

## ΛΥΣΕΙΣ ΘΕΜΑΤΩΝ

Από τον καθηγητή Πληροφορικής Σολωμό Κωνσταντίνο του ΕΠΑΛ Βόνιτσας

ΘΕΜΑ Α (Μονάδες 12)

A1.

α. Η ψηφιακή υπογραφή ενός ηλεκτρονικού μηνύματος χρησιμοποιείται για την απόδειξη της ταυτότητας του αποστολέα, καθώς και για την ακεραιότητα των δεδομένων. Σωστό. Δες σελίδα 324 του βιβλίου στη μέση Η ψηφιακή υπογραφή είναι.... Για την ακεραιότητα των δεδομένων (θέμα αναμενόμενο να ζητηθεί και ως ανάπτυξη θεωρίας)

β. Το μήκος της MAC διεύθυνσης στο σύστημα Ethernet είναι 64 bits. Λάθος, είναι 48 bits (Σελίδα 247 τελευταία παράγραφος)

γ. Οι δρομολογητές είναι ειδικές συσκευές που διασυνδέουν μεταξύ τους διαφορετικά δίκτυα. Σωστό

δ. Το κόστος της υπηρεσίας ISDN είναι ανεξάρτητο της κίνησης. Λάθος Ο χρήστης πληρώνει όδο διαρκεί η χρήση σελίδα 205 δεύτερη παράγραφος. Για αυτό και δεν συμφέρει για 24ωρη σύνδεση στο διαδίκτυο.

ε. Σκοπός του πρωτοκόλλου ARP είναι να μετατρέπει τις IP διευθύνσεις στις αντίστοιχες φυσικές, έτσι ώστε οι εφαρμογές να απαλλαγούν από αυτό το έργο. Σωστό, Σελίδα 255 πρώτη παράγραφος

στ. Ένα δίκτυο intranet δεν περιορίζεται σε συγκεκριμένη γεωγραφική περιοχή, αντίθετα μπορεί να εκτείνεται σε διαφορετικές περιοχές, όπου βρίσκονται γραφεία ή εγκαταστάσεις ενός οργανισμού. Σωστό. Είναι ο ορισμός του Intranet

A2. Να μεταφέρετε στο τετράδιό σας το γράμμα της σωστής απάντησης. (Μονάδες 5)

Στην ασυμμετρική κρυπτογράφηση, εάν ο Α θέλει να εξασφαλίσει την εμπιστευτικότητα των δεδομένων που θα στείλει προς τον Β, δηλαδή να εξασφαλίσει ότι ο Β θα μπορεί να καταλάβει το περιεχόμενο του μηνυματός του, τότε:

Η σωστή απάντηση είναι η α, θα κρυπτογραφήσει το μήνυμα με το δημόσιο κλειδί του Β. (Μην ξεχνάτε, ότι στην ασυμμετρική κρυπτογράφηση, η κωδικοποίηση και η αποκωδικοποίηση δεν γίνεται με το ίδιο κλειδί, αλλά με συνδυασμό δημόσιου και ιδιωτικού κλειδιού του ενός ή του άλλου. Αν κωδικοποιείται το μήνυμα με το δημόσιο κλειδί του Β θα αποκωδικοποιηθεί ΜΟΝΟ με το ιδιωτικό κλειδί του Β, άρα μόνο ο Β θα μπορεί να το διαβάσει. Δείτε σελίδα 323 του σχολικού βιβλίου. Είναι το σχήμα της εμπιστευτικότητας, το πρώτο σχήμα. (Αναμενόμενο θέμα και για θεωρία)

A3. Να γράψετε στο τετράδιό σας τους αριθμούς 1, 2, 3, 4 από τη στήλη Α και δίπλα ένα από τα γράμματα α, β, γ, δ, ε της στήλης Β που δίνει τη σωστή αντιστοίχιση. Σημειώνεται ότι ένα γράμμα από τη στήλη Β θα περισσέψει. (Μονάδες 8)

Αντιστοίχιση
1. Υπηρεσία εικονικού τερματικού γ (port 23, είναι υπηρεσία telnet)
2. Υπηρεσία αποστολής μηνύματος μέσω ηλεκτρονικού ταχυδρομείου (δ, port 25)
3. Υπηρεσία αποστολής FTP εντολών, (α port 21)
4. Υπηρεσία αποστολής δεδομένων με FTP από τον πελάτη (ε, port 20) (πονηρή λεπτομέρεια του βιβλίου)

ΘΕΜΑ Β

B1. Τι ονομάζεται επικοινωνιακό υποδίκτυο και ποιο είναι το έργο του; **Μονάδες 8**

B2. Ποιες είναι οι διαφορές του UDP πρωτοκόλλου από το TCP πρωτόκολλο; **Μονάδες 12**

