hackerspace.gr

Freedom of Speech

Κρυπτογραφία και ασφαλής
ανταλλαγή πληροφοριών στο Internet

Freedom of Speech

Ποιός ;
&
Γιατί ;

Κρυπτογραφία

- Τι είναι
- Ιστορικά
- Στόχοι
- Είδη Μοντέρνων Αλγορίθμων
- Μοντέλα Εμπιστοσύνης

Κρυπτογραφία

Τι είναι

- **Κρυπτολογία = κρυπτογραφία + κρυπτανάλυση**
- **Κρυπτογραφία**: μελέτη, ανάπτυξη και χρήση τεχνικών κρυπτογράφησης.
  - Παρέχει μηχανισμούς ώστε 2 ή περισσότερα μέλη να μπορούν να επικοινωνήσουν χωρίς κάποιος τρίτος να μπορεί να διαβάσει τις πληροφορίες που ανταλλάσονται.
- **Κρυπτανάλυση**: μελετά τρόπους παραβίασης μεθόδων κρυπτογράφησης.
- **Στεγανογραφία**: απόκρυψη πληροφορίας μέσα σε ένα μέσο.

Στεγανογραφία != Κρυπτογραφία

Κρυπτογραφία

Ιστορικά

- **<1900**: μέσω επεξεργασίας της γλωσσικής δομής των μυνημάτων
  - π.χ. Αλγόριθμος του Καίσαρα: αντικατάσταση γραμμάτων του κειμένου με γράμματα που βρισκόταν 3 θέσεις μπροστά
    - PAX ROMANA -(encrypt)--> SDA URPDQD
- **1900-1950**: Κρυπτομηχανές
  - Ηλεκτρομηχανές με ρότορες
    - Enigma
- **1950- Σήμερα**: Ψηφιακά/Υπολογιστικά συστήματα
  - Άμεση σύνδεση με δυσεπίλυτα μαθηματικά προβλήματα

Κρυπτογραφία

Στόχοι Μοντέρνας κρυπτογραφίας

- **Ιδιωτικότητα/Εμπιστευτικότητα**
  - Το μύνημα θα πρέπει να μπορούν να το διαβάζουν μόνο εξουσιοδοτημένα μέλη.
- **Αυθεντικοποίηση**
  - Τα μέλη πρέπει να μπορούν να εξακριβώσουν τις ταυτότητές τους.
- **Ακεραιότητα**
  - Το μύνημα δεν έχει αλλάξει κατά την μετάδοση από τον αποστολέα στο παραλήπτη.
- **Μη-Απάρνηση**
  - Ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του μηνύματος.

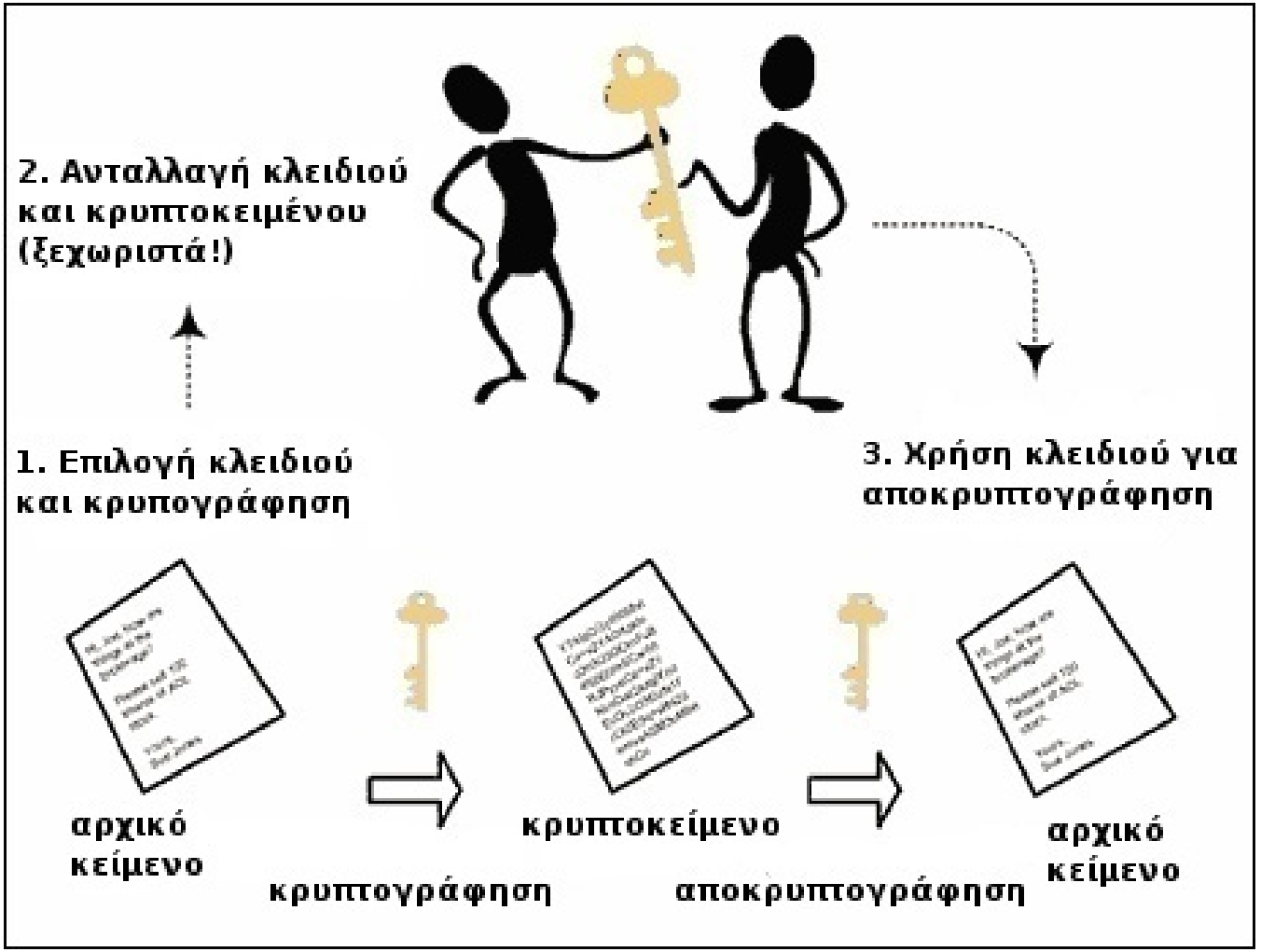
Κρυπτογραφία

Είδη Μοντέρνων Αλγορίθμων

- **Κρυφού κλειδιού (Secret Key Cryptography)**
  - Ένα μοναδικό κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση. (DES,AES,RC4)
- **Δημοσίου Κλειδιού (Public Key Cryptography)**
  - Ένα κλειδί (δημόσιο) για την κρυπτογράφηση και ένα άλλο (ιδιωτικό) για την αποκρυπτογράφηση. (RSA,D-H)
- **Κατακερματισμού (Hashes)**
  - Μετασχηματισμός σε μη αντιστρέψιμο (one-way) κρυπτοκείμενο. (MD5,SHA1)

Κρυπτογραφία

Χρήση κρυφού κλειδιού (SKC)

