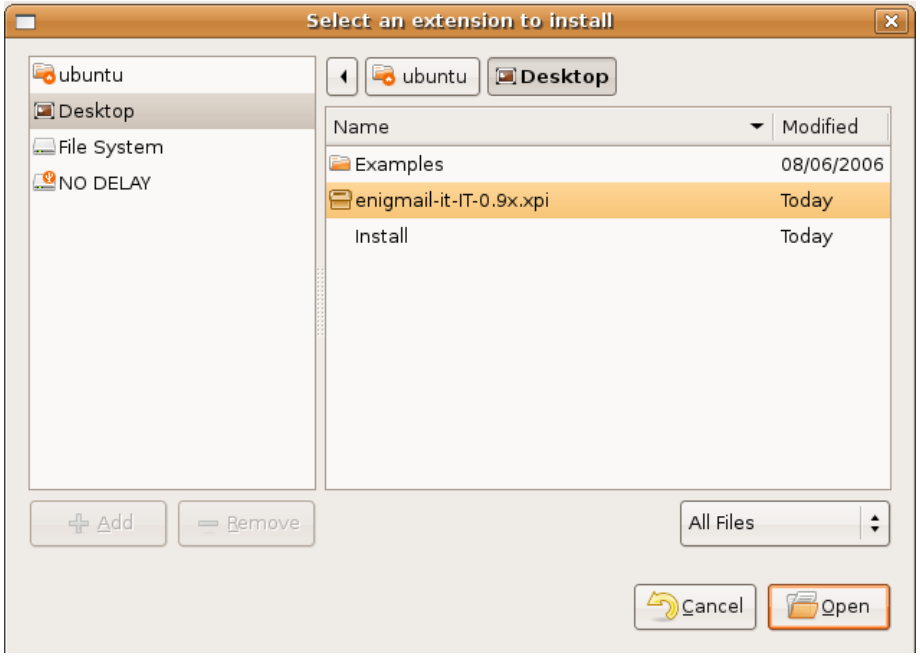
Struttura di GnuPG

- Una volta create le chiavi ci saranno dei nuovi files nella directory utente:
  - *~/.gnupg/secring.gpg*
    - Il file che rappresenta il portahiavi delle chiavi private (da custodire gelosamente!)
  - *~/.gnupg/pubring.gpg*
    - Il file che rappresenta il portachiavi delle chiavi pubbliche
  - *~/.gnupg/gpg.conf*
    - Un file di configurazione dalla semplice sintassi, che permette di specificare alcune opzioni
  - ~/.gnupg/trustdb.gpg
    - Specifica il database delle chiavi fidate (*trusted*)

Enigmail

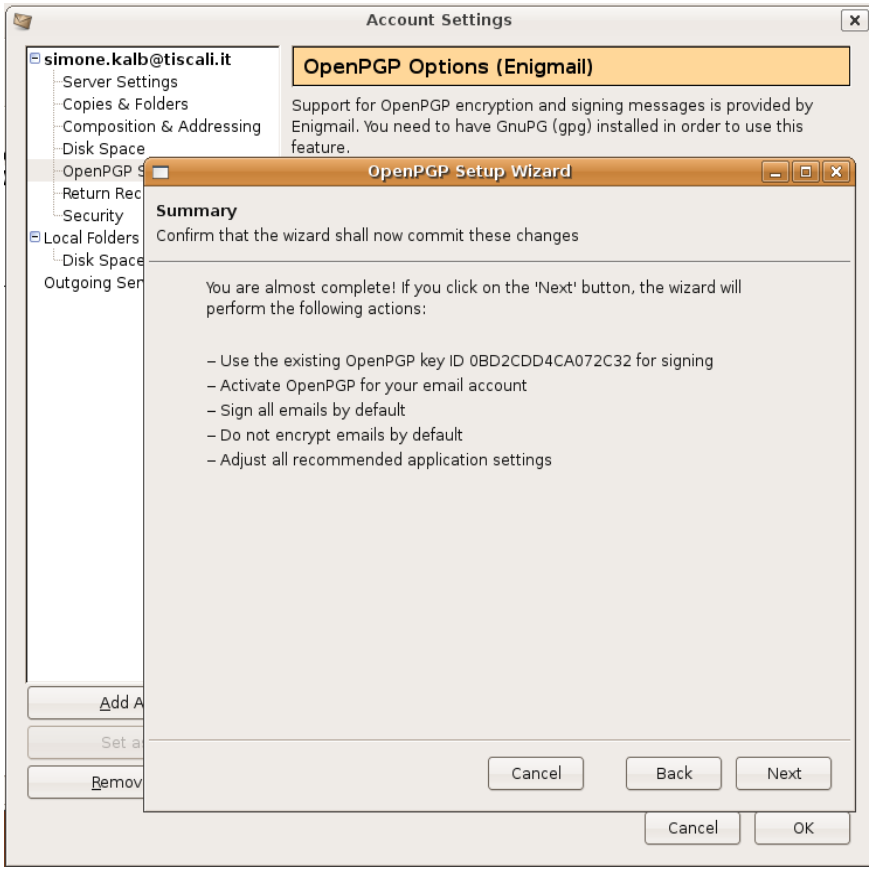
- Vedremo l'integrazione di GnuPg con il client di posta Mozilla Thunderbird
- Enigmail è un'estensione gratuita per Thunderbird (doppia licenza GPL e MPL)
- È un frontend per GnuPG, fa praticamente tutto quello che fa GnuPG, ma più facilmente
- *http://enigmail.mozdev.org*

