GPG & ΚΡΥΠΤΟΓΡΑΦΙΑ

Κ. Καραντίας, Δ. Ζήνδρος

Επιμέλεια διαφανειών: Π. Αγγελάτος

Στόχος της ώρας

- Έννοιες στην ασύμμετρη κρυπτογραφία
- GPG
- Κρυπτογράφηση & αποκρυπτογράφηση μηνυμάτων
- Ψηφιακές υπογραφές & επιβεβαίωση
- Web-of-trust & υπογραφή κλειδιών

Όσο ξεκινάμε...

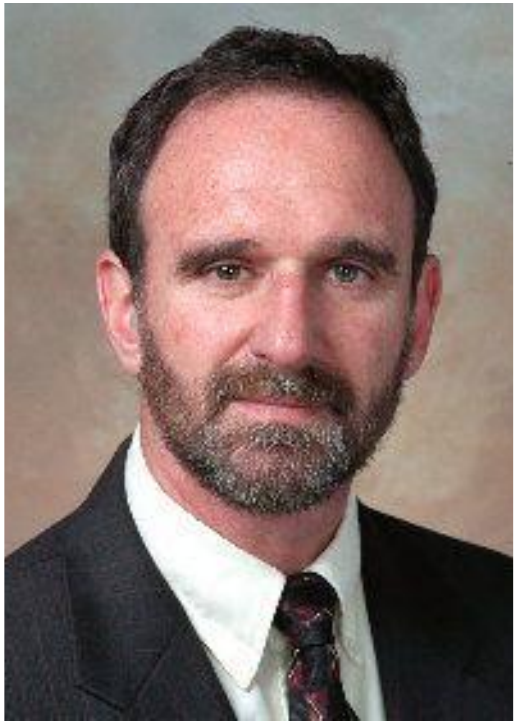
- Κατεβάστε το GPG για το σύστημά σας:
  - Αν έχετε Linux, το έχετε ήδη
  - Αν έχετε Windows, Gpg4win:
    - http://gpg4win.org/
  - Αν έχετε Mac, GPG Suite:
    - https://gpgtools.org/
- Εγκαταστήστε το

Ασύμμετρη κρυπτογραφία

- Diffie & Hellman, 1976
- RSA – Rivest, Shamir, Adleman, 1977
- Κάθε άνθρωπος έχει ένα **ζεύγος κλειδιών**:
  - Ιδιωτικό κλειδί & Δημόσιο κλειδί
  - Τα κλειδιά συνδέονται μαθηματικά
  - Για κάθε ιδιωτικό κλειδί υπάρχει μοναδικό δημόσιο
  - Για κάθε δημόσιο κλειδί υπάρχει μοναδικό ιδιωτικό
  - Από το ιδιωτικό μπορούμε να βρούμε το δημόσιο
  - Από το δημόσιο δεν μπορούμε να βρούμε το ιδιωτικό

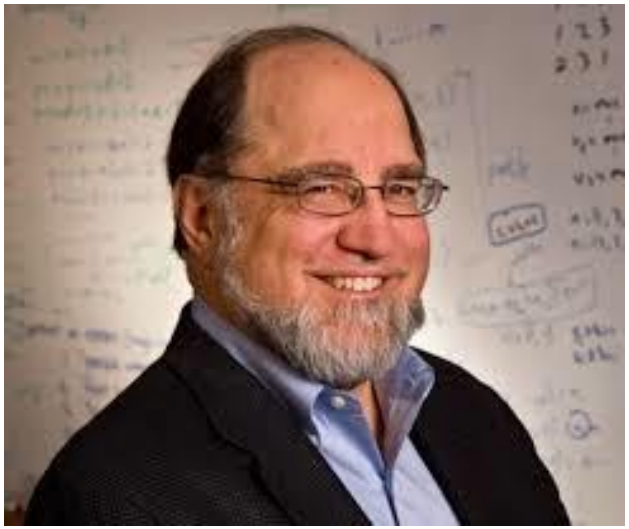
Diffie & Hellman

Whitfield Diffie

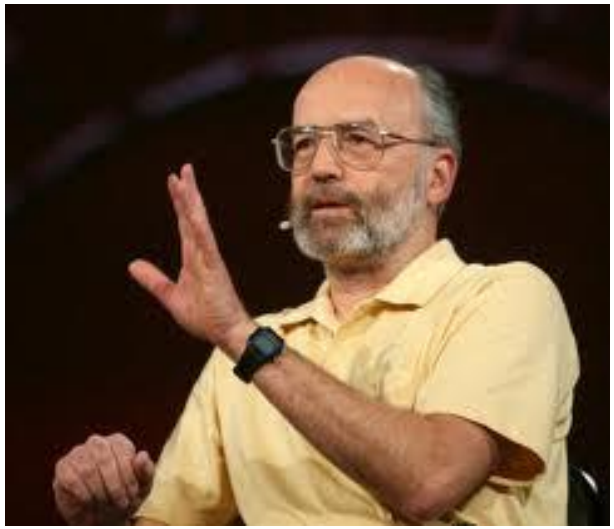


Martin Hellman

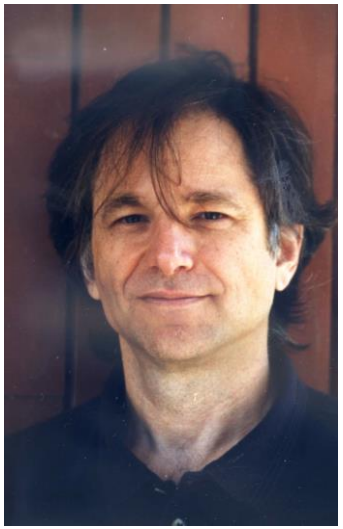
RSA



Ron Rivest



Adi Shamir



Leonard Adleman

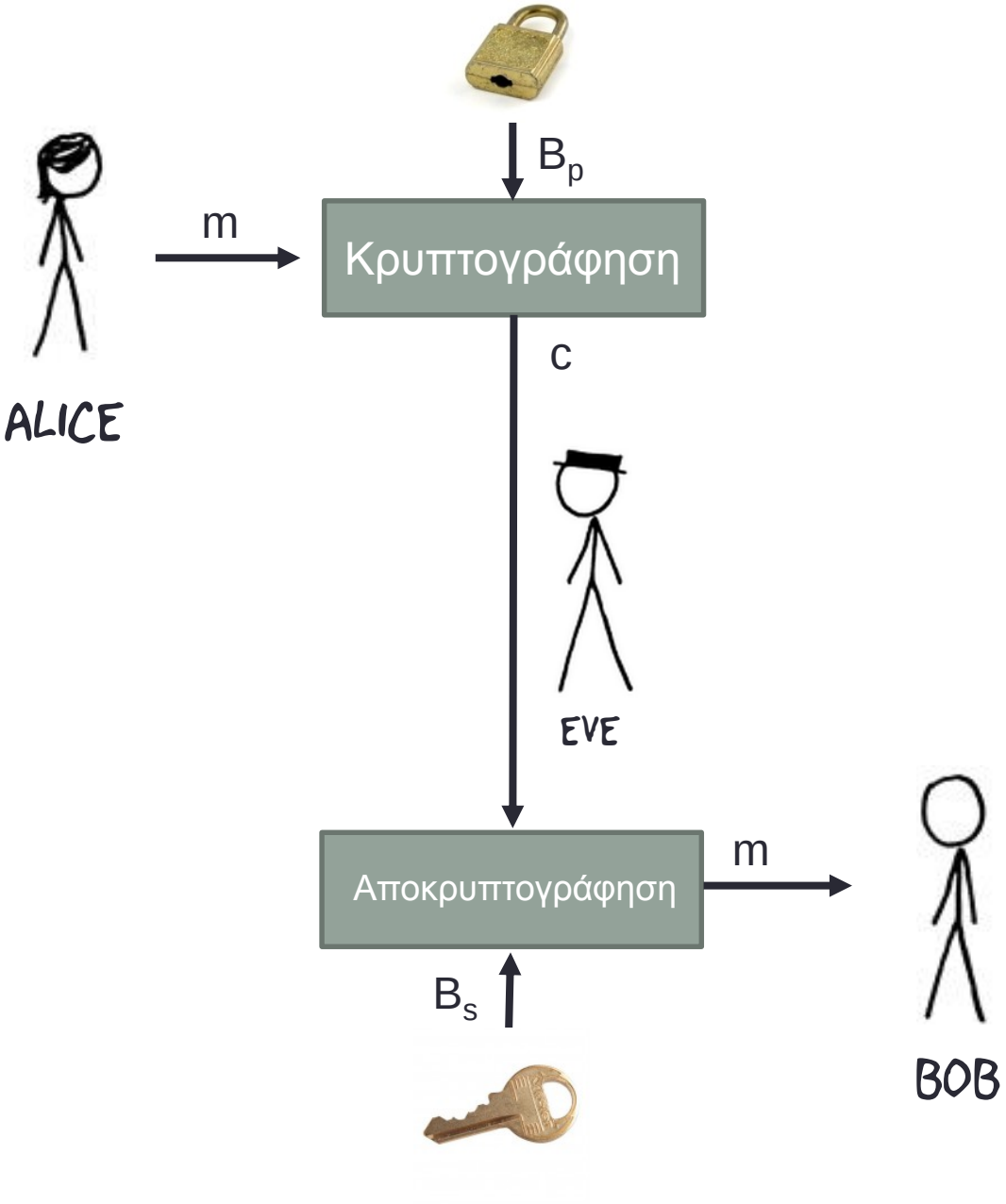
Ασύμμετρη κρυπτογραφία

- Αρχή λειτουργίας:
  - Ό,τι κρυπτογραφείται με το δημόσιο κλειδί κάποιου, αποκρυπτογραφείται από το αντίστοιχο ιδιωτικό του.
  - Ό,τι κρυπτογραφείται με το ιδιωτικό κλειδί κάποιου, αποκρυπτογραφείται από το αντίστοιχο δημόσιο του.