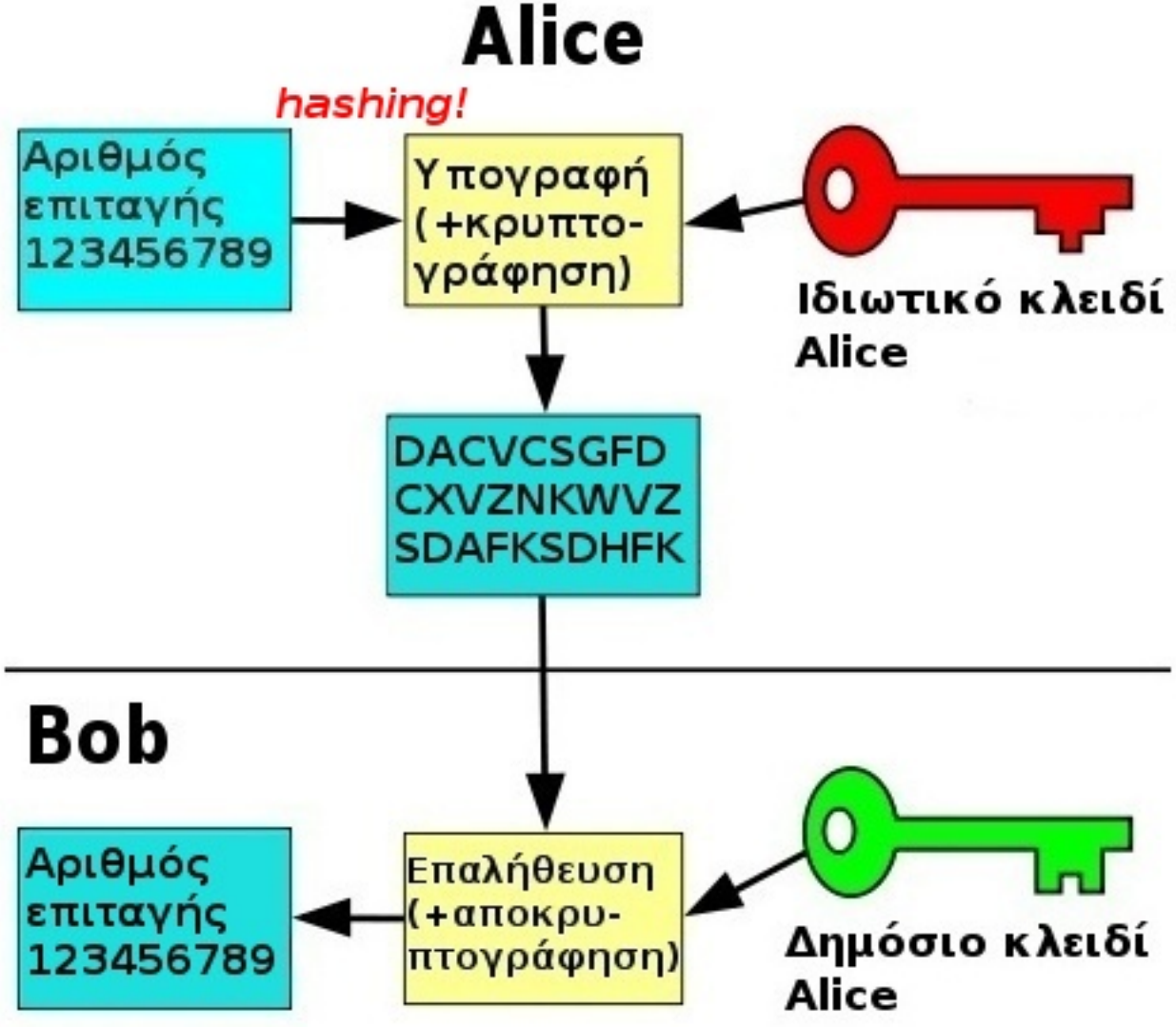


Κρυπτογραφία

Χρήση δημοσίου κλειδιού (PKC)

Κρυπτογραφία

Χρήση PKC για υπογραφή/πιστοποίηση



Κρυπτογραφία

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

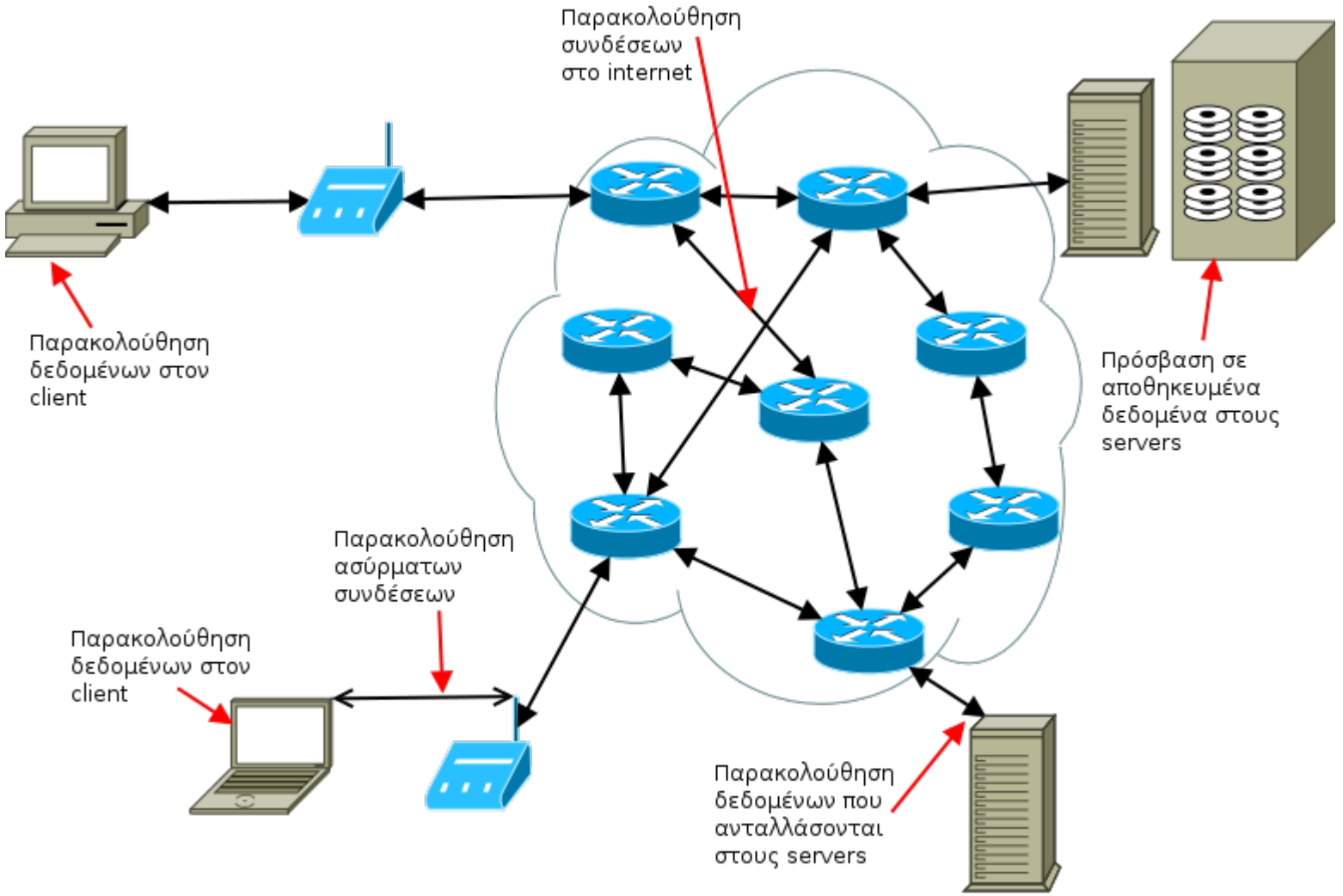
Κρυπτογραφία

Μοντέλα Εμπιστοσύνης

- **P**retty **G**ood **P**rivacy **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.

Freedom of Speech

Αυτή τη στιγμή στο Internet (Wild West)



Freedom of Speech

Κρυπτογράφηση συνδέσεων

- Web
- E-mail
- Instant Messaging

WEB (HTTP)

Η επικοινωνία (port 80) γίνεται χωρίς κρυπτογράφηση.
Διακρίνονται ευαίσθητα δεδομένα (π.χ. Usernames/Passwords)


```
0x0370:  312e 312e 7574 6d63 636e 3d28 6469 7265  1.1.utmccn=(dire
0x0380:  6374 297c 7574 6d63 7372 3d28 6469 7265  ct)|utmcsr=(dire
0x0390:  6374 297c 7574 6d63 6d64 3d28 6e6f 6e65  ct)|utmcmd=(none
0x03a0:  290d 0a43 6f6e 7465 6e74 2d54 7970 653a  )..Content-Type:
0x03b0:  2061 7070 6c69 6361 7469 6f6e 2f78 2d77  .application/x-w
0x03c0:  7777 2d66 6f72 6d2d 7572 6c65 6e63 6f64  ww-form-urlencod
0x03d0:  6564 0d0a 436f 6e74 656e 742d 4c65 6e67  ed..Content-Leng
0x03e0:  7468 3a20 3132 360d 0a0d 0a6c 6f67 3d6d  th:.126....log=m
0x03f0:  7975 7365 726e 616d 6526 7077 643d 6d79  yusername&pwd=my
0x0400:  7061 7373 776f 7264 2677 702d 7375 626d  password&wp-subm
0x0410:  6974 3d4c 6f67 2b49 6e26 7265 6469 7265  it=Log+In&redire
0x0420:  6374 5f74 6f3d 6874 7470 2533 4125 3246  ct_to=http%3A%2F
0x0430:  2532 4677 7777 2e76 6f69 642e 6772 2532  %2Fwww.void.gr%2
0x0440:  466b 6172 6769 6725 3246 626c 6f67 2532  Fkargig%2Fblog%2
0x0450:  4677 702d 6164 6d69 6e25 3246 2674 6573  Fwp-admin%2F&tes
0x0460:  7463 6f6f 6b69 653d 31                   tcookie=1
```

Freedom of Speech

HTTPS (HTTP Secure)

- Ο client ζητάει μια ασφαλή σύνδεση (port 443) από το server και αναφέρει τους αλγόριθμους που υποστηρίζει
- Ο server διαλέγει τον ισχυρότερο αλγόριθμο και ενημερώνει τον client
- Ο server στέλνει το ψηφιακό του πιστοποιητικό στον client (Όνομα, Υπογραφή από Certificate Authority, Δημόσιο Κλειδί)
- Ο client επιβεβαιώνει το πιστοποιητικό/υπογραφή με το τοπικά αποθηκευμένο δημόσιο κλειδί του Certificate Authority. Μπορεί να επικοινωνήσει με το CA για να επιβεβαιώσει πως δεν έχει ανακληθεί το πιστοποιητικό.
- Ο client δημιουργεί ένα τυχαίο αριθμό και τον κρυπτογραφεί με το δημόσιο κλειδί του server. Στέλνει τον αριθμό στον server.
- Ο server αποκρυπτογραφεί τον αριθμό αυτό με το ιδιωτικό του κλειδί και τον χρησιμοποιεί ως κλειδί κρυπτογράφησης για την αποστολή δεδομένων.

