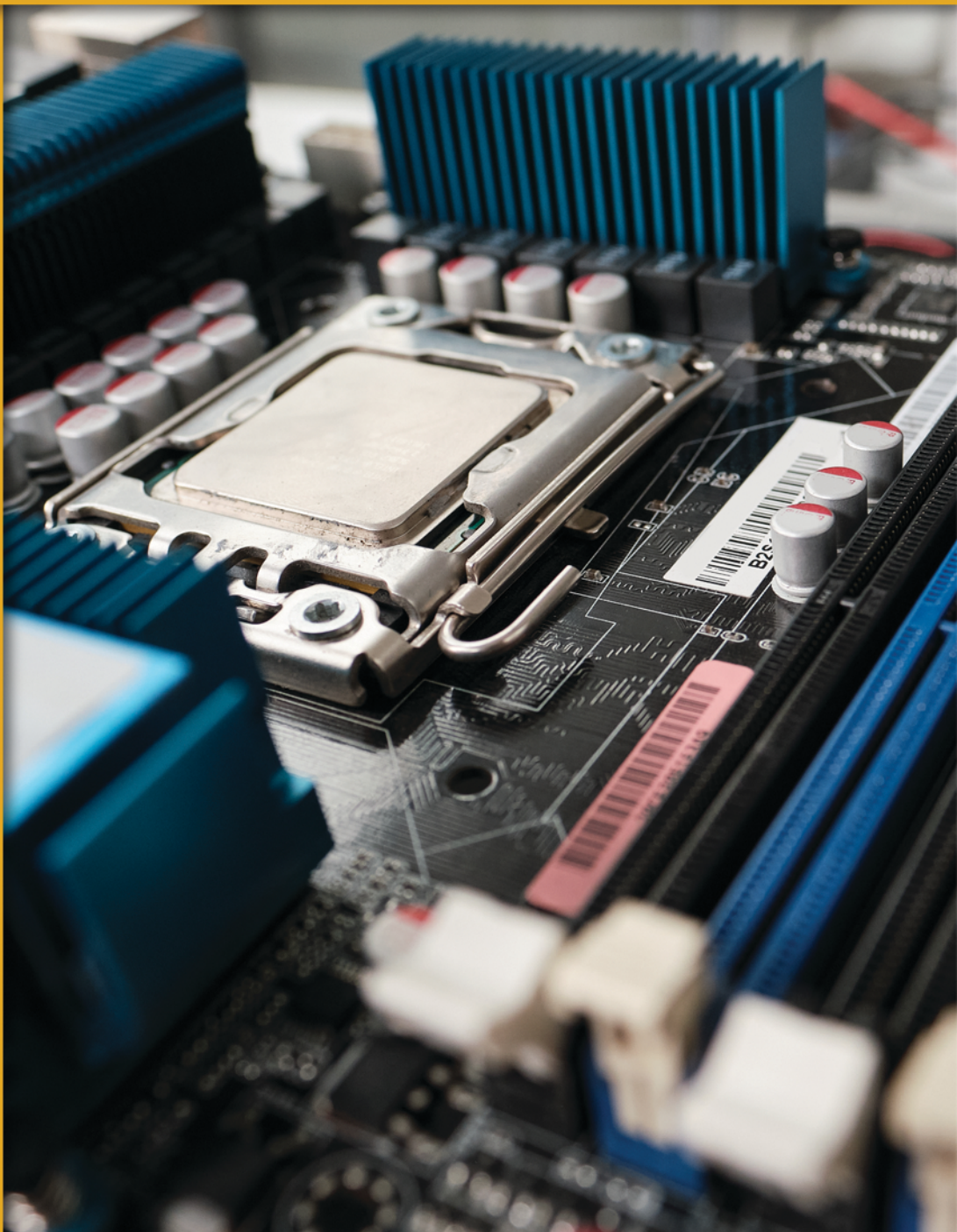


Α΄ Τάξη Γυμνασίου
ΠΛΗΡΟΦΟΡΙΚΗ



ΒΙΒΛΙΟ ΜΑΘΗΤΗ
ΣΥΜΠΛΗΡΩΜΑΤΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΥΛΙΚΟ

ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΘΡΗΣΚΕΥΜΑΤΩΝ ΚΑΙ ΑΘΛΗΤΙΣΜΟΥ
ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ

ΠΛΗΡΟΦΟΡΙΚΗ

Α΄ Τάξη Γυμνασίου

ΒΙΒΛΙΟ ΜΑΘΗΤΗ

ΣΥΜΠΛΗΡΩΜΑΤΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΥΛΙΚΟ

Αθήνα, Ιούλιος 2024

ΣΥΝΤΟΝΙΣΜΟΣ Ζέρβας Κωνσταντίνος, Σύμβουλος Α΄ του Ινστιτούτου Εκπαιδευτικής Πολιτικής

**ΕΠΙΣΤΗΜΟΝΙΚΗ
ΕΠΟΠΤΕΙΑ** Κοζύρης Νεκτάριος, Καθηγητής Εθνικού Μετσόβιου Πολυτεχνείου

**ΕΚΠΟΝΗΣΗ-
ΑΝΑΜΟΡΦΩΣΗ-
ΕΠΙΜΕΛΕΙΑ ΠΕΡΙΕΧΟΜΕΝΟΥ** Ζέρβας Κωνσταντίνος, Σύμβουλος Α΄ του Ινστιτούτου Εκπαιδευτικής Πολιτικής
Βλουχάκη Όλγα, Σύμβουλος Β΄ του Ινστιτούτου Εκπαιδευτικής Πολιτικής

ΕΚΠΟΝΗΣΗ Αθανασάκου Πηνελόπη, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Αλεξούδα Γεωργία, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Βολονάκης Παντελής, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Βραχνός Ευριπίδης, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Γώγουλος Γεώργιος, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Διαμαντής Ευστράτιος, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Ευαγγελινός Αιμιλιανός, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Ζάχος Γεώργιος, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Κοκκόρη Αθηνά, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Κολεγά Ευαγγελία, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Μακράκη Ευαγγελία, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Μαραγκός Κωνσταντίνος, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Μαρίτσας Αντώνιος, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Μαστοροδήμος Δημήτριος, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Μπαμπαλώνα Ελένη, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Παντελοπούλου Σταυρούλα, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Παπαδάκης Σπυρίδων, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Συμεωνίδης Συμεών, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86
Τζελέπη Σοφία, Σύμβουλος Εκπαίδευσης Πληροφορικής ΠΕ86

ΔΗΜΙΟΥΡΓΙΑ ΕΞΩΦΥΛΛΟΥ Σπίνος Ιωάννης, Εκπαιδευτικός Πληροφορικής ΠΕ86

Δράση για την επικαιροποίηση/ανανέωση του σχολικού βιβλίου Πληροφορικής Γυμνασίου (Πράξη 2/11-01-2024 του Δ.Σ. του ΙΕΠ, Ανακοίνωση με αρ. πρωτ. 382/17-01-2024 (ΑΔΑ: Ρ0Γ2ΟΞΛΔ-Γ0Ι), Πράξη 5/25-01-2024 του Δ.Σ. του ΙΕΠ με αρ. πρωτ. 1020/01-02-2024 (ΑΔΑ: 9Ω6ΘΟΞΛΔ-1ΒΚ), Πράξη 24/30-04-2024 του Δ.Σ. του ΙΕΠ με αρ. πρωτ. 3841/10-05-2024 (ΑΔΑ: ΨΦ45ΟΞΛΔ-ΛΩΝ) και Πράξη 47/22-08-2024 του Δ.Σ. του ΙΕΠ)

ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ

Σπυρίδων Δουκάκης

Πρόεδρος του Ινστιτούτου Εκπαιδευτικής Πολιτικής

Υπεύθυνος Δράσης

Κωνσταντίνος Ζέρβας

Σύμβουλος Α΄ του Ινστιτούτου Εκπαιδευτικής Πολιτικής



ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΘΡΗΣΚΕΥΜΑΤΩΝ & ΑΘΛΗΤΙΣΜΟΥ
ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ

Το παρόν εκπονήθηκε στο πλαίσιο της δράσης «Μαζί για την Εκπαίδευση», με ευθύνη της Επιστημονικής Μονάδας Φυσικών Επιστημών, Τεχνολογίας, Μαθηματικών και Τεχνών (STEM/STEAM) του Τμήματος Β΄: Προγραμμαμάτων Σπουδών και Εκπαιδευτικού Υλικού του Ινστιτούτου Εκπαιδευτικής Πολιτικής

Ενότητα 5

ΓΝΩΡΙΖΩ ΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΕΠΙΚΟΙΝΩΝΩ

Διαδίκτυο και Παγκόσμιος Ιστός

Διαδίκτυο των Πραγμάτων

Πνευματικά Δικαιώματα

5.5 Διαδίκτυο των Πραγμάτων (ΔτΠ)

Το **Διαδίκτυο των Πραγμάτων** (Internet of Things ή **IoT**) είναι συσκευές, ή αλλιώς αντικείμενα (πράγματα), που θα μπορούσαν να συνδεθούν στο Διαδίκτυο, με σκοπό να το χρησιμοποιήσουν ως μέσο επικοινωνίας και ανταλλαγής πληροφοριών. Με άλλα λόγια, χρησιμοποιείται η υποδομή του Διαδικτύου προκειμένου οι συσκευές αυτές να μεταφέρουν τα δεδομένα που καθορίζονται από το λογισμικό που ενσωματώνουν. Με τον τρόπο αυτό, εκτιμάται ότι θα έχουν σύνδεση στο Διαδίκτυο περισσότερες από 40 δισεκατομμύρια συσκευές έως το 2025 σε όλον τον κόσμο και ο αριθμός τους θα αυξάνεται ραγδαία όσο περνούν τα χρόνια.



