

# Athens CryptoParty #1

## Pretty Good Privacy (PGP)

# Athens CryptoParty #1

## Pretty Good Privacy (PGP)

- **Δημιουργία:** Phil Zimmerman (ακτιβιστής ενάντια στα πυρηνικά) 1991
  - Σκοπός: να ανταλλάσουν ασφαλή μηνύματα οι ακτιβιστές στις τότε online πλατφόρμες (BBS)
  - Cypherpunks
- **Δικαστήρια:** “*munitions* export without a license” 1993
  - US export regulation: κλειδί > 40bit == **Munition!** (μεταφρ: πυρομαχικά)
  - Τύπωσε τον κώδικα σε βιβλίο (MIT) και το διέθεσε (PGP Source Code and Internals)
    - Η εξαγωγή βιβλίων προστατεύεται από το 1<sup>st</sup> Amendment (Freedom of Speech) άρα ήταν νόμιμο.
- **Εταιρία:** Viacrypt/PGP 1996
- **Προτυποποίηση:** OpenPGP 1997
  - Free Software Foundation → GnuPG (GPG) 1999

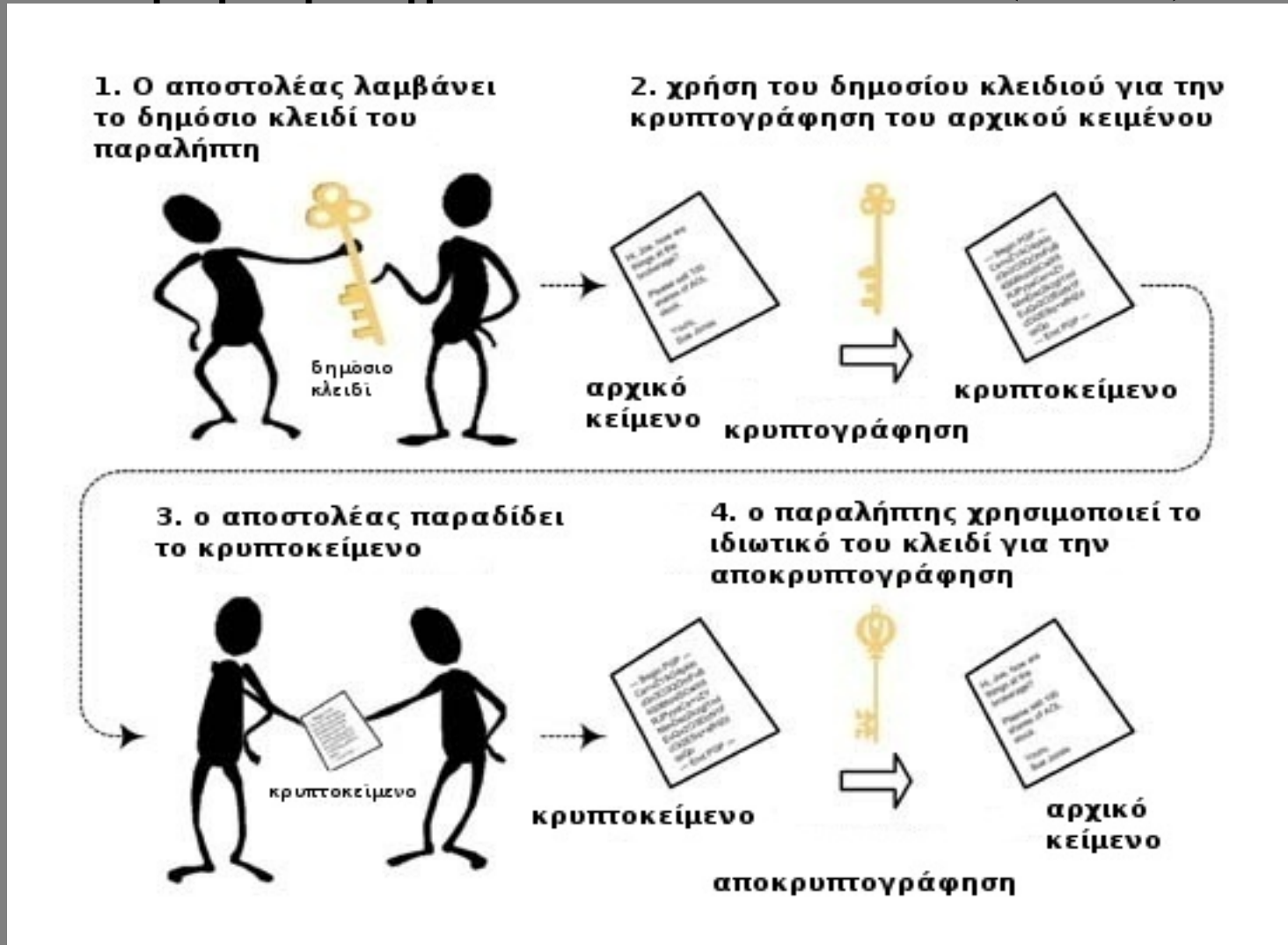
# Athens CryptoParty #1

## Pretty Good Privacy (PGP)

- Δημιουργία ιστού εμπιστοσύνης
  - Οι χρήστες υπογράφουν τα κλειδιά άλλων χρηστών που έχουν γνωρίσει προσωπικά και τους εμπιστεύονται.
  - Ανεβάζουν τις υπογραφές τους σε ειδικούς keyservers στο internet.
  - Οι χρήστες βασίζονται στις υπογραφές ανθρώπων που **γνωρίζουν προσωπικά** οι ίδιοι για να εμπιστευτούν κάποιο τρίτο.
  - Δημιουργία ενός τεράστιου γράφου εμπιστοσύνης.
    - Keysigning Parties
  - **Προσοχή ποιόν υπογράφετε!**

