ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ

Βασιλάκης Β., Δρακόπουλος Ι., Θεμελής Θ., Κωνσταντοπούλου Μ.

ΕΙΔΙΚΑ ΘΕΜΑΤΑ
ΣΤΟ ΥΛΙΚΟ ΚΑΙ ΣΤΑ
ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Γ΄ Τάξη ΤΟΜΕΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΕΠΑ.Λ.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
Πρόεδρος: **Γκλαβάς Σωτήριος**

ΓΡΑΦΕΙΟ ΕΡΕΥΝΑΣ, ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ Β΄
Προϊστάμενος: **Μάραντος Παύλος**

Επιστημονικά Υπεύθυνος: **Δρ.Τσαπέλας Θεοδόσιος**

ΣΥΓΓΡΑΦΙΚΗ ΟΜΑΔΑ:
Βασιλάκης Βασίλειος, MSc, Εκπαιδευτικός Πληροφορικής
Δρακόπουλος Ιωάννης, MSc, Εκπαιδευτικός Πληροφορικής
Θεμελής Θεόδωρος, MSc, Εκπαιδευτικός Πληροφορικής
Κωνσταντοπούλου Μαρία-Δήμητρα, MSc, MEd, Εκπαιδευτικός Πληροφορικής

ΕΠΙΜΕΛΕΙΑ – ΣΥΝΤΟΝΙΣΜΟΣ ΟΜΑΔΑΣ:
Κωτσάκης Σταύρος, Σχολικός Σύμβουλος Πληροφορικής

ΦΙΛΟΛΟΓΙΚΗ ΕΠΙΜΕΛΕΙΑ
Γιακουμής Φώτιος, Εκπαιδευτικός Φιλόλογος

Περιεχόμενα

Οδηγίες προς τον Εκπαιδευτικό

Προτεινόμενη Διδακτική Μεθοδολογία

Η διδασκαλία του μαθήματος προτείνεται να στηριχθεί στις αρχές του **επικοδομητισμού και της ανακαλυπτικής μάθησης**. Σύμφωνα με αυτές, η μάθηση δεν μεταδίδεται αλλά είναι μια διαδικασία προσωπικής ενεργής κατασκευής της γνώσης που στηρίζεται πάνω στις προηγούμενες γνώσεις των μαθητών, οι οποίες θα πρέπει πρώτα να τροποποιηθούν κατάλληλα, ώστε να εξαλειφθούν πρότερες λανθασμένες αντιλήψεις που μπορεί να σταθούν εμπόδιο στην οικοδόμηση της νέας γνώσης. Μέσα από ανακαλυπτικού τύπου δραστηριότητες (πειράματα, δοκιμές, επαλήθευση και διάψευση) οι μαθητές θα κατακτήσουν νέες γνώσεις και δεξιότητες, καθώς η φύση του μαθήματος απαιτεί την πραγματοποίηση ασκήσεων στον περιβάλλον του σχολικού εργαστηρίου πληροφορικής.

Ο ρόλος του εκπαιδευτικού οφείλει να είναι **εμψυχωτικός, συμβουλευτικός, καθοδηγητικός και υποστηρικτικός**. Η εργασία των μαθητών σε ομάδες κρίνεται απαραίτητη, καθώς ο κοινωνιοπολιτισμικός παράγοντας παίζει ουσιώδη ρόλο στη μάθηση, αφού οι μαθητές δεν κατασκευάζουν τη γνώση μέσα σε ένα πολιτισμικό και επικοινωνιακό κενό, αλλά στα ευρύτερα πλαίσια, μέσα στα οποία η γνώση δημιουργείται και σηματοδοτείται. Με τη βοήθεια του σχολικού εργαστηριακού περιβάλλοντος, οι μαθητές αναμένεται να καταφέρουν να επιτύχουν την οικοδόμηση γνώσεων που δεν θα μπορούσαν να κατακτήσουν εργαζόμενοι ατομικά.

Ο εκπαιδευτικός οφείλει κατά τον σχεδιασμό του συγκεκριμένου μαθήματος για το σχολικό έτος, να προσεγγίσει την ύλη του μαθήματος βασισμένος **στις οδηγίες του Προγράμματος Σπουδών**. Οι προτεινόμενες ασκήσεις και δραστηριότητες έχουν μια προτεινόμενη δομή εκτέλεσης, την οποία ο εκπαιδευτικός μπορεί να την προσαρμόσει στις ανάγκες των διδακτικών αναγκών των μαθητών, όπως τις έχει διαγνώσει ο ίδιος μέσα από διερευνητικές ασκήσεις και δραστηριότητες.

Καθώς η φύση του μαθήματος είναι προσανατολισμένη στο εργαστηριακό και πρακτικό μέρος της θεωρίας του υλικού και των δικτύων των Η/Υ, οφείλει να **είναι κατάλληλα προετοιμασμένος, τόσο ο ίδιος όσο και ο εξοπλισμός του εργαστηρίου**, ώστε να είναι σε θέση να προσαρμόσει και να υλοποιήσει τις προτεινόμενες εργαστηριακές δραστηριότητες στο σχολικό εργαστήριο. Για τον σκοπό αυτό παρουσιάζονται παρακάτω ορισμένες οδηγίες, ώστε να βοηθηθεί ο εκπαιδευτικός στην καλύτερη προετοιμασία του και στην αποτελεσματικότερη εκτέλεση των ασκήσεων που θα υλοποιήσει.