Ασύμμετρη κρυπτογραφία

- Η Alice θέλει να στείλει ένα μήνυμα στον Bob
- Δεν θέλει να το διαβάσουν άλλοι
- Ο καθένας έχει το ιδιωτικό και δημόσιο κλειδί του
- Η Alice κρυπογραφεί το μήνυμά της **με το δημόσιο κλειδί του Bob**
- Στέλνει στο δίκτυο το κρυπτογραφημένο κείμενο
- Ο Bob λαμβάνει το κρυπτογραφημένο κείμενο
- Ο Bob αποκρυπτογραφεί το κρυπτογραφημένο κείμενο **με το ιδιωτικό κλειδί του**
- Λαμβάνει το αρχικό κείμενο

- A_s
  - Alice's secret – μυστικό κλειδί
- A_p
  - Alice's public – δημόσιο κλειδί
- B_s
  - Bob's secret – μυστικό κλειδί
- B_p
  - Bob's public – δημόσιο κλειδί
- $c = E(B_p, m)$
  - encrypt – κρυπτογράφηση m με κλειδί B_p
  - δίνει ως αποτέλεσμα κρυπτοκείμενο c
- $m = D(B_s, c)$
  - decrypt – αποκρυπτογράφηση c με κλειδί B_s
  - δίνει ως αποτέλεσμα το καθαρό κείμενο m
- Ορθότητα: $D(B_s, E(B_p, m)) = m$


B_p
m
Κρυπτογράφηση
c
ALICE
EVE
Αποκρυπτογράφηση
m
B_s
BOB

Από την θεωρία στην πράξη

- PGP
  - Pretty Good Privacy
  - Όρισε το OpenPGP πρωτόκολλο για κρυπτογράφηση/αποκρυπτογράφηση
  - Πρώτη ευρείας χρήσης ασύμμετρη κρυπτογραφία
  - Phil Zimmermann, 1991
- GPG
  - Ελεύθερη υλοποίηση

Phil Zimmermann

Δημιουργία κλειδιού

- gpg --gen-key
  - Δημιουργεί ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού
- Το δημόσιο κλειδί αποθηκεύεται στον υπολογιστή σας
- Καλές πρακτικές:
  - 4096 bits
  - RSA/RSA
- Χρησιμοποιείστε το πραγματικό σας όνομα
- Χρησιμοποιείστε το προσώπικό σας e-mail

Passphrase

- Προστατεύει το κλειδί σας
- Σας ζητείται πριν τη χρήση του ιδιωτικού σας κλειδιού
- Χρησιμοποιείστε ένα δυνατό passphrase
  - Τουλάχιστον 20 χαρακτήρες
  - Χρησιμοποιείστε κάποια φράση
- Είστε υπεύθυνοι για το κλειδί σας!
- Δεν υπάρχει “forgot password”
  - Αποθηκεύεται στον υπολογιστή σας
  - Κανένας άλλος δεν έχει πρόσβαση σ’ αυτό

```
dionyziz@erdos ~ % gpg --gen-key
```

```
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
```

```
RSA keys may be between 1024 and 8192 bits long.
What keysize do you want? (2048) 4096
Requested keysize is 4096 bits
```

Ημερομηνία λήξης κλειδιού

- Καλή πρακτική: Λήξη σε 1 έτος
  - Σε περίπτωση θανάτου, μη διαθεσιμότητας κ.ό.κ.
- Ο ιδιοκτήτης του κλειδιού μπορεί να το ανανεώσει
- gpg --edit-key F44EAFF8
- Προσθέστε στο ημερολόγιό σας να το ανανεώσετε

```
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) 1y
Key expires at Sat Feb 14 12:39:29 2015 EET
Is this correct? (y/N) y
```

Προσωπικές πληροφορίες

- Όνομα και επώνυμο
- E-mail
- Προτιμήστε να χρησιμοποιήσετε:
  - Τα πλήρη πραγματικά σας στοιχεία
  - Το προσωπικό e-mail σας
- Το όνομά σας θα χρησιμοποιείται για να υπογράφετε ψηφιακά, γι’αυτό πρέπει να είναι το πραγματικό

```
Real name: Bob Squarepants
Email address: bob@security-class.gr
Comment:
You selected this USER-ID:
    "Bob Squarepants <bob@security-class.gr>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
You need a Passphrase to protect your secret key.
```

```
pub   4096R/0C986F9B 2014-02-14 [expires: 2015-02-14]
      Key fingerprint = 57AB 0B68 74B7 C2C7 81A2  B867 FA55 458A 0C98 6F9B
uid                  Bob Squarepants <bob@security-class.gr>
sub   4096R/33875DCC 2014-02-14 [expires: 2015-02-14]
```