Εικόνα 5.9. Το Διαδίκτυο των Πραγμάτων (ελεύθερη διανομή από needpix.com)

Τα αντικείμενα αυτά χρησιμοποιούνται για να εξυπηρετήσουν ανθρώπινες δραστηριότητες και μπορεί να βρίσκονται σε διάφορα σημεία, όπως για παράδειγμα, σε σπίτια, αυτοκίνητα, βιομηχανίες, νοσοκομεία, στην ύπαιθρο, ή ακόμα μπορούμε και να τα φοράμε (wearables). Πολλές φορές περιέχουν και στοιχεία Τεχνητής Νοημοσύνης. Στη συνέχεια, θα περιγράψουμε παραδείγματα τέτοιων διασυνδέσεων και θα αναδείξουμε οφέλη και κινδύνους που γεννά η χρήση της τεχνολογίας αυτής για τον άνθρωπο.

Το έξυπνο κινητό τηλέφωνο (smartphone) είναι ένα από τα αντικείμενα που εμπλέκονται με το Διαδίκτυο των Πραγμάτων σε καθημερινή βάση και έχει μια ποικιλία δυνατοτήτων. Μας επιτρέπει να συνδεόμαστε στο Διαδίκτυο με ασύρματο τρόπο και να αντλούμε πληροφορίες από τον Παγκόσμιο Ιστό για θέματα που μας ενδιαφέρουν. Διαθέτει εφαρμογή που διευκολύνει την πλοήγησή μας σε έναν προορισμό. Επίσης, επιτρέπει την αναγνώριση της τοποθεσίας όπου βρισκόμαστε και μετά, μέσω σύνδεσης με τη μετεωρολογική ή άλλη υπηρεσία, εμφανίζει δεδομένα για τον καιρό που επικρατεί εκεί. Το γεγονός αυτό θα μας βοηθήσει να ντυθούμε κατάλληλα, ή να προστατευτούμε, σύμφωνα με τα μηνύματα που θα λάβουμε από την πολιτική προστασία (γνωστό και ως μήνυμα από το 112).

Άλλα παραδείγματα συσκευών με σύνδεση στο Διαδίκτυο είναι οι σταθεροί και φορητοί υπολογιστές, τα έξυπνα ρολόγια (smartwatches) και οι έξυπνες τηλεοράσεις (smartTVs). Η λίστα, όμως, είναι μεγάλη και τα παρα-

δείγματα αυτά δεν την εξαντλούν, αλλά είναι χαρακτηριστικά. Ας παρουσιάσουμε τώρα μερικές από τις υπηρεσίες που προσφέρονται στον άνθρωπο μέσω των αντικειμένων που σχετίζονται με το Διαδίκτυο των Πραγμάτων, μαζί με μια σύντομη περιγραφή των λειτουργιών τους.

Σε ένα σπίτι θα μπορούσαμε να έχουμε συσκευές που θα μας επέτρεπαν να ανοίγουμε ή να κλείνουμε από απόσταση τα φώτα, καθώς και το σύστημα κλιματισμού, ή να παίρνουν την κατάλληλη απόφαση ανάλογα με τις μετεωρολογικές συνθήκες. Επίσης, θα μπορούσαν να ελέγχουν το συνολικό επίπεδο κατανάλωσης της ενέργειας και να μας ειδοποιούν όταν αυτή υπερβαίνει ένα προκαθορισμένο όριο ή να προτείνουν τρόπους εξοικονόμησης, ανάλογα με τα δεδομένα κατανάλωσής μας που θα αναλύουν.

Σε γεωργικές καλλιέργειες, συσκευές θα μπορούσαν να συλλέγουν πληροφορίες για το επίπεδο υγρασίας στο έδαφος και να ενημερώνονται για τον καιρό που θα επικρατήσει στην περιοχή, με σκοπό να ενεργοποιήσουν το σύστημα αυτόματου ποτίσματος.

Στο θαλάσσιο περιβάλλον, το Διαδίκτυο των Πραγμάτων θα μπορούσε να περιλαμβάνει συσκευές για έγκαιρη προειδοποίηση για επερχόμενο τσουνάμι, ύστερα από την εκδήλωση ενός υποθαλάσσιου σεισμού.

Σε μια βιομηχανία, συσκευές θα μπορούσαν να ελέγχουν τα μηχανήματα και να ενημερώνουν από απόσταση τους συντηρητές τους, είτε για βλάβες, είτε για προβλήματα στη λειτουργία τους, προκειμένου να επεμβαίνουν έγκαιρα για την αντιμετώπισή τους και να μην επηρεάζεται ιδιαίτερα ο ρυθμός παραγωγής.

Σε μια αποθήκη, συσκευές θα μπορούσαν να ελέγχουν τον αριθμό των τεμαχίων ενός προϊόντος και, όταν αυτός δεν είναι ικανοποιητικός, να ειδοποιούν αυτόματα τον υπεύθυνο για να προχωρήσει σε νέα παραγγελία.

Συσκευές συνδεδεμένες στο σώμα ενός ασθενούς θα μπορούσαν να ενημερώνουν από απόσταση τον ιατρό του, για να μπορέσει να επέμβει έγκαιρα σε περίπτωση που διαπιστωθεί ένα πρόβλημα. Κάποιες από τις συσκευές αυτές τις φοράμε (wearables), όπως τα έξυπνα ρολόγια, τα οποία μπορούν να μετρήσουν τους παλμούς της καρδιάς, τα βήματα που διανύουμε ή τις θερμίδες που «καίει» ο οργανισμός μας.

Σε ένα αυτοκίνητο, συσκευές θα μπορούσαν να ελέγχουν τον φόρτο στην κυκλοφορία αυτοκινήτων μιας πόλης, με σκοπό να προτείνουν στον οδηγό την ενδεδειγμένη διαδρομή που θα πρέπει να ακολουθήσει για να φτάσει πιο γρήγορα στον προορισμό του. Επιπλέον, θα μπορούσαν να του προτείνουν να ακινητοποιήσει το αυτοκίνητο, σε περίπτωση που αντιλαμβάνονται πιθανά σημάδια κόπωσης του.

Συσκευές μέτρησης των ρύπων στην ατμόσφαιρα θα μπορούσαν να συλλέγουν τα κατάλληλα δεδομένα, τα οποία στη συνέχεια θα αξιοποιεί η Πολιτεία, προκειμένου να παίρνει αποφάσεις περιορισμού της ρύπανσης.

Με τα παραδείγματα που μόλις περιγράψαμε, μπορούμε να καταλάβουμε ότι το Διαδίκτυο των Πραγμάτων είναι μια χρήσιμη τεχνολογία για τον άνθρωπο. Τον βοηθά στην παρακολούθηση και τον έλεγχο δεδομένων από απόσταση, του παρέχει εξοικονόμηση χρόνου και χρημάτων, τον απαλλάσσει από τετριμμένες και συχνά κουραστικές εργασίες, ενώ μπορεί να συμβάλλει σημαντικά στην προστασία της υγείας του και του φυσικού περιβάλλοντος στο οποίο διαβιώνει.

Από την άλλη πλευρά, η χρήση λειτουργιών που έχουν σχέση με το Διαδίκτυο των Πραγμάτων περιέχει και κινδύνους, που συνδέονται με την ασφάλεια των προσωπικών δεδομένων και την προστασία της ιδιωτικότητας, την ασφαλή λειτουργία των ίδιων των συσκευών και την προστασία από τη μόλυνση με κακόβουλο λογισμικό. Επίσης, ο μεγάλος όγκος δεδομένων που παράγεται δημιουργεί προβλήματα αποθηκευτικού χώρου και η ανομοιογένεια των συσκευών και των δεδομένων που διακινούνται, προκαλεί δυσκολίες στην εύκολη επικοινωνία μεταξύ τους. Τέλος, η ανάπτυξη της τεχνολογίας του Διαδικτύου των Πραγμάτων και η ολοένα και μεγαλύτερη διείσδυσή της σε διάφορους τομείς ανθρώπινων δραστηριοτήτων, μπορεί να οδηγήσει στη μείωση

των θέσεων εργασίας, χωρίς η δημιουργία νέων θέσεων να καλύπτει αυτή την απώλεια. Αυτό είναι ένα θέμα που θα πρέπει να εξεταστεί με την απαραίτητη κοινωνική ευαισθησία.

5.5.1 Ερωτήσεις

E.1: Τι είναι το Διαδίκτυο των Πραγμάτων;

E.2: Περιγράψτε δύο παραδείγματα από την καθημερινή ζωή, που δεν αναφέρονται στην ενότητα αυτή, σχετικά με το Διαδίκτυο των Πραγμάτων.

E.3: Περιγράψτε τρία προβλήματα που δημιουργεί το Διαδίκτυο των Πραγμάτων.

5.6 Πνευματικά δικαιώματα

Η νομοθεσία περί πνευματικών δικαιωμάτων προστατεύει τα δημιουργήματα του ανθρώπινου νου που είναι πρωτότυπα και δίνει στον δημιουργό τους δύο αποκλειστικά δικαιώματα:

- το αποκλειστικό δικαίωμα να εκμεταλλεύεται τα έργα του όπως θέλει, βγάζοντας ακόμα και χρήματα από αυτά (περιουσιακό δικαίωμα) και
- το αποκλειστικό δικαίωμα αφενός να αναγνωρίζεται ως ο δημιουργός των έργων του και αφετέρου να αποφασίζει αν και πώς θα χρησιμοποιηθούν τα έργα αυτά από τους άλλους (ηθικό δικαίωμα).