Installazione



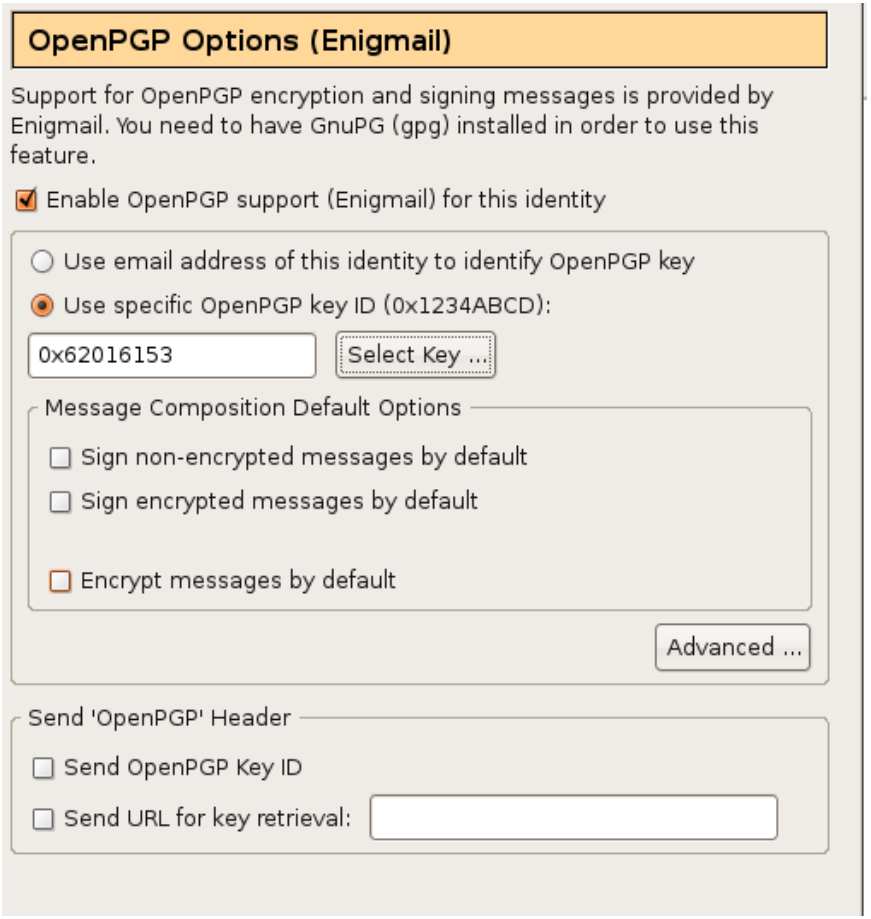
- Recuperiamo il file da: `http://www.mozilla-enigmail.org/downloads/lang/0.9x/enigmail-it-IT-0.9x.xpi`
- Per l'installazione: Strumenti/Componenti Aggiuntivi/Installa e selezionamo il file