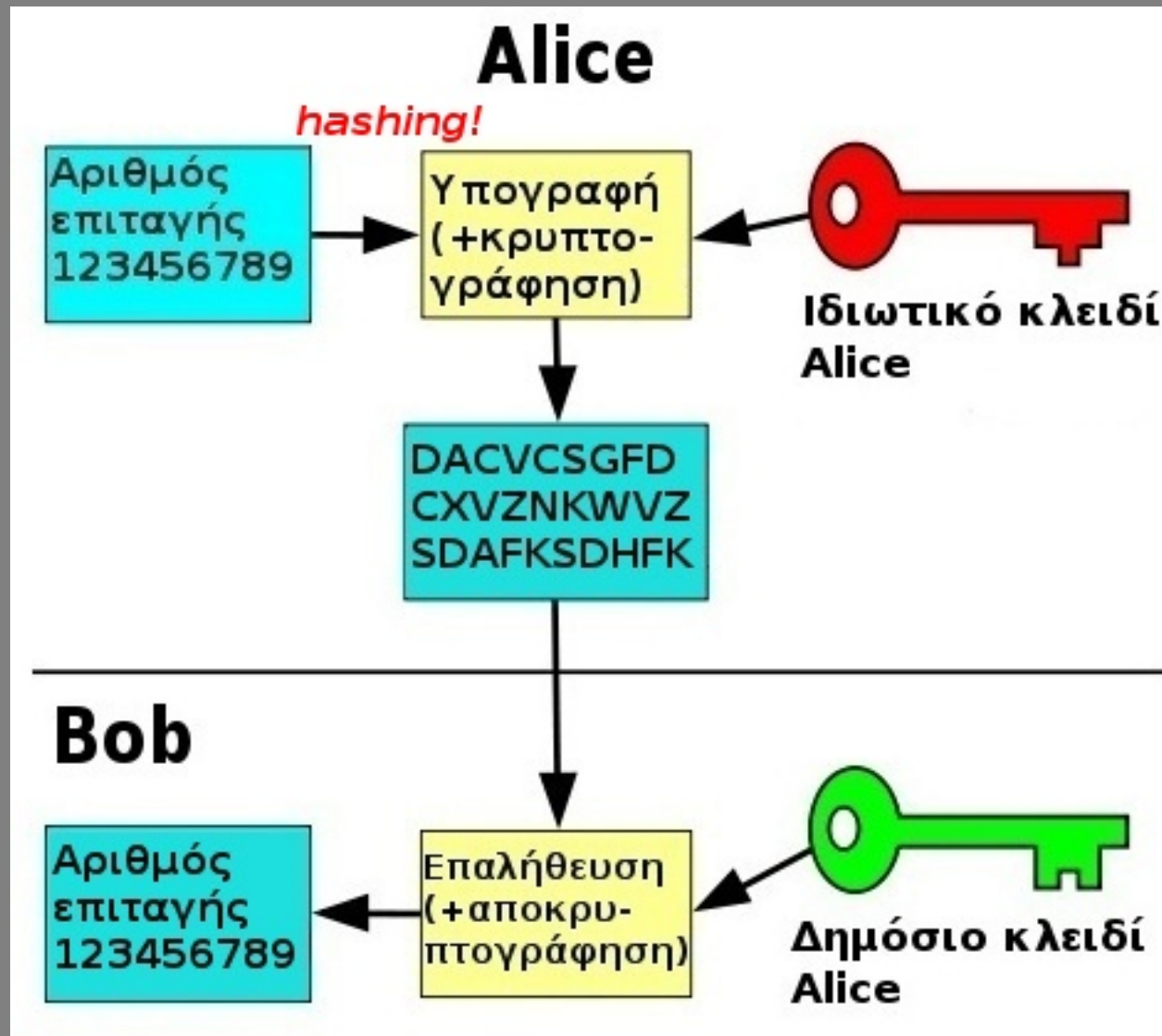
# Athens CryptoParty #1

## Χρήση δημοσίου κλειδιού (PKC)



# Athens CryptoParty #1

Χρήση PKC για υπογραφή/πιστοποίηση



# Athens CryptoParty #1

Πως δουλεύει ένας αλγόριθμος PKC

Diffie-Hellman και διακριτοί λογάριθμοι  
(μην φοβάστε δεν δαγκώνει!)

<https://www.youtube.com/v/3QnD2c4Xovk>

Πηγή: <https://twitter.com/#!/artoftheproblem>

# Athens CryptoParty #1

## Μοντέλα Εμπιστοσύνης

- **Pretty Good Privacy Web of Trust**

- Ο κάθε χρήστης ταυτοποιεί/υπογράφει αυτούς που ο ίδιος εμπιστεύεται.
- Χρησιμοποιείται μεταξύ χρηστών.
- Άναρχη δομή.

- **Certificate Authorities**

- Υπηρεσίες/εταιρίες που εκδίδουν ψηφιακά πιστοποιητικά.
- Πιστοποιητικό = Όνομα κατόχου + Υπογραφή από Certificate Authority + Δημόσιο κλειδί κατόχου
- Πιστοποιούν πως ένα δημόσιο κλειδί ανήκει στον φερόμενο ως ιδιοκτήτη.
- Χρησιμοποιείται μεταξύ χρηστών και δημοσίων υπηρεσιών στο Internet (π.χ. HTTPS, Email).
- Ιεραρχική Δομή.