Συνεπώς, αν θέλουμε να αξιοποιήσουμε κάποιο έργο που δεν είναι δικό μας, θα πρέπει να πάρουμε την άδεια του δημιουργού για όσο διάστημα ισχύουν τα πνευματικά του δικαιώματα (δηλαδή έως και 70 χρόνια μετά τον θάνατό του). Ποια έργα προστατεύονται όμως από πνευματικά δικαιώματα και ποια όχι;

Προστατεύονται από πνευματικά δικαιώματα	Δεν προστατεύονται από πνευματικά δικαιώματα
- Λογοτεχνικά έργα (βιβλία, ποιήματα, άρθρα, μυθιστορήματα, παραμύθια, σενάρια, σίχοι, επιστημονικά κείμενα κ.λπ.). - Μουσικά έργα (συνθέσεις, τραγούδια, μουσικές διασκευές κ.λπ.). - Θεατρικά έργα, σενάρια, χορογραφίες κ.λπ. - Οπτικοακουστικά έργα (ταινίες, ντοκιμαντέρ, βίντεο κλιπ, τηλεοπτικές εκπομπές κ.λπ.). - Έργα εικαστικών και εφαρμοσμένων τεχνών (πίνακες ζωγραφικής, εικονογραφήσεις, γλυπτά, σχέδια κοσμημάτων, επίπλων κ.λπ.). - Αρχιτεκτονικά έργα (αρχιτεκτονικά σχέδια, σχεδιαγράμματα κ.λπ.). - Βάσεις δεδομένων και προγράμματα Η/Υ.	- Έργα που δεν έχουν καταγραφεί ή ηχογραφηθεί (αυθόρμητες ομιλίες, ζωντανές παραστάσεις κ.λπ.). - Απλές λέξεις και φράσεις (τίτλος, όνομα συγκροτήματος, σλόγκαν, λογότυπο κ.λπ.). - Ιδέες και έννοιες (ιδέα για συγγραφή βιβλίου που θα μπορούμε να γράψει ο καθένας). - Νόμοι, δικαστικές αποφάσεις/κείμενα. - Εκφράσεις λαϊκής παράδοσης (γνωμικά, παροιμίες, λαϊκοί χοροί). - Ειδήσεις, πληροφορίες και απλά γεγονότα. - Μαθηματικοί τύποι, διαδικασίες και μέθοδοι. - Έργα που έχει λήξει η προστασία των πνευματικών δικαιωμάτων τους.

Υπάρχει τρόπος να χρησιμοποιήσουμε τις δημιουργίες των άλλων χωρίς να παραβιάζουμε τα πνευματικά τους δικαιώματα;

5.6.1 Δίκαιη Χρήση

Ένας τρόπος να χρησιμοποιήσουμε τις δημιουργίες των άλλων χωρίς να παραβιάζουμε τα πνευματικά τους δικαιώματα είναι η Δίκαιη Χρήση (Fair Use).



Παράδειγμα 2 – Δίκαιη Χρήση

Ο Θέμης, μαθητής της Α΄ Γυμνασίου, ανέλαβε στο μάθημα των Καλλιτεχνικών να δημιουργήσει μια παρουσίαση για τη ζωή και τα έργα του διάσημου ζωγράφου και εφευρέτη Leonardo da Vinci.

Ψάχνοντας στον Παγκόσμιο Ιστό για υλικό σχετικό με το θέμα του, εντόπισε μια ιστοσελίδα με ένα εξαιρετικό άρθρο για τη ζωή του Leonardo da Vinci και πολλές φωτογραφίες από τα έργα του. Το πρώτο που σκέφτηκε ήταν να αντιγράψει το άρθρο και να ολοκληρώσει, εύκολα και χωρίς κόπο, την παρουσίασή του.

Ωστόσο, είχε ακούσει, πως η αντιγραφή περιεχομένου από το Διαδίκτυο, χωρίς την άδεια του δημιουργού, είναι σοβαρό **ποινικό** αδίκημα και τιμωρείται με χρηματικό πρόστιμο ή/και ποινή φυλάκισης σε κάποιες περιπτώσεις. Ψάχνοντας να βρει μια λύση, απευθύνθηκε στην καθηγήτρια Καλλιτεχνικών, η οποία του μίλησε για τη Δίκαιη Χρήση.

Σύμφωνα με τη Δίκαιη Χρήση, ο Θέμης μπορούσε να εντάξει μία με δύο φωτογραφίες και ένα μικρό μέρος του άρθρου στην παρουσίασή του, χωρίς να ζητήσει την άδεια του δημιουργού, καθώς η φύση της εργασίας του ήταν δημιουργική, είχε εκπαιδευτικό σκοπό, η ποσότητα της πληροφορίας ήταν περιορισμένη και δε θα έβλαπτε οικονομικά τον δημιουργό του άρθρου.



Εικόνα 5.10. Άρθρο με έργα του Leonardo da Vinci

(Δημιουργήθηκε στο DALLÉ-3 με την προτροπή: «Δημιουργήστε μια εικόνα που μοιάζει με άρθρο σε ιστοσελίδα, αφιερωμένο στα έργα τέχνης του Leonardo da Vinci. Η εικόνα πρέπει να περιλαμβάνει: έναν ελκυστικό τίτλο στο επάνω μέρος που λέει «Τα Έργα του Leonardo da Vinci». Υποδείγματα φωτογραφιών των πιο διάσημων έργων του da Vinci, όπως η «Μόνα Λίζα» και «Ο Τελευταίος Δείπνος», τοποθετημένες σε πλαίσια με λεπτομερείς περιγραφές κάτω από κάθε εικόνα. Παρακαλώ χρησιμοποιήστε μια καθαρή, σύγχρονη αισθητική για το σχεδιασμό της σελίδας, με έμφαση στην ευκρίνεια και την προσβασιμότητα»).



Η Δίκαιη Χρήση, αποτελεί εξαίρεση του νόμου πνευματικών δικαιωμάτων και μας επιτρέπει να χρησιμοποιούμε τις δημιουργίες των άλλων, χωρίς την άδειά τους, αρκεί να **αναφέρουμε** το όνομα τους και να τηρούμε τις ακόλουθες προϋποθέσεις:

- Η **φύση** της εργασίας μας είναι δημιουργική.
- Ο **σκοπός** της αφορά σε εκπαίδευση, έρευνα, ενημέρωση ή κριτική.
- Η **ποσότητα** των πληροφοριών που χρησιμοποιούμε είναι περιορισμένη.
- Η **χρήση** της είναι μη κερδοσκοπική.

5.6.2 Δημόσιος Τομέας

Ένας ακόμα τρόπος να χρησιμοποιήσουμε δημιουργίες άλλων, χωρίς να παραβιάζουμε τα πνευματικά τους δικαιώματα είναι να πάρουμε έργα που έχουν περιέλθει στον Δημόσιο Τομέα (Public Domain).



Παράδειγμα 3 – Δημόσιος Τομέας

Συνεχίζοντας την αναζήτηση υλικού για την παρουσίασή του ο Θέμης, εντόπισε μια εντυπωσιακή ψηφιακή εικόνα, αντίγραφο της Mona Lisa, ενός από τα πιο δημοφιλή έργα του Leonardo da Vinci.

Κάνοντας κλικ πάνω της, εμφανίστηκε στην περιγραφή της η φράση «Public Domain», (Δημόσιος Τομέας). Διαβάζοντας τη φράση αυτή, ο Θέμης θυμήθηκε (το είχε αναφέρει η καθηγήτριά του) ότι πρόκειται για εικόνα, της οποίας τα πνευματικά δικαιώματα έχουν λήξει και ανήκει πλέον στον Δημόσιο Τομέα.

Συνεπώς, ο Θέμης μπορούσε να χρησιμοποιήσει την εικόνα αυτή ελεύθερα, χωρίς να χρειάζεται να πάρει άδεια από τον δημιουργό της. Επίσης, θα μπορούσε να την τροποποιήσει, αλλάζοντας για παράδειγμα τη φωτεινότητά της και βάζοντας έτσι τη δική του καλλιτεχνική πινελιά στο έργο αυτό.



Εικόνα 5.11. Η Mona Lisa με δικαιώματα Δημόσιου Τομέα (Ανακτήθηκε από File:Mona Lisa.jpg - Wikimedia Commons)

Τα έργα που περιέρχονται στον Δημόσιο Τομέα (όπως εικόνες, ήχοι, βιβλία, κείμενα, φωτογραφίες, ταινίες, επιστημονικά άρθρα κ.ά.) δημιουργήθηκαν πριν πολλά χρόνια και δεν προστατεύονται πια από πνευματικά δικαιώματα. Συνεπώς, είναι ελεύθερα για αντιγραφή, τροποποίηση και διαμοιρασμό.



Περιεχόμενο που έχει περιέλθει στον Δημόσιο Τομέα μπορούμε να βρούμε σε βιβλιοθήκες, μουσεία, καθώς και σε πολλές διαδικτυακές πλατφόρμες, όπως η **Wikimedia Commons** (με πολυμέσα), η **Project Gutenberg** (με e-books, κυρίως από λογοτεχνικά έργα), η **Internet Archive** (με βιβλία, ταινίες, μουσική), η **Public Domain Review** (με περιεχόμενο για τέχνη, λογοτεχνία, ιστορία και πολιτισμό).

5.6.3 Άδειες Creative Commons

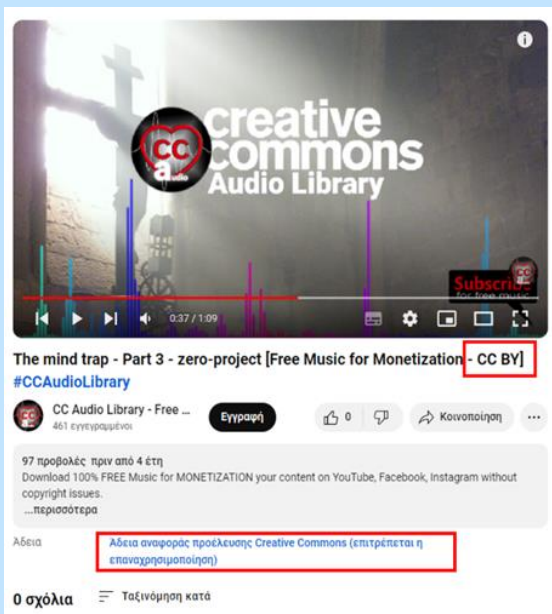
Οι άδειες Creative Commons είναι ο δημοφιλέστερος τύπος αδειών πνευματικών δικαιωμάτων. Ανήκουν σε έναν μη κερδοσκοπικό οργανισμό, που προσφέρει έναν απλό και δωρεάν τρόπο αδειοδότησης των ψηφιακών μας έργων. Δίνουν, δηλαδή, τη δυνατότητα στους δημιουργούς να ορίζουν σαφώς τα δικαιώματα πνευματικής ιδιοκτησίας που θέλουν να παραχωρήσουν στους άλλους, ώστε να μη χρειάζεται να τους ζητούν άδεια κάθε φορά που θέλουν να χρησιμοποιήσουν τις δημιουργίες τους.