1ο Κεφάλαιο
Μέθοδοι Αύξησης των Επιδόσεων ενός Υπολογιστικού Συστήματος

Επειδή ο υπερχρονισμός είναι μια διαδικασία που εξαρτάται άμεσα από το υλικό που βρίσκεται εγκατεστημένο στους ηλεκτρονικούς υπολογιστές (Η/Υ) του Σχολικού Εργαστηρίου, οι ασκήσεις είναι ενδεικτικές και περιέχουν γενικές οδηγίες για την εκπόνησή τους. Ο Εκπαιδευτικός οφείλει να εντοπίσει τις παραμέτρους στο BIOS των Η/Υ που χρειάζεται να χρησιμοποιηθούν, να δοκιμάσει ποιο από τα προτεινόμενα προγράμματα παραμετροποίησης λειτουργεί καλύτερα στο εργαστηριακό του περιβάλλον και να δοκιμάσει τις τιμές παραμέτρων των μονάδων υλικού που δείχνουν τα βασικά επιτεύγματα απόδοσης του υπερχρονισμού.

ΙΔΙΑΙΤΕΡΗ ΠΡΟΣΟΧΗ στην αύξηση της θερμοκρασίας στα συστήματα που εφαρμόζεται ο υπερχρονισμός! Η μεγάλη θερμότητα μπορεί να επιφέρει μη αναστρέψιμες βλάβες στο υλικό.

Άσκηση 2η

Για την ολοκλήρωση της άσκησης απαιτείτε η εγκατάσταση ενός προγράμματος παρακολούθησης, με προτεινόμενο το LinX. Προτείνονται επίσης τα:

Πρόγραμμα παρακολούθησης:

- LinX (Windows): http://www.softpedia.com/get/System/Benchmarks/LinX-benchmark.shtml#download
- CPU-Z (Windows): http://www.cpuid.com/softwares/cpu-z.html
- i-Nex (Linux): http://www.omgubuntu.co.uk/2014/02/nex-cpu-z-hardware-stat-tool-linux
- Πρόγραμμα παραμετροποίησης:
- Prime95 (Windows/Linux): http://www.mersenne.org/download/

Ωστόσο ο εκπαιδευτικός μπορεί να επιλέξει ο ίδιος άλλα ελεύθερα λογισμικά για τον ίδιο σκοπό.

Άσκηση 3η

Το Stress tool (Linux) περιλαμβάνεται με τη διανομή των περισσότερων εκδόσεων Linux. Για την εγκατάσταση του stress σε Debian ή Ubuntu Linux χρησιμοποιείται η εντολή:

apt-get install stress

Για περισσότερες πληροφορίες εγκατάστασης αλλά και των παραμέτρων των εντολών που εφαρμόζονται στην άσκηση στο:

http://www.cyberciti.biz/faq/stress-test-linux-unix-server-with-stress-ng/

Άσκηση 4η

Για την παρακολούθηση της θερμοκρασίας μπορείτε να χρησιμοποιήσετε την εφαρμογή CPU Thermometer που θα τη βρείτε στο: http://www.cputhermometer.com/

Άσκηση 6η

Ιδιαίτερη προσοχή στην εκτέλεση αυτής της άσκησης, γιατί η αύξηση της τάσης του ηλεκτρικού ρεύματος μπορεί να καταστρέψει την ΚΜΕ. Γενικότερα προτείνεται κατά την εκτέλεση της **άσκησης να μην να αυξηθεί η τάση πάνω από 0,2 μονάδες από το αρχικό της επίπεδο** με απλό σύστημα ψύξης ή 0,4 μονάδες με ενισχυμένο σύστημα ψύξης.

Άσκηση 7η

Τα βίντεο που προτείνει η άσκηση προς προβολή είναι στην αγγλική γλώσσα, ωστόσο δεν είναι απαραίτητος ο ήχος παρά μόνο η παρατήρηση του τρόπου τοποθέτησης των καρτών γραφικών, των γεφυρών καθώς και της τροποποίησης των παραμέτρων για ενεργοποίηση της τεχνολογίας SLI/Crossfire.

Προτείνεται η συγκεκριμένη άσκηση να πραγματοποιηθεί σε ομάδες συζήτησης.

Άσκηση 8η

Αν υπάρχει διαθέσιμος εξοπλισμός στο σχολικό εργαστήριο, να γίνει επίδειξη του τρόπου εφαρμογής διπλών καρτών γραφικών σε ένα σύστημα.