# Athens CryptoParty #1

## Χρήση PGP

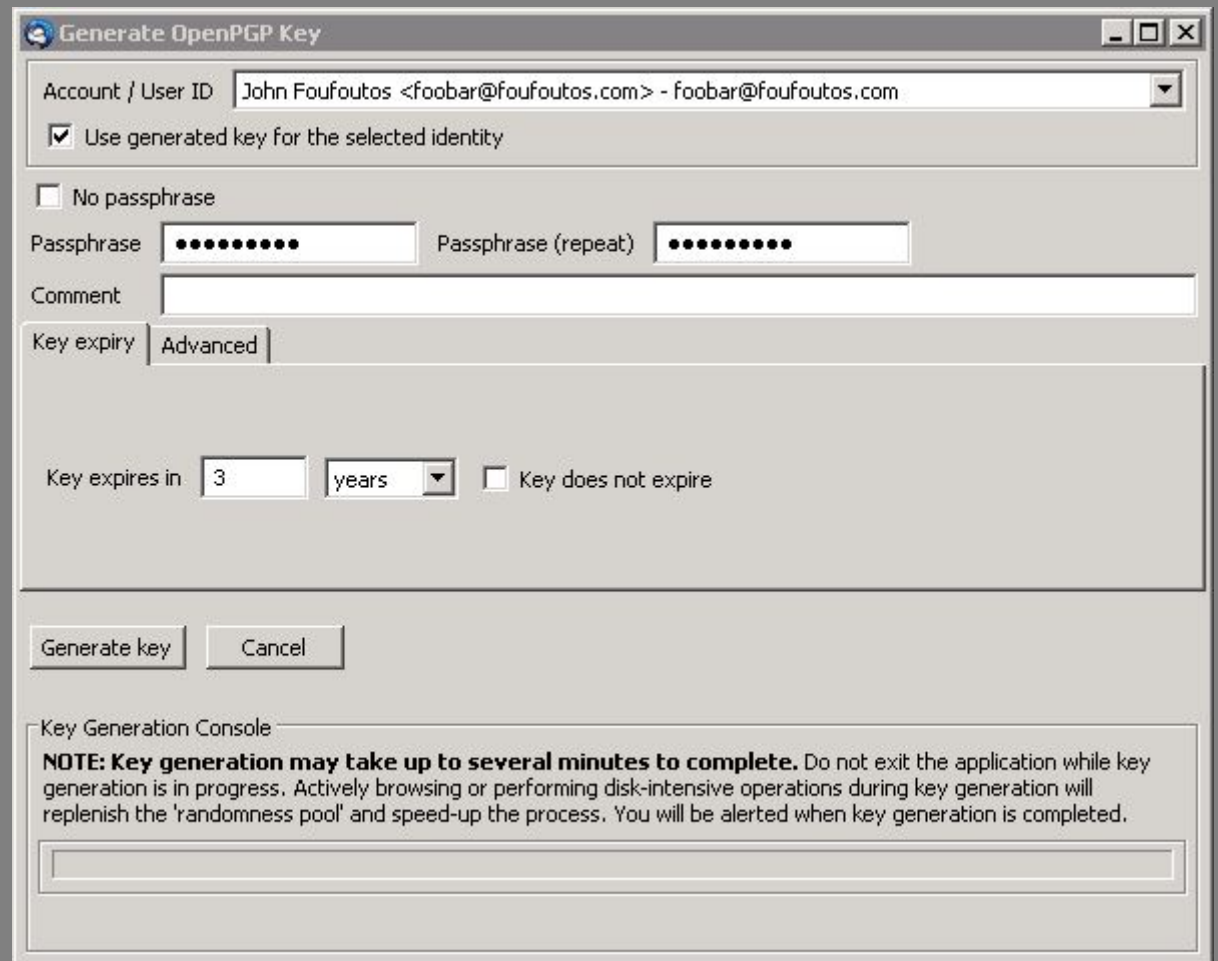
- **Ο δύσκολος δρόμος: γραμμή εντολών**
- **Μέσω του plugin enigmail στο Thunderbird**
- **Μέσω γραφικών εργαλείων (Seahorse, GPA, κ.α)**



# Athens CryptoParty #1

## Χρήση PGP μέσω enigmail

**Δημιουργία νέου κλειδίου:**  
OpenPGP → Key  
Management → Generate →  
New keypair



Generate OpenPGP Key

Account / User ID: John Foufoutos <foobar@foufoutos.com> - foobar@foufoutos.com

Use generated key for the selected identity

No passphrase

Passphrase: ..... Passphrase (repeat): .....