Freedom of Speech

WEB (HTTPS)

Όλα τα δεδομένα μεταδίδονται κρυπτογραφημένα.


```
0x02e0:  a631 d6e4 20ee 1a07 207c 7818 7107 633b  .1.......|x.q.c;
0x02f0:  c83a fadc dfc1 d5c5 45ee b4ea 310c 57fc  .:......E...1.W.
0x0300:  9e66 a442 d31a 9031 6869 1d94 9bef 8dac  .f.B...1hi......
0x0310:  659a 3813 0a6c ba32 5fbe 4521 61c5 bc90  e.8..l.2_.E!a...
0x0320:  540d bdba 63f7 d938 c496 256f 4d41 67de  T...c..8..%oMAg.
0x0330:  62e3 2efe 8331 4446 8f8e 5939 4d1d 79c0  b....1DF..Y9M.y.
0x0340:  a12f 2c76 59a1 9a04 4d2c 8ccd 4382 438e  ./,vY...M,..C.C.
0x0350:  8f9b 9ec2 583d d5fe 199d da2c fbf0 379e  ....X=.....,..7.
0x0360:  702a eeec ddb2 4d33 f42f eada b559 7404  p*....M3./...Yt.
0x0370:  029d 2cbb 7e8b d3c5 4dea 3d69 addb 3dbd  ..,.~...M.=i..=.
0x0380:  8dfb 6cea c8d3 3be3 f949 4296 7697 0da3  ..l...;..IB.v...
0x0390:  b848 f1a1 8efd 1d35 722b 2d2c 69b5 639d  .H.....5r+-,i.c.
0x03a0:  6ba1 282b 0403 2f6f 858d 9f21 88e7 046a  k.(+../o...!...j
0x03b0:  4372 432b 8b6d 4e06 6ffd 1b2c c02b 255e  CrC+.mN.o..,.+%^
0x03c0:  24fd cd60 fd9a e577 cafc 0507 247c dc90  $..`...w....$|..
0x03d0:  0509 0722 1ae5 8b4c 7034 7691 6c59 4bf9  ..."...Lp4v.lYK.
0x03e0:  abef b675 4e9d 15ca 7c48 8223            ...uN...|H.#
```

Freedom of Speech

HTTPS (HTTP Secure)

- Χρησιμοποιεί το Certificate Authority μοντέλο εμπιστοσύνης.
- Οι browsers προειδοποιούν αν κάποιο πιστοποιητικό δεν είναι έγκυρο.
  - Προσοχή στις ειδοποιήσεις! Διαβάστε προσεκτικά τα μυνήματα λάθους και μην τις αγνοείτε!
- Πρέπει πάντα να χρησιμοποιείται.
  - Webmail
  - E-banking
  - Οπουδήποτε δίνουμε προσωπικά δεδομένα (όνομα,διεύθυνση,κτλ)
  - Social Networking sites
- Χρήσιμα plugins: https://www.eff.org/https-everywhere by Electronic Frontier Foundation (*** διαγωνισμός μετάφρασης ***)
  - Χρησιμοποιεί αυτόματα HTTPS για γνωστά websites (Firefox,Chrome)

Προβλήματα του HTTPS

- Προστατεύει από ενδιάμεσους και όχι από όσους έχουν έλεγχο στον HTTPS Server.
- Δυσκολία στην χρήση client certificates για πιστοποίηση.
- Τι γίνεται αν κάποιος αλλάξει το πιστοποιητικό ενός server ?
- Τι γίνεται αν κάποιος ελέγχει ένα Certificate Authority και βγάλει ένα δεύτερο πιστοποιητικό με το ίδιο όνομα αλλά για ένα διαφορετικό server ?
- Πιθανή αντιμετώπιση σε επίπεδο HTTPS μέσω κατανεμημένων “συμβολαιογράφων” (notaries) που καταργούν την ανάγκη για Certificate Authorities.
  - Χρήσιμα plugins: http://convergence.io/ by Moxie Marlinspike
- Για το μέλλον: DNSSEC

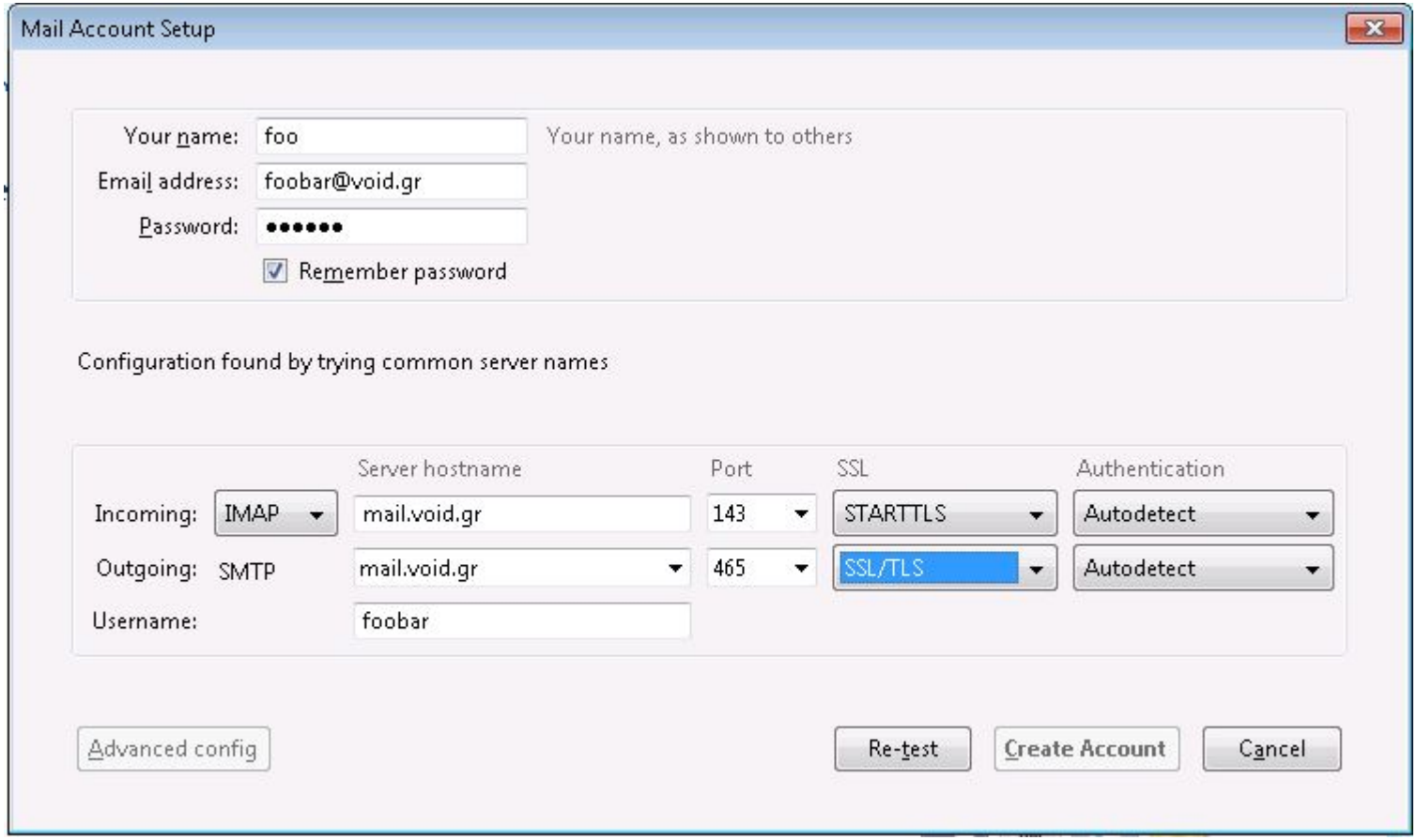
E-mail (SMTP/POP3/IMAP)

- Αν ο mail server το υποστηρίζει, προβάλει ένα υπογεγραμμένο πιστοποιητικό (αντίστοιχο με ότι συμβαίνει στο HTTPS)
- Συνήθεις πόρτες επικοινωνίας

Πρωτόκολλο / Μέθοδος Κρυπτογράφησης	*Καθόλου κρυπτογράφηση ή **STARTTLS***	***SSL***
SMTP	25	465
POP3	110	995
IMAP	143	993

- Συνήθεις επιλογές κρυπτογραφίας mail clients (προτείνομενα με *):
  - **Never**: Καμία κρυπτογράφηση
  - **TLS, if available**: Ίδια πόρτα, ο client ρωτάει αν ο server υποστηρίζει κρυπτογράφηση και αν όχι προχωράει χωρίς.
  - **STARTTLS**: Ίδια πόρτα, ο client ρωτάει αν ο server υποστηρίζει κρυποτογράφηση και αν όχι δεν συνδέεται. (*)
  - **SSL**: Διαφορετική πόρτα, υποχρεωτική κρυπτογράφηση (*)