Παράδειγμα 4 – Άδειες Creative Commons (CC)

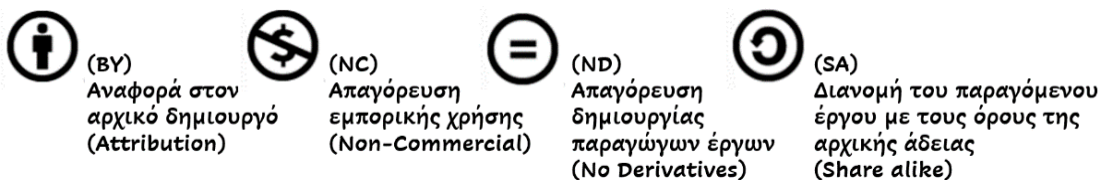
Μετά την αναζήτηση εικόνων και κειμένου, ο Θέμης αποφάσισε να εισάγει στην παρουσίασή του και έναν ήχο υποβάθρου, ώστε να την κάνει πιο ελκυστική. Πού θα έβρισκε, όμως, το κατάλληλο μουσικό κομμάτι και πώς θα ζητούσε άδεια από τον δημιουργό;

Μετά από αρκετή ώρα αναζήτησης στον Παγκόσμιο Ιστό, ο Θέμης βρήκε το μουσικό κομμάτι που έψαχνε σε μια πλατφόρμα διαμοιρασμού βίντεο, ωστόσο το μουσικό κομμάτι στον τίτλο του είχε την ένδειξη CC-BY. Ψάχνοντας πληροφορίες για την ένδειξη αυτή, ανακάλυψε ότι πρόκειται για μια άδεια Creative Commons (CC), που είχε δοθεί από τον δημιουργό του κομματιού, ώστε να γνωρίζει όποιος το χρησιμοποιεί ότι θα πρέπει να αναφέρει το όνομά του. Έτσι, ο Θέμης ενσωμάτωσε το μουσικό κομμάτι στην παρουσίασή του και δεν παρέλειψε να αναφέρει το όνομα του δημιουργού. Ανακάλυψε, επίσης, έναν εύκολο τρόπο να διαμοιράζεται τις δικές του δημιουργίες, προσθέτοντας σε κάθε έργο του την κατάλληλη άδεια CC, ώστε να μπορεί όποιος άλλος επιθυμεί να χρησιμοποιεί τα έργα του, χωρίς να χρειάζεται να ζητήσει την άδειά του και χωρίς να παραβιάζει τα πνευματικά του δικαιώματα.



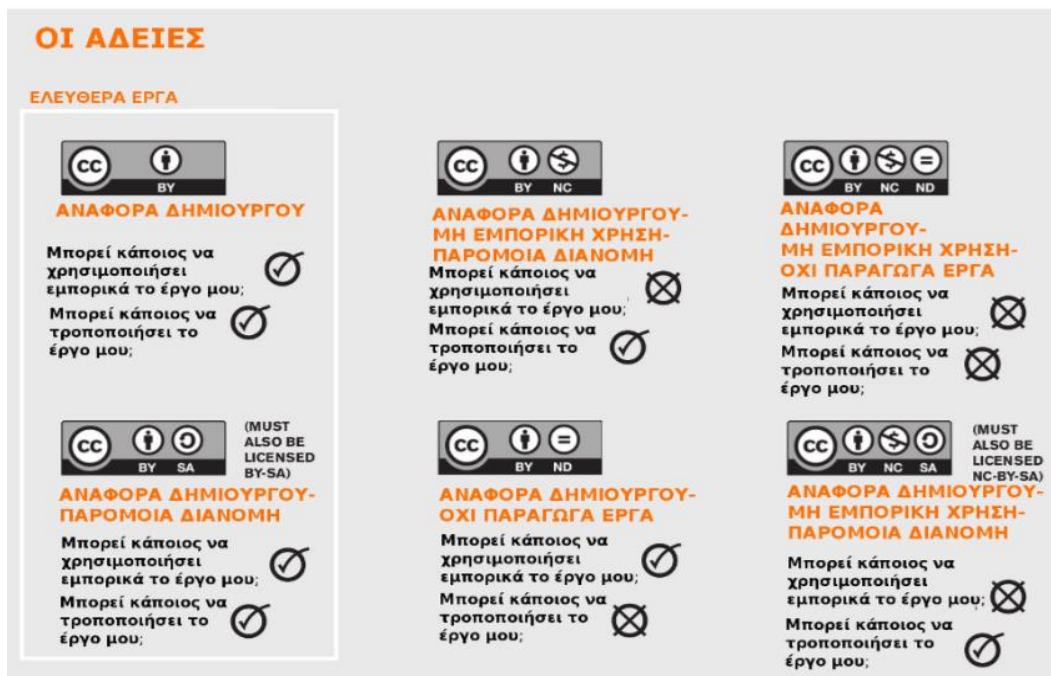
Εικόνα 5.12. Μουσικό κομμάτι με άδεια χρήσης CC-BY [Ανακτήθηκε από The mind trap - Part 3 - zero-project [Free Music for Monetization - CC BY] #CCAudioLibrary (youtube.com)]

Υπάρχουν 4 βασικοί τύποι δικαιωμάτων Creative Commons που απεικονίζονται στην Εικόνα 5.16.



Εικόνα 5.13. Τύποι αδειών Creative Commons

Ο συνδυασμός των παραπάνω τύπων δικαιωμάτων οδηγεί σε έξι διαφορετικούς τύπους αδειών (Εικόνα 5.14), μέσω των οποίων οι δημιουργοί πρωτότυπων έργων δηλώνουν πόσα και ποια δικαιώματα θέλουν να εκχωρήσουν στους άλλους. Όλες οι άδειες προβλέπουν ότι όποιος χρησιμοποιεί το έργο θα πρέπει να κάνει αναφορά στον αρχικό δημιουργό, διασφαλίζοντας τη φήμη του.



Εικόνα 5.14. Οι άδειες Creative Commons με απλά λόγια
(Ανακτήθηκε από <https://www.openbook.gr/creative-commons-licenses/>)



Πολλοί ιστότοποι διαθέτουν ψηφιακό περιεχόμενο με άδειες Creative Commons, όπως οι **Wikimedia Commons** (εικόνες, βίντεο, ήχους), **Openverse** (εικόνες, ήχους), **Pixabay** (εικόνες, βίντεο, σχέδια, ήχους, μουσική), **Flaticon** (εικονίδια και γραφικά), **freemusicarchive** (ήχους) κ.ά.

5.6.4 Πνευματικά δικαιώματα και Τεχνητή Νοημοσύνη

Το θέμα των πνευματικών δικαιωμάτων στην εποχή της Τεχνητής Νοημοσύνης είναι πολύ σύνθετο και εξελίσσεται συνεχώς. Όπως είδαμε παραπάνω, όταν ένας άνθρωπος δημιουργεί ένα έργο, αυτό βάσει νόμου προστατεύεται από πνευματικά δικαιώματα που διασφαλίζουν ότι κανείς δεν μπορεί να το αντιγράψει, να το τροποποιήσει ή να το χρησιμοποιήσει χωρίς την άδειά του. Τι γίνεται, όμως, όταν ένα πρόγραμμα Τεχνητής Νοημοσύνης δημιουργεί ένα έργο (εικόνα, ήχο, βίντεο); Εδώ τα πράγματα είναι πιο περίπλοκα καθώς σε πολλές χώρες, τα πνευματικά δικαιώματα προϋποθέτουν ανθρώπινη δημιουργία. Συνεπώς, οι προκλήσεις που προκύπτουν όταν μιλάμε για Τεχνητή Νοημοσύνη και πνευματικά δικαιώματα αφορούν κυρίως:

- την απόδοση δικαιωμάτων σε έργα που δημιουργούνται από Τεχνητή Νοημοσύνη,
- τον καθορισμό της ιδιοκτησίας των δεδομένων που χρησιμοποιούνται για την εκπαίδευση των μοντέλων Τεχνητής Νοημοσύνης. Πολλές φορές, αυτά τα δεδομένα περιέχουν εικόνες, κείμενα, ήχους που έχουν δημιουργήσει άλλοι άνθρωποι και προστατεύονται από πνευματικά δικαιώματα και
- την προστασία των δημιουργών.

Η νομοθεσία της Ευρωπαϊκής Ένωσης, την οποία ακολουθεί και η Ελλάδα, απαιτεί ένα έργο να έχει δημιουργηθεί από άνθρωπο για να προστατεύεται από πνευματικά δικαιώματα. Συνεπώς, έργα που δημιουργούνται από την Τεχνητή Νοημοσύνη, χωρίς ανθρώπινη παρέμβαση, δεν προστατεύονται από πνευματικά δικαιώματα. Επιπλέον, η νομοθεσία της Ευρωπαϊκής Ένωσης, απαιτεί τη δημοσίευση λεπτομερών περιλήψεων του περιεχομένου που χρησιμοποιείται για την εκπαίδευση των μοντέλων των συστημάτων Τεχνητής Νοημοσύνης «γενικής χρήσης».

Τέλος, εκτός από τα παραπάνω, υπάρχουν και ηθικά ζητήματα που προκύπτουν από την ευρεία χρήση της Τεχνητής Νοημοσύνης, όπως ο αντίκτυπος των έργων στους παραδοσιακούς δημιουργούς.



Δραστηριότητα 3 – Δημιουργία Ψηφιακής Σχολικής Εφημερίδας

Μελέτη Περίπτωσης: Στο Γυμνάσιο «Μέγας Αλέξανδρος», μια ομάδα μαθητών και μαθητριών αποφασίζει να δημιουργήσει μια ψηφιακή σχολική εφημερίδα για να μοιραστεί ιδέες, ειδήσεις και δημιουργικές εργασίες με τη σχολική κοινότητα.