Comment: \_\_\_\_\_

Key expiry: Advanced

Key expires in: 3 years  Key does not expire

Generate key Cancel

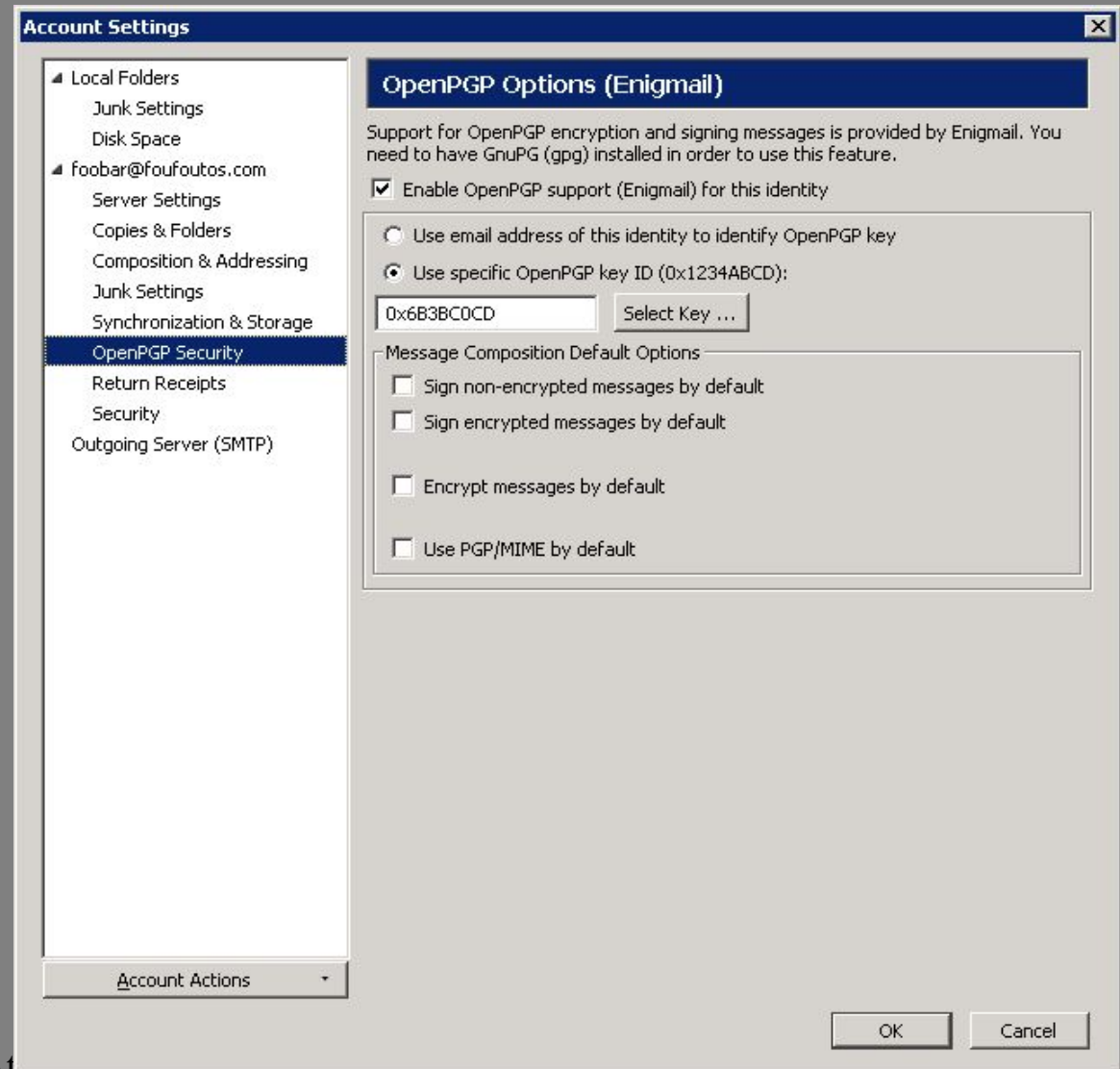
Key Generation Console

**NOTE: Key generation may take up to several minutes to complete.** Do not exit the application while key generation is in progress. Actively browsing or performing disk-intensive operations during key generation will replenish the 'randomness pool' and speed-up the process. You will be alerted when key generation is completed.