Ρυθμίσεις Thunderbird



Instant Messaging

- Το **MSN Messenger/Yahoo! Messenger** ΔΕΝ υποστηρίζουν κρυπτογράφηση των connections. **ΑΠΟΦΥΓΕΤΕ ΤΑ**!

```
▽ MSN Messenger Service
    MSG 31 A 206\r\n
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    User-Agent: pidgin/2.7.3\r\n
    X-MMS-IM-Format: FN=Segoe%20UI; EF=; CO=0; PF=0; RL=0\r\n
    \r\n
    omg my passwords are cleartext!
```

```
0000  00 1d 1c 01 57 f5 00 22  41 1e d8 06 08 00 45 00   ....W.." A.....E.
0010  01 10 a4 2f 40 00 40 06  56 10 c0 a8 01 5f 40 04   .../@.@. V...._@.
0020  3d 9d 96 21 07 47 d5 ab  37 45 18 33 01 a7 80 18   =..!.G.. 7E.3....
0030  be 5a 40 ab 00 00 01 01  08 0a 09 65 26 fa 13 ce   .Z@..... ...e&...
0040  81 9b 4d 53 47 20 33 31  20 41 20 32 30 36 0d 0a   ..MSG 31  A 206..
0050  4d 49 4d 45 2d 56 65 72  73 69 6f 6e 3a 20 31 2e   MIME-Ver sion: 1.
0060  30 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   0..Conte nt-Type:
0070  20 74 65 78 74 2f 70 6c  61 69 6e 3b 20 63 68 61    text/pl ain; cha
0080  72 73 65 74 3d 55 54 46  2d 38 0d 0a 55 73 65 72   rset=UTF -8..User
0090  2d 41 67 65 6e 74 3a 20  70 69 64 67 69 6e 2f 32   -Agent:  pidgin/2
00a0  2e 37 2e 33 0d 0a 58 2d  4d 4d 53 2d 49 4d 2d 46   .7.3..X- MMS-IM-F
00b0  6f 72 6d 61 74 3a 20 46  4e 3d 53 65 67 6f 65 25   ormat: F N=Segoe%
00c0  32 30 55 49 3b 20 45 46  3d 3b 20 43 4f 3d 30 3b   20UI; EF =; CO=0;
00d0  20 50 46 3d 30 3b 20 52  4c 3d 30 0d 0a 0d 0a 6f    PF=0; R L=0....o
00e0  6d 67 20 6d 79 20 70 61  73 73 77 6f 72 64 73 20   mg my pa sswords
00f0  61 72 65 20 63 6c 65 61  72 74 65 78 74 21 20 09   are clea rtext! .
```

Freedom of Speech

Instant Messaging

- **Αποφύγετε** το **Skype** για ευαίσθητες επικοινωνίες. Έχει κρυπτογράφηση άλλα όχι ανοιχτών προτύπων.
  - Δεν γνωρίζουμε ποιος έχει πρόσβαση στα πρωτόκολλα κρυπτογράφησης άρα και ποιός/πώς μπορεί να αποκρυπτογραφήσει τις συνομιλίες.
- **Αποφύγετε** platforms που γίνεται **server-side logging** των επικοινωνιών (πχ Facebook).
  - Google Talk* → Gmail→Settings→Chat→Never Save Chat History
- Προτιμήστε IM platforms που υποστηρίζουν το πρωτόκολλο **XMPP** (Jabber, Google Talk*). Open source/Open Standards.

Freedom of Speech

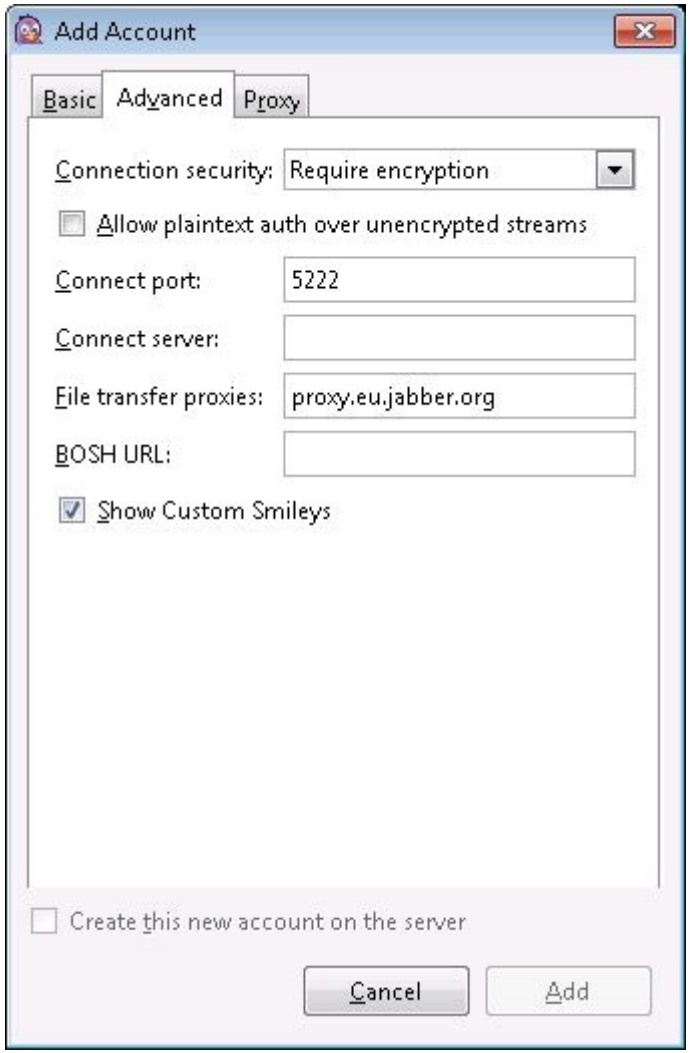
Instant Messaging

- Προτείνονται **open source clients**
  - Pidgin (Linux, BSD, Windows, OS X, κ.α)
  - Empathy (Linux, BSD)
  - Miranda IM (Windows)
  - Adium (OS X)
- Για group chatting το **IRC** μπορεί ακόμα να είναι πολύ χρήσιμο (χρήση encryption plugins)!
- Η πλατφόρμα **SILC** θεωρείται γενικά ασφαλής αλλά θέλει προσοχή γιατί έχει και αυτή ευπάθειες.

Freedom of Speech

Ρυθμίσεις Pidgin για Google Talk/Jabber

- Connection Security:
  - Require Encryption
  - ~~Use encryption if available~~
  - Use old-style SSL
    (different port: 5223)



Freedom of Speech

Διάλειμμα

Freedom of Speech

Κρυπτογράφηση περιεχομένου

- E-MAIL
- Instant Messaging

Κρυπτογράφηση E-mail

2 βασικοί τρόποι:

- S/MIME
  - Στηρίζεται στο Certification Authority μοντέλο εμπιστοσύνης μεταξύ χρηστών/υπηρεσιών.
- PGP
  - Στηρίζεται στο (δικό του) PGP μοντέλο εμπιστοσύνης μεταξύ χρηστών.

Freedom of Speech

Κρυπτογράφηση E-mail με S/MIME

- **S**ecure/**M**ultipurpose **I**nternet **M**ail **E**xtensions
- Ο χρήστης απευθύνεται σε μια υπηρεσία παροχής πιστοποιητικών που του εκδίδει ένα στη διεύθυνση/ονομά του.
  - Class 1: επιβεβαίωση From-address
  - Class 2: επιβεβαίωση πραγματικού ονόματος/εταρίας
- Υπηρεσίες δωρεάν παροχής class 1 προσωπικών πιστοποιητικών:
  - Comodo: https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate
  - StartSSL: https://www.startssl.com/?app=12
  - Cacert: http://www.cacert.org/

Freedom of Speech

Κρυπτογράφηση E-mail με S/MIME

- Αν ο χρήστης Α δεν έχει ήδη το δημόσιο κλειδί του Β το αναζητεί σε ειδικές μηχανές αναζήτησης.
- Ο χρήστης Α κρυπτογραφεί το e-mail με το δημόσιο κλειδί του Β. Ο Α υπογράφει το e-mail με το ιδιωτικό του κλειδί.
- Ο Β αποκρυπτογραφεί το e-mail με το ιδιωτικό του κλειδί και επιβεβαιώνει την υπογραφή του Α μέσω του CA.

Χρήση S/MIME με Thunderbird

- Export Certificate από τον Browser (πχ Firefox)
  - Tools → Options → Advanced → Encryption → View Certificates → Your Certificates → Backup (και δίνουμε ένα καλό password)
- Θέτουμε Master Password (στον Thunderbird)
  - Tools → Options → Security → Passwords → Use Master Password
- Εισαγωγή του exported certificate
  - Tools → Options → Advanced Certificates → View certificates → Import
- Χρήση του certificate
  - Tools → Account Settings → (επιλογή account) → Security → Digital Signing/Encryption (επιλογή certificate)

Freedom of Speech

Pretty Good Privacy (PGP)

- **Δημιουργία**: Phil Zimmerman (ακτιβιστής ενάντια στα πυρηνικά) 1991
  - Σκοπός: να ανταλλάσουν ασφαλή μυνήματα 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 1st Amendment (Freedom of Speech) άρα ήταν νόμιμο.
- **Εταιρία**: Viacrypt/PGP 1996
- **Προτυποποίηση**: OpenPGP 1997
  - Free Software Foundation → GnuPG (GPG) 1999

Freedom of Speech

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!***

Χρήση PGP

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

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
```

Freedom of Speech

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 χρήστων:

- gpg --list-keys

Freedom of Speech

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

Freedom of Speech

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
```