4ο Κεφάλαιο
Συστοιχίες Υπολογιστών (Computer Clusters)

- Η άσκηση αυτή μπορεί να πραγματοποιηθεί είτε με χρήση εικονικών μηχανών, είτε με απευθείας εκκίνηση φυσικών υπολογιστών από live-cd. Στην δεύτερη περίπτωση πάντως θα χρειαστούν τόσα CD όσοι και οι υπολογιστές που θα χρησιμοποιηθούν, ενώ υπάρχει και ο κίνδυνος να μην αναγνωριστούν οι κάρτες δικτύου των φυσικών υπολογιστών, αν δεν είναι κάποιο από τα συνηθισμένα μοντέλα. Για το λόγο αυτό τα βήματα δίνονται με χρήση εικονικών μηχανών.
- Πριν την έναρξη της άσκησης θα πρέπει να έχετε αντιγράψει το αρχείο **clusterKNOPPIX_PI.iso** στους υπολογιστές των μαθητών ή σε κάποιο φάκελο προσβάσιμο από το δίκτυο.
- Το λειτουργικό σύστημα είναι ρυθμισμένο να παίρνει IP διεύθυνση μέσω DHCP. Αν το εργαστήριο χρησιμοποιεί στατικές διευθύνσεις και δεν έχει DHCP server, η απόδοση της IP μπορεί να γίνει χειροκίνητα πατώντας στο εικονίδιο με τον πιγκουίνο και επιλέγοντας **Network/Internet → Network card configuration**.

- Η ισχύς της συστοιχίας θα φανεί καλύτερα αν δεν εκτελούν το test όλοι μαζί οι μαθητές, αλλά κάθε ομάδα με τη σειρά. Αν υπάρχει διαθέσιμος βιντεοπροβολέας μπορεί να γίνει και επίδειξη από τον καθηγητή.

- Για την εύρεση της τιμής του π χρησιμοποιήθηκε ο αλγόριθμος των James Gregory (1638-1675) και Gottfried Leibniz (1646-1716), που υπολογίζει την τιμή του π σαν άθροισμα άπειρων όρων σειράς με γενικό τύπο:

$$\pi = 4 \cdot \sum_{i=1}^{\infty} (-1)^{i+1} \frac{1}{2i-1}$$

  Είναι ένας από τους πιο αργούς (αλλά και πιο απλούς) τρόπους να υπολογιστεί το π, πράγμα που αναδεικνύει την βελτίωση των επιδόσεων κατά την εκτέλεσή του σε συστοιχία.
- Μπορεί να γίνει δοκιμή της συμπεριφοράς της συστοιχίας σε μεμονωμένο υπολογιστή με την εκτέλεση ταυτόχρονα πάνω από μίας εικονικής μηχανής.

5ο Κεφάλαιο
Βασικές Εντολές Δικτύωσης

Άσκηση ενότητας 5.3

Υποθέτοντας ότι έχει εγκατασταθεί το wireshark μπορούμε να υλοποιήσουμε πολύ απλές ασκήσεις που δείχνουν τη λειτουργία του σε πολύ απλό επίπεδο.

Θα πρέπει ο εκπαιδευτικός να έχει πειραματιστεί με το wireshark για να κατευθύνει τους μαθητές στην υλοποίηση της άσκησης.

Λήψη του wireshark : https://www.wireshark.org/download.html

Οδηγός χρήσης του wireshark :

https://www.wireshark.org/download/docs/user-guide-a4.pdf

Tutorial 1: http://www-scf.usc.edu/~csci571/Special/Tutorials/wireshark_html/wireshark.html

Tutorial 2:http://cs.gmu.edu/~astavrou/courses/ISA_674_F12/Wireshark-Tutorial.pdf

6ο Κεφάλαιο
Δικτυακά Μέσα Αποθήκευσης

Άσκηση 1η

- Πρέπει να προσθέσετε στην εικονική μηχανή δύο εικονικούς δίσκους ίδιου μεγέθους.
- Η δημιουργία του RAID-1 γίνεται μέσω της επιλογής **RAID Management.**
- Η δημιουργία του διαμερίσματος γίνεται μέσω της επιλογής **File Systems.**

Άσκηση 2η

- Κατά τη δημιουργία του φακέλου θα πρέπει να προσέξετε στα δικαιώματα να επιλέξετε **Everyone: read/write**
- Στην δημιουργία του κοινόχρηστου φακέλου, η επιλογή **Public** θα πρέπει να είναι **Only guests**

7ο Κεφάλαιο
Εγκατάσταση και Διαχείριση Διακομιστή, Απομακρυσμένη Πρόσβαση

Άσκηση 1η

Θα πρέπει να έχετε δημιουργήσει λογαριασμούς χρηστών για κάθε ένα μαθητή πριν την υλοποίηση της άσκησης. Η δημιουργία χρηστών μπορεί να γίνει χρησιμοποιώντας την εντολή **sudo adduser ονομα_χρήστη**.

Άσκηση 3η

Θα πρέπει να έχετε δημιουργήσει λογαριασμούς χρηστών για κάθε ένα μαθητή πριν από την παραπάνω διαδικασία. Η δημιουργία χρηστών μπορεί να γίνει χρησιμοποιώντας την εντολή **sudo**

8ο Κεφάλαιο
Ασφάλεια Δεδομένων και Δικτύων

2η Άσκηση (Σε εργαστηριακό περιβάλλον Windows)

- Η αλλαγή της MAC διεύθυνσης μπορεί να γίνει και από τη γραμμή εντολών με τις ακόλουθες π.χ. εντολές:

  sudo ifconfig eth0 down

  sudo ifconfig eth0 hw ether 00:11:22:33:44:55

  sudo ifconfig eth0 up

  Η πρώτη και η τελευταία είναι για διακοπή και επαναφορά της σύνδεσης, ενώ η ενδιάμεση αλλάζει τη MAC διεύθυνση. Στην περίπτωση αυτή πάντως το αποτέλεσμα δεν είναι μόνιμο.