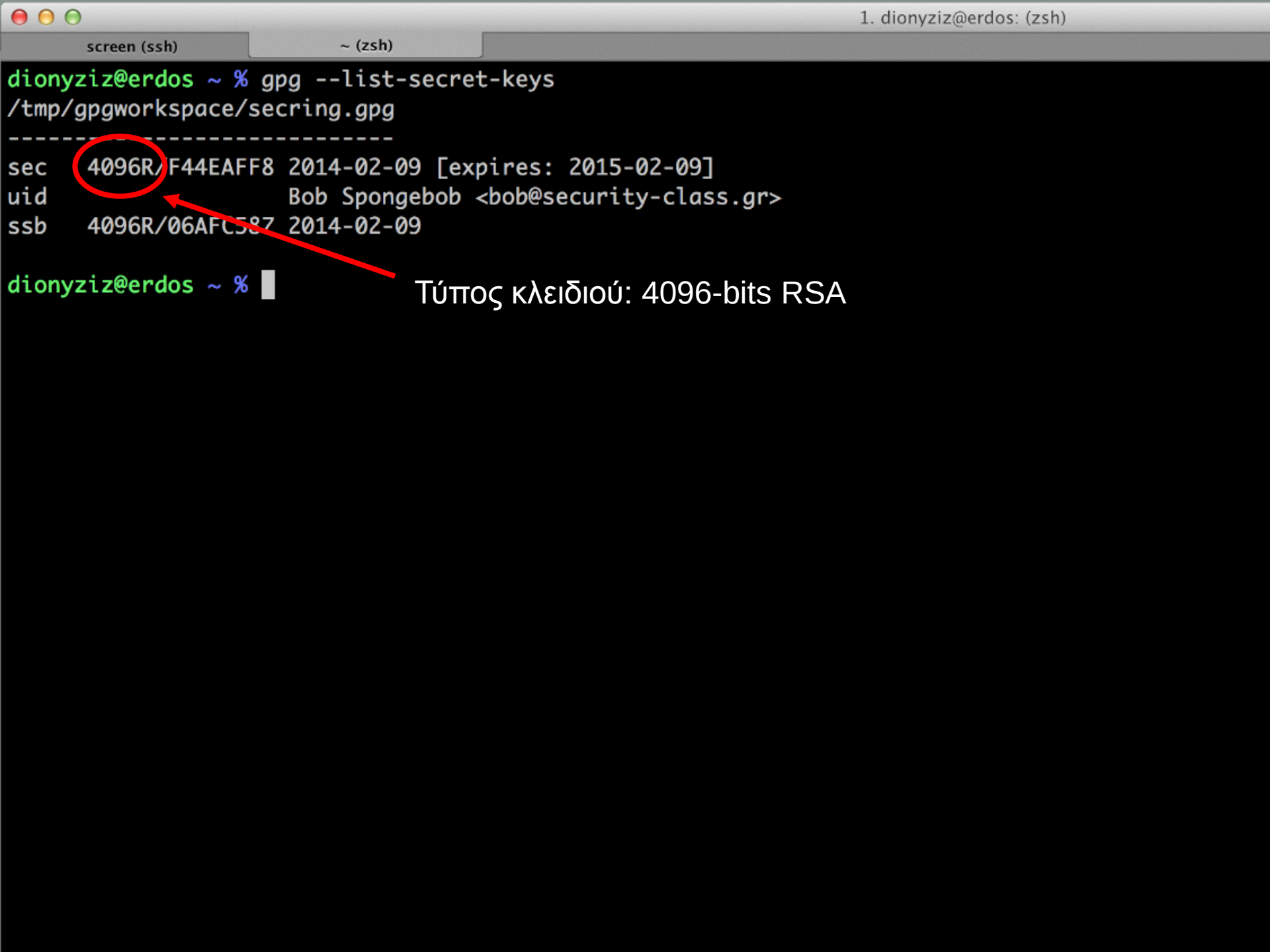
```
dionyziz@erdos ~ % gpg --gen-key
gpg (GnuPG/MacGPG2) 2.0.20; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 8192 bits long.
What keysize do you want? (2048) 4096
Requested keysize is 4096 bits
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) 1y
Key expires at Mon Feb  9 23:24:36 2015 EET
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Bob Spongebob
Email address: bob@security-class.gr
Comment:
You selected this USER-ID:
    "Bob Spongebob <bob@security-class.gr>"

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

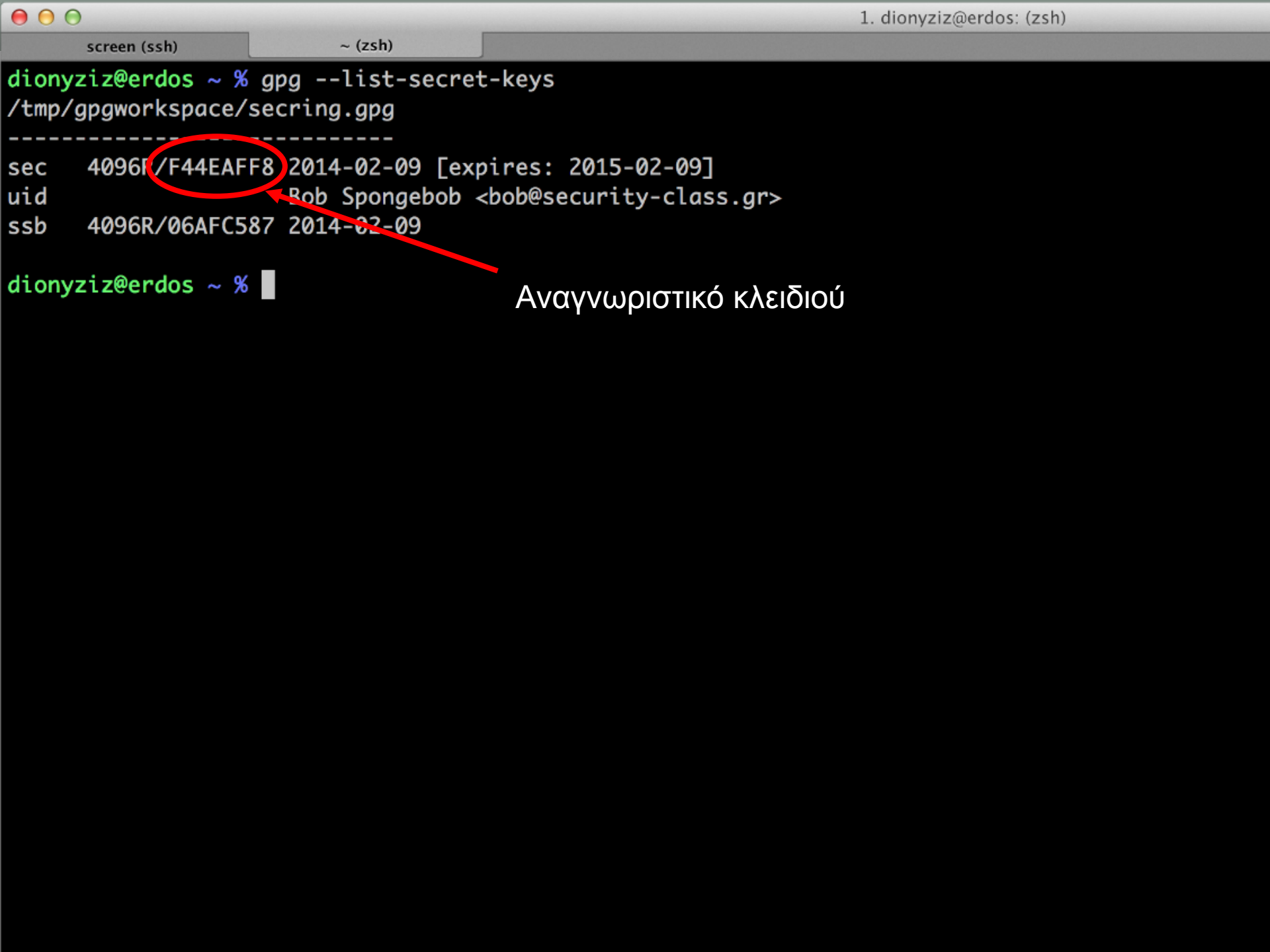
Πληροφορίες κλειδιών

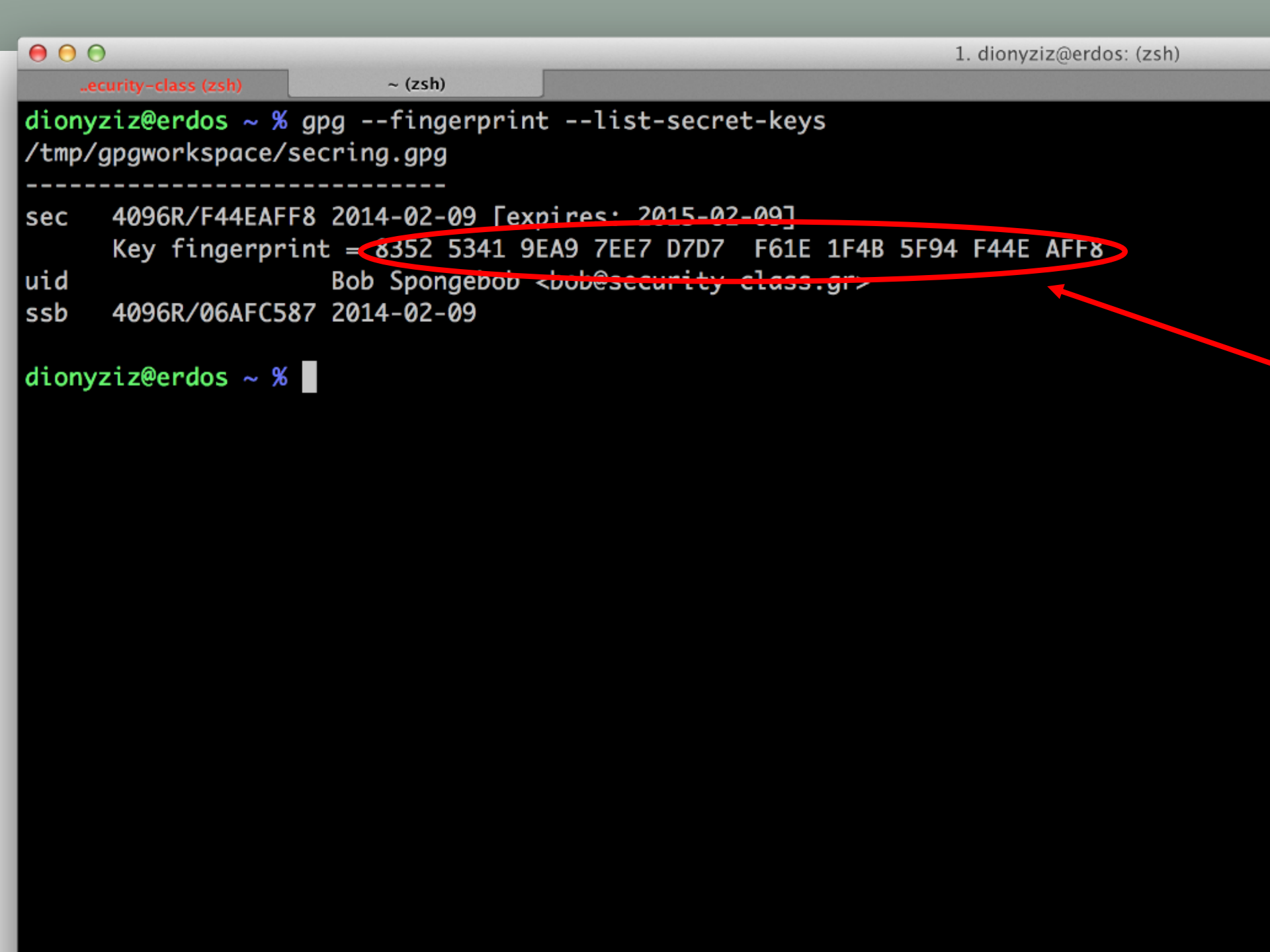
- Όνομα και επώνυμο
- Διεύθυνση e-mail
- Τύπος (RSA) και μέγεθος (4096 bits)
- Αποτύπωμα
  - Μοναδικό για κάθε κλειδί
  - Δεν μπορεί να το μιμηθεί κάποιος
- Αναγνωριστικό
  - Τα τελευταία 8 ψηφία του αποτυπώματος

Προβολή κλειδιών

- gpg --list-secret-keys
  - Εμφανίζει τα δημόσια κλειδιά για τα οποία υπάρχουν ιδιωτικά αποθηκευμένα τοπικά
- gpg --fingerprint --list-secret-keys
  - ...μαζί με τα αποτυπώματά τους


1. dionyziz@erdos: (zsh)
screen (ssh)
~ (zsh)
dionyziz@erdos ~ % gpg --list-secret-keys
/tmp/gpgworkspace/secring.gpg
sec 4096R/F44EAFF8 2014-02-09 [expires: 2015-02-09]
uid Bob Spongebob <bob@security-class.gr>
ssb 4096R/06AFC587 2014-02-09
dionyziz@erdos ~ %
Τύπος κλειδιού: 4096-bits RSA


1. dionyziz@erdos: (zsh)
screen (ssh)
~ (zsh)
dionyziz@erdos ~ % gpg --list-secret-keys
/tmp/gpgworkspace/secring.gpg
sec 4096R/F44EAFF8 2014-02-09 [expires: 2015-02-09]
uid Bob Spongebob <bob@security-class.gr>
ssb 4096R/06AFC587 2014-02-09
dionyziz@erdos ~ %
Αναγνωριστικό κλειδιού


1. dionyziz@erdos: (zsh)
..ecurity-class (zsh)
~ (zsh)
dionyziz@erdos ~ % gpg --fingerprint --list-secret-keys
/tmp/gpgworkspace/secring.gpg
sec 4096R/F44EAFF8 2014-02-09 [expires: 2015-02-09]
Key fingerprint = 8352 5341 9EA9 7EE7 D7D7 F61E 1F4B 5F94 F44E AFF8
uid Bob Spongebob <bob@security-class.gr>
ssb 4096R/06AFC587 2014-02-09
dionyziz@erdos ~ %

Key server

- Server που μας βοηθά να δημοσιεύουμε τα κλειδιά μας
- Μπορείτε να δημοσιεύετε τα κλειδιά σας οπουδήποτε
  - π.χ. προσωπική σας σελίδα (δείτε https://dionyziz.com/gpg)
- Είναι πιο εύκολο σε έναν key server
- Υπάρχουν πολλοί
- Μοιράζονται μεταξύ τους τα κλειδιά
- Ανεβάζουμε το κλειδί μας σε κάποιον
- Καταλήγει σε όλους
- Όποιος θέλει μπορεί να μας βρει

Δημοσίευση κλειδιού

- Δημοσίευση δημόσιου κλειδιού:
- gpg --keyserver pgp.mit.edu --sendkeys AFB046C7
- Επισκευθείτε το http://pgp.mit.edu και βρείτε το όνομά σας
  - Μπορείτε να αναζητήσετε με βάση το όνομα: Dionysis Zindros
  - Ή με βάση το e-mail: dionyziz
  - Ή με βάση το αναγνωριστικό: 0xAFB046C7

Λήψη κλειδιού

- Κατεβάστε το κλειδί κάποιου άλλου:
- Βρείτε το στο http://pgp.mit.edu και αντιγράψτε το αναγνωριστικό
- Τρέξτε:
- gpg --keyserver pgp.mit.edu --recvkeys AFB046C7

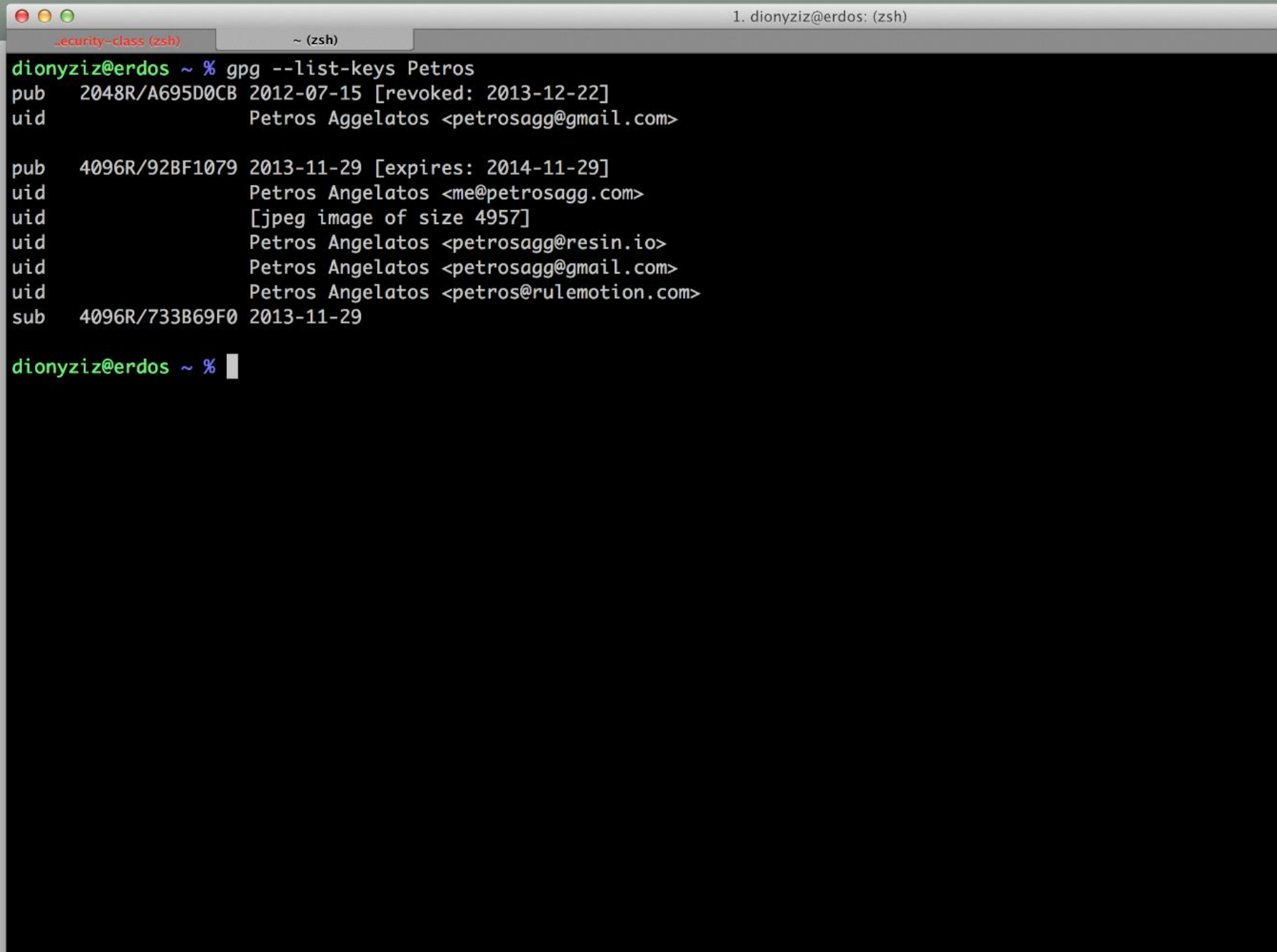
```
dionyziz@erdos ~ % gpg --keyserver pgp.mit.edu --recv-keys 92BF1079
gpg: requesting key 92BF1079 from hkp server pgp.mit.edu
gpg: key 92BF1079: public key "Petros Angelatos <me@petrosagg.com>" imported
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2015-02-14
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