Freedom of Speech

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 *
```

Freedom of Speech

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

Freedom of Speech

Χρήση PGP μέσω enigmail

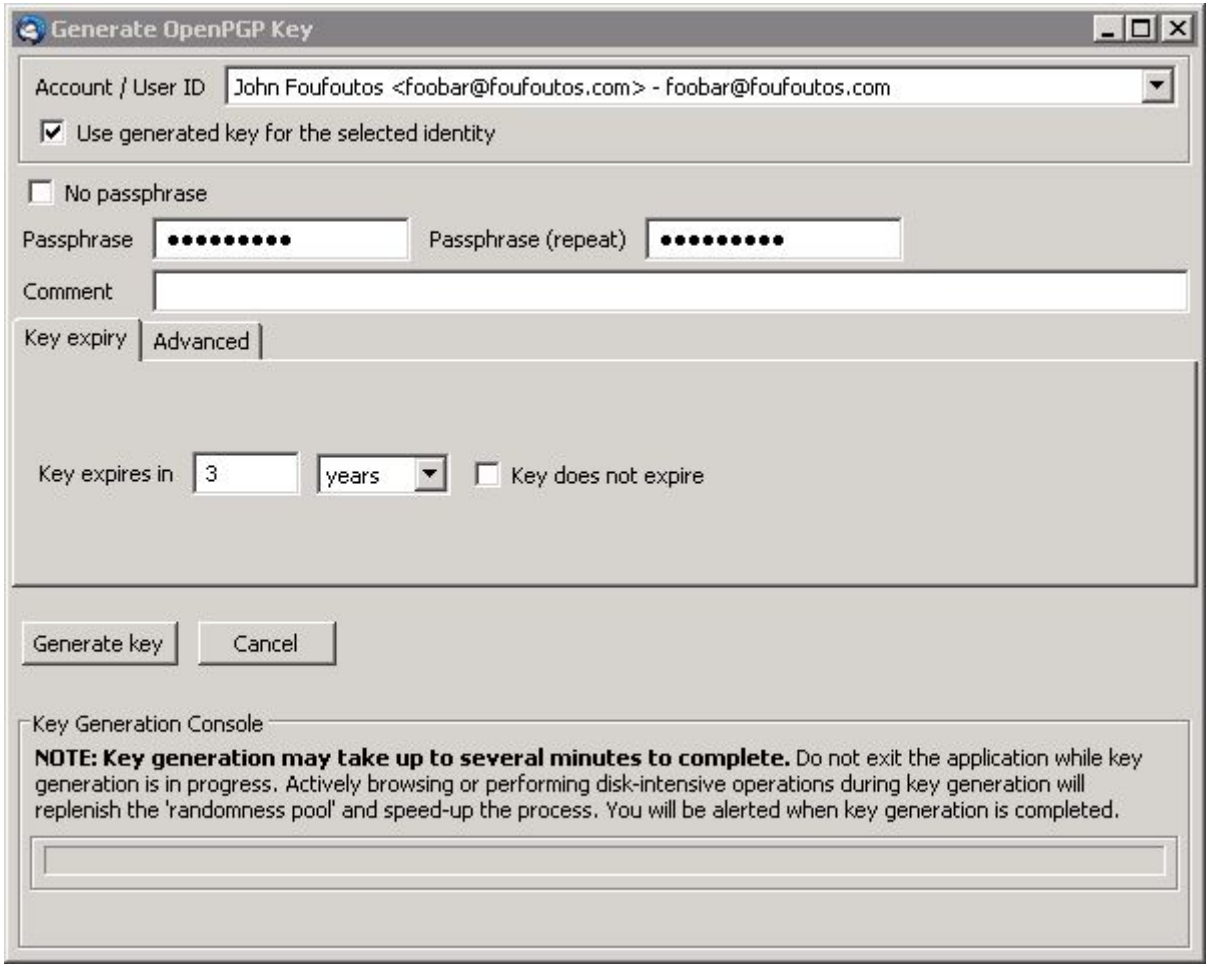
- Extension για **Thunderbird**
- Τρέχει σε **Windows/Linux/BSD/Mac OS X**
- Σε Linux/BSD/Mac OS X απαιτείται η εγκατάσταση του **gpg**
- Σε windows απαιτείται η εγκατάσταση του πακέτου **gpg4win**: http://www.gpg4win.org/
- Εγκατάσταση του Enigmail στο Thunderbird μέσω:

  Tools → Add-ons → (search) Enigmail
- Σε κάποιες διανομές Linux υπάρχει σε πακέτο: enigmail

Freedom of Speech

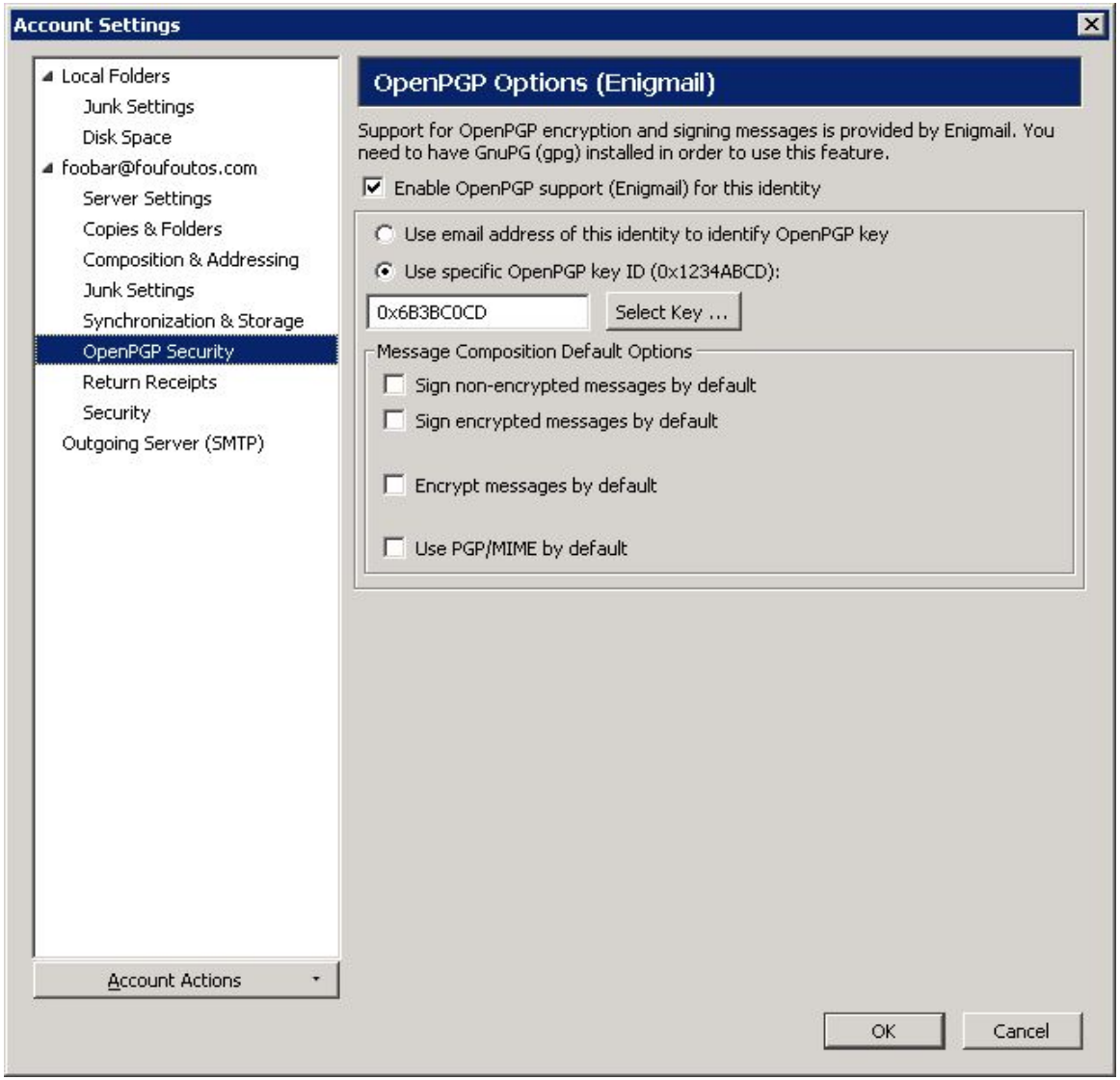
Χρήση PGP μέσω enigmail