Installazione



- Un wizard ci seguirà lungo il processo d'inizializzazione di Enigmail
- Al termine di questo, una linguetta 'OpenPGP' ci apparirà nelle preferenze dell'account di posta

Configurazione



- Nelle preferenze dell'account appare un'opzione per OpenPGP
- Selezionare *Enable OpenPGP support*
- Selezionare la chiave relativa a quell'account
- Selezionare eventuali opzioni

Importare una chiave pubblica

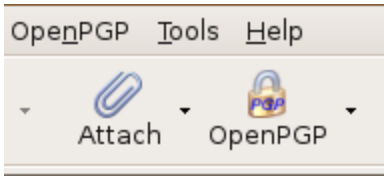
- Da linea di comando abbiamo visto:

```
$ gpg --import pubkey.txt
```

- Invece da Thunderbird, entriamo nel menù OpenPGP e clicchiamo su Gestione delle chiavi, dopo di che dal menù File selezioniamo 'Importa chiavi da un file'.
- Sempre dalla finestra di gestione delle chiavi, si può accedere ad altre opzioni come l'utilizzo di smartcard
- Le smartcard vengono fornite anche con la Fellowship alla Free Software Foundation [7]
- Sono un metodo sicuro e facile per crittare i propri dati

Nuovo messaggio

- D'ora in poi quando andremo a creare un nuovo messaggio, apparirà un'icona con il lucchetto



- Da lì si può selezionare se crittare il messaggio, firmarlo solamente, oppure tutt'e due
- Prendiamo ad esempio il caso in cui vogliamo autenticare il messaggio
- Per la verifica della firma da parte del destinatario è buona norma inserire l'impronta digitale nella mail
- Questa è chiamata fingerprint

Fingerprint

- È una stringa di caratteri che serve per fare dei controlli incrociati sulla validità della firma
- È presente nelle proprietà della firma
- Si presenta così:

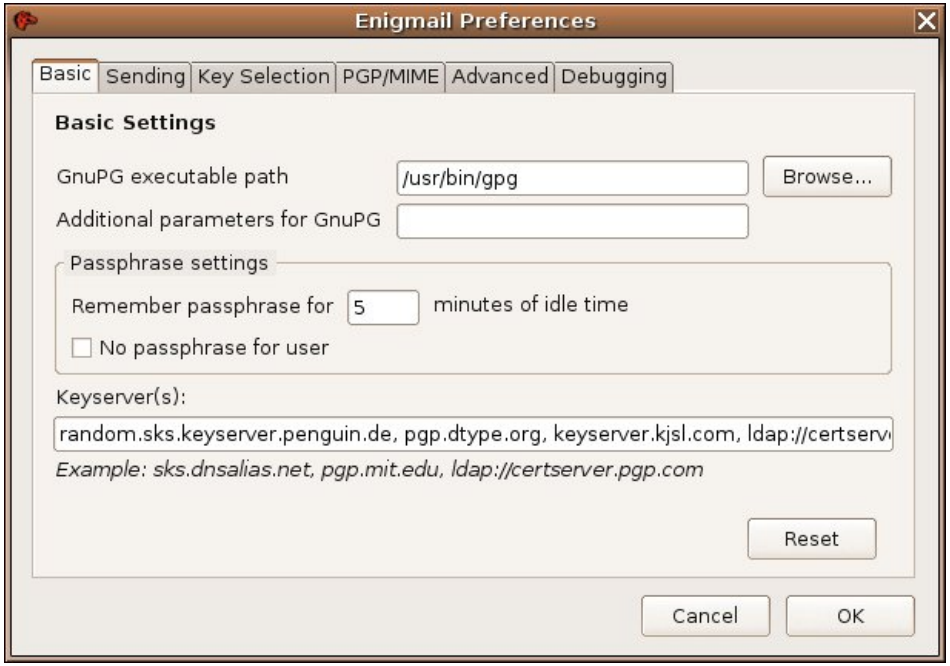
```
Fingerprint: [A696 6EA5 F253 BC42 A513 43AC 29BE D6E4
  D69C 62E4]
```

- Da linea di comando possiamo fare:

```
$gpg --fingerprint mittente@email.it
```

- Una volta inserita la fingerprint nella mail firmata, il destinatario può verificare che le due fingerprint coincidano, pena l'alterazione del messaggio