Μπορείτε να τους βοηθήσετε να αξιοποιήσουν ψηφιακό υλικό από το Διαδίκτυο (όπως άρθρα, φωτογραφίες, μουσική, βίντεο κ.ά.), αποφεύγοντας την παραβίαση των πνευματικών δικαιωμάτων;

Χωριστείτε σε ομάδες των 2-4 ατόμων, συζητήστε και καταγράψτε τι απόψεις σας στα παρακάτω ζητήματα:

- Ποια νομικά ή ηθικά ζητήματα μπορεί να αντιμετωπίσει η ομάδα μαθητών και μαθητριών κατά τη χρήση περιεχομένου από το Διαδίκτυο;
- Ποιες εναλλακτικές λύσεις θα τους προτείνετε για τη νόμιμη χρήση αυθεντικού υλικού;

Προτείνετε, τουλάχιστον, δύο ιστότοπους που διαθέτουν ψηφιακό περιεχόμενο (εικόνες, ήχους, βίντεο, άρθρα κ.λπ.) με άδειες Creative Commons, που να είναι κατάλληλο για τη σχολική εφημερίδα.



Δραστηριότητα 4 – Διαγωνισμός Δημιουργίας Ψηφιακού Περιεχομένου

Το σχολείο σας διοργανώνει έναν διαγωνισμό δημιουργίας πρωτότυπου ψηφιακού περιεχομένου και για να λάβετε μέρος, ατομικά ή ομαδικά, θα πρέπει να ακολουθήσετε τα παρακάτω βήματα:

Βήμα 1: Επιλογή Κατηγορίας

- Επιλέξτε μία από τις ακόλουθες κατηγορίες ψηφιακού περιεχομένου (Ψηφιακό άρθρο, Βίντεο, Εικόνα ή Μουσική σύνθεση) για τη δημιουργία σας.

Βήμα 2: Κανόνες Δημιουργίας Περιεχομένου

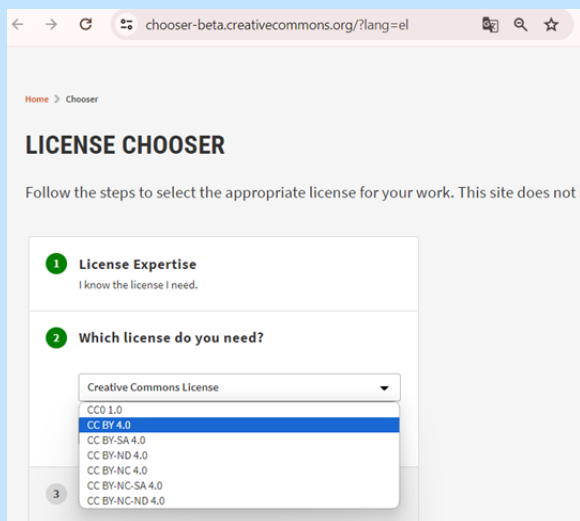
- Όλες οι δημιουργίες πρέπει να είναι πρωτότυπες.
- Πρέπει να αναφέρονται όλες οι πηγές που χρησιμοποιήθηκαν.
- Δεν επιτρέπεται να χρησιμοποιηθεί περιεχόμενο χωρίς άδεια χρήσης.

Βήμα 3: Υποβολή

- Η υποβολή των εργασιών θα πρέπει να γίνει έως την προθεσμία που έχει ορίσει ο/η εκπαιδευτικός της τάξης.

Βήμα 4: Επιλογή- Δημιουργία άδειας Creative Commons

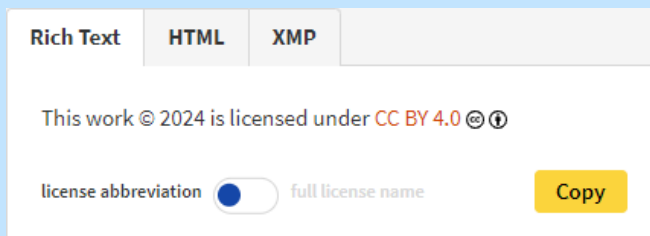
- Επισκεφθείτε την ιστοσελίδα Creative Commons και διαβάστε για τους διαφορετικούς τύπους αδειών που προσφέρονται. Εξετάστε τις έξι βασικές άδειες για να καταλάβετε τι επιτρέπει η κάθε μία (π.χ. αναφορά δημιουργού, μη εμπορική χρήση κ.λπ.).



- Σκεφτείτε τον τύπο του έργου που έχετε δημιουργήσει και πώς θέλετε να το χρησιμοποιούν οι άλλοι. Σκεφτείτε, δηλαδή, αν θέλετε να επιτρέψετε την εμπορική χρήση, τις τροποποιήσεις στο έργο σας κ.ά. και με βάση τις απαντήσεις σας, επιλέξτε την άδεια που ταιριάζει καλύτερα στις ανάγκες σας. Συμβουλευτείτε τον/την εκπαιδευτικό Πληροφορικής, αν δυσκολεύεστε να αποφασίσετε.

- Αφού καταλήξετε στην άδεια που ταιριάζει στο έργο σας, χρησιμοποιείστε τα βήματα του οδηγού (που βρίσκεται στο μενού Licenses and Tools -> chooser) της ιστοσελίδας Creative Commons για να δημιουργήσετε την άδεια CC για το έργο σας.

- Αρχικά διαλέξτε την άδεια της επιλογής σας.
- Συμπληρώστε τα χαρακτηριστικά της άδειας (τίτλο, όνομα δημιουργού, σύνδεσμο του έργου, ημερομηνία κ.ά.).
- Πατήστε DONE για να δημιουργηθεί η άδειά σας στο πλαίσιο κάτω δεξιά.
- Αντιγράψτε με το COPY την άδειά σας και χρησιμοποιήστε την στο έργο σας.



Βήμα 5: Αξιολόγηση

Κάθε ομάδα θα αξιολογήσει τις δημιουργίες των υπόλοιπων ομάδων χρησιμοποιώντας τον παρακάτω πίνακα διαβαθμισμένων κριτηρίων (ρουμπρίκα).

Κριτήρια	Άριστο (5 πόντοι)	Καλό (3-4 πόντοι)	Ανεπαρκές (1-2 πόντοι)	Σχόλια
Πρωτοτυπία	Το έργο είναι πρωτότυπο	Το έργο είναι αρκετά πρωτότυπο αλλά υπάρχουν κάποιες ομοιότητες με άλλα έργα.	Το έργο είναι κυρίως αντιγραφή ήδη υπαρχόντων έργων.	
Ποιότητα Περιεχομένου	Το περιεχόμενο είναι εξαιρετικά καλά οργανωμένο και πλήρες.	Το περιεχόμενο είναι καλά οργανωμένο αλλά θα μπορούσε να είναι πιο πλήρες.	Το περιεχόμενο είναι ανοργανώτο και ελλιπές.	
Σεβασμός στα Πνευματικά Δικαιώματα	Όλες οι πηγές έχουν άδεια χρήσης. Η αναφορά των πηγών είναι πλήρης και ακριβής. Το έργο δεν παραβιάζει καμία νομοθεσία ή ηθική κανόνα περί πνευματικών δικαιωμάτων.	Οι περισσότερες πηγές έχουν άδεια χρήσης αλλά υπάρχουν 1-2 όπου η αναφορά δεν είναι πλήρης ή η άδεια δεν είναι σαφής. Η αναφορά των πηγών είναι κατά βάση σωστή αλλά λείπουν μερικές λεπτομέρειες.	Χρησιμοποιούνται πηγές χωρίς άδεια χρήσης. Υπάρχουν σημαντικές παραλείψεις στην αναφορά των πηγών. Το έργο περιέχει στοιχεία που παραβιάζουν τα πνευματικά δικαιώματα τρίτων.	

Βήμα 6: Παρουσίαση και Βραβεία

Οι καλύτερες δημιουργίες (με την μεγαλύτερη βαθμολογία) θα παρουσιαστούν στην τάξη, θα λάβουν βραβεία και θα δημοσιευτούν στην ιστοσελίδα του σχολείου.

5.6.5 Ερωτήσεις

E.1: Ποια είναι η διαφορά μεταξύ πνευματικών δικαιωμάτων και των αδειών Creative Commons;

E.2: Γιατί ένας καλλιτέχνης/δημιουργός θα επέλεγε να χρησιμοποιήσει μια άδεια Creative Commons για το έργο του;

E.3: Απαντήστε τις επόμενες προτάσεις με Σωστό ή Λάθος. Τεκμηριώστε την απάντησή σας.		Σ	Λ
1	Τα πνευματικά δικαιώματα προστατεύουν μόνο τα λογοτεχνικά έργα, όπως τα βιβλία και τα ποιήματα.	☐	☐
2	Μπορείς να χρησιμοποιήσεις οποιαδήποτε εικόνα βρίσκεις στο Διαδίκτυο για εκπαιδευτικούς σκοπούς χωρίς άδεια.	☐	☐
3	Τα έργα που βρίσκονται στον Δημόσιο Τομέα μπορούν να αναπαραχθούν, τροποποιηθούν και διανεμηθούν χωρίς κανέναν περιορισμό.	☐	☐
4	Η Δίκαιη Χρήση επιτρέπει την ελεύθερη χρήση έργων υπό ορισμένες προϋποθέσεις.	☐	☐
5	Οι μαθηματικοί τύποι και οι επιστημονικές θεωρίες προστατεύονται από πνευματικά δικαιώματα.	☐	☐
6	Τα πνευματικά δικαιώματα διαρκούν για πάντα.	☐	☐

Ενότητα 6

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Κυβερνοασφάλεια

Ενότητα 6. Κυβερνοασφάλεια

6.1 Εισαγωγή

Το Διαδίκτυο, από τη γένεσή του, ξεκίνησε ως αγαθό για καλό σκοπό και καλή χρήση με στόχο τη διευκόλυνση της ακαδημαϊκής κοινότητας, των χρηστών και των διαφόρων φορέων. Ωστόσο, με την πάροδο των χρόνων, άρχισε βαθμιαία να εμφανίζεται το φαινόμενο της κακής χρήσης του Διαδικτύου από κακόβουλους χρήστες. Η **κυβερνοασφάλεια** είναι ο τομέας της Πληροφορικής που ασχολείται με την προστασία συστημάτων, δικτύων και δεδομένων από ψηφιακές επιθέσεις. Οι κύριοι στόχοι της κυβερνοασφάλειας περιλαμβάνουν:

- **Εμπιστευτικότητα** (Confidentiality): Διασφάλιση ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε ευαίσθητες πληροφορίες.
- **Ακεραιότητα** (Integrity): Προστασία των δεδομένων από μη εξουσιοδοτημένους χρήστες, εξασφαλίζοντας ότι τα δεδομένα είναι ακριβή και αξιόπιστα.
- **Διαθεσιμότητα** (Availability): Εξασφάλιση ότι τα συστήματα και τα δεδομένα είναι διαθέσιμα στους χρήστες όταν τα χρειάζονται.

