



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών,

Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής

Ροή Δ, Μάθημα: Ασφάλεια Δικτύων Υπολογιστών (Εξάμηνο 8<sup>ο</sup>)

### Τρίτη Εργαστηριακή Άσκηση : Φύλλο Απαντήσεων

#### **Συγκέντρωση πληροφοριών και ανίχνευση αδυναμιών σε δίκτυα υπολογιστών**

|                                      |
|--------------------------------------|
| Όνοματεπώνυμο: Γιώργος Κυριακόπουλος |
| Αριθμός Μητρώου: 03118153            |
| Εξάμηνο: 8ο                          |

#### **Ερώτηση 3.1**

[www.caltech.edu](http://www.caltech.edu)

\$ nslookup [www.caltech.edu](http://www.caltech.edu)

IP Addresses: 104.18.14.60, 104.18.15.60

Server IP Address: 147.102.222.210

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\labuser>nslookup www.caltech.edu
Server: achilles.noc.ntua.gr
Address: 147.102.222.210

Non-authoritative answer:
Name: www.caltech.edu.cdn.cloudflare.net
Addresses: 104.18.14.60, 104.18.15.60
Aliases: www.caltech.edu

C:\Documents and Settings\labuser>
```

Για τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου:

```
C:\WINDOWS\system32\cmd.exe

primary name server = ns1.cloudflare.net
responsible mail addr = dns.cloudflare.com
serial = 1653285198
refresh = 10000 (2 hours 46 mins 40 secs)
retry = 2400 (40 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)

C:\Documents and Settings\labuser>nslookup -query=MX www.caltech.edu
Server: achilles.noc.ntua.gr
Address: 147.102.222.210

Non-authoritative answer:
www.caltech.edu canonical name = www.caltech.edu.cdn.cloudflare.net

cloudflare.net
primary name server = ns1.cloudflare.net
responsible mail addr = dns.cloudflare.com
serial = 1653285198
refresh = 10000 (2 hours 46 mins 40 secs)
retry = 2400 (40 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)

C:\Documents and Settings\labuser>
```

Για τους εξυπηρετητές DNS (βγαίνει ίδια απάντηση με το -query=MX και δεν μας δίνονται συνολικά οι πληροφορίες που θέλουμε):

```
C:\WINDOWS\system32\cmd.exe

primary name server = ns1.cloudflare.net
responsible mail addr = dns.cloudflare.com
serial = 1653285198
refresh = 10000 (2 hours 46 mins 40 secs)
retry = 2400 (40 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)

C:\Documents and Settings\labuser>nslookup -query=NS www.caltech.edu
Server: achilles.noc.ntua.gr
Address: 147.102.222.210

Non-authoritative answer:
www.caltech.edu canonical name = www.caltech.edu.cdn.cloudflare.net

cloudflare.net
primary name server = ns1.cloudflare.net
responsible mail addr = dns.cloudflare.com
serial = 1653285590
refresh = 10000 (2 hours 46 mins 40 secs)
retry = 2400 (40 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)