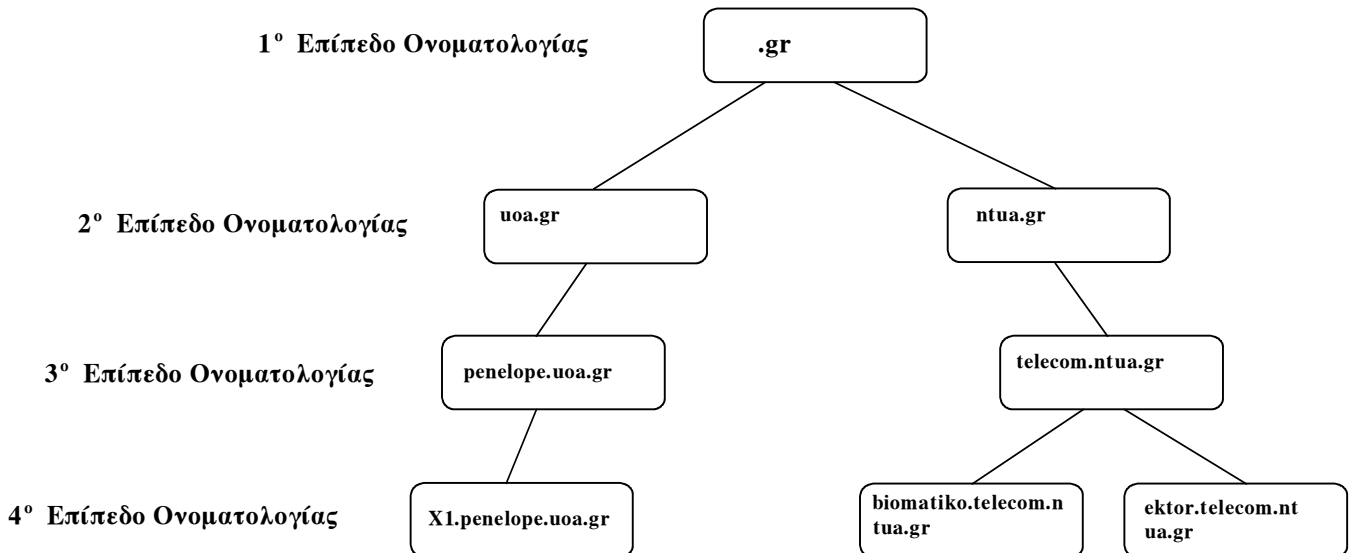
B3. Προσδιορίστε την έννοια της **εγκυρότητας** (μον. 2) και γράψτε τον ορισμό της **ασφάλειας πληροφοριών** (μον. 3).

**Δείτε σχολικό βιβλίο σελίδα 220 για το B1, σελίδα 240 για το B2, σελίδες 315,316 για το B3**

ΘΕΜΑ Γ (μονάδες 25)

Γ1. Αφού μεταφέρετε το παρακάτω σχήμα στο τετράδιό σας, να συμπληρώσετε τα κενά λαμβάνοντας υπόψη την ιεραρχική οργάνωση χώρου ονομάτων DNS για τα συστήματα: **α)** x1.penelope.uoa.gr **β)** ektor.telecom.ntua.gr **γ)** biomatiko.telecom.ntua.gr. (Μονάδες 8)

Όπως στο παράδειγμα-σχήμα του βιβλίου, ξεκινούμε από την πιο γενικό χώρο στην ονοματολογία και διευκρινίζουμε κατεβαίνοντας επίπεδα. Προσοχή να διαλέξουμε το σωστό κλαδί για τις δύο διευθύνσεις με κοινή ονοματολογία στο 3<sup>ο</sup> επίπεδο



Γ2. Ένα IP αυτοδύναμο πακέτο έχει διασπαστεί σε τέσσερα (4) κομμάτια Α, Β, Γ, Δ ίδιου μήκους, τα οποία έχουν φτάσει με τυχαία σειρά στον προορισμό τους, όπως απεικονίζεται στον παρακάτω πίνακα:

	A	B	Γ	Δ
Αναγνώριση	100	100	100	100
MF	1	1	0	1
Δείκτης εντοπισμού τμήματος (ΔΕΤ)	80	160	240	0

α) Αφού μεταφέρετε τον πίνακα στο τετράδιό σας, να συμπληρώσετε τα κενά. Μονάδες 8

**More Fragments, MF**, σημαίνει αν ακολουθούν άλλα κομμάτια από το πακέτο (MF=1 ακολουθούν, MF=0 δεν ακολουθούν). Ο Δείκτης εντοπισμού τμήματος δείχνει τη σειρά των πακέτων. Το κομμάτι με το μεγαλύτερο ΔΕΤ (240) είναι το τελευταίο, και άρα δεν ακολουθούν άλλα κομμάτια μετά από αυτό (MF=0)

β) Ποιο από τα τέσσερα (4) κομμάτια θα φτάσει τελευταίο στον προορισμό του; Μονάδες 4

Η ερώτηση είναι διατυπωμένη λάθος. Σύμφωνα με τον πίνακα, το τελευταίο κομμάτι (που θα φτάσει τελευταίο) θα είναι το Δ. Προφανώς θέλουν να ρωτήσουν για το ποιο θα είναι το τελευταίο κομμάτι του πακέτου, που είναι αυτό με το μεγαλύτερο ΔΕΤ, δηλαδή το Γ.