Όταν τελειώσετε τη μελέτη αυτής της ενότητας θα μπορείτε να απαντήσετε στις παρακάτω ερωτήσεις:

- Τι σημαίνουν οι έννοιες «αγαθό», «απειλή», «ζημία»;
- Ποια μέτρα ασφάλειας μπορούμε να λάβουμε σε επίπεδο υπολογιστή;
- Ποια μέτρα ασφάλειας μπορούμε να λάβουμε σε επίπεδο δικτύου;
- Ποια είδη κρυπτογράφησης έχουμε;
- Τί είναι τα ψηφιακά πιστοποιητικά και τί οι ψηφιακές υπογραφές;

6.2 Απειλές και μέτρα προστασίας

Η έννοια της προστασίας αγαθών γενικότερα έχει να κάνει ουσιαστικά με το τι είναι αυτό που θεωρούμε χρήσιμο και άξιο προστασίας. Για παράδειγμα, κανείς δε θέλει να χάσει το USB flash του, διότι μπορεί το κόστος του USB να μην είναι υψηλό, ωστόσο τα δεδομένα που περιέχει είναι πιθανό να αντιστοιχούν σε πολλές ώρες εργασίας. Ωστόσο, τα πράγματα γίνονται πιο σοβαρά αν θεωρήσουμε άλλα μεγαλύτερης κλίμακας παραδείγματα, όπως τα κέντρα δεδομένων (data centers), τα οποία έχουν αποθηκευμένη τεράστια πληροφορία που ανήκει σε χρήστες, τα αποθετήρια, τα δεδομένα τραπεζών, τα δεδομένα από τα κεντρικά συστήματα εταιρειών και δημοσίων φορέων, ακόμη και απόρρητα στρατιωτικά ή ιατρικά δεδομένα.



Οτιδήποτε είναι άξιο προστασίας ονομάζεται **αγαθό** (asset) και το αγαθό έχει **αξία** (value). Η αξία αυτή των αγαθών μειώνεται αν υποστούν **ζημία** (harm). Το αγαθό είναι ευάλωτο σε πιθανούς **κινδύνους** (dangers) και απειλές. Για να εξαλείψουμε αυτούς τους κινδύνους, οι οποίοι είναι δυνατό να βλάψουν τα αγαθά μας, υιοθετούμε **μέτρα προστασίας**. Η **ζημία** μπορεί να προκληθεί στους πόρους ενός πληροφοριακού συστήματος, στην δικτυακή υποδομή ακόμη και στην κτιριακή υποδομή που φιλοξενεί ένα data center.



Με τον όρο **απειλή** περιγράφουμε οποιοδήποτε γεγονός δύναται να επιφέρει μερική ή ολική αλλοίωση των αγαθών. Μπορεί να συμβεί με **φυσικό** ή με **ηλεκτρονικό τρόπο**. Κατ' αρχάς, τα data centers και όλοι οι προσωπικοί υπολογιστές γενικότερα, πρέπει να προστατεύονται από τη φυσική πρόσβαση μη εξουσιοδοτημένων χρηστών. Άρα, πρώτη και βασική παράμετρος ασφάλειας είναι ο **έλεγχος της φυσικής πρόσβασης** στα data centers. Επίσης, πρέπει να προστατεύονται και από **φυσικούς κινδύνους**, όπως φωτιά, πλημμύρες και σεισμούς. Αξίζει να σημειωθεί, πως το δίκτυο συνιστά κρίσιμη υποδομή και θα πρέπει να λειτουργεί δυναμικά σε όλες τις περιπτώσεις.

Σύγχρονος τρόπος ζωής και απειλές:

Σήμερα αρκετοί χρησιμοποιούν τα κοινωνικά δίκτυα και ανεβάζουν τις φωτογραφίες τους και άλλα προσωπικά δεδομένα. Επίσης, σχεδόν όλοι πραγματοποιούμε ηλεκτρονικές πληρωμές για την αγορά προϊόντων, την κράτηση εισιτηρίων, την κράτηση δωματίων σε ξενοδοχεία καθώς και διατραπεζικές συναλλαγές. Είναι κατανοητό πως όταν πραγματοποιούμε τραπεζικές συναλλαγές θέλουμε αυτές να εκτελούνται με ασφάλεια και, βεβαίως, δεν επιθυμούμε οι κωδικοί μας να διαρρεύσουν, καθώς κάτι τέτοιο θα είχε ως πιθανή συνέπεια το άδειασμα του λογαριασμού μας. Επιπρόσθετα, υπάρχουν στον κόσμο διάσπαρτοι **κακοπροαίρετοι χρήστες-hackers**, οι οποίοι προσπαθούν με διάφορους τρόπους να αποκτήσουν πρόσβαση στον υπολογιστή μας, στα δεδομένα και στους κωδικούς μας. Ακριβώς το ίδιο επιχειρούν και σε μεγάλες εταιρείες, τράπεζες, οργανισμούς και φορείς του δημοσίου.

6.3 Επίπεδα ασφάλειας και εφαρμογή τους

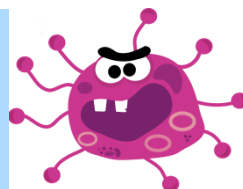
Η ασφάλεια εφαρμόζεται τόσο σε επίπεδο **υπολογιστή** όσο και σε επίπεδο **δικτύου** και **πληροφοριακών συστημάτων**. Στο δίκτυο, βέβαια, συμπεριλαμβάνεται και το **νέφος (cloud)**, καθώς και το **Διαδίκτυο των Πραγμάτων**. Για να ανταπεξέλθουμε σε αυτές τις απειλές, υιοθετούμε **μέτρα προστασίας**, τόσο σε επίπεδο υπολογιστή, όσο και σε επίπεδο δικτύου και πληροφοριακών συστημάτων.

6.3.1 Ασφάλεια σε επίπεδο υπολογιστή

Κατ' αρχάς, μόνο από την περιήγησή μας σε κάποιους μη ασφαλείς ιστότοπους είναι δυνατό να μολυνθεί ο υπολογιστής μας. Συγκεκριμένα, ο υπολογιστής μας είναι δυνατό να «κολλήσει» ιούς, σκουλήκια, να τύχει εγκατάστασης λογισμικού δούρειου ίππου, Ransomware, Malvertising, Phishing και άλλα. Επιπρόσθετα, κίνδυνο συνιστά κάθε μολυσμένη συσκευή που συνδέεται στο σύστημά μας, όπως τα USB sticks.

Σε ό,τι αφορά στην προστασία σε επίπεδο προσωπικού υπολογιστή, ένας χρήστης θα πρέπει να έχει ενεργοποιημένες τις ενημερώσεις του λειτουργικού συστήματος (system updates), καθώς με αυτόν τον τρόπο εγκαθίστανται οι νέες εκδόσεις του συστήματος. Η μητρική εταιρεία του λειτουργικού εντοπίζει πιθανές **ευπάθειες (vulnerabilities) του συστήματος** και με αυτόν τον τρόπο τις αποκαθιστά και τις διορθώνει.

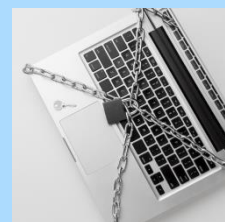
Επιπρόσθετα, θα πρέπει ο χρήστης να έχει εγκαταστήσει **Αντιϊκό Λογισμικό (antivirus)** στο σύστημά του, έτσι ώστε να προστατεύεται από **ιούς (viruses)**, κατά την επίσκεψη ιστοτόπων, το κατέβασμα λογισμικού από το Διαδίκτυο, μολυσμένα μηνύματα ηλεκτρονικού ταχυδρομείου κ.λπ.



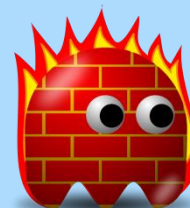
Υπάρχει μεγάλη ποικιλία αντιϊκών λογισμικών, τα οποία παρέχουν ολοκληρωμένες λύσεις για απειλές όπως **σκουλήκια (worms)**, **δούρειους ίππους** κ.ά. Ο δούρειος ίππος (trojan horse) είναι λογισμικό το οποίο κρύβεται σε ένα φαινομενικά αβλαβές πρόγραμμα ή αρχείο. Στόχος του είναι να ξεγελάσει τον χρήστη να το εγκαταστήσει ή να το εκτελέσει στον υπολογιστή του, επιτρέποντας, έτσι, στους εισβολείς να αποκτήσουν πρόσβαση στο σύστημα και να πραγματοποιήσουν κακόβουλες ενέργειες.



Το **RansomeWare** είναι **κακόβουλο λογισμικό** το οποίο κλειδώνει τον χρήστη έξω από το σύστημά του με αποτέλεσμα να μην μπορεί να έχει πρόσβαση στα αρχεία και στις συσκευές του. Οι επιτιθέμενοι στοχεύουν οργανισμούς και άτομα, κρυπτογραφώντας τα δεδομένα τους και απαιτώντας συχνά πληρωμή, συνήθως σε κρυπτονομίσματα, για να τους δώσουν το κλειδί αποκρυπτογράφησης.