C:\Documents and Settings\labuser>
```

Όχι, δεν μπορώ να διακρίνω μηχανήματα που τρέχουν συγκεκριμένες υπηρεσίες. Δεν μου δίνονται οι κατάλληλες πληροφορίες.

### Ερώτηση 3.2

[www.princeton.edu](http://www.princeton.edu)

Στέλνονται από εμένα ICMP πακέτα με Type = 8, Code = 0 (Echo ping request) και επιστρέφονται ICMP πακέτα με Type = 0, Code = 0 (Echo ping reply). Το περιεχόμενο τους είναι η λατινική αλφάβητος από το a μέχρι το w (σε hex μορφή από 61 μέχρι 77 και πίσω) και ξανά από την αρχή και έχει μέγεθος payload 32 bytes.

### Ερώτηση 3.3

[www.lse.ac.uk](http://www.lse.ac.uk)

### Ερώτηση 3.4

[www.auth.gr](http://www.auth.gr)

Εργαλείο IP whois του RIPE: <https://apps.db.ripe.net/search/query.html>

Η παραχώρηση αυτή αφορά το υποδίκτυο 155.207.0.0, αφού η διεύθυνση είναι η 155.207.1.12 με Range 155.207.0.0/16. Η έδρα του οργανισμού βρίσκεται στη Θεσσαλονίκη στη Μακεδονία. Ανήκει στο αυτόνομο σύστημα AS5470 - Aristotle University of Thessaloniki.

### Ερώτηση 3.5

[el-gr.facebook.com](http://el-gr.facebook.com)

Εργαλείο looking glass της Hurricane Electric: <https://lg.he.net/>

|    |           |           |           |                                                                             |
|----|-----------|-----------|-----------|-----------------------------------------------------------------------------|
| 1  | *         | *         | *         | ?                                                                           |
| 2  | 139<br>ms | 317<br>ms | 176<br>ms | <b>palo-b24-link.telia.net</b> (195.12.255.209)                             |
| 3  | 229<br>ms | 152<br>ms | 149<br>ms | <b>nyk-bb2-link.ip.twelve99.net</b> (62.115.122.37)                         |
| 4  | 293<br>ms | 174<br>ms | 243<br>ms | <b>ldn-bb1-link.ip.twelve99.net</b> (62.115.113.21)                         |
| 5  | 150<br>ms | 150<br>ms | 219<br>ms | <b>prs-bb1-link.ip.twelve99.net</b> (62.115.135.25)                         |
| 6  | 159<br>ms | 166<br>ms | 237<br>ms | <b>ffm-bb1-link.ip.twelve99.net</b> (62.115.123.12)                         |
| 7  | 185<br>ms | 250<br>ms | 165<br>ms | <b>win-bb3-link.ip.twelve99.net</b> (62.115.137.203)                        |
| 8  | 284<br>ms | 188<br>ms | 161<br>ms | <b>win-b2-link.ip.twelve99.net</b> (62.115.114.185)                         |
| 9  | 283<br>ms | 201<br>ms | 299<br>ms | <b>edgenetwork-ic341188-win-b2.ip.twelve99-cust.net</b><br>(62.115.175.215) |
| 10 | 199<br>ms | 300<br>ms | 199<br>ms | <b>po103.psw01.vie1.tfbnw.net</b> (31.13.27.135)                            |
| 11 | 186<br>ms | 178<br>ms | 188<br>ms | 173.252.67.17                                                               |
| 12 | 174<br>ms | 182<br>ms | 189<br>ms | <b>edge-star-shv-01-vie1.facebook.com</b> (31.13.84.8)                      |

Ναι, μπορώ να καταλάβω από τα ονόματα των DNS ότι βρίσκονται σε συγκεκριμένες πόλεις όπως palo – Palo Alto, nyk – New York, ldn – London, prs – Paris κλπ.

### Ερώτηση 3.6

Εργαλείο Visual Traceroute: <http://en.dnstools.ch/visual-traceroute.html>

### Ερώτηση 3.7

[www.uoa.gr](http://www.uoa.gr)

Ο εξυπηρετητής χρησιμοποιεί Linux λειτουργικό σύστημα και nginx λογισμικό εξυπηρετητή ιστού. Το όνομα του αρμόδιου εξυπηρετητή DNS για την περιοχή στην οποία ανήκει είναι ns1.uoa.gr.

### Ερώτηση 3.8

```
02:59:16.225274 ARP, Request who-has 10.10.10.3 tell 10.10.10.4, length 28
    0x0000: 0001 0800 0604 0001 0800 2710 d751 0a0a .....Q..
    0x0010: 0a04 0000 0000 0000 0a0a 0a03 .....
02:59:16.228019 ARP, Reply 10.10.10.3 is-at 08:00:27:d4:16:3c (oui Unknown), length 46
    0x0000: 0001 0800 0604 0002 0800 27d4 163c 0a0a .....<..
    0x0010: 0a03 0800 2710 d751 0a0a 0a04 0000 0000 .....Q.....
    0x0020: 0000 0000 0000 0000 0000 0000 0000 .....
02:59:16.228031 IP 10.10.10.4.38915 > 10.10.10.3.33434: UDP, length 32
    0x0000: 4500 003c 1faa 0000 0111 71ed 0a0a 0a04 E..<.....q.....
    0x0010: 0a0a 0a03 9803 829a 0028 2854 4041 4243 .....((T@ABC
    0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS
    0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^_
02:59:16.228332 IP 10.10.10.3 > 10.10.10.4: ICMP 10.10.10.3 udp port 33434 unreachable, length 36
    0x0000: 4500 0038 000f 0000 4001 529c 0a0a 0a03 E..8....@.R.....
    0x0010: 0a0a 0a04 0303 1a56 0000 0000 4500 003c .....V....E..<
    0x0020: 1faa 0000 0111 71ed 0a0a 0a04 0a0a 0a03 .....q.....
    0x0030: 9803 829a 0028 c7e0 .....(..
02:59:16.229412 IP 10.10.10.4.53418 > 10.10.10.3.33435: UDP, length 32
    0x0000: 4500 003c 1fab 0000 0111 71ec 0a0a 0a04 E..<.....q.....
    0x0010: 0a0a 0a03 d0aa 829b 0028 2854 4041 4243 .....((T@ABC
    0x0020: 4445 4647 4849 4a4b 4c4d 4e4f 5051 5253 DEFGHIJKLMNOPQRS
    0x0030: 5455 5657 5859 5a5b 5c5d 5e5f TUVWXYZ[\]^_
```

Το ανώτερο στρώμα των πακέτων που παρήχθησαν από το traceroute είναι UDP. Το περιεχόμενο τους είναι η αλφάβητος ABC έως και XYZ και το μήκος του payload είναι 32 bytes. Τα πακέτα που ελήφθησαν ως απάντηση είναι τύπου ICMP.

Εδώ χρησιμοποιούνται UDP πακέτα, ενώ στο tracert των Windows χρησιμοποιούνται ICMP πακέτα. Κατά τα άλλα, προσφέρουν τις ίδιες πληροφορίες.

### Ερώτηση 3.9

Τρέχοντας \$ telnet 10.10.10.2 βγαίνει σφάλμα Connection Refused, πιθανόν διότι το port του telnet (23) είναι πίσω από κάποιο firewall.

Τρέχοντας \$ telnet 10.10.10.2 80 για να συνδεθώ στην υπηρεσία HTTP, εμφανίζεται πάλι ένα Bad Request και βλέπω ότι τρέχει lighttpd για εξυπηρετητή ιστού σε έκδοση 1.4.35.

### Ερώτηση 3.10

### Ερώτηση 3.11

10.10.10.3

### Ερώτηση 3.12

Ζητούμενη τεχνική scan: SYN