Δημιουργία νέου κλειδίου:
OpenGPG → Key Management → Generate → New keypair



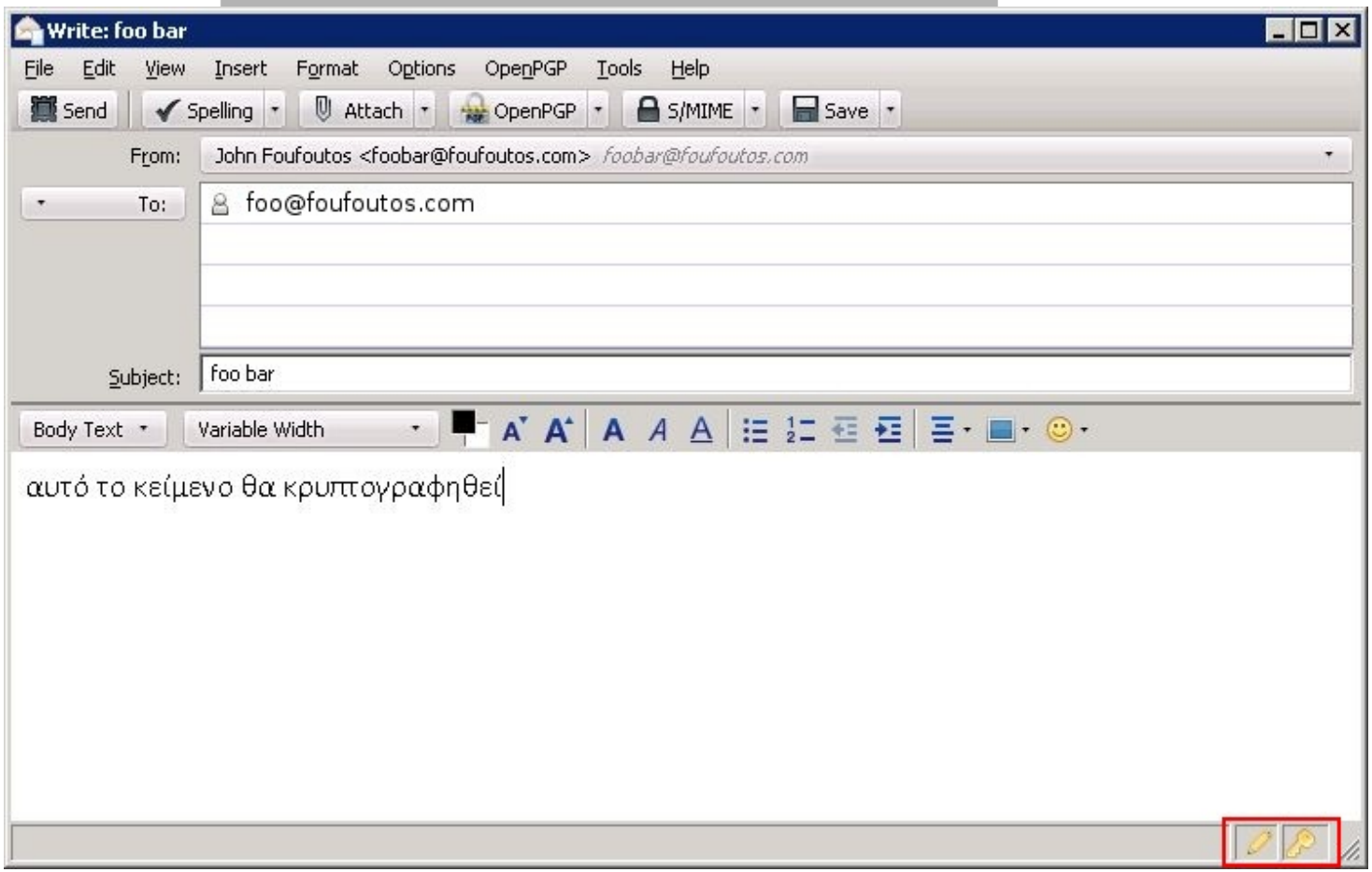
Χρήση PGP μέσω enigmail

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



Χρήση PGP μέσω enigmail

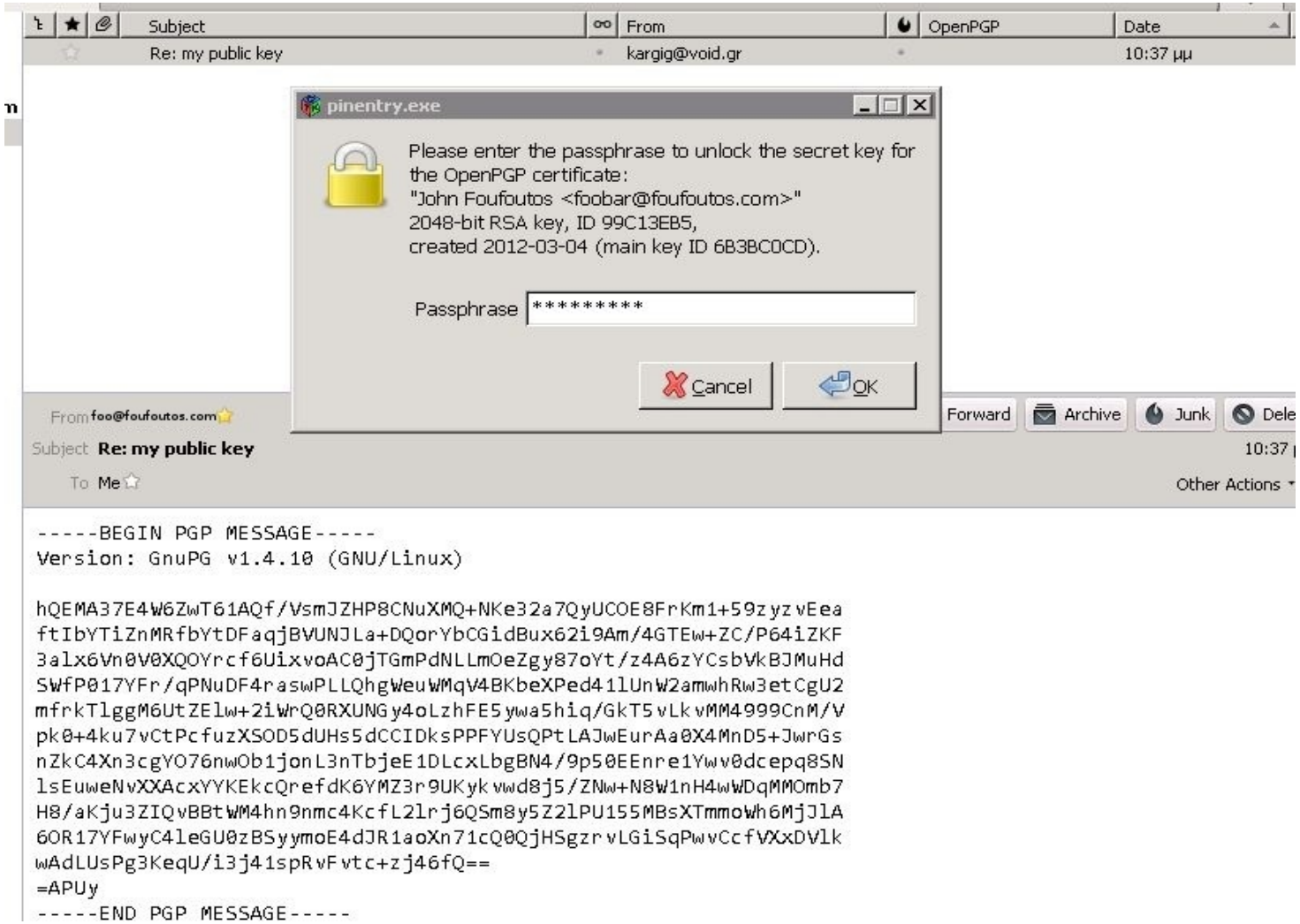
Νέο E-mail:
OpenPGP → Sign/Encrypt Message



Freedom of Speech

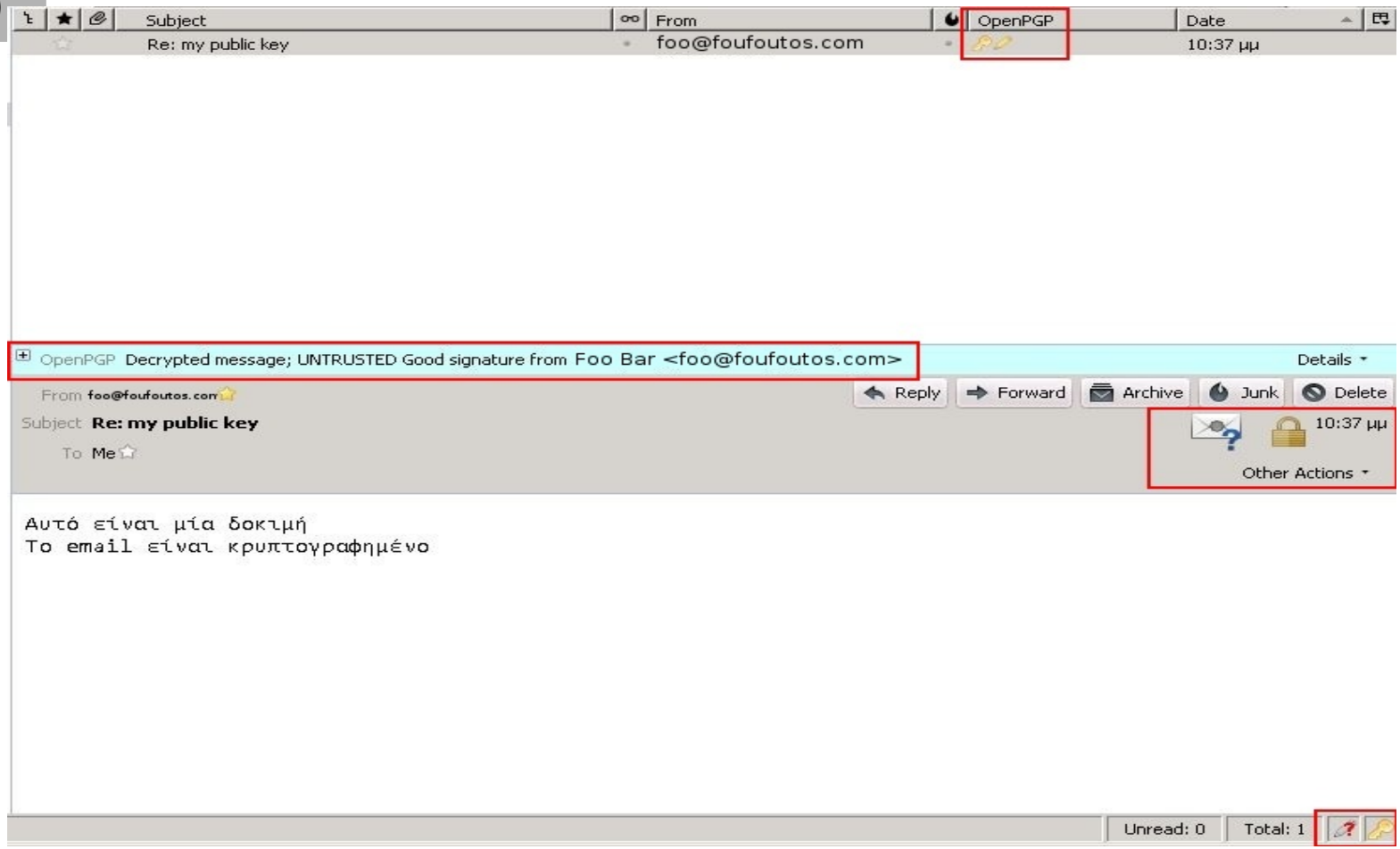
Χρήση PGP μέσω enigmail

Εισερχόμενο E-mail:
(πριν την αποκρυπτογράφηση)



Χρήση PGP μέσω enigmail

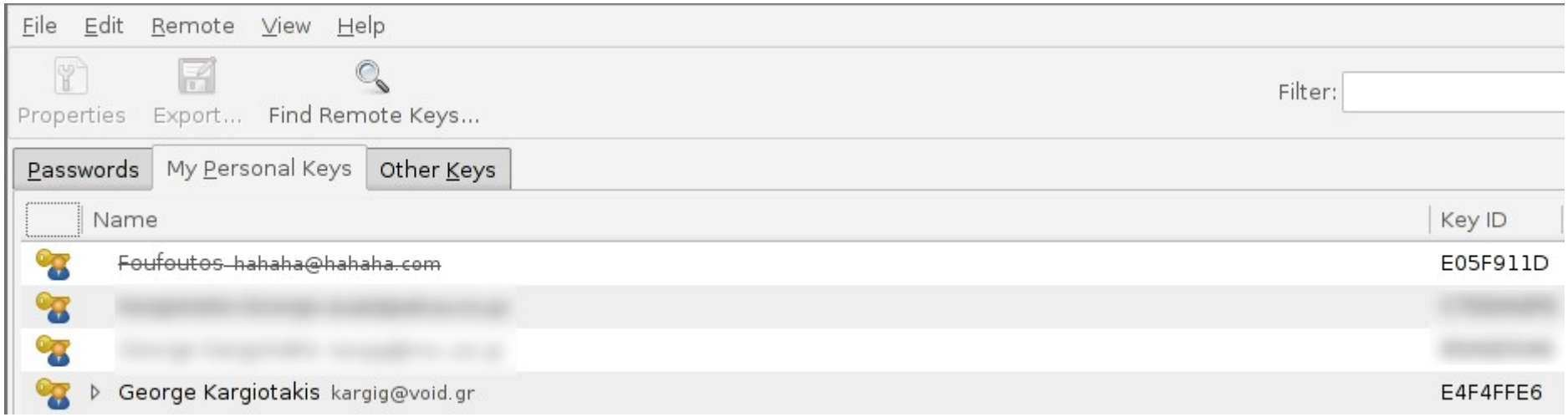
Εισερχόμενο E-mail:
(μετά την αποκρυπτογράφηση)



Seahorse (Linux)

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

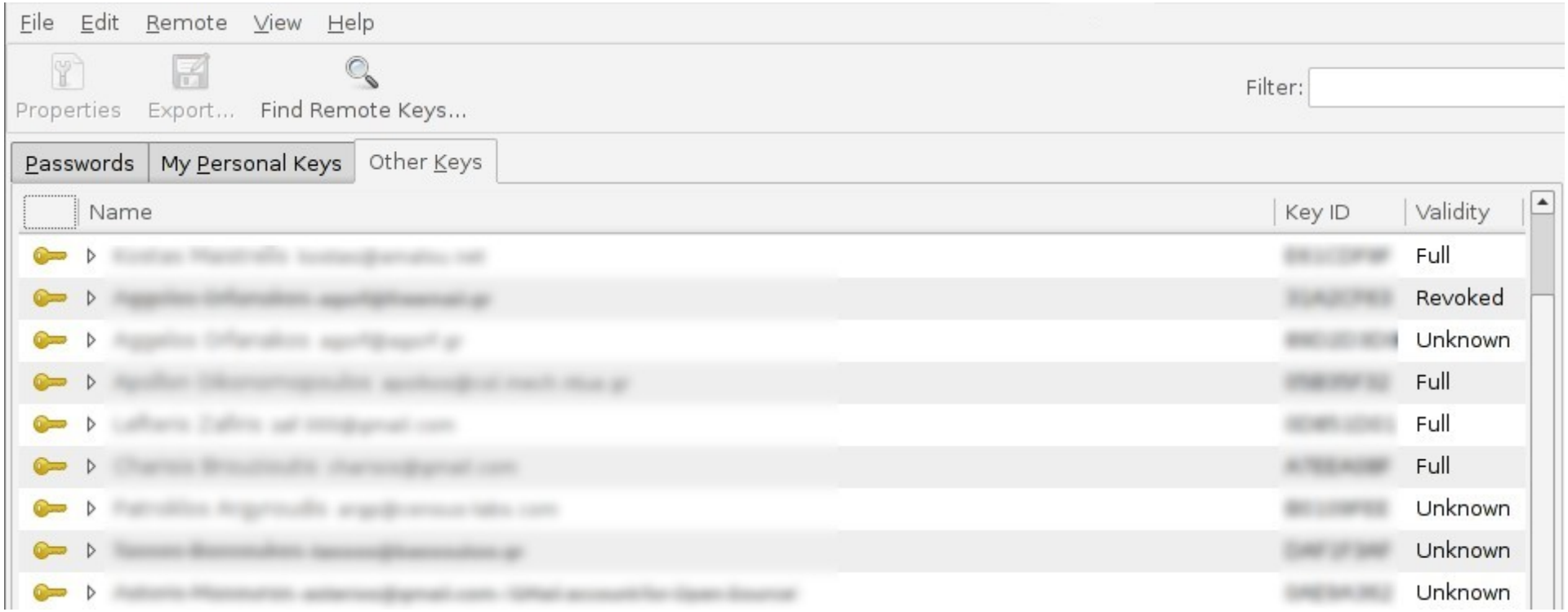
Προσωπικά κλειδιά



Freedom of Speech