- Εκτός αυτών, το εργαλείο macchanger, διαθέσιμο από το Software Center μπορεί να χρησιμοποιηθεί για αλλαγή της MAC διεύθυνσης.

3η Άσκηση (Σε εργαστηριακό περιβάλλον)

- Να τονισθεί ότι η αντικατάσταση γραμμάτων με σύμβολα ή ψηφία εξασφαλίζει από μόνη της ότι ο κωδικός θα είναι απαραβίαστος, καθώς προγράμματα ανεύρεσης κωδικών λαμβάνουν υπ' όψη τέτοιου είδους αντικαταστάσεις.
- Μια πιθανή, αλλά όχι μοναδική, λύση της άσκησης είναι ακόλουθη:

a	**b**	**c**	**E**	**B**	**i**	**L**	**q**
@	6	(	3	8	!	1	9
Z	**D**	**M**	**H**	**T**	**t**	**O**	**G**
2	I>	^^	#	7	+	0	&

4η Άσκηση (Σε εργαστηριακό περιβάλλον)

- Η άσκηση αυτή έχει σαν σκοπό να δώσει στους μαθητές ένα βιωματικό παράδειγμα μιας διαδικασίας (υπολογισμού) που ενώ γίνεται εύκολα προς τη μία κατεύθυνση, είναι σχεδόν αδύνατο να γίνει προς την αντίστροφη, πράγμα που είναι το χαρακτηριστικό των μονόδρομων συναρτήσεων κατατεμαχισμού.
- Για την εύρεση των λέξεων χρησιμοποιήθηκε το "Ερμηνευτικό Λεξικό της Νέας Ελληνικής" που είναι διαθέσιμο στο Ψηφιακό Σχολείο (*http://ebooks.edu.gr/modules/ebook/show.php/SGYM-A112/459/3008,12098/*), αλλά και σε μορφή pdf (προτείνεται) στη διεύθυνση *http://www.pi-schools.gr/books/gymnasio/erm_lex_a_b_c_gymn/s_1_100.pdf*
- Για να μπορέσει ο Βασίλης να βρει την λέξη της Αντιγόνης, χωρίς να τη γνωρίζει ο ίδιος (ερώτηση 2), θα πρέπει να εργασθεί ανάποδα και να βρει όλα τα λήμματα που στον ορισμό τους έχουν σαν 5η λέξη την "Διάφορα" και μετά από αυτές, αυτήν που έχει σαν 4η λέξη την "Μαγαζί" κ.ο.κ. και να το κάνει αυτό για κάθε λέξη που του δίνει η Αντιγόνη.
- Τελικά αυτό που μπορεί να κάνει ο Βασίλης (ερώτηση 3) είναι να εφαρμόσει τον αλγόριθμο για κάθε λέξη στο λεξικό, να σημειώσει τα αποτελέσματα και να φτιάξει έτσι έναν "πίνακα αντίστροφης αναζήτησης" (reverse lookup table), που θα συμβουλεύεται από εδώ και στο εξής. Πρέπει όμως να γίνει φανερό ότι ενώ τα λήμματα ενός λεξικού είναι περιορισμένα, οι κωδικοί που μπορεί να αποτελούνται από οποιονδήποτε συνδυασμό ενός συνόλου χαρακτήρων είναι πολύ περισσότεροι.
- Μια επιπλέον ερώτηση που μπορεί να τεθεί είναι τι θα γίνει αν η Αντιγόνη αλλάξει τον κανόνα και να ζητήσει βάθος 6 ή 7 λέξεων. Στην περίπτωση αυτή θα πρέπει ο Βασίλης να φτιάξει νέο πίνακα από την αρχή.
- Ο σκοπός των ερωτήσεων 5-10 είναι ο μαθητής να δει ότι ακόμη και η αλλαγή ενός bit στη αρχική λέξη, έχει σαν αποτέλεσμα την παραγωγή μιας τελείως διαφορετικής σύνοψης.
- Ο σκοπός των ερωτήσεων 11-12 είναι ο μαθητής να διαπιστώσει ότι το μέγεθος της σύνοψης είναι σταθερό, ανεξάρτητα του μεγέθους της φράσης εισόδου. Άρα όσο πιο μεγάλη η σύνοψη τόσο μικρότερη η πιθανότητα συγκρούσεων.
- Ο πίνακας του ερωτήματος 13 συμπληρωμένος:

Αλγόριθμος	Πλήθος Χαρακτήρων Σύνοψης	Πλήθος bit Σύνοψης
Adler32	8	64
CRC32	8	64
Haval	32	256
MD2	32	256
MD4	32	256
MD5	32	256

RipeMD128	32	256
RipeMD160	40	320
SHA-1	40	320
SHA-256	64	512
SHA-384	96	768
SHA-512	128	1024
Tiger	48	384
Whirlpool	128	1024

5η Άσκηση (Σε εργαστηριακό περιβάλλον)

- Ο πίνακας του ερωτήματος 4 συμπληρωμένος (κάποιοι από τους κωδικούς που δεν υπήρχαν τη στιγμή της συγγραφής στον αντίστοιχο πίνακα μπορεί να προστεθούν αργότερα).