```

INFO: Can't import python gnuplot wrapper . Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
WARNING: No route found for IPv6 destination :: (no default route?)
INFO: Can't import python Crypto lib. Won't be able to decrypt WEP.
INFO: Can't import python Crypto lib. Disabled certificate manipulation tools
Welcome to Scapy (2.2.0)
>>> sr1(IP(dst="10.10.10.2")/TCP(dport=22,flags="S"))
Begin emission:
.*Finished to send 1 packets.

Received 2 packets, got 1 answers, remaining 0 packets
<IP  version=4L  ihl=5L  tos=0x0  len=44  id=38  flags=DF  frag=0L  ttl=64  proto=tcp  ch
ksum=0x128d  src=10.10.10.2  dst=10.10.10.4  options=[]  |<TCP  sport=ssh  dport=ftp_
data  seq=180719883  ack=1  dataofs=6L  reserved=0L  flags=SA  window=65535  chksum=0xd
401  urgptr=0  options=[('MSS', 1460)]  |<Padding  load='\x00\x00'  |>>>
>>> sr1(IP(dst="10.10.10.2")/TCP(dport=23,flags="S"))
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
<IP  version=4L  ihl=5L  tos=0x0  len=40  id=39  flags=DF  frag=0L  ttl=64  proto=tcp  ch
ksum=0x1290  src=10.10.10.2  dst=10.10.10.4  options=[]  |<TCP  sport=telnet  dport=f
tp_data  seq=0  ack=1  dataofs=5L  reserved=0L  flags=RA  window=0  chksum=0x878b  urgpt
r=0  |<Padding  load='\x00\x00\x00\x00\x00\x00'  |>>>
>>> _

```

Παρατηρώ ότι και στα δύο μηνύματα λαμβάνω απάντηση με ACK = 1, κάτι που σημαίνει ότι οι θύρες αυτές είναι ανοιχτές για εισερχόμενες συνδέσεις.

### Ερώτηση 3.13

50000 – 51999

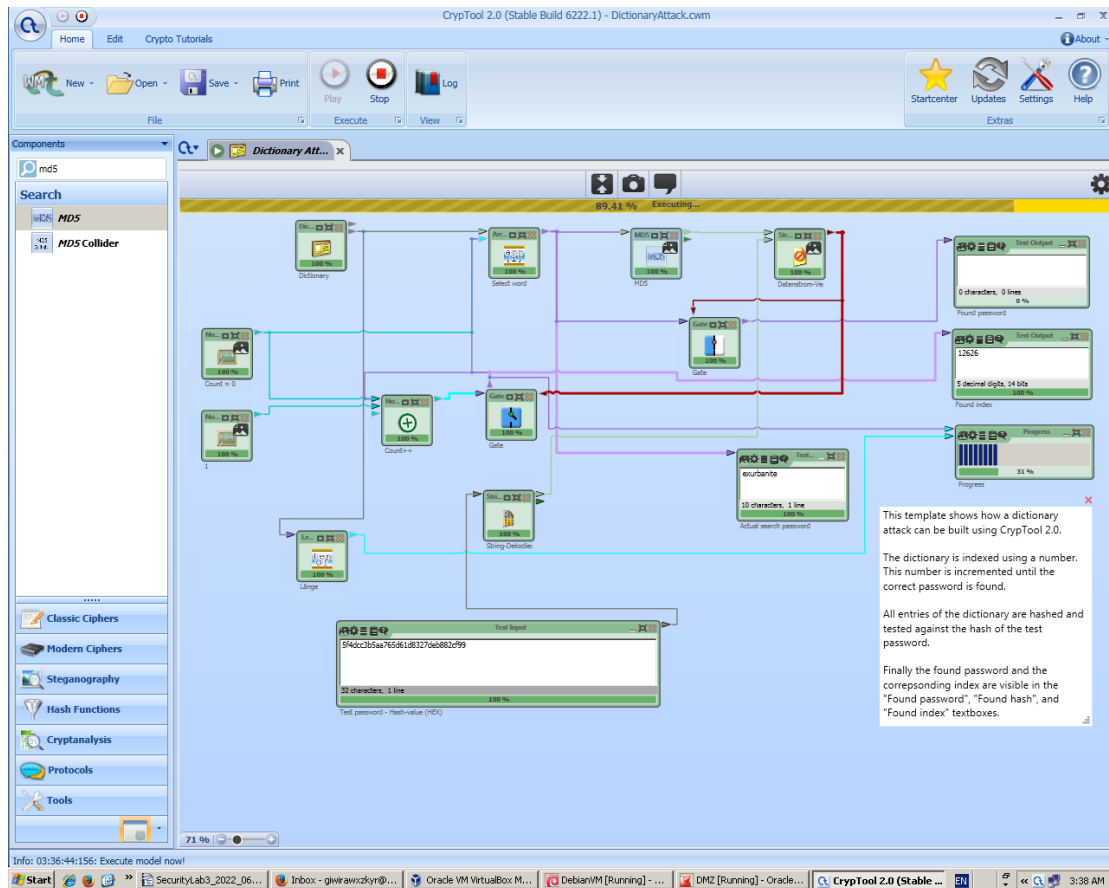
### Ερώτηση 3.14

10.10.10.2

### Ερώτηση 3.15

Το username είναι user, ενώ για το password μας δίνεται ένα hash μήκους 32 χαρακτήρων, άρα 128 bits, που σημαίνει πως έχουμε MD5 hash function, επειδή είναι το μόνο με 128 μήκος hash.

Τελικά το password είναι password.



### Ερώτηση 3.16

Η σύνδεση μέσω SSH εμφανίζει ένα προειδοποιητικό μήνυμα, πως ο λογαριασμός αυτός δεν είναι προσωρινά διαθέσιμος και πως η σύνδεση αυτή έκλεισε. ("This account is currently not available. Connection to 10.10.10.2 closed")