Προβολή κλειδιών

- Προβολή όλων των κλειδιών:
- gpg --list-keys

- Αναζήτηση συγκεκριμένου κλειδιού:
- gpg --list-keys Karantias

```
dionyziz@erdos ~ % gpg --list-keys
/Users/dionyziz/.gnupg/pubring.gpg
---------------------------------
pub   2048D/00D026C4 2010-08-19 [expires: 2015-08-18]
uid                  GPGTools Team <team@gpgtools.org>
uid                  GPGMail Project Team (Official OpenPGP Key) <gpgmail-devel@lists.gpgmail.org>
uid                  GPGTools Project Team (Official OpenPGP Key) <gpgtools-org@lists.gpgtools.org>
uid                  [jpeg image of size 5871]
sub   2048g/DBCBE671 2010-08-19 [expires: 2015-08-18]

pub   4096R/57F14792 2011-06-05 [revoked: 2013-12-22]
uid                  Dionysis Zindros <dionyziz@kamibu.com>

pub   1024D/33621D72 2011-06-06 [revoked: 2013-12-22]
uid                  Dionysis Zindros <dionyziz@gmail.com>
uid                  Dionysis Zindros <dionyziz@kamibu.com>

pub   2048R/63FEE659 2003-10-16
uid                  Erinn Clark <erinn@torproject.org>
uid                  Erinn Clark <erinn@debian.org>
uid                  Erinn Clark <erinn@double-helix.org>
sub   2048R/EB399FD7 2003-10-16

pub   1024D/F0D6B1E0 2004-06-06
uid                  TrueCrypt Foundation <info@truecrypt-foundation.org>
uid                  TrueCrypt Foundation <contact@truecrypt.org>
sub   4077g/6B136ECF 2004-06-06

pub   2048R/A695D0CB 2012-07-15 [revoked: 2013-12-22]
uid                  Petros Aggelatos <petrosagg@gmail.com>

pub   2048R/6D812522 2013-05-16
uid                  Nikolaos Danopoulos <danopoulosnikos@gmail.com>
sub   2048R/F0095BCF 2013-05-16

pub   4096R/A6085C57 2013-04-30
uid                  Manio Saldingen <maniosaldingen@gmail.com>
```


1. dionyziz@erdos: (zsh)
ecurity-class (zsh)
~ (zsh)
dionyziz@erdos ~ % gpg --list-keys Petros
pub   2048R/A695D0CB 2012-07-15 [revoked: 2013-12-22]
uid   Petros Aggelatos <petrosagg@gmail.com>
pub   4096R/92BF1079 2013-11-29 [expires: 2014-11-29]
uid   Petros Angelatos <me@petrosagg.com>
uid   [jpeg image of size 4957]
uid   Petros Angelatos <petrosagg@resin.io>
uid   Petros Angelatos <petrosagg@gmail.com>
uid   Petros Angelatos <petros@rulemotion.com>
sub   4096R/733B69F0 2013-11-29
dionyziz@erdos ~ %

Κρυπτογράφηση μηνύματος

- Η κρυπτογράφηση γίνεται με το **δημόσιο κλειδί του παραλήπτη**
- Πρέπει πρώτα να έχουμε κατεβάσει το κλειδί του παραλήπτη και να φαίνεται στο gpg --list-keys

- gpg -a --encrypt --recipient “Konstantinos Karantias”
- Πληκτρολογούμε το μήνυμά μας
- Λήγουμε με enter και end of file
  - Ctrl + D στο Linux & Mac
  - Ctrl + Z και enter στα Windows

Κρυπτογραφημένο μήνυμα

-----BEGIN PGP MESSAGE-----
Version: GnuPG/MacGPG2 v2.0.20 (Darwin)

hQIMA/Q/0aJzO2nwAQ/9EQLRQlXB/xTCm8eLYs3sFwDglix4Hvc2Vxipo+KLUwbD
3PkzwkvPbNckzi0Wb2lAmu7UXBRnS1i++iATD+8bDGeCLN1GCdVnOefkij6JVSxS
NKXPJV9tdBTd9oBwCtKCuMlrIeIvZHm9Bvf52vKfB1z/fr6gviS78Z21ZAoBoPKF
9KGQqmD9IMaXQzVN+OJaftulViqlIN1HuAowggqUZbcX8M8AUMgDSGv0DhPyJy7J
R7blowS7b3pTUIjLmkJqDF30eVa0A+JeeVG3NSdf1hy/PYEgFpekce0UEax6P/w2
aDgKBPLnLnrEYRWlJFVhhC5BeUExoHS7/HmLWX1JHS7Nj7AWElr6F91Zem1rfl7Q
VI7BK6wdwz1cnjZQG5I+9IGoG68gYZoyUwGjy/QzkzGUI3TtCSz7pFnaMGnvhz7B
suSp7ACKGpIpnqjLBdH0zzCiEBbGnmPfLbDBMOltK3O34bOTxjNB7hmp5ijN6Q3i
tuC1HypX6FhOpex4NBTxVCFNGPHWtntoDl2OymstcMWxun2wBkUXPUZob5/lScXP
qqY0mjbDoyPFg97qM0MeRJhUEwjJGLXP3o6qeXvjE5eYd6gds2NgtGjFr8OVbeyi
YXNjmJFnHCX+4Fjx4KxuYpdsZjdM6K7/GQhfJAV4lLSenzTp1LkQTZibYwJwrJXS
SQGq9zcYoxJ6qevhcoDRa3tlhjbmKhejIPRaxJw2x9tVXSapX//xQO3KInoOZAJ3
niP4+UD3CR7ufQH/Y6ZNa36r/Z1KalLq5jo=
=BuYS
-----END PGP MESSAGE-----

Κρυπτογράφηση μηνύματος

- Στέλνουμε όλο το μήνυμα από το:
  - ----BEGIN PGP MESSAGE----
- έως το:
  - ----END PGP MESSAGE----
- Συμπεριλαμβάνοντας αυτά τα κομμάτια