# Athens CryptoParty #1

## Χρήση PGP μέσω enigmail

**Χρήση κλειδιού από account:**  
Tools → Account Settings →  
OpenPGP Security

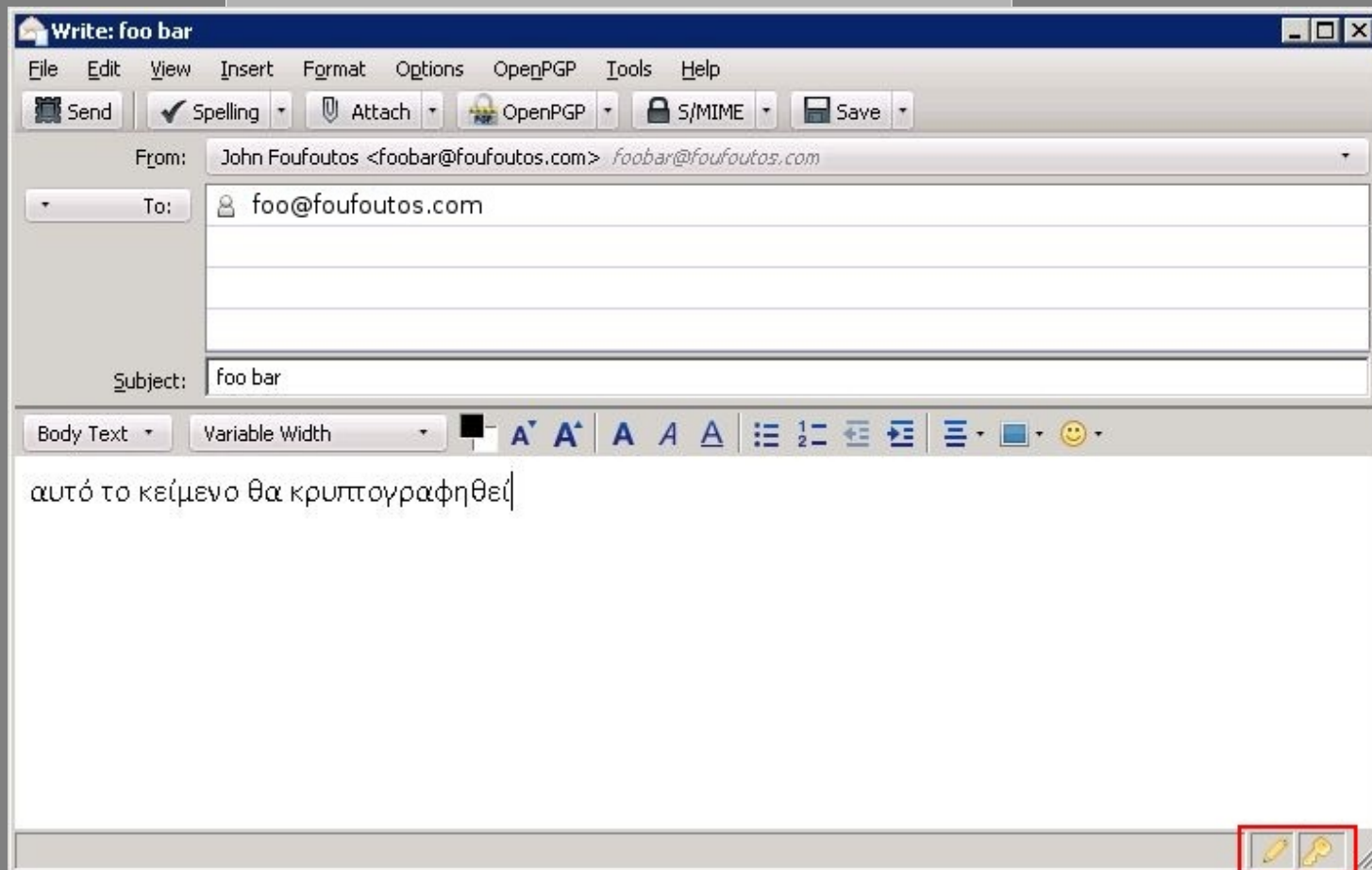


# Athens CryptoParty #1

## Χρήση PGP μέσω enigmail

**Νέο E-mail:**

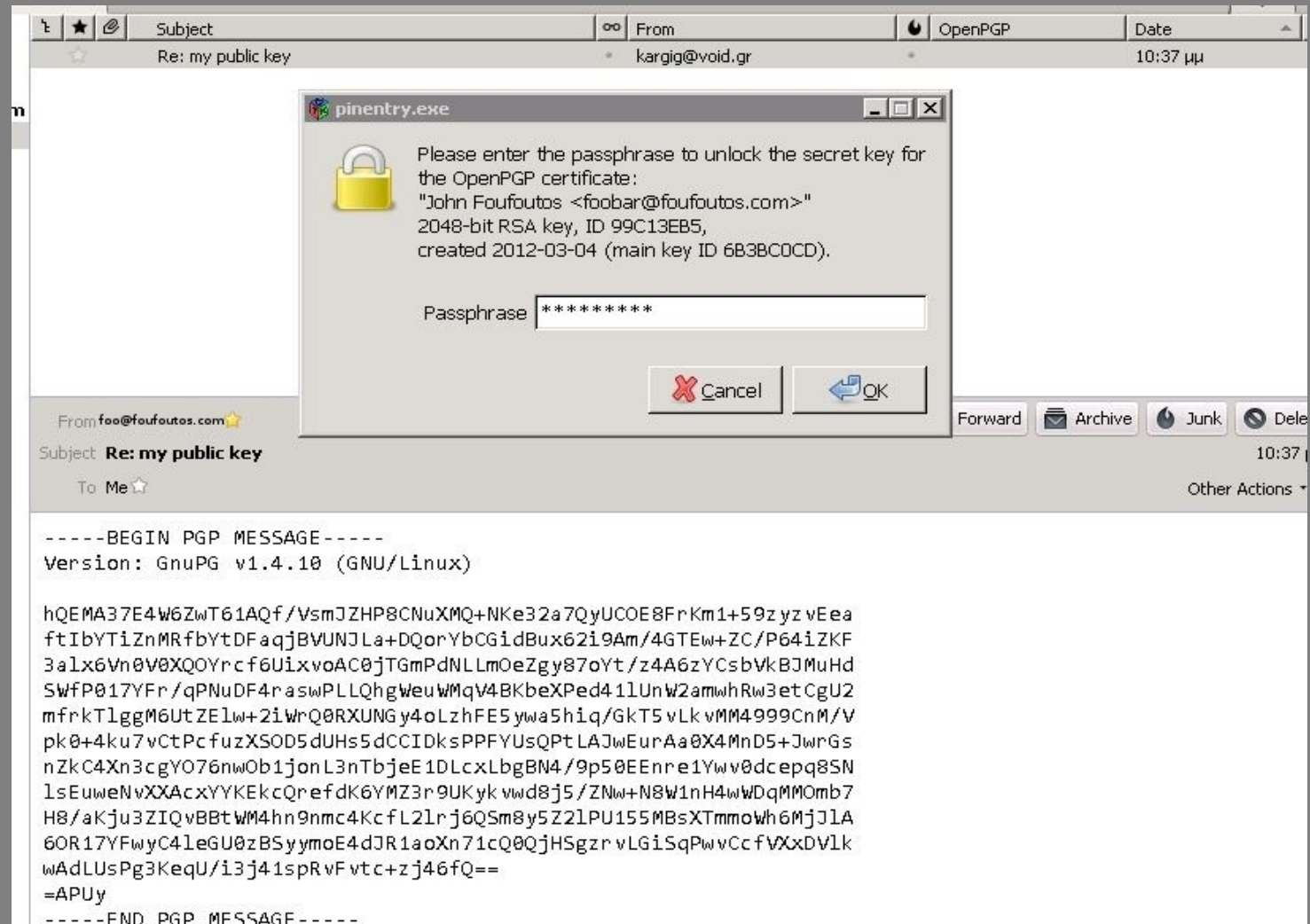
OpenPGP → Sign/Encrypt Message



# Athens CryptoParty #1

## Χρήση PGP μέσω enigmail

**Εισερχόμενο E-mail:**  
(πριν την  
αποκρυπτογράφηση)

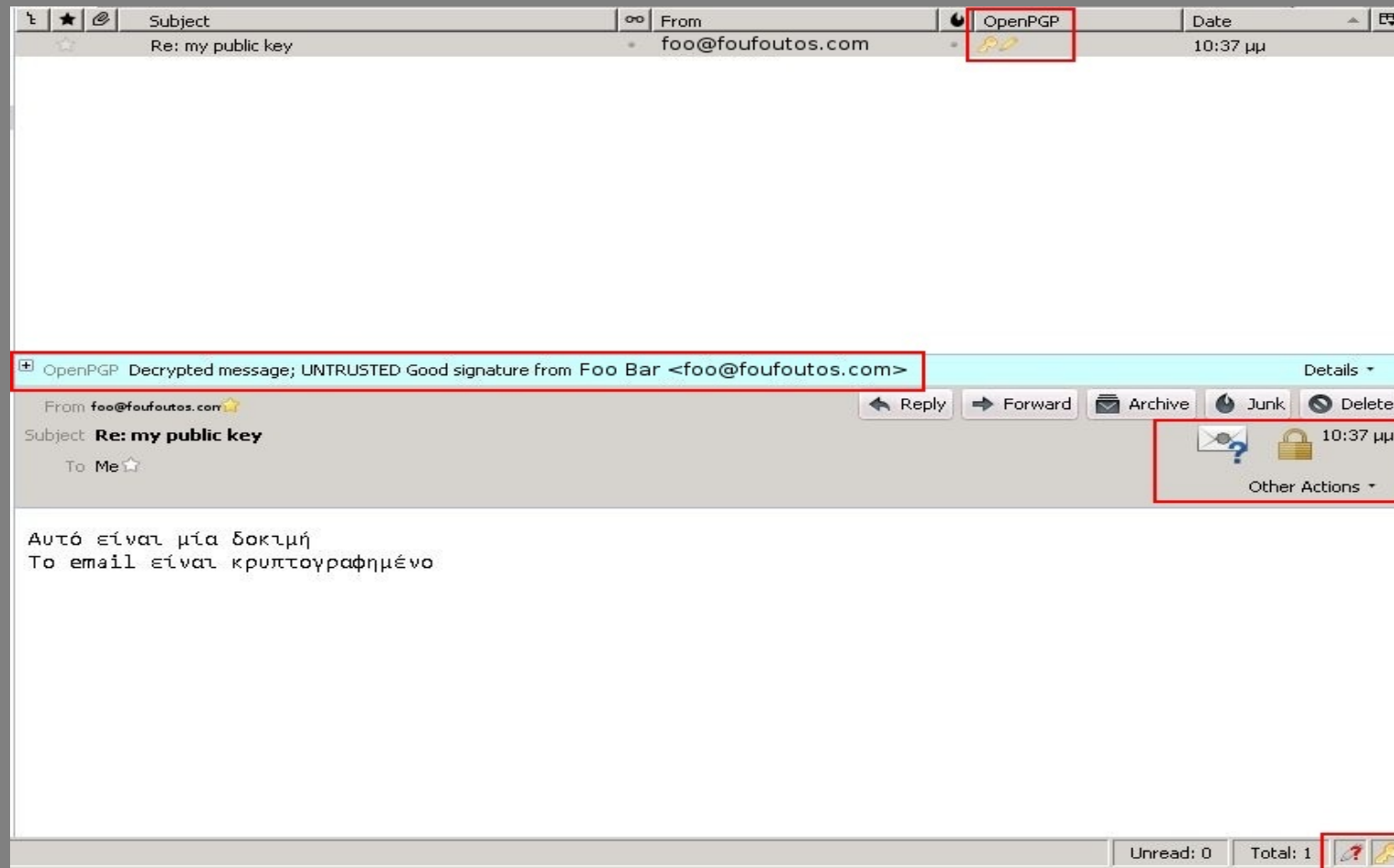


The screenshot shows an email client window with a subject line "Re: my public key" and a sender "kargig@void.gr". A dialog box titled "pinentry.exe" is overlaid on the email content, asking for a passphrase to unlock a secret key for the OpenPGP certificate of "John Foufoutos <foobar@foufoutos.com>". The dialog box contains a yellow padlock icon and a text field with "\*\*\*\*\*" for the passphrase. Below the dialog box, the email header shows "From: foo@foufoutos.com" and "Subject: Re: my public key". The main body of the email is a PGP message starting with "-----BEGIN PGP MESSAGE-----" and "Version: GnuPG v1.4.10 (GNU/Linux)". The message content is a long string of base64-encoded text, ending with "-----END PGP MESSAGE-----".