```
Last login: Wed May 13 20:39:58 2015 from 10.10.10.4
FreeBSD 10.1-RELEASE (GENERIC) #0 r274401: Tue Nov 11 22:51:51 UTC 2014

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories: https://www.FreeBSD.org/security/
FreeBSD Handbook: https://www.FreeBSD.org/handbook/
FreeBSD FAQ: https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums: https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with: pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed: freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages: man man
FreeBSD directory layout: man hier

Edit /etc/motd to change this login announcement.
This account is currently not available.
Connection to 10.10.10.2 closed.
root@debian:~#
```

Προσπαθώντας να συνδεθώ με ftp στον ίδιο λογαριασμό, η σύνδεση πετυχαίνει.

```
root@debian:~# ftp 10.10.10.2
Connected to 10.10.10.2.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 15 allowed.
220-Local time is now 03:45. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 15 minutes of inactivity.
Name (10.10.10.2:root): user
331 User user OK. Password required
Password:
230 OK. Current directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

### Ερώτηση 3.17

fiona

### Ερώτηση 3.18

### Ερώτηση 3.19

### Ερώτηση 3.20



```

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,52AF70029B289A36

hj8M0/XuvHIhpXKXaLWl1QeVG5QSmufgYF0esanhuzzYuYd127uQvuPIteHEXX7
WaPj59PBKRCHL3/+S3ALk/wNRhFQTyMIQ6Hh14V05wQ03qJt2qXrMCy5oJ0sken9
FuM+PX6iGw7nkV7S1wRoJ6DGPt1uoxruTHTWZpVpN9ds5Uw31Pe0IQhjBgheG6Uy
6dUJfEJWFp71U9gE1GH/utY1Gk4oK7HCNmTcNTbQ10hDXaumMNBv3XhxiuHugMi
UAF60Z6obgUP1xpRvWJNi+ZufDhnS4uMIubSn/MkInCtpMzr06SaXibnKn/VIDc
umPc9A5sqEoe99Aw0GNvXcoCXdhNQLKcc5PxAAGr2KbqJtRqVSIYSC6dqWE4jKi0
V3no/B1zx1SQStQ11A77CbRfp2a2EXTtHLR7sg/6es8Frz+hq4LffN02KinJUgrx
r9bB1rrr8sAHMkuZ8oip4D0qs/GvSKJg5ZLvrWtCLg5J+aQAfEN9bNy7b3z5ftSe
LX77qKb/H6AqG19r2RYSqX8X73RHSRLRqx4XdZu8qVvKoZ+KePIOUvg2xLFCHzVtC
7Y23UgP/cydygjm3554rWn5m6CX3VQvKoDT1hYW1BENoPFtc/haQopLbkqk0SVp6
1Bk3I7dI9sWRnH0H90uLSbWgk11ma8T+1P72jrPVH4ItQ10Yy10Jg45FBNXoJb1J
bfRI7DRxYld+R6i2+oKCMxJhIQBwdSRc/6FeAsNM1R6qCmlyIc4TReguVZKxfMw0