Το **τείχος προστασίας (Firewall)** εφαρμόζεται είτε σε επίπεδο υπολογιστή είτε σε επίπεδο δικτύου. Είναι κανόνες, γενικά, όλα τα δίκτυα να προστατεύονται με τείχος προστασίας, το οποίο επιτρέπει πρόσβαση μόνο σε συγκεκριμένες διευθύνσεις του δικτύου και σε συγκεκριμένες υπηρεσίες και απαγορεύει οτιδήποτε άλλο. Κάθε οικιακός υπολογιστής έχει ενσωματωμένο τείχος προστασίας στο λειτουργικό σύστημα, ωστόσο αν ο χρήστης επιθυμεί μπορεί να εγκαταστήσει επιπλέον λογισμικό προστασίας στο σύστημά του.



Ένα κακόβουλο e-mail τύπου **phishing** είναι δυνατό να περιέχει ιό με συνέπεια να μολυνθεί ο υπολογιστής μας και να ρισκάρουμε με αυτόν τον τρόπο την αλλοίωση ή απώλεια των δεδομένων μας.

Σε αυτήν την περίπτωση μπορεί να λάβουμε ένα e-mail που να φαίνεται ότι αποστολέας είναι η τράπεζά μας και μας προτρέπει να δώσουμε τους κωδικούς μας για να ξεκλειδώσουμε τον λογαριασμό μας. Εάν δεν είμαστε προσεκτικοί και ακολουθήσουμε την προτροπή του e-mail, είναι πιθανό να πέσουμε θύματα απάτης, διότι με αυτόν τον τρόπο θα εκχωρήσουμε τους κωδικούς μας σε κάποιον άγνωστο ο οποίος παρουσιάζεται ως εκπρόσωπος της τράπεζας.



**Δε δίνουμε ποτέ και σε κανέναν τους κωδικούς μας!**

Όταν θέλουμε να προβούμε σε διατραπεζική συναλλαγή, πληκτρολογούμε ολόκληρη την ηλεκτρονική διεύθυνση της τράπεζας μόνοι μας και δεν πατάμε ποτέ σύνδεσμο που μας έχουν στείλει. Βέβαια, οι πιο έμπειροι χρήστες είναι σε θέση να διακρίνουν την προέλευση του ηλεκτρονικού ταχυδρομείου και να καταλάβουν ότι πρόκειται για παραπλανητικό e-mail.

**Προστασία προσωπικών δεδομένων**

Δε δίνουμε ποτέ τα προσωπικά μας στοιχεία (ονοματεπώνυμο, τηλέφωνο, διεύθυνση κατοικίας, κωδικούς) στα Μέσα Κοινωνικής Δικτύωσης δίκτυα και καλό είναι να μην ανεβάζουμε φωτογραφίες. Επίσης, δεν κοινοποιούμε την πληροφορία ότι είμαστε διακοπές!

**Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος**

Στην Ελληνική Αστυνομία λειτουργεί η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και εκεί μπορεί να απευθυνθεί οποιοσδήποτε θεωρεί ότι έχει υποστεί ζημία η ιδιωτικότητά του.

(<https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/diefthynsi-dioxis-ilektronikou-egklimatos/>)

**Δραστηριότητα 1**

1. Ελέγξτε εάν ο υπολογιστής σας έχει εγκατεστημένο αντιϊικό λογισμικό. Προχωρήστε σε έναν έλεγχο συστήματος (scan for viruses).
2. Ενεργοποιείτε την «Ενημέρωση του Λ.Σ.». Τί επιτυγχάνετε με αυτό; Ενεργοποιήστε και το τείχος προστασίας.

6.3.2 Ασφάλεια δικτύου και πληροφοριακών συστημάτων

Σε κάθε περίπτωση, εκτός από τους υπολογιστές μας, θα πρέπει να προστατεύονται και τα δίκτυα από κακόβουλες ενέργειες. Πολύ σημαντικό παράγοντα συνιστά η προστασία στα δίκτυα υπολογιστών, στο νέφος, στο Διαδίκτυο των Πραγμάτων και στα πληροφοριακά συστήματα. Στο νέφος και στα πληροφοριακά συστήματα φυλάσσονται πολύ σημαντικά δεδομένα και τις περισσότερες φορές είναι πιθανό να αφορούν σε κρίσιμες υποδομές, όπως είναι οι κρατικοί οργανισμοί, τράπεζες, φορείς, εταιρείες κ.λπ.

Τείχος προστασίας στα δίκτυα - FireWall

Το βασικότερο θέμα στην ασφάλεια των δικτύων είναι η προστασία του εσωτερικού δικτύου των χρηστών καθώς και των εξυπηρετητών. Γι' αυτόν τον λόγο εφαρμόζεται διαφορετικό επίπεδο ασφάλειας τόσο στο εσωτερικό δίκτυο, όσο και στους εξυπηρετητές. Κύρια μέριμνα που λαμβάνουμε στο εσωτερικό δίκτυο είναι η γενικότερη απαγόρευση εισερχόμενης κίνησης, ενώ στους εξυπηρετητές επιτρέπουμε συγκεκριμένου είδους αιτήματα, όπως για υπηρεσίες Web, mail κ.λπ. Η ανάπτυξη FireWall για την προστασία ενός δικτύου είναι σημαντική διαδικασία και απαιτεί εξειδικευμένους μηχανικούς αναλόγως του μεγέθους του δικτύου.

Πληροφοριακά Συστήματα

Στα πληροφοριακά συστήματα και στους εξυπηρετητές γενικότερα εφαρμόζονται συγκεκριμένα μέτρα προστασίας αναλόγως του είδους της υπηρεσίας. Για παράδειγμα, στην υπηρεσία **ηλεκτρονικού ταχυδρομείου** εφαρμόζονται κεντρικά μέτρα AntiSpam, αντιϊικής προστασίας, μαύρες λίστες αποστολών (black lists) κ.λπ. Ομοίως σε κάθε υπηρεσία εφαρμόζονται τα ανάλογα με αυτή μέτρα προστασίας.

Επίσης, στα πεδία που δίνουμε ευαίσθητα δεδομένα όπως κωδικούς εισόδου, εφαρμόζουμε πρόσθετη ασφάλεια, ούτως ώστε να μην μπορεί κάποιος χρήστης να εκτελέσει κακόβουλο κώδικα (exploit) μέσω του πεδίου αυτού. Για παράδειγμα, οι κωδικοί υφίστανται **Κρυπτογράφηση**. Όταν λοιπόν εισάγουμε τους κωδικούς μας σε μια σελίδα, παρατηρούμε ότι το πρωτόκολλο έχει μετατραπεί από http σε https. Αυτό σημαίνει ότι η απομακρυσμένη υπηρεσία χρησιμοποιεί τα **πρωτόκολλο SSL/TLS** το οποίο παρέχει κρυπτογράφηση στα δεδομένα μας και μέσω αυτού ο εξυπηρετητής διαθέτει και **πιστοποιητικά ασφάλειας (certificates)**. Τα πιστοποιητικά τα εκδίδει ο αντίστοιχος φορέας. Με τη χρήση των πρωτοκόλλων αυτών επιτυγχάνουμε τα ακόλουθα:



Εμπιστευτικότητα (confidentiality): Μη εξουσιοδοτημένοι χρήστες δεν είναι δυνατό να έχουν πρόσβαση σε ιδιωτικά δεδομένα.



Ακεραιότητα (Integrity): Διασφαλίζεται ότι τα δεδομένα μας δεν έχουν υποστεί αλλοίωση από μη εξουσιοδοτημένους χρήστες.



Αυθεντικοποίηση - Έλεγχος ταυτότητας: Επιβεβαιώνεται ότι η πληροφορία προέρχεται από τον πραγματικό αποστολέα της, δηλαδή από αυτόν που νομίζουμε ότι ήρθε.

Η χρήση της τεχνολογίας **SSO (Single Sign On) πάνω από πρωτόκολλο SSL/TLS** σε συνδυασμό κυρίως με την **OTP (One Time Password)** παρέχει μια πρόσθετη δικλίδα ασφαλείας στα πληροφοριακά συστήματα. Με την SSO η ταυτοποίηση γίνεται μία φορά σε ένα δίκτυο μέσω κρυπτογραφημένων κωδικών και μετά ο χρήστης εξουσιοδοτείται για όλες τις υπηρεσίες του. Για παράδειγμα, όταν εισερχόμαστε στον ιστότοπο του gov.gr, δίνουμε τους κωδικούς μας μία φορά (SSO), ανεξαρτήτως της υπηρεσίας ή των εξυπηρετητών που θα χρειαστούν για τη διεκπεραίωση του αιτήματός μας. Ωστόσο, παρατηρούμε, ότι ενώ πληκτρολογούμε τη διεύθυνση <http://www.gov.gr/>, συνδεόμαστε αυτόματα σε ασφαλή σύνδεση με πρωτόκολλο SSL/TLS στη διεύθυνση <https://www.gov.gr/>. Επιπρόσθετα, έρχεται ένα μήνυμα OTP στο κινητό τηλέφωνο του χρήστη ως πρόσθετη μορφή αυθεντικοποίησης και ζητείται, πέραν των κωδικών, και η καταχώρηση αυτού του αριθμού.

6.4 Κρυπτογραφία – Είδη κρυπτογράφησης

Όταν στέλνουμε τα δεδομένα μας και θέλουμε να μεταφερθούν με ασφάλεια, δηλαδή θέλουμε να μην μπορούν να διαβαστούν από μη εξουσιοδοτημένους χρήστες ακόμη και αν αυτά περιέλθουν στην κατοχή τους, τότε εμείς θα πρέπει να έχουμε προβεί στην κρυπτογράφηση τους πριν την αποστολή.



Κρυπτογράφηση είναι η εφαρμογή μια τεχνικής για την μετατροπή της πληροφορίας σε μορφή μη αναγνωρίσιμη, έτσι ώστε κατά την αποθήκευση ή τη μεταφορά της να μην μπορεί να αναγνωστεί από μη εξουσιοδοτημένα άτομα.



Αποκρυπτογράφηση είναι η αντίστροφη τεχνική και εφαρμόζεται μόνο από εξουσιοδοτημένα άτομα με στόχο την ανάκτηση της αρχικής πληροφορίας.