Κωδικός	**Αποτέλεσμα (✓ ή ✗)**	**Κωδικός**	**Αποτέλεσμα (✓ ή ✗)**
letmein	✓	password!	✓
password	✓	p@ssw0rd!	✓
independent	✓	BadBoy	✗
corresponding	✗	thisisatest	✓
discovery	✓	!nd3p3nI)ent	✗
discoveries	✗	123456789	✓

6η Άσκηση (Σε εργαστηριακό περιβάλλον Windows, Linux)

- Η σελίδα από την οποία μπορείτε να κατεβάσετε το live-cd του ophcrack είναι η: *http://sourceforge.net/projects/ophcrack/files/ophcrack-livecd/3.6.0/*
- Σε περίπτωση που θέλετε να χρησιμοποιήσετε το ophcrack με εικονική μηχανή (ή κανονικό υπολογιστή) με windows xp θα πρέπει να κατεβάσετε το αρχείο "ophcrack-xp-livecd-3.6.0.iso". Αυτό συμβαίνει διότι τα Windows XP και προγενέστερα χρησιμοποιούν μία λιγότερο ασφαλή μέθοδο διαχείρισης των κωδικών (LM Hashes αντί NTLM Hashes), σπάζοντας τους κωδικούς με πλήθος έως και 14 χαρακτήρες σε δύο κομμάτια και υπολογίζοντας ξεχωριστή σύνοψη για τον καθένα. Για περισσότερες πληροφορίες δείτε: https://technet.microsoft.com/en-us/magazine/ 2006.08.securitywatch.aspx και http://www.windowsecurity.com/articles-tutorials/ authentication_and_encryption/How-Cracked-Windows-Password-Part1.html
- Το αρχείο «ophcrack-notables-livecd-3.6.0.iso» περιέχει μόνο το πρόγραμμα (χωρίς πίνακες) και προορίζεται μόνο για χρήση με πίνακες που κατεβάζουμε ξεχωριστά.

8η Άσκηση (Σε εργαστηριακό περιβάλλον Linux)

- Το kali Linux είναι ο απόγονος της διάσημης διανομής BackTrack. Μπορείτε να το κατεβάσετε από τη σελίδα: https://www.kali.org/downloads/ Το μέγεθός του είναι περίπου 3GB.
- Το εργαλείο John the Ripper έχει τη δυνατότητα να χρησιμοποιήσει καταλόγους λέξεων (wordlists) με τα πιο συχνά χρησιμοποιούμενα password (για διάφορες γλώσσες). Τέτοιες λίστες είναι διαθέσιμες για μεταφόρτωση είτε δωρεάν (http://download.openwall.net/pub/wordlists/) ή με πληρωμή (https://sites.fastspring.com/openwallfs/instant/wordlists).
- Το johnny έχει τη δυνατότητα να χρησιμοποιήσει wordlists, από την επιλογή Options → Wordlist mode.
- Όπως και σε όλα τα εργαλεία του Linux η μεγαλύτερη ευελιξία στη χρήση τους επιτυγχάνεται με τη χρήση από τη γραμμή εντολών. Ωστόσο για μεγαλύτερη ευκολία στους μαθητές, κυρίως σε αυτούς που δεν είναι εξοικειωμένοι με το Linux, επιλέχθηκε εδώ η χρήση του γραφικού front-end.

9η Άσκηση (Σε εργαστηριακό περιβάλλον Windows)

- Ο πίνακας του ερωτήματος 4 συμπληρωμένος:

Κωδικός	**Πληροί το Ελάχιστο Μήκος;**	**Περιέχει μέρος του ονόματος χρήστη**	**Πλήθος κατηγοριών χαρακτήρων**	**Πληροί τους κανόνες;**
letmein	ΝΑΙ (7≥6)	ΟΧΙ	1	ΟΧΙ
Chargers1	ΝΑΙ (9≥6)	ΟΧΙ	3	ΝΑΙ
Panthers1	ΝΑΙ (9≥6)	ΟΧΙ	3	ΝΑΙ

#apanag12!	NAI (10≥6)	NAI	3	OXI
!QaZ2	OXI (5<6)	OXI	4	OXI
Prototype1	NAI (10≥6)	OXI	3	NAI
@WSX2wsx	NAI (8≥6)	OXI	4	NAI

- Ο πίνακας του ερωτήματος 7 συμπληρωμένος:

Πολιτική	Παλιά Τιμή	Νέα Τιμή
Ελάχιστη διάρκεια κωδικού πρόσβασης	0	5
Ελάχιστο μήκος κωδικού πρόσβασης	0	8
Επιβολή ιστορικού κωδικών πρόσβασης	0	1
Μέγιστη διάρκεια κωδικού πρόσβασης	42	30