Seahorse

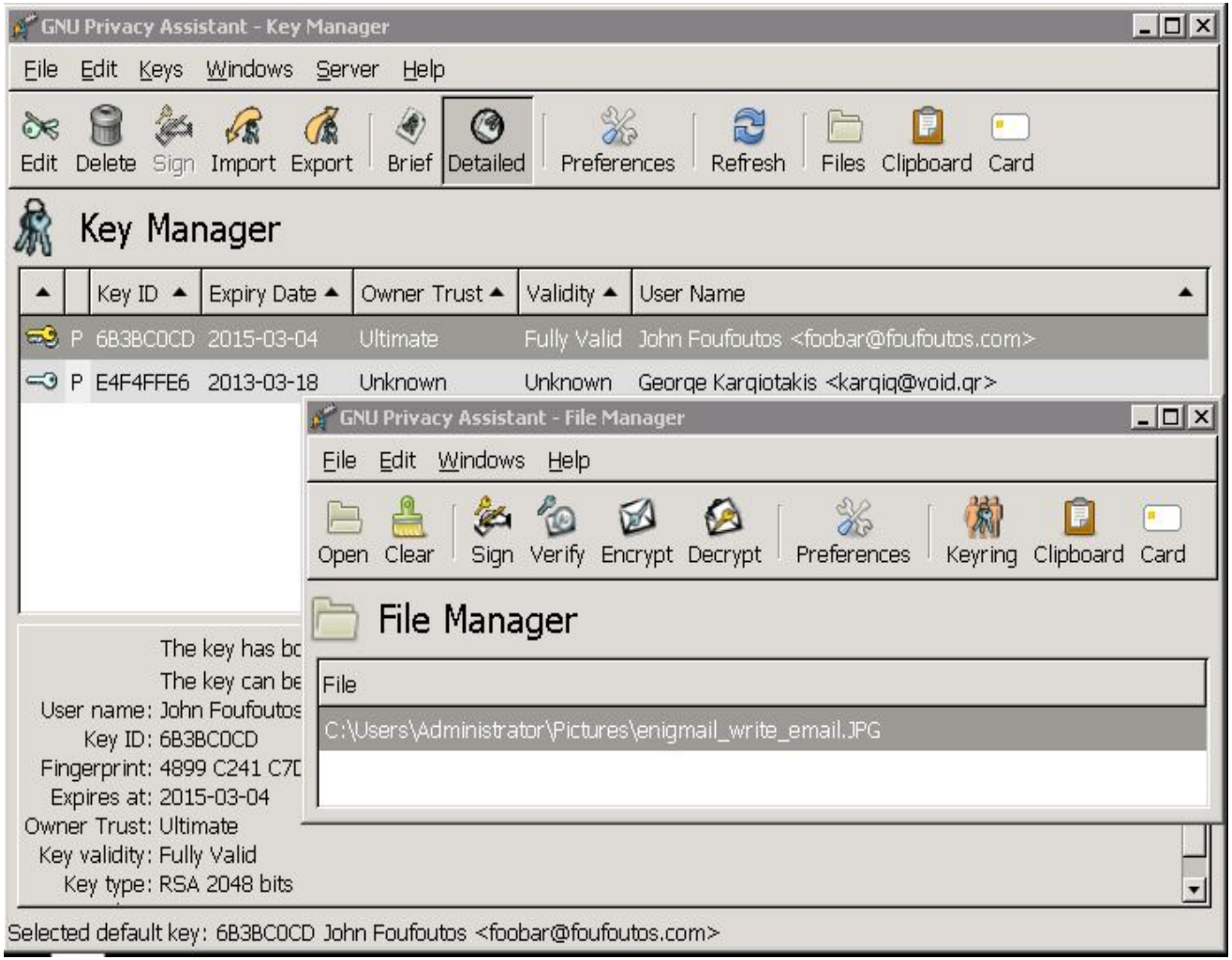
Κλειδιά τρίτων



Freedom of Speech

GNU Privacy Assistant (Linux/Windows)

- Διαχείριση Κλειδιών / υπογραφών
- Κρυπτογράφηση αρχείων
- Κρυπτογράφηση Clipboard



Freedom of Speech

Off-The-Record Messaging

- Plugin για IM (Pidgin, Adium)
- Κρυπτογραφεί το περιεχόμενο των ομιλιών σε IM μέσω εφήμερων κλειδιών
- Ιδιότητες:
  - Κρυπτογράφηση των περιεχομένων
  - Αυθεντικοποίηση χρηστών - την ώρα της συνομιλίας
  - (*) Διαψευσιμότητα – Τα μυνήματα δεν είναι υπογεγραμμένα
  - (*) Perfect Forward Secrecy – Αν υποκλαπεί ένα ιδιωτικό κλειδί στο μέλλον, δεν μπορούν να αποκρυπτογραφηθούν προηγούμενες συνομιλίες

Off-The-Record Messaging

Χωρίς OTR