Αποκρυπτογράφηση μηνύματος

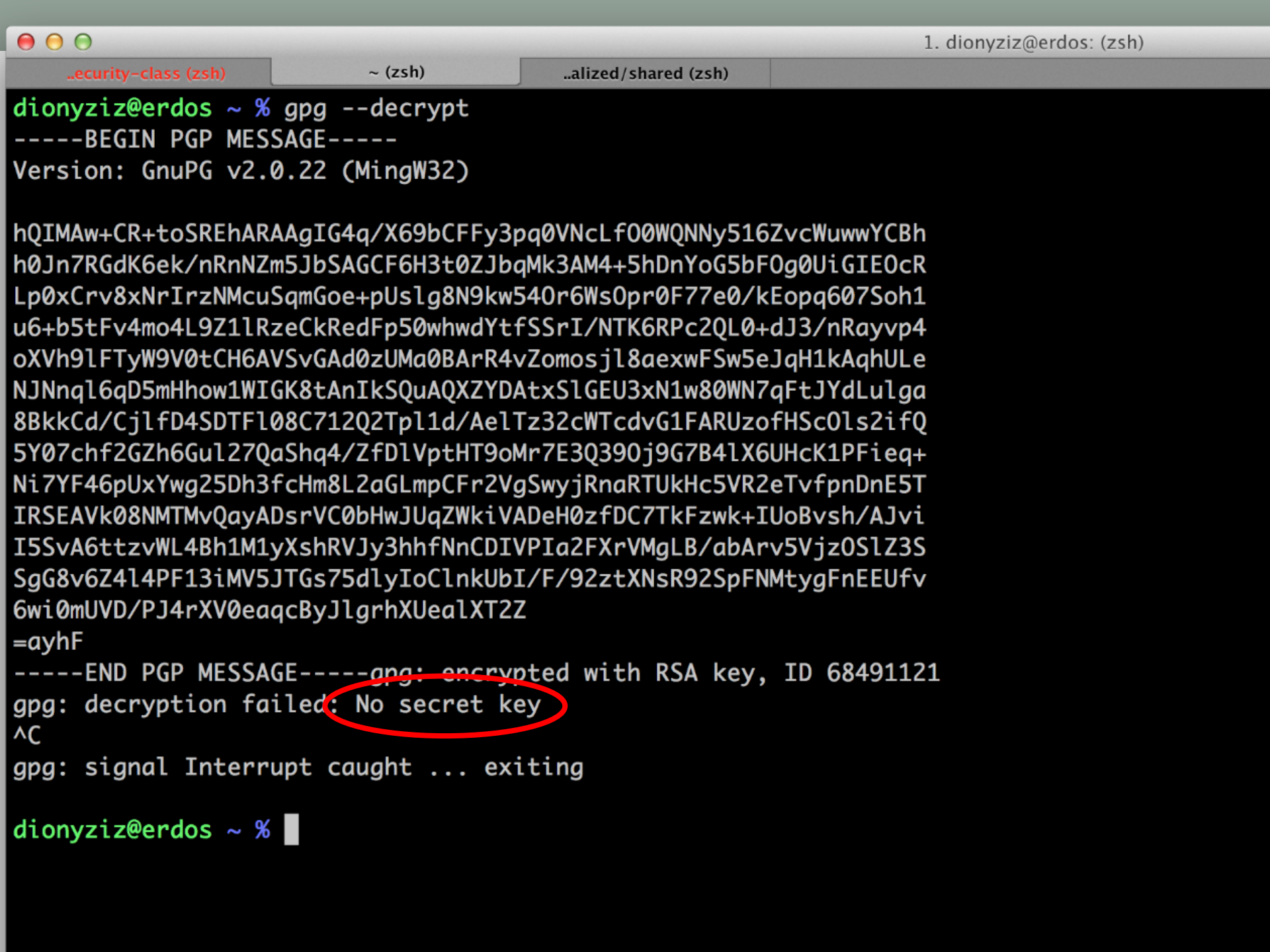
- gpg --decrypt
- Κάνουμε copy/paste το μήνυμά μας
  - Από το ----BEGIN PGP MESSAGE----
  - Έως το ----END PGP MESSAGE----
- Λήγουμε με enter & end of file

Quiz

- Η Alice στέλνει ένα κρυπτογραφημένο μήνυμα στον Bob
- Πριν το στείλει θέλει να επιβεβαιώσει ότι είναι σωστό
- Μπορεί να αποκρυπτογραφήσει αυτό που κρυπτογράφησε;

Quiz

- Η Alice στέλνει ένα κρυπτογραφημένο μήνυμα στον Bob
- Πριν το στείλει θέλει να επιβεβαιώσει ότι είναι σωστό
- Μπορεί να αποκρυπτογραφήσει αυτό που κρυπτογράφησε;
- Όχι!
- Η κρυπτογράφηση έγινε με το δημόσιο κλειδί του Bob.
- Η Alice δεν έχει το ιδιωτικό κλειδί του Bob.
- Ό,τι κρυπτογραφείται με το δημόσιο κλειδί κάποιου, αποκρυπτογραφείται με το αντίστοιχο ιδιωτικό!


1. dionyziz@erdos: (zsh)
..ecurity-class (zsh)
~ (zsh)
..alized/shared (zsh)
dionyziz@erdos ~ % gpg --decrypt
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.22 (MingW32)
hQIMAw+CR+toSREhARAAgIG4q/X69bCFFy3pq0VNcLfO0WQNNy516ZvcWuwwYCBh
h0Jn7RGdK6ek/nRnNZm5JbSAGCF6H3t0ZJbqMk3AM4+5hDnYoG5bFOg0UiGIEOcR
Lp0xCrv8xNrIrzNMcuSqmGoe+pUslg8N9kw54Or6WsOpr0F77e0/kEopq607Soh1
u6+b5tFv4mo4L9Z1lRzeCkRedFp50whwdYtfSSrI/NTK6RPc2QL0+dJ3/nRayvp4
oXVh9lFTyW9V0tCH6AVSvGAd0zUMa0BArR4vZomosjl8aexwFSw5eJqH1kAqhULe
NJNnql6qD5mHhow1WIGK8tAnIkSQuAQXZYDAtxSlGEU3xN1w80WN7qFtJYdLulga
8BkkCd/CjlfD4SDTFl08C712Q2Tpl1d/AelTz32cWTcdvG1FARUzofHScOls2ifQ
5Y07chf2GZh6Gul27QaShq4/ZfDlVptHT9oMr7E3Q39Oj9G7B4lX6UHcK1PFieq+
Ni7YF46pUxYwg25Dh3fcHm8L2aGLmpCFr2VgSwyjRnaRTUkHc5VR2eTvfpnDnE5T
IRSEAVk08NMTMvQayADsrVC0bHwJUqZWkiVADeH0zfDC7TkFzwk+IUoBvsh/AJvi
I5SvA6ttzvWL4Bh1M1yXshRVJy3hhfNnCDIVPIa2FXrVMgLB/abArv5VjzOSlZ3S
SgG8v6Z4l4PF13iMV5JTGs75dlyIoClnkUbI/F/92ztXNsR92SpFNMtygFnEEUfv
6wi0mUVD/PJ4rXV0eaqcByJlgrhXUealXT2Z
=ayhF
-----END PGP MESSAGE-----gpg: encrypted with RSA key, ID 68491121
gpg: decryption failed: No secret key
^C
gpg: signal Interrupt caught ... exiting
dionyziz@erdos ~ %

Ασύμμετρη κρυπτογραφία

- Αρχή λειτουργίας:
  - Ό,τι κρυπτογραφείται με το δημόσιο κλειδί κάποιου, αποκρυπτογραφείται από το αντίστοιχο ιδιωτικό του.
  - **Ό,τι κρυπτογραφείται με το ιδιωτικό κλειδί κάποιου, αποκρυπτογραφείται από το αντίστοιχο δημόσιο του.**

- **Γιατί χρειάζεται αυτό;**

Quiz

- Τι συμβαίνει αν η Alice κρυπτογραφήσει ένα μήνυμα με το ιδιωτικό κλειδί της;
- Ποιος μπορεί να το διαβάσει;