Invio Chiavi pubbliche



- Andiamo in OpenPGP->Gestione delle chiavi
- Dopo aver selezionato una chiave la inviamo al keyserver dal menù omonimo
- Così le nostre chiavi saranno disponibili a tutti
- Si possono anche cercare chiavi utili

Web of Trust

- Le chiavi importate hanno necessità di essere autenticate dal proprietario
- È necessario che qualcuno garantisca per loro
- Web of trust è una rete in cui tutte le chiavi che possiede un nostro contatto fidato sono automaticamente fidate
- Ci si 'fida' che i nostri contatti fidati abbiamo a loro volta altri contatti fidati
- Ci sono vari livelli di fiducia

Tipologie di utilizzo

- **Firma:** il messaggio viene firmato con la propria chiave privata, che attesta il fatto che il messaggio arriva proprio da me.
- **Cifra il messaggio:** il messaggio viene cifrato con la chiave pubblica del destinatario
- Questa viene scaricata dal keyserver nel caso non esista tra quelle disponibili

Demo

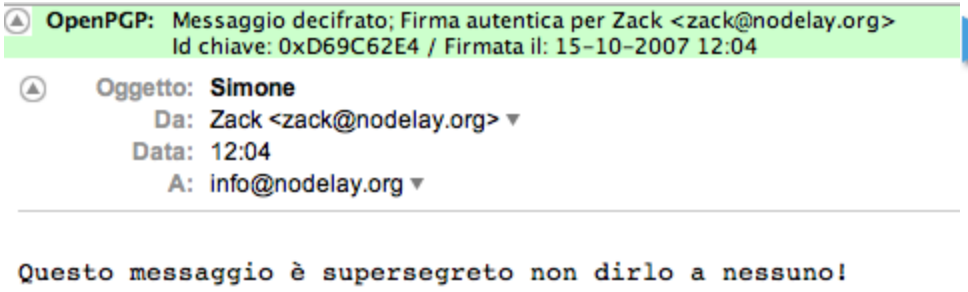
Oggetto: **Simone**
Da: Zack <zack@nodelay.org>
Data: 12:04
A: info@nodelay.org

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-15
Version: GnuPG v1.4.7 (Darwin)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org