10η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows)

- Μπορείτε να κατεβάσετε το πρόγραμμα KeePass από την τοποθεσία http://keepass.info/

13η Άσκηση (Σε εργαστηριακό περιβάλλον)

- Το κρυπτογραφημένος κείμενο μπορείτε να το κατεβάσετε από την σελίδα https://docs.google.com/document/pub?id=1n-8KmbLHxnsB9ZafulAc9qZ5u-X5vP6Uj3Wbs0ysJQA (κάτω από την ενότητα 5)

19η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows)

- Η εφαρμογή μπορεί να βρεθεί στην τοποθεσία http://ppgp.sourceforge.net/ Η έκδοση Standalone Application είναι φορητή εφαρμογή και μπορεί να εκτελείται και από ένα usb flash disk.
- Έχει τον περιορισμό ότι μπορεί να παράγει κλειδιά μεγέθους μέχρι 1024 bit, αλλά μπορεί να εισάγει (import) και κλειδιά μεγαλύτερου μεγέθους
- Είναι εύκολη στη χρήση για μια εισαγωγή στην κρυπτογράφηση Δημόσιου-Ιδιωτικού κλειδιού.

21η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows)

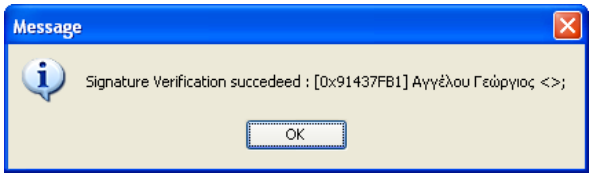
- Το PortablePGP έχει τη δυνατότητα να υπογράψει ψηφιακά το κρυπτογραφημένο αρχείο έτσι ώστε να είναι δυνατή η επιβεβαίωση της ταυτότητας του αποστολέα. Για το σκοπό αυτό στην καρτέλα της κρυπτογράφησης μπορεί να συμπληρωθεί το πεδίο [Sign]. Στην

λίστα εμφανίζονται τα Ιδιωτικά κλειδιά που είναι αποθηκευμένα στην εφαρμογή. Στην περίπτωση αυτή θα ζητηθεί ο κωδικός του χρήστη που θα επιλεγεί.

- Αν στη διαδικασία της κρυπτογράφησης επιλέξετε το κουτάκι «Ascii armored» τότε το κρυπτογραφημένο αρχείο που θα προκύψει θα αποτελείται από ASCII χαρακτήρες. Η δυνατότητα αυτή χρησιμοποιείται στην περίπτωση που το κρυπτογραφημένο αρχείο θα αποσταλεί με κάποια εφαρμογή που δεν υποστηρίζει συνημμένα (σπάνιο πια) ή στην περίπτωση που χρειάζεται να ενσωματωθεί π.χ. στο αρχείο ενός επεξεργαστή κειμένου.
- Στην ίδια καρτέλα μπορεί να γίνει απευθείας κρυπτογράφηση κειμένου χωρίς να αποθηκευτεί πρώτα σε αρχείο (Encrypt Text).

22η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows)

- Αν κατά τη διάρκεια της κρυπτογράφησης έχει συμπεριληφθεί και ψηφιακή υπογραφή, θα εμφανιστεί μήνυμα που θα επιβεβαιώνει τον αποστολέα.



23η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows)

- Το PortablePGP έχει τη δυνατότητα να δημιουργεί ψηφιακές υπογραφές και σε αυτόνομα αρχεία. Στην περίπτωση αυτή η ψηφιακή υπογραφή αποθηκεύεται σε ξεχωριστό αρχείο με το ίδιο όνομα και κατάληξη .sig. Για να γίνει επαλήθευση χρειάζεται φυσικά και το αρχικό αρχείο δεδομένων και το αρχείο της υπογραφής.

24η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows)

- Παρά το ότι ο συγκεκριμένος Server το υποστηρίζει, το PortablePGP δεν έχει τη δυνατότητα να υπογράψει κλειδιά άλλων χρηστών για τη δημιουργία ιστού εμπιστοσύνης. Αν κάτι τέτοιο είναι επιθυμητό θα πρέπει να χρησιμοποιηθεί κάποια άλλη εφαρμογή όπως π.χ, το επίσης δωρεάν και cross-platform OpenPGP Studio (http://www.goanywheremft.com/products/openpgp-studio/download).
- Αν χρησιμοποιείτε e-mail για την ανταλλαγή αρχείων στο χώρο του εργαστηρίου καλό θα ήταν να επιλέξετε κάποιον τοπικό e-mail server ώστε οι μαθητές να μην μπορούν να στείλουν spam ή υβριστικά μηνύματα στα e-mail των χρηστών του Key Server.
- Η Εθνική Πύλη Δημόσιας Διοίκησης (http://www.ermis.gov.gr/) προσφέρει υπηρεσίες έκδοσης και διαχείρισης ψηφιακών πιστοποιητικών σε εγγεγραμμένους χρήστες.