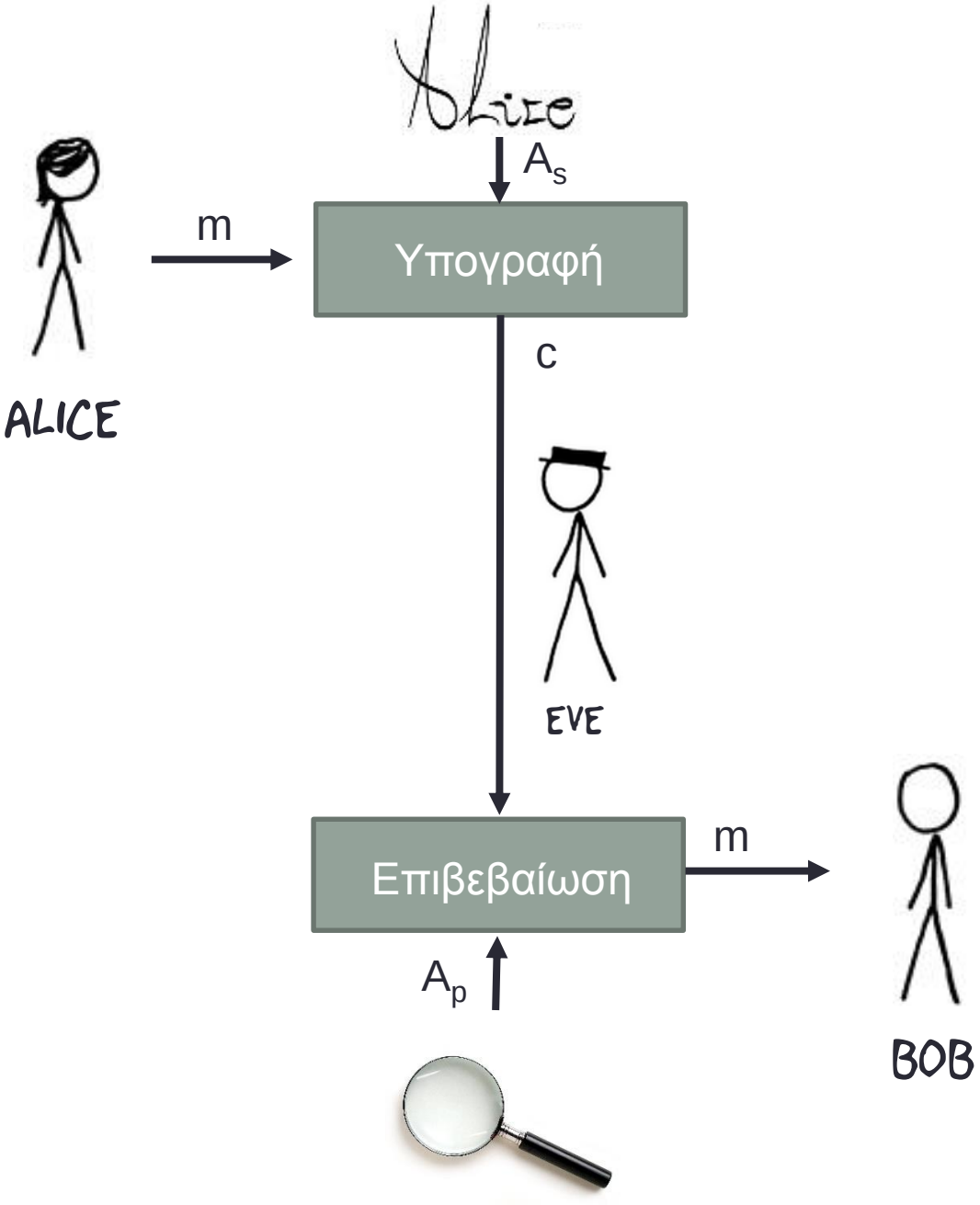
Ψηφιακές υπογραφές

- Η Alice θέλει να στείλει ένα μήνυμα στον Bob
- Ο Bob θέλει να επιβεβαιώσει ότι το έγραψε η Alice
- Ο καθένας έχει το ιδιωτικό και δημόσιο κλειδί του
- Η Alice κρυπογραφεί το μήνυμά της με το **ιδιωτικό κλειδί της**
- Στέλνει στο δίκτυο το κρυπτογραφημένο κείμενο
- Ο Bob λαμβάνει το κρυπτογραφημένο κείμενο
- Ο Bob αποκρυπτογραφεί το κρυπτογραφημένο κείμενο με το **δημόσιο κλειδί της Alice**
- Λαμβάνει το αρχικό κείμενο

Ψηφιακές υπογραφές

- Η Alice θέλει να στείλει ένα μήνυμα στον Bob
- Ο Bob θέλει να επιβεβαιώσει ότι το έγραψε η Alice
- Ο καθένας έχει το ιδιωτικό και δημόσιο κλειδί του
- Η Alice **υπογράφει** το μήνυμά της με το **ιδιωτικό κλειδί της**
- Στέλνει στο δίκτυο το **υπογεγραμμένο** κείμενο
- Ο Bob λαμβάνει το **υπογεγραμμένο** κείμενο
- Ο Bob **επιβεβαιώνει** το υπογεγραμμένο κείμενο με το **δημόσιο κλειδί της Alice**

- A_s
  - Alice's secret – μυστικό κλειδί
- A_p
  - Alice's public – δημόσιο κλειδί
- B_s
  - Bob's secret – μυστικό κλειδί
- B_p
  - Bob's public – δημόσιο κλειδί
- $c = S(B_s, m)$
  - sign – υπογραφή του μηνύματος m με κλειδί B_s
  - δίνει ως αποτέλεσμα κρυπτοκείμενο c
- $m = V(B_p, c, m)$
  - verify – επιβεβαίωση υπογραφής c με κλειδί B_p
- Ορθότητα: $V(B_p, S(B_s, m), m) = true$

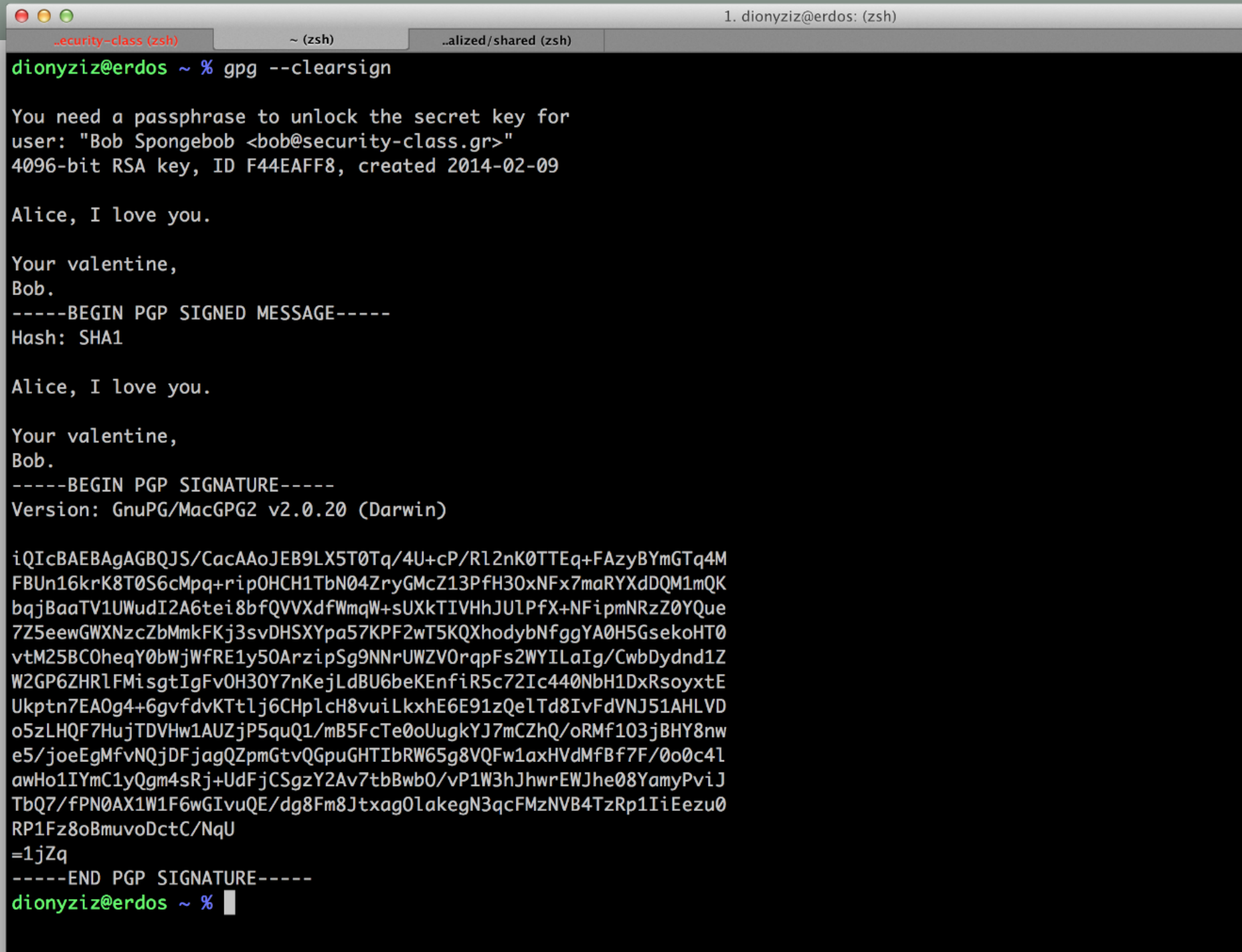

Alice
A_s
m
Υπογραφή
c
ALICE
EVE
Επιβεβαίωση
m
A_p
BOB

Ψηφιακές υπογραφές

- Πιο ασφαλείς από τις συμβατικές υπογραφές
- Δεν μπορούν να παραχαρακτούν
- Περιλαμβάνουν το αρχικό καθαρό κείμενο μαζί με την υπογραφή
- Είναι **συνδεδεμένες** με το κείμενο που υπογράφονται
- Κάθε υπογραφή είναι διαφορετική και εξαρτάται από το κείμενο
- Αν αλλάξει το κείμενο, η υπογραφή δεν είναι πια έγκυρη!
- Δεν γίνεται να αντιγράψω μία υπογραφή και να τη βάλω σε άλλο κείμενο
- Είστε ενδεχομένως νομικά υπεύθυνοι γι’ αυτές!

Δημιουργία ψηφιακής υπογραφής

- gpg --clearsign
- Πληκτρολογούμε το μήνυμα που θέλουμε να υπογράψουμε
- Λήγουμε με enter και end of file
- Στέλνουμε το αποτέλεσμα
- Από το:
  - ----BEGIN PGP MESSAGE----
- Έως το:
  - ----END PGP SIGNATURE----


1. dionyziz@erdos: (zsh)
..ecurity-class (zsh)
~ (zsh)
..alized/shared (zsh)
dionyziz@erdos ~ % gpg --clearsign
You need a passphrase to unlock the secret key for
user: "Bob Spongebob <bob@security-class.gr>"
4096-bit RSA key, ID F44EAFF8, created 2014-02-09
Alice, I love you.
Your valentine,
Bob.
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
Alice, I love you.
Your valentine,
Bob.
-----BEGIN PGP SIGNATURE-----
Version: GnuPG/MacGPG2 v2.0.20 (Darwin)
iQIcBAEBAgAGBQJS/CacAAoJEB9LX5T0Tq/4U+cP/Rl2nK0TTEq+FAzyBYmGTq4M
FBUn16krK8T0S6cMpq+ripOHCH1TbN04ZryGMcZ13PfH3OxNFx7maRYXdDQM1mQK
bqjBaaTV1UWudI2A6tei8bfQVVXdfWmqW+sUXkTIVHhJUlPfX+NFipmNRzZ0YQue
7Z5eewGWXNzcZbMmkFKj3svDHSXYpa57KPF2wT5KQXhodybNfggYA0H5GsekoHT0
vtM25BCOheqY0bWjWfRE1y5OArzipSg9NNrUWZVOrqpFs2WYILaIg/CwbDydnd1Z
W2GP6ZHRlFMisgtIgFvOH3OY7nKejLdBU6beKEnfiR5c72Ic440NbH1DxRsoyxtE
Ukptn7EAOg4+6gvfdvKTtlj6CHplcH8vuiLkxhE6E91zQelTd8IvFdVNJ51AHLVD
o5zLHQF7HujTDVHw1AUZjP5quQ1/mB5FcTe0oUugkYJ7mCZhQ/oRMf1O3jBHY8nw
e5/joeEgMfvNQjDFjagQZpmGtvQGpuGHTIbRW65g8VQFw1axHVdMfBf7F/0o0c4l
awHo1IYmC1yQgm4sRj+UdFjCSgzY2Av7tbBwbO/vP1W3hJhwrEWJhe08YamyPviJ
TbQ7/fPN0AX1W1F6wGIvuQE/dg8Fm8JtxagOlakegN3qcFMzNVB4TzRp1IiEezu0
RP1Fz8oBmuvoDctC/NqU
=1jZq
-----END PGP SIGNATURE-----
dionyziz@erdos ~ %

Υπογεγραμμένο μήνυμα

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Alice, I love you.