Ys9Kpks8RsdTMeX+WUODSA24geR1m0Jxx7+4nLRCiPvYIloTrWfQKjpY/2xxMT9U
QoPulxch5+Y4/VtjZTPDLy1GtjBo3ufIBduYdSYxx5ha6h6ERK052KfXn2S3xN1K
DE4Me6Y12N71CW6FT0BDOx9URLe231CXMJnA8PVPm0pUfBXf6S2Q+qvZDBdvBQFr
SaqDU+RfOluCQglVqW08Jkv156UYASo/Lmd47GshQU8WYfLj0t9s68iKc9m/wlfd
jbG9QXIb7mL4jPEjFfow15ov37jwWVjG56X5Xaj9q6FFsXbqRBDW0Bs78Bny/nF9
hp5/pseEULfInKnYfKoascxCH2oc0e1f0B1k+cXq+JOKJ8jMjjbYXNBTwoNhSDqp
bVoJwpyj5fCMTPCJJ3X5F4o3P1fFu31yRd/EnP8LXMs0fG3N40zOrdsExwSdf/qZ
bfHYtBgSIVDvUz1ks0IvpJK2rYUGUJJ4HDBXXE/0eWNMbbbzF6WwuEYttQsksnpyw
keyset_03118153.pem_

```

```

-----BEGIN RSA PRIVATE KEY-----
MIIEEowIBAAKCAQEAXvGhQze5v+pCEh1gDrrF8hEsnBzyF44oriE/xaCpQ+yEB5TR
Ii5bhH91gbQH6eWaxDqI+JmyJghBC5KogRffBWzvYz8bTy+zkrWwPweAlt7KK3yt
egdX0Su4Ki00/d5VJmYUrLCEnAFDKQwqb8YvSvsLpd9RHewrc/R3/5BeEsUFIth
baCGYJf86AgsR3ouBgASN1GDzW116C0qxBKJrcC/B3026/y/URkNoeZuQhUro5ue
IZUqIDUnExyT3FL/HXFXC3i2u8RhuHAAttKxvXSC8X0mwuc165V3g/ntU9KyJVj4E
zCtvNo4VD6wgS/7m19oL8xx/dMf+nyEJc7nRFwIDAQABAoIBAQCf4o1dmD4YqWwF
/WDS6MNYUjiMY2qFcbVs4pFfxZdsKDCMamwtXjo0mkUS6YjdFMLD+SqJtc7oRoFJu
AGGIYNFFbHd6ejjdxMN8A2w2LS0UPfke5Qw2aISwD1Ukft1KUHTKg6VQW18DW4H6
bPEW+7Uhc1LDVE4IauhrQMYEka7rzanEBPsgHV27TNPgvfnD0vryK8Xj+We9WmwX
r9gtL6sDCF3r0AaNEncJVQHT3hDY2lsqdRQxjblUgq77EY8mniRLrKq6Y1sqW1G/
j9C3F/683YcKYuwVJnn4cdtisp07a/Cf6t6kRqG5pyxb7pHmp3AyMEIGLeyCi195
uKqf5YcJAoGBA0bAeNHQ3J2JGiTUUCTbHZF0YuvVNVWFAM01CUD1AXudHINcLKg
116xjsaAKrtIqFfw/ihXnma+kqKQhPj4YvhyExCgOITzRyIb7YpWrhZPY17QRuY+
vidyH7P2Vuksrs10C7hrtBbtFPpdbauGJoRQBHKR5CjPhfm7nChCXx1AoGBANy2
MXo57pxL0xRhdoG7udHJIjHPqgiHDQwm2rzIO61cbkGdN+DoKMwV9DwoEPvbSbCm
+dmD5/f5GsTVZMnx75pTq7zB4UFx5b5Esvmb5fCAR2f96dbKjHi8cSmytdM5Y+EK
UzLC3WbkyEuEocssuBBAGdPz7nBc1+HgZ0n189XbAoGAYdNn2Uwuu3rMYqC/+WAL
gPYYQCfsxyTfBxbzUXX2BS26oD+ib41KhIqyB0WB0DTtaZr5pRDATr6sW875ELP9
AWcbPgku705WUdeVNPjahQrSoW+bHzGqW/7o3Usv0XLxcvx0/SsgeaTnJkvrY68b
LvXx05m0DXunb2qv23/qDAECgYBXMbc8RVTJ9H6wZ4ys1iAkC+TOAAPjYI88BJPD
80cDepuoW1cwCCfN8MJrXZzQEYL6ogzE7QKgiY4Uwy5Dfcwd2P5Y9PNrqnaMA5H9
YKSnrDYH9FOEWULD1BbU1WBV0S9vQWf6/tb/B1VG2GAe50zURq6teInz2Ap51xnt
Z0Y+zwKBGfZyCbaxDXqPLlgsa1yx4tUPZzoc2SrfpCTT2s01ze2A/G3zNjS03mmQ
:_