# Athens CryptoParty #1

## Χρήση PGP μέσω enigmail

**Εισερχόμενο E-mail:**  
(μετά την  
αποκρυπτογράφηση)



# Athens CryptoParty #1

## Seahorse (Linux)

- Διαχείριση κλειδιών/υπογραφών
  - Εύρεση χρηστών
  - Εισαγωγή / επεξεργασία κλειδιών
  - Υπογραφή κλειδιών

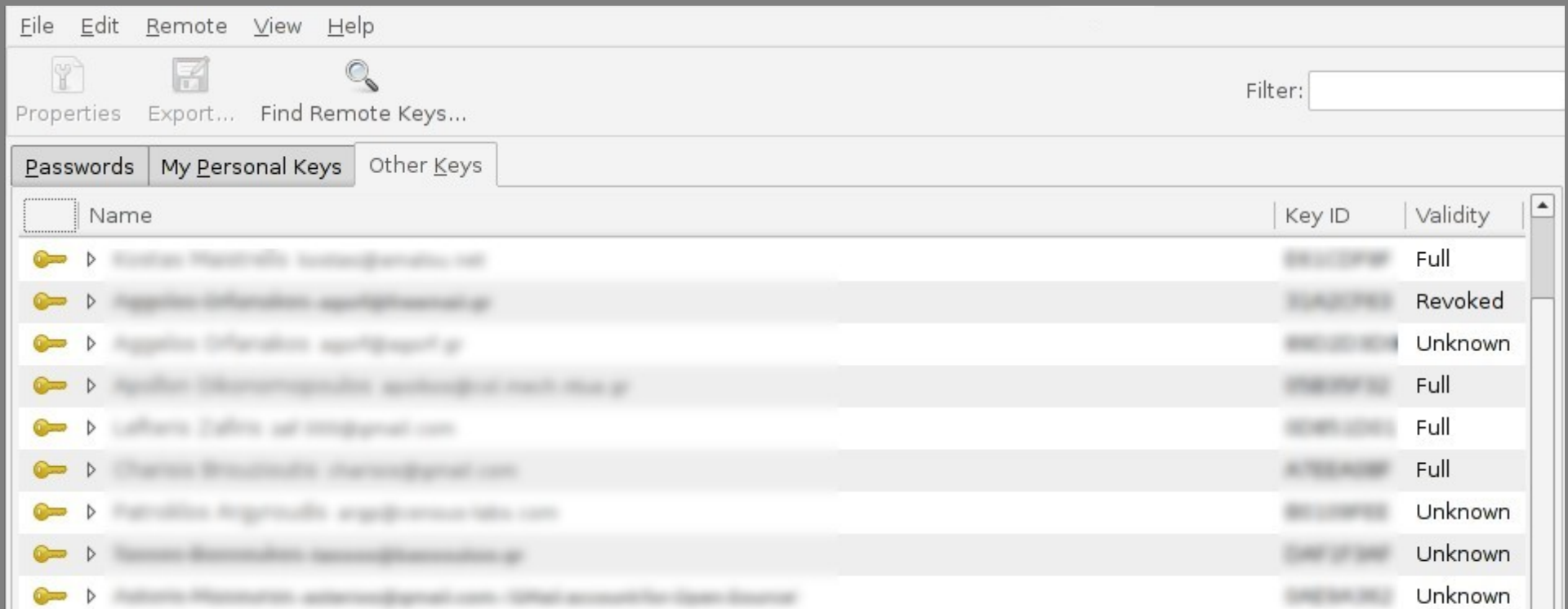
### Προσωπικά κλειδιά



# Athens CryptoParty #1

## Seahorse

### Κλειδιά τρίτων



The screenshot shows the Seahorse application window. The menu bar includes File, Edit, Remote, View, and Help. Below the menu bar are icons for Properties, Export..., and Find Remote Keys..., along with a Filter: input field. The main area has three tabs: Passwords, My Personal Keys, and Other Keys. The Other Keys tab is active, displaying a table of keys.

| Name        | Key ID    | Validity |
|-------------|-----------|----------|
| ▶ [blurred] | [blurred] | Full     |
| ▶ [blurred] | [blurred] | Revoked  |
| ▶ [blurred] | [blurred] | Unknown  |
| ▶ [blurred] | [blurred] | Full     |
| ▶ [blurred] | [blurred] | Full     |
| ▶ [blurred] | [blurred] | Full     |
| ▶ [blurred] | [blurred] | Unknown  |
| ▶ [blurred] | [blurred] | Unknown  |
| ▶ [blurred] | [blurred] | Unknown  |

# Athens CryptoParty #1

## GNU Privacy Assistant (Linux/Windows)

- Διαχείριση Κλειδιών / υπογραφών
- Κρυπτογράφηση αρχείων
- Κρυπτογράφηση Clipboard

The screenshot displays the GNU Privacy Assistant (GPG4win) interface. The main window is titled "GNU Privacy Assistant - Key Manager" and contains a menu bar (File, Edit, Keys, Windows, Server, Help) and a toolbar with icons for Edit, Delete, Sign, Import, Export, Brief, Detailed, Preferences, Refresh, Files, Clipboard, and Card. Below the toolbar is a table of keys:

|   | Key ID     | Expiry Date | Owner Trust | Validity    | User Name                             |
|---|------------|-------------|-------------|-------------|---------------------------------------|
| 🔑 | P 6B3BC0CD | 2015-03-04  | Ultimate    | Fully Valid | John Foufoutos <foobar@foufoutos.com> |
| 🔑 | P E4F4FFE6 | 2013-03-18  | Unknown     | Unknown     | George Karqiotakis <karqiq@void.gr>   |

Below the table, a detailed view of the selected key (6B3BC0CD) is shown:

The key has been imported from a file.  
The key can be used for signing and encryption.  
User name: John Foufoutos  
Key ID: 6B3BC0CD  
Fingerprint: 4899 C241 C7D  
Expires at: 2015-03-04  
Owner Trust: Ultimate  
Key validity: Fully Valid  
Key type: RSA 2048 bits

An inset window titled "GNU Privacy Assistant - File Manager" is also visible, showing a menu bar (File, Edit, Windows, Help) and a toolbar with icons for Open, Clear, Sign, Verify, Encrypt, Decrypt, Preferences, Keyring, Clipboard, and Card. The File Manager window shows a file list with the following entry:

| File   |
|--|
| C:\Users\Administrator\Pictures\enigmail_write_email.JPG |

At the bottom of the Key Manager window, the text "Selected default key: 6B3BC0CD John Foufoutos <foobar@foufoutos.com>" is displayed.