Your valentine,
Bob.
-----BEGIN PGP SIGNATURE-----
Version: GnuPG/MacGPG2 v2.0.20 (Darwin)

iQIcBAEBAgAGBQJS/CacAAoJEB9LX5T0Tq/4U+cP/Rl2nK0TTEq+FAzyBYmGTq4M
FBUn16krK8T0S6cMpq+ripOHCH1TbN04ZryGMcZ13PfH3OxNFx7maRYXdDQM1mQK
bqjBaaTV1UWudI2A6tei8bfQVVXdfWmqW+sUXkTIVHhJUlPfX+NFipmNRzZ0YQue
7Z5eewGWXNzcZbMmkFKj3svDHSXYpa57KPF2wT5KQXhodybNfggYA0H5GsekoHT0
vtM25BCOheqY0bWjWfRE1y5OArzipSg9NNrUWZVOrqpFs2WYILaIg/CwbDydnd1Z
W2GP6ZHRlFMisgtIgFvOH3OY7nKejLdBU6beKEnfiR5c72Ic440NbH1DxRsoyxtE
Ukptn7EAOg4+6gvfdvKTtlj6CHplcH8vuiLkxhE6E91zQelTd8IvFdVNJ51AHLVD
o5zLHQF7HujTDVHw1AUZjP5quQ1/mB5FcTe0oUugkYJ7mCZhQ/oRMf1O3jBHY8nw
e5/joeEgMfvNQjDFjagQZpmGtvQGpuGHTIbRW65g8VQFw1axHVdMfBf7F/0o0c4l
awHo1IYmC1yQgm4sRj+UdFjCSgzY2Av7tbBwbO/vP1W3hJhwrEWJhe08YamyPviJ
TbQ7/fPN0AX1W1F6wGIvuQE/dg8Fm8JtxagOlakegN3qcFMzNVB4TzRp1IiEezu0
RP1Fz8oBmuvoDctC/NqU
=1jZq
-----END PGP SIGNATURE-----

Επιβεβαίωση υπογραφής

- Η επιβεβαίωση γίνεται με το **δημόσιο κλειδί του αποστολέα**
- Πρέπει πρώτα να έχουμε κατεβάσει το δημόσιο κλειδί του αποστολέα και να φαίνεται στο gpg --list-keys

- gpg --verify
- Κάνουμε επικόλληση το μήνυμα

- Θα πρέπει να δούμε:
  - Good signature → Έγκυρη υπογραφή
  - Bad signature → Λάθος υπογραφή

Πρόβλημα

- Ο καθένας μπορεί να δημοσιεύσει ένα κλειδί με όνομα Dionysis Zindros και e-mail dionyziz@gmail.com
- Κανείς δεν επιβεβαιώνει αυτό το όνομα!
- Κανείς δεν επιβεβαιώνει αυτή τη διεύθυνση;
- Πώς ξέρουμε ότι το κλειδί ανήκει πραγματικά στον υποτιθέμενο κάτοχό του;

Μία ερωτική ιστορία

- Η Alice και ο Bob είναι ένα αγαπημένο ζευγάρι
- Η Alice στέλνει στον Bob ένα ερωτικό μήνυμα

Μία ερωτική ιστορία

- Η Eve είναι μυστικά ερωτευμένη με τον Bob
- Θέλει να διαβάσει τι στέλνει η Alice στον Bob

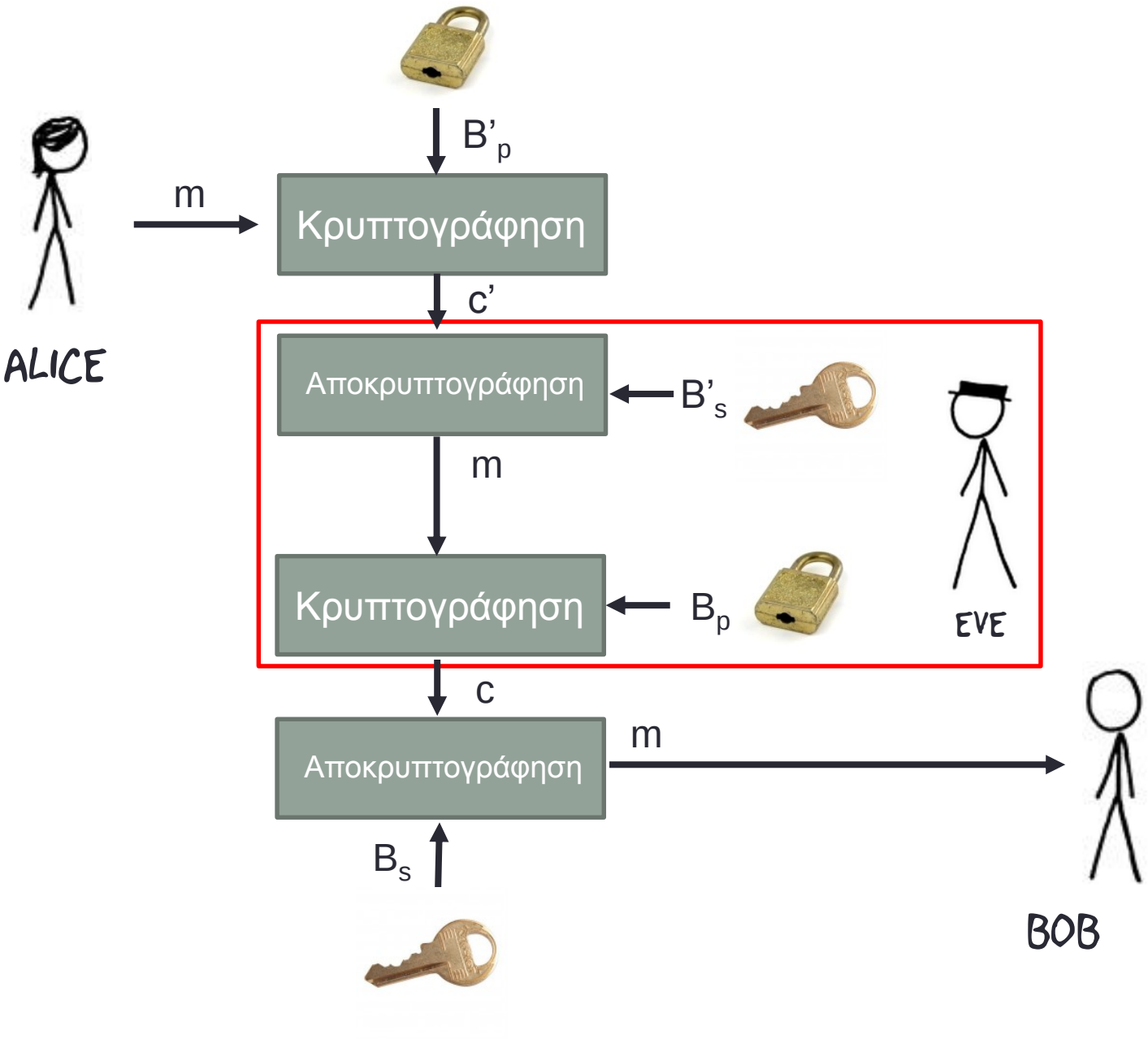
Woman-in-the-middle

- Η Eve φτιάχνει ένα **ψεύτικο** ζεύγος κλειδιών που προσποιείται ότι είναι ο Bob και το ανεβάζει στον keyserver.
- Η Alice κατεβάζει το ψεύτικο κλειδί του Bob και **νομίζει** ότι κρυπτογραφεί μηνύματα για τον Bob.

Woman-in-the-middle

- Η Eve λαμβάνει το μήνυμα από την Alice που απευθύνεται στον Bob και είναι κρυπτογραφημένο με το **ψεύτικο** κλειδί του Bob.
- Η Eve αποκρυπτογραφεί το μήνυμα, αφού έχει το μυστικό κλειδί.
- Η Eve κρυπτογραφεί το μήνυμα με το **πραγματικό** κλειδί του Bob και το στέλνει στον πραγματικό Bob.

- A_s
  - Alice’s secret – μυστικό κλειδί
- A_p
  - Alice’s public – δημόσιο κλειδί
- B_s
  - Bob’s secret – μυστικό κλειδί
- B_p
  - Bob’s public – δημόσιο κλειδί
- B'_s
  - Eve’s secret – μυστικό κλειδί του **ψεύτικου** Bob
- B'_p
  - Eve’s public – δημόσιο κλειδί του **ψεύτικου** Bob


B'p
m
Κρυπτογράφηση
c'
ALICE
Αποκρυπτογράφηση
B's
m
Κρυπτογράφηση
Bp
EVE
c
Αποκρυπτογράφηση
m
Bs
BOB

Πώς αμυνόμαστε;

- Επιβεβαιώνουμε την ταυτότητα του κατόχου ενός κλειδιού
  - Άμεσα
  - Έμμεσα

Άμεση επιβεβαίωση

- Από κοντά συνάντηση με το άτομο που επιβεβαιώνουμε
- **Μόνο με άτομα που ήδη γνωρίζουμε**
- Επιβεβαιώνουμε ότι το **όνομά** τους στο κλειδί είναι πραγματικό
- Επιβεβαιώνουμε ότι τους ανήκει η διεύθυνση **e-mail** του κλειδιού τους
- Επιβεβαιώνουμε ότι το **πλήρες αποτύπωμα** του κλειδιού τους στον υπολογιστή τους είναι αυτό που υπογράφουμε