25η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows)

- Το πρόγραμμα στεγανογραφίας Steg μπορείτε να το μεταφορτώσετε από τη διεύθυνση https://steg.drupalgardens.com/. Υπάρχει έκδοση για Windows, Linux και MAC OS X.
- Το πρόγραμμα κρύβει μηνύματα μόνο μέσα σε ένα αρχείο εικόνας. Υπάρχουν εφαρμογές που μπορούν να κρύψουν μηνύματα χρησιμοποιώντας πολλά διαφορετικά αρχεία (και διαφορετικών τύπων, π.χ. .jpg, .mp3, .mp4, .pdf κ.α.) επιτρέποντας έτσι την απόκρυψη μεγαλύτερων μηνυμάτων, όπως π.χ. το openPuff (http://embeddedsw.net/OpenPuff_Steganography_Home.html).

- Το Steg έχει και τη δυνατότητα να κάνει κρυπτογράφηση και να προσθέτει ψηφιακή υπογραφή στα κρυμμένα δεδομένα, είτε συμμετρική, είτε ασυμμετρική, είτε εισάγοντας κλειδιά που ήδη υπάρχουν, είτε δημιουργώντας εκείνη τη στιγμή.

29η, 30η και 31η Άσκηση (Σε εργαστηριακό περιβάλλον Windows)

- Το Firewall των Windows XP έχει σαφώς λιγότερες δυνατότητες από αυτό των Windows 7 με σημαντικότερη την αδυναμία ελέγχου εξερχόμενων συνδέσεων. Ωστόσο υπάρχει η δυνατότητα αποκλεισμού εφαρμογών και εισερχόμενων συνδέσεων.

32η και 33η Άσκηση (Σε εργαστηριακό περιβάλλον Linux)

- Το iptables και το ufw λειτουργούν από γραμμή εντολών. Έχουν σαφώς περισσότερες δυνατότητες, αλλά δεν είναι φιλικά για αρχάριους χρήστες.
- Το gufw περιλαμβάνει και προκαθορισμένους κανόνες για συγκεκριμένες εφαρμογές, που όμως απλά έχουν προεπιλεγμένες τις θύρες που αυτές χρησιμοποιούν για την επικοινωνία τους.

36η Άσκηση (Σε εργαστηριακό περιβάλλον)

- Οι proxy server του Πανελλήνιου Σχολικού Δικτύου συνήθως απαγορεύουν, για ευνόητους λόγους, την πρόσβαση σε σελίδες ανώνυμων μεσολαβητών. Ελέγξτε πρώτα αν επιτρέπεται η πρόσβαση σε αυτόν που θέλετε να χρησιμοποιήσετε.
- Μια αναζήτηση για «anonymous proxy server» θα σας δώσει πληθώρα εναλλακτικών επιλογών.

37η και 38η Άσκηση (Σε εργαστηριακό περιβάλλον Windows-Linux)

- Αν ο φορέας που σας συνδέει στο Internet δεν επιτρέπει τη σύνδεση στο δίκτυο Tor θα πρέπει στο αρχικό παράθυρο ρυθμίσεων να πατήσετε το κουμπί [Configure] και να ορίσετε μία Tor Bridge. Οι γέφυρες Tor είναι κόμβοι που δεν εμφανίζονται στους καταλόγους του Tor κι έτσι είναι δύσκολο για κάποιον ISP να τους αποκλείσει όλους.
- Από το κουμπί [Connect] θα έχετε και τη δυνατότητα σε περίπτωση που χρησιμοποιείτε Proxy server να δηλώσετε τα στοιχεία του.

9ο Κεφάλαιο
Τεχνολογίες Ασύρματης Δικτύωσης

Άσκηση 1η

- Για να πραγματοποιηθεί η άσκηση αυτή χρειάζεται την ύπαρξη κάποιου ασύρματου access point ή δρομολογητή που να μπορεί να μεταφερθεί στο Εργαστήριο Πληροφορικής. Χρειάζεται επίσης η ύπαρξη κάποιου υπολογιστή ή φορητής συσκευής με ασύρματη κάρτα δικτύου. Οι οδηγίες δίνονται για τη συσκευή WRT300N της Linksys. Σε διαφορετική συσκευή θα είναι διαφορετική και η δομή των σελίδων ρύθμισης.
- Εναλλακτικά και εφόσον υπάρχει η δυνατότητα μπορεί να χρησιμοποιηθεί λογισμικό προσομοίωσης όπως π.χ. το Packet Tracer της Cisco.
- Η διεύθυνση του router είναι ενδεικτική και θα πρέπει να προσαρμοστεί στις διευθύνσεις που χρησιμοποιεί το εργαστήριο Πληροφορικής. Στην περίπτωση που στο Εργαστήριο

υπάρχει DHCP Server (που είναι και η πιο συνηθισμένη) θα πρέπει να απενεργοποιηθεί ο DHCP Server του router (Setup ® Basic Setup ® DHCP Server Settings).