```

Ο λόγος που γίνεται η συμμετρική κρυπτογράφηση στο κλειδί είναι διότι ένας χρήστης θα θέλει να κρυπτογραφήσει και να αποκρυπτογραφήσει το κλειδί, οπότε δεν υπάρχει λόγος για να υπάρξει ασύμμετρη κρυπτογράφηση, αφού είναι το ίδιο άτομο μόνο που θα το χρησιμοποιήσει.

### Ερώτηση 3.21

|   |  |
|---|--|
| n |  |
| e |  |
| d |  |
| p |  |

(Εάν στον παραπάνω πίνακα δεν μπορείτε εύκολα να κάνετε copy-paste τα ζητούμενα, παραθέστε το σχετικό screenshot.)

```
Private-Key: (2048 bit)
modulus:
  00:c6:f1:a1:43:37:b9:bf:ea:42:12:1d:60:0e:ba:
  c5:f2:11:2c:9c:1c:f2:17:8e:28:ae:21:3f:c5:a0:
  a9:43:ec:84:07:94:d1:22:2e:5b:84:7f:75:81:b4:
  07:e9:e5:9a:5c:3a:88:f8:99:b2:26:08:41:0b:92:
  a8:81:17:df:05:6c:ef:63:3f:1b:4f:2f:b3:92:b5:
  b0:3f:07:80:2e:de:ca:2b:7c:ad:7a:07:57:d1:2b:
  b8:2a:23:b4:fd:de:55:24:c9:98:52:b2:c2:12:70:
  05:0c:a4:30:a9:bf:18:bd:2b:ec:2e:97:7d:44:77:
  b0:ad:cf:d1:df:fe:41:78:4b:14:14:8b:61:6d:a0:
  86:60:97:fc:e8:08:2c:47:7a:2e:06:00:12:36:51:
  83:cd:69:75:e8:2d:2a:c4:12:89:ad:c0:bf:07:73:
  b6:eb:fc:bf:51:19:0d:a1:e6:6e:42:15:2b:a3:9b:
  9e:21:95:2a:20:35:27:13:1c:93:dc:52:ff:1d:71:
  57:0b:78:b6:bb:c4:61:b8:70:2d:b6:4c:6f:5d:20:
  bc:5c:e9:b0:b9:c9:7a:e5:5d:e0:fe:7b:54:f4:ac:
  89:56:3e:04:cc:2b:6f:36:8e:15:0f:ac:20:4b:fe:
  e6:d7:da:0b:f3:1c:7f:74:c7:fe:9f:21:09:73:b9:
  d1:17
publicExponent: 65537 (0x10001)
privateExponent:
  00:85:e2:8d:5d:98:3e:18:ab:05:85:fd:60:ec:e8:
  c3:58:52:38:8c:63:6a:85:71:b5:6c:e2:91:71:65:
  :_
```

```
privateExponent:
  00:85:e2:8d:5d:98:3e:18:ab:05:85:fd:60:ec:e8:
  c3:58:52:38:8c:63:6a:85:71:b5:6c:e2:91:71:65:
  db:24:0c:23:1a:9b:0b:57:8e:8d:26:91:44:ba:62:
  37:45:30:b0:fe:4a:a2:6d:73:ba:11:a0:52:6e:00:
  68:08:60:d1:45:6c:77:7a:7a:38:dd:c4:c3:7c:03:
  6c:36:2e:cd:14:3d:f9:1e:e5:0c:36:68:84:b0:0f:
  55:24:7e:dd:4a:50:7b:4a:83:a5:50:5a:5f:03:5b:
  81:fa:6c:f1:16:fb:b5:21:72:52:c3:54:4e:08:6a:
  e8:6b:40:c6:04:91:ae:eb:cd:a3:44:6c:fb:20:85:
  5d:bb:4c:d3:e0:bd:f9:c3:d2:fa:f2:2b:c5:e3:f9:
  67:bd:5a:6c:31:af:da:ad:2f:ab:03:08:5d:eb:38:
  06:8d:12:77:09:55:01:d3:de:10:d8:66:5b:2a:75:
  14:31:8d:b9:54:82:ae:fb:11:8f:26:9e:24:4b:ac:
  aa:ba:62:5b:2a:5b:51:bf:8f:d0:b7:17:fe:bc:dd:
  87:0a:62:ec:15:26:79:f8:71:db:62:b2:9d:3b:6b:
  f0:9f:ea:de:a4:46:a1:b9:a7:2c:5b:ee:91:e6:a7:
  70:32:30:42:06:2d:ec:82:8a:5f:79:b8:aa:9f:e5:
  87:09
prime1:
  00:e6:c0:78:d1:d0:dc:9d:89:1a:24:d4:50:24:db:
  1d:91:4c:d1:8b:af:54:d5:56:14:03:34:94:25:03:
  d4:05:ee:74:72:0d:70:b2:86:d6:5e:b1:8e:c6:80:
  2a:bb:48:a8:57:f0:fe:28:57:9e:66:be:92:a2:90:
  :_
```

```
prime1:
  00:e6:c0:78:d1:d0:dc:9d:89:1a:24:d4:50:24:db:
  1d:91:4c:d1:8b:af:54:d5:56:14:03:34:94:25:03:
  d4:05:ee:74:72:0d:70:b2:86:d6:5e:b1:8e:c6:80:
  2a:bb:48:a8:57:f0:fe:28:57:9e:66:be:92:a2:90:
  84:f8:f8:62:f8:72:13:10:a0:38:84:f3:47:22:1b:
  ed:8a:56:ae:16:4f:62:5e:d0:46:e6:3e:be:27:72:
  84:ce:cf:d9:5b:a4:b2:bb:35:38:2e:e1:ae:d0:5b:
  b4:53:e9:75:b6:ae:18:9a:11:40:11:ca:47:90:a3:
  3e:17:e6:ee:70:a1:09:7c:75
prime2:
  00:dc:b6:31:7a:39:ee:9c:4b:d3:14:61:76:81:bb:
  b9:d1:c9:22:38:4f:42:08:87:0d:0c:26:66:bc:c8:
  d3:a9:5c:6e:41:9d:37:e0:e8:28:cc:15:f4:3c:28:
  10:fb:db:49:b0:a6:f9:d9:83:e7:f7:f9:1a:c4:d5:
  cc:c9:f1:ef:9a:53:ab:bc:c1:e1:41:71:e5:be:44:
  b2:f9:9b:e5:f0:80:47:67:fd:e9:d6:ca:8c:78:bc:
  71:29:b2:b5:d3:39:63:e1:0a:53:32:c2:dd:66:e4:
  c8:4b:84:a1:cb:2c:b8:10:40:19:d3:f3:ee:70:5c:
  d7:e1:e0:cf:49:e5:f3:d5:db
exponent1:
  61:d3:67:65:4c:2e:bb:7a:cc:62:a0:bf:f9:60:0b:
  80:f6:18:40:27:ec:c7:24:df:07:1c:db:51:75:f6:
  05:2d:ba:a0:3f:a2:6f:8d:4a:84:8a:b2:04:e5:81:
:_
```

```
exponent1:
  61:d3:67:65:4c:2e:bb:7a:cc:62:a0:bf:f9:60:0b:
  80:f6:18:40:27:ec:c7:24:df:07:1c:db:51:75:f6:
  05:2d:ba:a0:3f:a2:6f:8d:4a:84:8a:b2:04:e5:81:
  38:34:ed:69:9a:f9:a5:10:c0:4e:be:ac:5b:ce:f9:
  10:b3:fd:01:67:1b:3e:09:2e:ec:ee:56:51:d7:95:
  34:f8:da:85:0a:d2:a1:6f:9b:1f:31:aa:5b:fe:e8:
  de:e4:af:39:72:f1:72:fc:74:fd:2b:20:79:a4:e7:
  26:4b:eb:63:af:1b:2e:f5:f1:3b:99:8e:0d:7b:a7:
  6f:6a:af:db:7f:ea:0d:a1
exponent2:
  57:31:b7:3c:45:54:c9:f4:7e:b0:67:8c:ac:d6:20:
  24:0b:e4:f4:00:03:e3:60:8f:3c:04:93:c3:f3:47:
  03:7a:9b:a8:5a:57:30:08:27:cd:f0:c2:6b:5d:9c:
  d0:13:22:fa:a2:0c:c4:ed:02:a0:89:8e:14:c3:2e:
  43:7d:cc:1d:d8:fe:58:f4:f3:6b:aa:76:8c:03:91:
  fd:60:a4:a7:ad:d6:07:f4:5d:04:59:42:c3:94:16:
  d4:d5:60:55:d1:2f:6f:41:67:fa:fe:d6:ff:06:55:
  46:d8:60:1e:e7:4c:d4:46:ae:ad:78:89:f3:64:0a:
  79:97:19:ed:64:e6:3e:cf
coefficient:
  5c:d8:71:b6:b1:0d:7a:a9:2e:58:2c:6b:5c:b1:e2:
  d5:0f:67:3a:1c:65:2a:df:a4:24:d3:66:cd:35:cd:
  e6:40:fc:6d:f3:36:34:b4:de:69:90:45:8f:13:3a:
:_
```

```

34:f8:da:85:0a:d2:a1:6f:9b:1f:31:aa:5b:fe:e8:
de:e4:af:39:72:f1:72:fc:74:fd:2b:20:79:a4:e7:
26:4b:eb:63:af:1b:2e:f5:f1:3b:99:8e:0d:7b:a7:
6f:6a:af:db:7f:ea:0d:a1
exponent2:
57:31:b7:3c:45:54:c9:f4:7e:b0:67:8c:ac:d6:20:
24:0b:e4:f4:00:03:e3:60:8f:3c:04:93:c3:f3:47:
03:7a:9b:a8:5a:57:30:08:27:cd:f0:c2:6b:5d:9c:
d0:13:22:fa:a2:0c:c4:ed:02:a0:89:8e:14:c3:2e:
43:7d:cc:1d:d8:fe:58:f4:f3:6b:aa:76:8c:03:91:
fd:60:a4:a7:ad:d6:07:f4:5d:04:59:42:c3:94:16:
d4:d5:60:55:d1:2f:6f:41:67:fa:fe:d6:ff:06:55:
46:d8:60:1e:e7:4c:d4:46:ae:ad:78:89:f3:64:0a:
79:97:19:ed:64:e6:3e:cf
coefficient:
5c:d8:71:b6:b1:0d:7a:a9:2e:58:2c:6b:5c:b1:e2:
d5:0f:67:3a:1c:65:2a:df:a4:24:d3:66:cd:35:cd:
e6:40:fc:6d:f3:36:34:b4:de:69:90:45:8f:13:3a:
f3:0f:11:47:d7:ec:2d:e2:47:76:36:fc:f1:62:6b:
72:9e:4c:16:46:7c:27:e7:a5:d8:dc:87:1a:7e:52:
57:d2:6c:0c:85:72:25:b2:60:05:8f:be:b8:9f:d2:
4d:d0:f4:d5:66:56:84:07:af:42:18:ce:13:63:6c:
45:a3:fa:ad:a4:07:c7:bf:52:ad:84:54:de:4e:15:
36:9f:e5:28:02:4c:7e:1f
(END)_