γ) Ποιο είναι το μέγεθος του συνολικού αυτοδύναμου πακέτου σε bytes, αν η επικεφαλίδα του έχει μέγεθος 20 bytes; Μονάδες 5

Το ΔΕΤ συμβολίζει οκτάδες οκτάδων, δηλαδή οκτάδες bytes, που έχουν σταλεί μέχρι εκείνη τη στιγμή. Έχουν σταλεί 4 κομμάτια, με τη σειρά τα Δ, Α, Β, Γ. Τα κομμάτια είναι ίδιου μήκους, άρα και το 4<sup>ο</sup> είναι πλήρες όπως τα τρία πρώτα. ΆΡΑ έχουν αποσταλεί  $4 \cdot (\text{συνολικό μήκος κομματιού}) = 4 \cdot (20 \text{ bytes επικεφαλίδα} + 80 \cdot 8 \text{ bytes δεδομένα}) = 4 \cdot (20 + 640) = 4 \cdot 660 = 2640 \text{ bytes}$

#### ΘΕΜΑ Δ

Δ1. Δύο υποδίκτυα σε μία μικρή εταιρία είναι συνδεδεμένα μεταξύ τους με τη βοήθεια ενός δρομολογητή. Κάθε ένα από τα δίκτυα αυτά αποτελείται από τρεις (3) υπολογιστές (Α, Β, Γ και Ε, Ζ, ΣΤ αντίστοιχα). Το πρώτο υποδίκτυο είναι το

198.122.30.0 και το δεύτερο το 198.122.31.0. Θεωρούμε ότι ο δρομολογητής (Δ) έχει διευθύνσεις 198.122.30.1 και 198.122.31.1 στις διεπαφές του 1 και 2 με τα δύο υποδίκτυα αντίστοιχα, ενώ η διεπαφή 3 τον συνδέει με το διαδίκτυο (internet).

Αφού μεταφέρετε στο τετράδιό σας τον παρακάτω πίνακα, να συμπληρώσετε τα κενά. **Μονάδες 18**

**Πίνακας δρομολόγησης του δρομολογητή Δ**

Δίκτυο	Αναγνωριστικό Άμεσης /Εμμεσης Δρομολόγησης	Δρομολογητής	Αριθμός Διεπαφής
198.122.30.0	ΑΜΕΣΗ	<ΚΕΝΟ>	1
198.122.31.0	ΑΜΕΣΗ	<ΚΕΝΟ>	2
61.66.33.0	ΑΜΕΣΗ	<ΚΕΝΟ>	3

**Εύκολη άσκηση, όπως το παράδειγμα του βιβλίου. Ο Δρομολογητής συνδέεται άμεσα με όλα τα υποδίκτυα, άρα δεν χρησιμοποιεί άλλον δρομολογητή (συμπληρώνουμε τα πεδία με <κενό> ή το αφήνουμε κενό) και ο αριθμός διεπαφής αναγραμμένος επάνω στο σχήμα που δίνεται στην άσκηση.**

## **Δ2.**

**A)** Δίνεται η IP διεύθυνση 207.13.1.48/24 ενός υπολογιστή. Να προσδιορίσετε την IP διεύθυνση δικτύου που ανήκει ο υπολογιστής. ( Μονάδες 4)

Η διεύθυνση δικτύου είναι 24 bits οπότε η διεύθυνση υποδικτύου είναι  $32-24=8$  Bits

Άρα δεν μας ενδιαφέρουν τα τελευταία 8 bits. **Η διεύθυνση δικτύου είναι 207.13.1.XX**

**B)** Δίνονται οι IP διευθύνσεις:

α) 10.10.10.1

β) 172.16.3.5

γ) 192.168.1.6

Να προσδιορίσετε τις κλάσεις που ανήκουν οι παραπάνω IP διευθύνσεις. **Μονάδες 3**

Δίνονται:  $10_{10} = 00001010_2$ ,  $172_{10} = 10101100_2$ ,  $192_{10} = 11000000_2$

Εύκολη άσκηση, είναι απλή εφαρμογή της θεωρίας τους βιβλίου. Η άσκηση μας διευκολύνει, γιατί μας δίνει έτοιμη τη δυαδική αναπαράσταση των διευθύνσεων IP για το πρώτο ψηφίο.

Οι κλάσεις είναι ως γνωστόν από τη θεωρία

A → 0

B → 10

C → 110

D → 1110

Άρα η διεύθυνση α είναι κλάσης A

Άρα η διεύθυνση β είναι κλάσης B

Άρα η διεύθυνση γ είναι κλάσης C