- Σε περίπτωση που δεν είναι δυνατή ούτε η σύνδεση φυσικού δρομολογητή, ούτε η χρήση προσομοίωσης, στην σελίδα *http://ui.linksys.com/WRT300N/0.93.9/* υπάρχει το περιβάλλον ρύθμισης της συσκευής Linksys WRT300N, με όλες τις διαθέσιμες επιλογές τις οποίες διαθέτει και το φυσικό μηχάνημα. Μπορούν να γίνουν αλλαγές τιμών, δεν μπορεί όμως να γίνει αποθήκευση των ρυθμίσεων.
- Στο διαδίκτυο υπάρχουν διαθέσιμες και οι ρυθμίσεις πολλών ακόμη ασύρματων δρομολογητών. Μια αναζήτηση για «router emulator» δίνει πληθώρα αποτελεσμάτων.

Άσκηση 3η

- Η εφαρμογή inSSIDer από την έκδοση 4 είναι επί πληρωμή. Ωστόσο παλιότερες εκδόσεις μπορούν να βρεθούν στο διαδίκτυο, π.χ. *http://inssider.en.softonic.com/download#downloading*. Η έκδοση 3 είναι και αυτή δωρεάν, αλλά δεν λειτουργεί σε Windows XP.
- Μπορείτε να κατεβάσετε την εφαρμογή Acrylic Wi-Fi Free από την ακόλουθη τοποθεσία: *https://www.acrylicwifi.com/en/*. Ένα video της λειτουργίας της (ενδεικτικό και για τις υπόλοιπες εφαρμογές μπορείτε να βρείτε στη διεύθυνση https://www.youtube.com/watch?v=ri7JfFx1kZQ
- Η εφαρμογή LinSSID είναι μπορεί να βρεθεί στο *http://sourceforge.net/projects/ linssid/* . Μπορεί ακόμη να εγκατασταθεί και από το Software Center προσθέτοντας ένα repository. Π.χ. στο Ubuntu μπορεί να εγκατασταθεί με τις ακόλουθες εντολές:

```
$ sudo add-apt-repository ppa:wseverin/ppa
$ sudo apt-get update
$ sudo apt-get install linssid
```

- Τα αποτελέσματα της έρευνας συχνοτήτων εξαρτώνται από το πλήθος και το είδος των ασύρματων δικτύων που είναι ενεργά στην περιοχή. Οι εφαρμογές έχουν τη δυνατότητα να σαρώσουν και την περιοχή των 5 GHz, αν φυσικά υπάρχει και η αντίστοιχη κάρτα δικτύου.

10ο Κεφάλαιο
Σύγχρονη καλωδίωση κτιρίου

Για συμπληρωματική αναφορά στη θεωρία του κεφαλαίου και πριν την εκτέλεση των ασκήσεων, μπορείτε να ανατρέξετε στην ύλη της Β' Λυκείου ΕΠΑΛ στο μάθημα του Υλικού και Δικτύων Η/Υ ή στις σημειώσεις του μαθήματος Δίκτυα Υπολογιστών της Γ' Λυκείου ΕΠΑΛ.

Άσκηση 1η

Η εκτέλεση της άσκησης μπορεί να γίνει είτε στο εργαστήριο είτε σε μια αίθουσα του σχολείου, όπου θα αποφασιστεί από την τάξη να μετατραπεί σε μια νέα εργαστηριακή αίθουσα με Η/Υ.

Για την αποτύπωση του δικτύου μπορείτε χα χρησιμοποιήσετε ένα οποιοδήποτε σχεδιαστικό πρόγραμμα με τα κατάλληλα δικτυακά σχήματα, πχ. MS Office Visio ή το Gliffy Network Diagram Software Online (https://www.gliffy.com/uses/network-diagram-software/)

Άσκηση 2η

Προτείνεται ο εκπαιδευτικός να δημιουργήσει το εικονικό περιβάλλον μέσα στο σχολικό εργαστήριο. Για την εφαρμογή των βημάτων, προτείνετε να γίνει πρώτα επίδειξη και μετά με εφαρμογή από τους μαθητές.

11ο Κεφάλαιο
Δικτύωση PowerLine

Για περισσότερες πληροφορίες σχετικά με την τεχνολογία powerline :
http://www.comsoc.org/best-readings/topic/powerline-communications#overbooks

Ενδεικτικός τρόπος διασύνδεσης με powerline :
http://www.pcadvisor.co.uk/how-to/network-wifi/set-up-powerline-networking-adaptors-3380482/

Άσκηση

Για την υλοποίησης της άσκησης προϋπόθεση είναι η ύπαρξη ζεύγους συσκευών powerline που θα υλοποιήσουν την μεταξύ τους επικοινωνία μέσω του τοπικού ηλεκτρικού δικτύου. Απαιτείται λοιπόν η προμήθεια powerline συσκευών, οι οποίες δεν είναι ιδιαίτερα ακριβές και μπορούν να αποτελέσουν στη συνέχεια μόνιμο εξοπλισμό του εργαστηρίου πληροφορικής. Επίσης, στο εργαστήριο, πρέπει να υπάρχουν εύκαιρα καλώδια Ethernet και ένα hub.

Ιδιαίτερη προσοχή να δοθεί ώστε να μην τοποθετηθεί μια powerline συσκευή με πολύπριζο. Με την τοποθέτησης κατευθείαν σε ηλεκτρικό απολήκτη (πρίζα) θα αποφύγουμε τυχόν απώλειες.