hQIOA2ox8kttpNwxEAgAmR4W67l1evxRl+OJywORGSqjgML3OxTEpGYfiwig04p2
cBzMKoI1PF/6mdb8Eo7w7xNuy4aQ4F9hQ6lmksX44Vl6qcyyuQzjuRT8z/DNyEha
GkchXQg39N+mZ0XEska+HKoc9w+u8/hG1al4pVOp6Cm6mlsQdrKltIbH/2yQOMkU
j6iPnz+vnsTRlR2pEG3j/x32M4DsPasydv7JQ2Bl30cXj/xagQlg3banRddGhAE0
SWN4wp8ndMJp0s/dVYMGxZAKubVDEm+uNYVKK/9A/C//aGiWioWueUhPHfbTxaG8
J/p2aJmPexzmW6pootNdsYbx2AoDhJpGgAhN9+Xv0gf+PvfWls0A+wq4Qd0oVQ3p
cHqFtSFjsF1O6bMvFFNfValWewQqE6tekSPR5ZZnHHeVjcygyWrYyNElgVP/bUUw
xx45oL8dd41r2BKM3MpEQsHoCA8pL1bnW2WUnDwzbPJJpgZz8MjyaHA/IQXcHcj7
VQ4RKOmOxc/9ah/M0Vprxd2NYLUL+Z7ONo51J+3mOIQXNsq5uODDITNJAqd7fdq7
/lXwlrSD0+uttIM+NoLsqOUMfo8kLc/PJSOalA721KzE+e2EhDSdVEiWVtmUtdmc
dDTB6iKBDcsUvXCwk+hMWwwmvYr6cI29SoV3/E8wCY5Sbi5ydv+7wjRu1FkxBwWH
UIUCDgPAddW6CH9TCBAH/jO1azZXwS63DsTCDSOjW2E9Evs7sjK2Eul3XohH/lFt
+haEkWTxlGAFqnaZwInuBMPdxlwZmt2X4K3Pp6Je1FRTmdoP2Cr6U15fUiZ2X+ie
pmpimt8Haisk/YL8321lssX2Kk5/QgRorMFg2lWUXYImQlXMlq4E4G/O6xO1b97j
uU9vliW+2kLSahhYsXN1EgtOijdacKoy2mMk6CnC/H6ih5psnfMZ+vtiBG+6jkak
fGYf5KtasLRmKuLq8OwzyQu+I3f3Yap/MnTkZVQFL2cregaLysqUcAfC/hFc5kWp
t5G9pBxlBchUl98YDuTDH/d9KgH3zeUibqz1cvVq4iwH/j+gP+qYtROQzx0fG09w
xfO6HYLbNIWwvYrivN/eO+E8qeROJodOjAWZnZM4q8OkKYohJRZWtz6b5L8UK0fN
t4RD6NYyvsFdRtBGqeGAH3lU88DXqmA8NDXED6Zj2unnsvlvWMAhukt5svDlscVe
4tSgffXY2g4EYdWThfjjAdIT9UqauWsE7r9GvEQ6oIEdlwcNavddz4yYg+6ztwah
nGJJuvizKFf+HZPv3bbJCfRUINI/bT+JoirTHRTg6lchHTWhnBWhpwAElH34TYqW
IyokhMFSKSK/Kx1Ezs9ZO3J6xCcts7IuLKLMxOr5cZxQ5yAnEzkBQ55GMI8Zaz/E
Gr/SugHrFWlO2zplhGe/qgKZYqCgakTr1Hh7eSf1WFphzqhlSisIxAB8Rk2Aegzk
6A+ssih02brCUKJQctNi/OZO2MZn2fTACbq5i0IfucYy0Y5dOoc767Vl8LR4VeCp
VzSGtGExDHSTPWOA6YW8hXXeZa9hBbZYvGneevDfpiOl8QJKnfnjbYaEpKP/z6X8
SwzolH4gshalvKHQ18rnuwuHfspQqBLQ1yJqz+rbMRpslhtoFsXOVygq87gNGw==
=tU2C
-----END PGP MESSAGE-----
```

- Cifriamo il messaggio con la chiave pubblica del destinatario
- Otteniamo un messaggio illeggibile
- Ora solo il destinatario potrà leggerlo
- La decrittazione avviene grazie alla chiave privata

Demo



- Una volta arrivato il messaggio il destinatario non dovrà fare altro che aprire la mail e cliccare su Decripta.
- Il messaggio decriptato apparirà
- Un lucchetto testimonierà l'autenticazione del messaggio

Perché GPG?

- Abbiamo visto come sia facile usare la crittografia
- È un metodo poco laborioso
- Ci consente di lavorare in sicurezza
- Le nostre conversazioni non possono essere intercettate
- Richiede una potenza di calcolo minima
- Non influisce sulle prestazioni
- Garantisce una forma di anonimato
- All'occorrenza certifica il mittente

Compatibilità con client di posta

- Evolution fornisce un supporto integrato per OpenPGP (a patto che Gpg sia installato)
- Kmail lo supporta tramite Ågipten 2 [8]
- Pine lo supporta tramite Pinepgp [9]
- Anche Mutt supporta GPG (vedi tutorial)

Conclusioni

- Abbiamo visto come sia facile configurare GnuPg e quanto sia utile
- È sempre buona norma firmare i messaggi, soprattutto quelli per cui si richiede autenticazione
- La crittografia della posta previene attacchi del tipo *Man-in-the-middle.*
- La crittografia non è la panacea di tutti i mali
- Non esiste una comunicazione sicura al 100%,
- GPG è comunque un ottimo strumento per la tutela della nostra privacy

Riferimenti

- http://www.gnupg.org/ [1]
- http://enigmail.mozdev.org/ [2]
- http://it.wikipedia.org/wiki/S/MIME [3]
- http://www.gpg4win.org/ [4]
- http://rot13page.googlepages.com/ [5]
- http://wordpress.altervista.org/QIT/ [6]
- https://www.fsfe.org/en/fsfeuser/register/(set)/1 [7]
- http://kontact.kde.org/kmail/kmail-pgpmime-howto.php [8]
- http://www.linuxsecurity.com/content/view/117565/49/ [9]

Grazie per l'attenzione.