Άμεση επιβεβαίωση

- Για να δηλώσουμε ότι επιβεβαιώσαμε άμεσα, **υπογράφουμε ψηφιακά** το δημόσιο κλειδί που επιβεβαιώσαμε.

```
dionyziz@erdos ~ % gpg --sign-key 92BF1079
```

```
pub  4096R/92BF1079  created: 2013-11-29  expires: 2014-11-29  usage: SC
                     trust: unknown       validity: unknown
sub  4096R/733B69F0  created: 2013-11-29  expires: never       usage: E
sub  4096R/DBCB42A1  created: 2013-11-29  expired: 2014-01-29  usage: S
sub  4096R/119ED5EF  created: 2014-02-03  expires: never       usage: S
[ unknown] (1). Petros Angelatos <me@petrosagg.com>
[ unknown] (2)  Petros Angelatos <petrosagg@resin.io>
[ unknown] (3)  Petros Angelatos <petrosagg@gmail.com>
[ unknown] (4)  Petros Angelatos <petros@rulemotion.com>
[ unknown] (5)  [jpeg image of size 4957]

Really sign all user IDs? (y/N) y
```

```
pub  4096R/92BF1079  created: 2013-11-29  expires: 2014-11-29  usage: SC
                     trust: unknown       validity: unknown
 Primary key fingerprint: BA81 DC1C D900 9B24 2F88  6FDD 4404 DDEE 92BF 1079

     Petros Angelatos <me@petrosagg.com>
     Petros Angelatos <petrosagg@resin.io>
     Petros Angelatos <petrosagg@gmail.com>
     Petros Angelatos <petros@rulemotion.com>
     [jpeg image of size 4957]

This key is due to expire on 2014-11-29.
Are you sure that you want to sign this key with your
key "Bob Squarepants <bob@security-class.gr>" (0C986F9B)

Really sign? (y/N) y
```

Άμεση επιβεβαίωση

- **Δημοσιεύουμε** την ψηφιακή υπογραφή μας πάνω στο δημόσιο κλειδί που επιβεβαιώσαμε

```
dionyziz@erdos ~ % gpg --keyserver pgp.mit.edu --send-keys 0D4A3BFD
gpg: sending key 0D4A3BFD to hkp server pgp.mit.edu
```

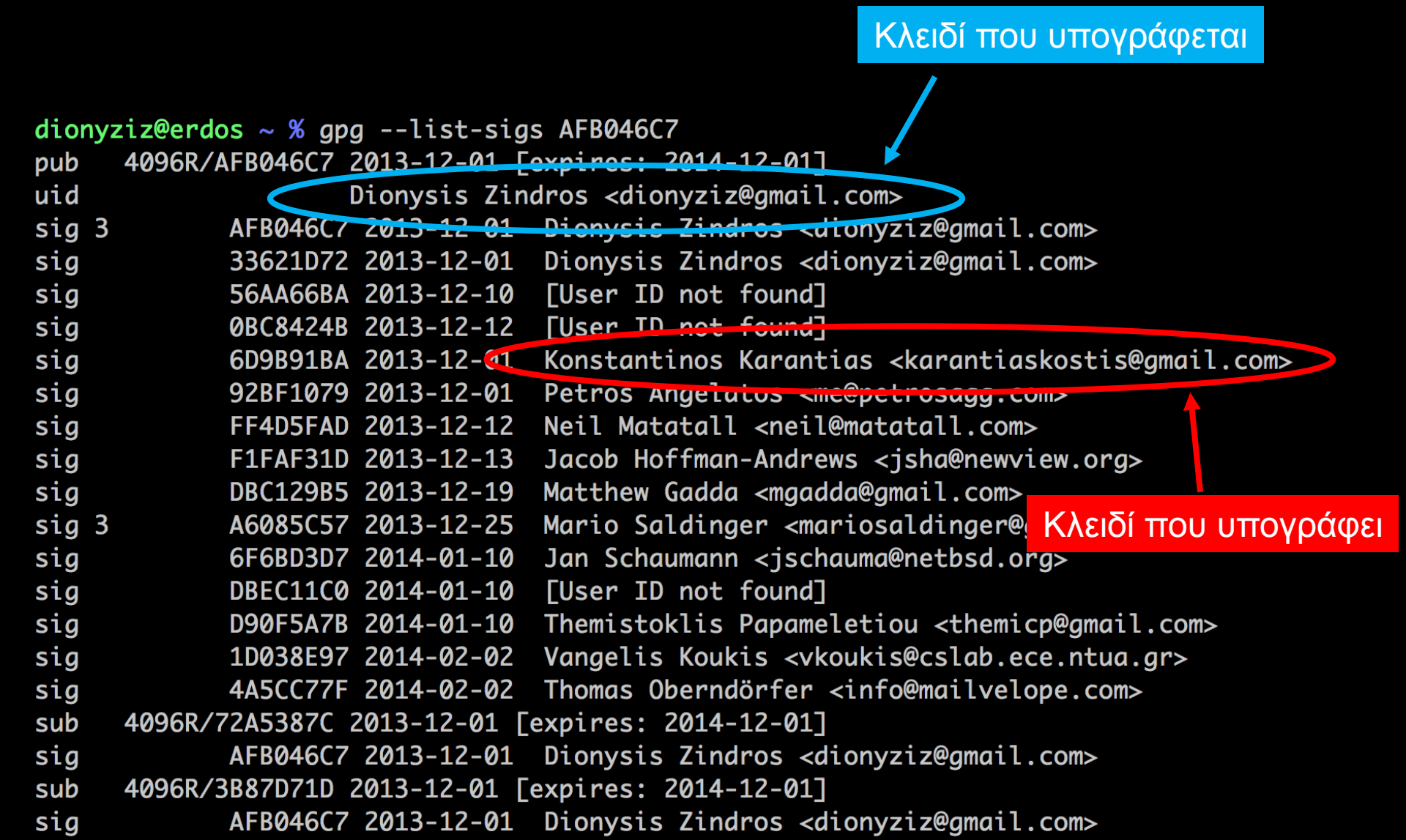
Έμμεση επιβεβαίωση

- Επιβεβαιώνουμε ότι κάποιος που εμπιστευόμαστε έχει υπογράψει το δημόσιο κλειδί
- Έχουμε την εγγύηση ότι έχει επιβεβαιώσει την ταυτότητα
- Μπορούμε να δούμε υπογραφές στον keyserver

```
uid Petros Angelatos <me@petrosagg.com>
sig  sig3  92BF1079 2013-11-29 __________ 2014-11-29 [selfsig]
sig  sig   A695D0CB 2013-11-29 __________ __________ Petros Aggelatos <petrosagg@gmail.com>
sig  sig   6D9B91BA 2013-11-29 __________ __________ Konstantinos Karantias <karantiaskostis@gmail.com>
sig  sig   AFB046C7 2013-12-01 __________ __________ Dionysis Zindros <dionyziz@gmail.com>
sig  sig3  92BF1079 2013-12-01 __________ 2014-11-29 [selfsig]
sig  sig   7F8FDFD9 2013-12-01 __________ __________ Lorenzo Stoakes <lstoakes@gmail.com>
sig  sig3  A6085C57 2013-12-25 __________ __________ Mario Saldinger <mariosaldinger@gmail.com>
sig  sig   1D038E97 2014-02-02 __________ __________ Vangelis Koukis <vkoukis@cslab.ece.ntua.gr>
sig  sig   4A5CC77F 2014-02-02 __________ __________ Thomas Oberndörfer <info@mailvelope.com>
```

Έμμεση επιβεβαίωση

- Δεν εμπιστευόμαστε τον keyserver
- Γι’αυτό επιβεβαιώνουμε και τις υπογραφές τοπικά
- Κατεβάζουμε το κλειδί που υπογράφεται με --recv-keys
- Κατεβάζουμε το κλειδί που υπογράφει με --recv-keys
- Βλέπουμε την υπογραφή με:
- gpg --list-sigs AFB046C7
- Ελέγχουμε την εγκυρότητα της υπογραφής:
- gpg --check-sigs AFB046C7


Κλειδί που υπογράφεται
dionyziz@erdos ~ % gpg --list-sigs AFB046C7
pub 4096R/AFB046C7 2013-12-01 [expires: 2014-12-01]
uid Dionysis Zindros <dionyziz@gmail.com>
sig 3 AFB046C7 2013-12-01 Dionysis Zindros <dionyziz@gmail.com>
sig 33621D72 2013-12-01 Dionysis Zindros <dionyziz@gmail.com>
sig 56AA66BA 2013-12-10 [User ID not found]
sig 0BC8424B 2013-12-12 [User ID not found]
sig 6D9B91BA 2013-12-01 Konstantinos Karantias <karantiaskostis@gmail.com>
sig 92BF1079 2013-12-01 Petros Angelatos
sig FF4D5FAD 2013-12-12 Neil Matatall <neil@matatall.com>
sig F1FAF31D 2013-12-13 Jacob Hoffman-Andrews <jsha@newview.org>
sig DBC129B5 2013-12-19 Matthew Gadda <mgadda@gmail.com>
sig 3 A6085C57 2013-12-25 Mario Saldinger
Κλειδί που υπογράφει
sig 6F6BD3D7 2014-01-10 Jan Schaumann <jschauma@netbsd.org>
sig DBEC11C0 2014-01-10 [User ID not found]
sig D90F5A7B 2014-01-10 Themistoklis Papameletiou <themicp@gmail.com>
sig 1D038E97 2014-02-02 Vangelis Koukis <vkoukis@cslab.ece.ntua.gr>
sig 4A5CC77F 2014-02-02 Thomas Oberndörfer <info@mailvelope.com>
sub 4096R/72A5387C 2013-12-01 [expires: 2014-12-01]
sig AFB046C7 2013-12-01 Dionysis Zindros <dionyziz@gmail.com>
sub 4096R/3B87D71D 2013-12-01 [expires: 2014-12-01]
sig AFB046C7 2013-12-01 Dionysis Zindros <dionyziz@gmail.com>

Μάθαμε

- Έννοιες στην ασύμμετρη κρυπτογραφία
- GPG
- Κρυπτογράφηση & αποκρυπτογράφηση μηνυμάτων
- Ψηφιακές υπογραφές & επιβεβαίωση
- Web-of-trust & υπογραφή κλειδιών

Συγχαρητήρια!

- Μπορείτε να επικοινωνείτε με ασφάλεια!

Ερωτήσεις;

- @gtklocker
- @dionyziz