```
▽ MSN Messenger Service
    MSG The_user12@hotmail.com \316\244\316\266\316\257\317\204\316\266\316\
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    User-Agent: pidgin/2.10.0\r\n
    X-MMS-IM-Format: FN=Lucida%20Grande; EF=; CO=0; PF=0; RL=0\r\n
    \r\n
    to password einai 123456
```

```
0000  00 22 41 1e d8 06 00 1d  1c 01 57 f5 08 00 45 38   ."A..... ..W...E8
0010  01 0c 50 05 40 00 71 06  aa 8c cf 2e 7c ec c0 a8   ..P.@.q. ....|...
0020  01 5f 07 47 cf 63 dd 9d  63 19 71 57 fc 31 80 18   ._.G.c.. c.qW.1..
0030  fa 31 57 bf 00 00 01 01  08 0a 17 a9 ce b7 0e d6   .1W..... ........
0040  0a 7a 4d 53 47 20 65 6d  6f 75 7a 65 6c 69 40 68   .zMSG Th e_user12@h
0050  6f 74 6d 61 69 6c 2e 63  6f 6d 20 ce a4 ce b6 ce   otmail.c om .....
0060  af cf 84 ce b6 ce b9 20  31 37 33 0d 0a 4d 49 4d   .......  173..MIM
0070  45 2d 56 65 72 73 69 6f  6e 3a 20 31 2e 30 0d 0a   E-Versio n: 1.0..
0080  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 74 65   Content- Type: te
0090  78 74 2f 70 6c 61 69 6e  3b 20 63 68 61 72 73 65   xt/plain ; charse
00a0  74 3d 55 54 46 2d 38 0d  0a 55 73 65 72 2d 41 67   t=UTF-8. .User-Ag
00b0  65 6e 74 3a 20 70 69 64  67 69 6e 2f 32 2e 31 30   ent: pid gin/2.10
00c0  2e 30 0d 0a 58 2d 4d 4d  53 2d 49 4d 2d 46 6f 72   .0..X-MM S-IM-For
00d0  6d 61 74 3a 20 46 4e 3d  4c 75 63 69 64 61 25 32   mat: FN= Lucida%2
00e0  30 47 72 61 6e 64 65 3b  20 45 46 3d 3b 20 43 4f   0Grande;  EF=; CO
00f0  3d 30 3b 20 50 46 3d 30  3b 20 52 4c 3d 30 0d 0a   =0; PF=0 ; RL=0..
0100  0d 0a 74 6f 20 70 61 73  73 77 6f 72 64 20 65 69   ..to pas sword ei
0110  6e 61 69 20 31 32 33 34  35 36                     nai 1234 56
```

Off-The-Record Messaging

Με OTR

```
MSN Messenger Service
    MSG The_user12@hotmail.com \316\244\316\266\316\257\317\204\316\266\316\271
    MIME-Version: 1.0\r\n
    Content-Type: text/plain; charset=UTF-8\r\n
    User-Agent: pidgin/2.10.0\r\n
    X-MMS-IM-Format: FN=Segoe%20UI; EF=; CO=0; PF=0; RL=0\r\n
    \r\n
    [truncated] ?OTR:AAIDAAAAAAEAAAACAAAAwD3eubEz2J45xoGERx0hJedTbcemMlVd+uLD
```

```
0000  00 22 41 1e d8 06 00 1d  1c 01 57 f5 08 00 45 38   ."A..... ..W...E8
0010  02 85 5b 46 40 00 72 06  6b 4c 40 04 3d 9d c0 a8   ..[F@.r. kL@.=...
0020  01 5f 07 47 bd 8b e0 1e  33 12 fa 13 5b 3d 80 18   ._.G.... 3...[=..
0030  fa c3 47 2d 00 00 01 01  08 0a 17 98 bb eb 0e d6   ..G-.... ........
0040  9d 47 4d 53 47 20 65 6d  6f 75 7a 65 6c 69 40 68   .GMSG Th e_user12@h
0050  6f 74 6d 61 69 6c 2e 63  6f 6d 20 ce a4 ce b6 ce   otmail.c om .....
0060  af cf 84 ce b6 ce b9 20  35 35 30 0d 0a 4d 49 4d   ....... 550..MIM
0070  45 2d 56 65 72 73 69 6f  6e 3a 20 31 2e 30 0d 0a   E-Versio n: 1.0..
0080  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 74 65   Content- Type: te
0090  78 74 2f 70 6c 61 69 6e  3b 20 63 68 61 72 73 65   xt/plain ; charse
00a0  74 3d 55 54 46 2d 38 0d  0a 55 73 65 72 2d 41 67   t=UTF-8. .User-Ag
00b0  65 6e 74 3a 20 70 69 64  67 69 6e 2f 32 2e 31 30   ent: pid gin/2.10
00c0  2e 30 0d 0a 58 2d 4d 4d  53 2d 49 4d 2d 46 6f 72   .0..X-MM S-IM-For
00d0  6d 61 74 3a 20 46 4e 3d  53 65 67 6f 65 25 32 30   mat: FN= Segoe%20
00e0  55 49 3b 20 45 46 3d 3b  20 43 4f 3d 30 3b 20 50   UI; EF=;  CO=0; P
00f0  46 3d 30 3b 20 52 4c 3d  30 0d 0a 0d 0a 3f 4f 54   F=0; RL= 0....?OT
0100  52 3a 41 41 49 44 41 41  41 41 41 41 45 41 41 41   R:AAIDAA AAAAEAAA
0110  41 43 41 41 41 41 77 44  33 65 75 62 45 7a 32 4a   ACAAAAwD 3eubEz2J
0120  34 35 78 6f 47 45 52 78  30 68 4a 65 64 54 62 63   45xoGERx 0hJedTbc
0130  65 6d 4d 6c 56 64 2b 75  4c 44 6f 65 4f 58 71 5a   emMlVd+u LDoeOXqZ
0140  4e 43 4a 74 77 55 54 52  74 72 5a 2b 49 73 41 46   NCJtwUTR trZ+IsAF
0150  58 75 7a 2b 47 54 79 54  49 51 4f 38 6a 55 69 4a   Xuz+GTyT IQO8jUiJ
0160  33 4e 33 46 67 30 66 33  7a 44 77 49 49 75 62 6b   3N3Fg0f3 zDwIIubk
0170  4f 5a 67 34 5a 51 41 68  57 50 51 4b 51 42 6b 4f   OZg4ZQAh WPQKQBkO
0180  74 58 6b 62 53 48 72 72  61 43 6c 57 32 68 46 47   tXkbSHrr aClW2hFG
0190  71 6d 65 37 36 2f 54 54  45 70 5a 50 6a 68 37 7a   qme76/TT EpZPjh7z
```

Freedom of Speech

Κέρδη κρυπτογράφησης επικοινωνιών

- Προστασία δική μας!
- Προστασία όσων το έχουν πραγματική ανάγκη!

Διαγωνισμός Μετάφρασης HTTPS-Everywhere

Κερδίστε ένα T-shirt από το EFF.org

- Δημιουργήστε ένα νέο PGP κλειδί (*) και ανεβάστε το σε ένα keyserver.
- Στείλτε ένα κρυπτογραφημένο και υπογεγραμμένο email στο kargig@void.gr που θα έχει το public key σας ως attachment ζητώντας τα αρχεία προς μετάφραση.
- Θα σας αποσταλούν links προς τα αρχεία με κρυπτογραφημένο και υπογεγραμμένο email.
- Αποκρυπτογραφήστε το, μεταφράστε τα αρχεία στα Ελληνικά και στείλτε πίσω τις απαντήσεις.
- Ο πρώτος που θα στείλει “σωστές” μετάφρασεις κερδίζει. (το email του νικητή θα αναρτηθεί στο wiki)
- Παραλαβή στην επόμενη παρουσίαση.

* Όσοι ήδη έχουν PGP κλειδί θα έχουν λίγο πιο δύσκολο έργο ;)

Freedom of Speech

Βιβλία

Ιστορικά:

- *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Simon Singh)

Τεχνικά:

- *Practical Cryptography* (Niels Ferguson,Bruce Schneier)
- *Handbook of Applied Cryptography* (A. J. Menezes, P. C. van Oorschot, S. A. Vanstone)

Μυθιστόρημα:

- *Cryptonomicon* (Neal Stephenson)

Freedom of Speech

Ευχαριστίες

- **hackerspace.gr**
- **dln.gr**
- **Όσοι έστειλαν ιδέες**
- **Όσοι επικοινώνησαν μαζί μου για να βοήθησουν :)**

- **EFF**

Freedom of Speech

Ερωτήσεις / Συζήτηση