```

```

46:d8:60:1e:e7:4c:d4:46:ae:ad:78:89:f3:64:0a:
79:97:19:ed:64:e6:3e:cf
coefficient:
5c:d8:71:b6:b1:0d:7a:a9:2e:58:2c:6b:5c:b1:e2:
d5:0f:67:3a:1c:65:2a:df:a4:24:d3:66:cd:35:cd:
e6:40:fc:6d:f3:36:34:b4:de:69:90:45:8f:13:3a:
f3:0f:11:47:d7:ec:2d:e2:47:76:36:fc:f1:62:6b:
72:9e:4c:16:46:7c:27:e7:a5:d8:dc:87:1a:7e:52:
57:d2:6c:0c:85:72:25:b2:60:05:8f:be:b8:9f:d2:
4d:d0:f4:d5:66:56:84:07:af:42:18:ce:13:63:6c:
45:a3:fa:ad:a4:07:c7:bf:52:ad:84:54:de:4e:15:
36:9f:e5:28:02:4c:7e:1f
root@debian:~# openssl rsa -in keyset_03118153.pem -pubout
Enter pass phrase for keyset_03118153.pem:
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAXvGhQze5v+pCEh1gDrrF
8hEsnBzyF44oriE/xacPQ+yEB5TRii5bhH91gbQH6eWaxDqI+JmyJghBC5KogRff
BWzvYz8bTy+zkrWwPweALT7KK3ytegdx0Su4Ki00/d5VJmmYUrLCEnAFDKQwqb8Y
vSvsLpd9RHewrc/R3/5BeEsUFithbaCGYJf86AgsR3ouBgASN1GDzWl16C0qxBKJ
rcC/B3026/y/URKNoe2uQhUro5ueIZUqIDUnExyT3FL/HXFXC3i2u8RhuHAttKxv
XSC8X0mwuc165V3g/ntU9KyJVj4EzCtvNo4VD6wgS/7m19oL8xx/dMf+nyEJc7nR
FwIDAQAB
-----END PUBLIC KEY-----
root@debian:~# _

```

## Ερώτηση 3.22

## Ερώτηση 3.23