# Athens CryptoParty #1

Ελληνικό Web of Trust

<http://members.hellug.gr/argp/>

by @argp

Δεν έχει ανανεωθεί από το 2008, **εθελοντές;**

# Athens CryptoParty #1

Δοκιμάστε το PGP στην πράξη! Στείλτε δοκιμαστικά emails προς **0xE4F4FFE6**

# Athens CryptoParty #1

Χρήση PGP μέσω γραμμής εντολών

## Δημιουργία κλειδιού:

– gpg --gen-key

- Τύπος (Type): DSA and Elgamal
- Μέγεθος Κλειδιού (Keysize): 2048bits
- Λήξη (Expiry): 3 χρόνια
- Όνομα/E-mail
- **Μυστική φράση (Passphrase) !!**

– gpg --list-secret-keys

```
sec 2048D/14FB501A 2012-03-04 [expires: 2015-03-04]
uid          John Foufoutos <john@foufoutos.com>
ssb 2048g/7E30159E 2012-03-04
```

# Athens CryptoParty #1

Χρήση PGP μέσω γραμμής εντολών

**Αναζήτηση/Εισαγωγή κλειδιού χρήστη:**

- gpg --search όνομα/email
  - Προσοχή! Μπορεί να υπάρχουν πολλά αποτελέσματα!
  - <http://pgp.mit.edu> Αναζήτηση και επιβεβαίωση υπογραφών
- gpg --recv-keys ABACADAE
- gpg --import όνομα\_αρχείου

**Λίστα δημοσίων κλειδιών χρηστών:**

- gpg --list-keys

# Athens CryptoParty #1

Χρήση PGP μέσω γραμμής εντολών

## **Κρυπτογράφηση αρχείου για χρήστη:**

– gpg -a -r foobar@foufoutos.com -e text.txt

- a: έξοδος σε μορφή κειμένου
- r: παραλήπτης
- e: κρυπτογράφηση

Θα παραχθεί το αρχείο text.txt.asc

## **Κρυπτογράφηση και υπογραφή αρχείου για χρήστη:**

– gpg -a -r foobar@foufoutos.com -es text.txt

- s: υπογραφή κειμένου

Θα ζητηθεί η μυστική φράση του αποστολέα

# Athens CryptoParty #1

## Χρήση PGP μέσω γραμμής εντολών

### Κρυπτογράφηση και υπογραφή αρχείου για χρήστη:

- `echo "Αυτό είναι μια δοκιμή." > text.txt`
- `gpg -a -r foobar@foufoutos.com -es text.txt`

```
You need a passphrase to unlock the secret key for
user: "John Foufoutos <john@foufoutos.com>"
2048-bit DSA key, ID 14FB501A, created 2012-03-04
```

```
gpg: ABACADAE: There is no assurance this key belongs to the named user
```

```
pub 2048g/ABACADAE 2010-06-25 Takis Foukarakis <foobar@foufoutos.com>
Primary key fingerprint: 8A23 C5BE A518 575E 2B21 818D 5AC0 1BC8 ABAC ADAE
```

It is NOT certain that the key belongs to the person named in the user ID. If you *\*really\** know what you are doing, you may answer the next question with yes.

```
Use this key anyway? (y/N) y
```

# Athens CryptoParty #1

Χρήση PGP μέσω γραμμής εντολών

**Αποκρυπτογράφηση αρχείου:**

- gpg -d text.txt.asc
  - d: αποκρυπτογράφηση

```
2048-bit ELG-E key, ID ABACADAE, created 2010-06-25
```

```
gpg: encrypted with 2048-bit ELG-E key, ID ABACADAE, created 2010-06-25
```

```
"Takis Foukarakis <foobar@foufoutos.com>"
```

Αυτό είναι μια δοκιμή.

```
gpg: Signature made Sun 04 Mar 2012 03:00:33 PM EET using DSA key ID 14FB501A
```

```
gpg: Can't check signature: public key not found *
```

# Athens CryptoParty #1

Χρήση PGP μέσω γραμμής εντολών

## Εξαγωγή δημοσίου κλειδιού:

- `gpg -a --output mypublickey.asc --export 14FB501A`
  - output: έξοδος σε αρχείο
  - export: εξαγωγή κλειδιού

## Υπογραφή δημοσίου κλειδιού:

- `gpg --sign-key ABACADAE`
  - sign-key: υπογραφή κλειδιού
- `gpg -a --output ABACADAE.signed-by.14FB501A.asc --export ABACADAE`

και αποστολή του αρχείου `ABACADAE.signed-by.14FB501A.asc` στον κάτοχο του κλειδιού

## Αποστολή δημοσίου κλειδιού σε keyserver:

- `gpg --import ABACADAE.signed-by.14FB501A.asc`
- `gpg --send-keys ABACADAE`



# Athens CryptoParty #1

## Χρήση PGP μέσω enigmail

- Extension για **Thunderbird**
- Τρέχει σε **Windows/Linux/BSD/Mac OS X**
- Σε Linux/BSD/Mac OS X απαιτείται η εγκατάσταση του **gpg**
- Σε windows απαιτείται η εγκατάσταση του πακέτου **gpg4win**: <http://www.gpg4win.org/>
- Εγκατάσταση του Enigmail στο Thunderbird μέσω:  
Tools → Add-ons → (search) Enigmail
- Σε κάποιες διανομές Linux υπάρχει σε πακέτο: enigmail