Η Κρυπτογράφηση διακρίνεται σε συμμετρική και ασύμμετρη.

Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση οι συμμετέχοντες στην επικοινωνία μοιράζονται ένα κοινό μυστικό κλειδί. Ο αποστολέας κρυπτογραφεί το μήνυμά του με αυτό το κλειδί και το στέλνει στον παραλήπτη. Ο παραλήπτης με τη σειρά του, γνωρίζοντας από πριν το κοινό μυστικό κλειδί, μπορεί και αποκρυπτογραφεί το μήνυμα και ανακτά το αρχικό κείμενο. Η **κρυπτογράφηση του Καίσαρα** (Caesar Cipher) αποτελεί το πιο γνωστό παράδειγμα συμμετρικής κρυπτογράφησης. Χρησιμοποιεί την τεχνική ολίσθησης του αλφαβήτου. Για παράδειγμα, εάν ολίσθίσουμε το αλφάβητο κατά δύο γράμματα το Α γίνεται Γ, το Β → Δ, το Γ → Ε κ.ο.κ. Το μυστικό κλειδί ορίζεται από τον αριθμό γραμμάτων που θα ολίσθίσουν.

Σχετικά με τον αλγόριθμο για την κρυπτογράφηση του Καίσαρα, μπορείτε να ανατρέξετε στο κεφάλαιο 8.3, στην ενότητα αλγόριθμοι κρυπτογράφησης.



Παράδειγμα 1

Έστω ότι θέλετε να κρυπτογραφήσετε με τον αλγόριθμο του Καίσαρα τη λέξη «ΚΑΛΗΜΕΡΑ» εφαρμόζοντας ολίσθηση των γραμμάτων κατά δύο. Ποιο είναι το παραγόμενο συμμετρικά κρυπτογραφημένο μήνυμα;

Απάντηση

Ολίσθαίνουμε τα γράμματα κατά δύο δεξιά και βρίσκουμε τα νέα γράμματα:

$K \rightarrow M, A \rightarrow \Gamma, \Lambda \rightarrow N, H \rightarrow I, M \rightarrow \Xi, E \rightarrow H, P \rightarrow T, A \rightarrow \Gamma$

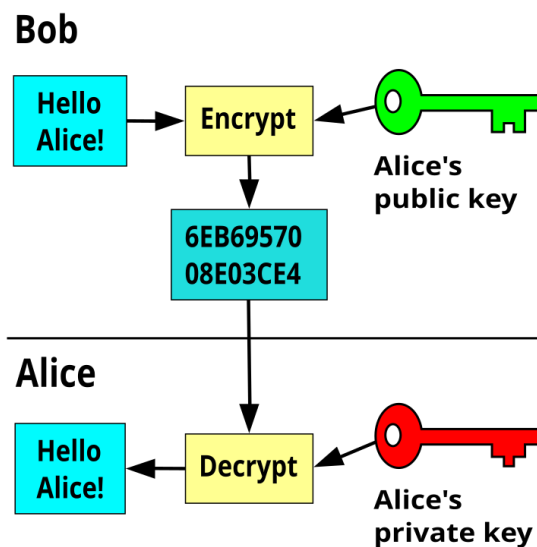
Άρα το κρυπτογραφημένο μήνυμα ή αλλιώς το **κρυπτογράφημα** θα είναι το: **ΜΓΝΙΞΗΤΓ**

Ασύμμετρη Κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση δε χρησιμοποιούμε ένα κοινό μυστικό κλειδί, γιατί αυτό μπορεί να διαρρεύσει. Αντιθέτως χρησιμοποιούμε ζευγάρια **Δημόσιου-Public** και **Ιδιωτικού-Private** κλειδιού. Το ένα χρησιμεύει στην κρυπτογράφηση του μηνύματος και το άλλο στην αποκρυπτογράφηση. Και τα δύο κλειδιά δημιουργούνται την ίδια στιγμή και συσχετίζονται μεταξύ τους.

Η Alice αποστέλλει στον Bob το δημόσιο κλειδί της και κρατάει το ιδιωτικό κλειδί μυστικό. Στη συνέχεια, ο Bob κρυπτογραφεί το μήνυμα που θέλει να στείλει με το δημόσιο κλειδί που έχει λάβει από την Alice και της στέλνει το μήνυμα κρυπτογραφημένο. Η Alice λαμβάνει το κρυπτογραφημένο μήνυμα από τον Bob και το αποκρυπτογραφεί με το ιδιωτικό της κλειδί. Κανείς άλλος δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, επειδή μόνο η ίδια η Alice γνωρίζει το ιδιωτικό της κλειδί. Το δημόσιο κλειδί είναι αυτό που μοιράζεται στο δίκτυο, ενώ το ιδιωτικό κλειδί δε διανέμεται σε κανέναν. Η κεντρική ιδέα στην οποία στηρίζεται η κρυπτογραφία δημόσιου κλειδιού είναι ότι, ενώ είναι εύκολο να βρούμε το γινόμενο δύο φυσικών αριθμών, είναι από δύσκολο έως ακατόρθωτο να βρούμε τους πρώτους παράγοντες ενός σύνθετου αριθμού.

Όταν, λοιπόν, συνδεόμαστε σε κάποιο site και βλέπουμε στην ηλεκτρονική διεύθυνση αντί για το πρωτόκολλο http να έχουμε https, τότε σημαίνει ότι ο ιστότοπος αυτός χρησιμοποιεί Ασύμμετρη Κρυπτογράφηση ή αλλιώς Κρυπτογράφηση Δημόσιου Κλειδιού. Σημειώνεται πως ένας από τους πιο γνωστούς και ευρέως χρησιμοποιούμενους αλγορίθμους κρυπτογράφησης δημόσιου κλειδιού είναι ο **RSA** των Rivest–Shamir–Adleman. Τέτοιου είδους κρυπτογράφηση χρησιμοποιούμε ακόμη στα Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Network- VPN), στις ψηφιακές υπογραφές, στις συναλλαγές με κρυπτονομίσματα και σε άλλες εφαρμογές.



Εικόνα 6.1. Ασύμμετρη Κρυπτογράφηση

Ψηφιακά Πιστοποιητικά και Ψηφιακή Υπογραφή

Στην προηγούμενη περίπτωση είδαμε τη χρήση του ιδιωτικού και του δημόσιου κλειδιού. Το δημόσιο κλειδί ωστόσο, μπορεί να επικυρώνεται και από φορείς πιστοποίησης ή αλλιώς από μια **Αρχή Πιστοποίησης (Certificate Authority - CA)**, η οποία είναι επίσημη και ανεξάρτητη. Η Αρχή Πιστοποίησης πιστοποιεί τον χρήστη που εκδίδει τα δημόσια κλειδιά. Συνεπώς, η επικύρωση του Δημοσίου Κλειδιού συνιστά τη δημιουργία ενός **ψηφιακού πιστοποιητικού** το οποίο συνδέεται, επίσης, με την ταυτότητα του ιδιοκτήτη του. Εφόσον, λοιπόν, κάποιος λάβει με την επίσημη προβλεπόμενη διαδικασία ένα ψηφιακό πιστοποιητικό μπορεί, για παράδειγμα, να θέτει ηλεκτρονική ψηφιακή υπογραφή στα έγγραφά του. Επίσης, στις συναλλαγές στο Διαδίκτυο, τα ηλεκτρονικά καταστήματα οφείλουν να χρησιμοποιούν έγκυρα ψηφιακά πιστοποιητικά από αναγνωρισμένες Αρχές Πιστοποίησης ώστε να διασφαλίζουν τις συναλλαγές των πελατών τους.



Παραδείγματα Αρχών Πιστοποίησης

- Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου: <https://aped.gov.gr>
- Η Υπηρεσία ψηφιακών πιστοποιητικών του Πανελληνίου Σχολικού Δικτύου: <https://ca.sch.gr/>

Η τεχνολογία Blockchain

Το Blockchain είναι μια τεχνολογία που επιτρέπει την αποθήκευση δεδομένων με ασφαλή, διαφανή και αμετάβλητο τρόπο. Αποτελείται από μια αλυσίδα μπλοκ (blocks), όπου κάθε ένα περιέχει έναν αριθμό εγγραφών (συναλλαγών) ψηφιακά υπογεγραμμένων από τους δημιουργούς τους. Επίσης κάθε μπλοκ περιέχει το ψηφιακό αποτύπωμα (hash) όλων των περιεχομένων του προηγούμενου. Τα μπλοκ αποθηκεύονται ανεξάρτητα σε κάθε υπολογιστή που συμμετέχει στη διαχείριση της αλυσίδας. Φανταστείτε ένα μεγάλο βιβλίο, όπου κάθε σελίδα αντιστοιχεί σε ένα μπλοκ. Αυτό το βιβλίο δε βρίσκεται σε ένα μόνο μέρος, αλλά αντίγραφά του υπάρχουν σε χιλιάδες υπολογιστές σε όλον τον κόσμο. Κάθε φορά που δημιουργείται μια νέα σελίδα, όλοι οι υπολογιστές που διατηρούν το βιβλίο εκτελούν μια διαδικασία, ώστε να φτάσουν σε συμφωνία (consensus) ότι το βιβλίο παραμένει σωστό. Αυτό έχει ως αποτέλεσμα το Blockchain να μην ελέγχεται μόνο από έναν κεντρικό οργανισμό. Έτσι, αν κάποιος προσπαθήσει να αλλάξει ένα μπλοκ (πχ. αφαιρώντας συναλλαγές) θα αλλάξει το ψηφιακό αποτύπωμά του, ακυρώνοντας όλα τα επόμενα. Στη συνέχεια, θα πρέπει να τα ξαναδημιουργήσει και να 'πείσει' τους υπόλοιπους υπολογιστές να συμφωνήσουν στην αλλαγή κάτι που είναι εξαιρετικά δύσκολο. Κατά συνέπεια, τα μπλοκ της αλυσίδας είναι πρακτικά αμετάβλητα.

Το Bitcoin ήταν η πρώτη εφαρμογή της τεχνολογίας Blockchain και εξακολουθεί να είναι η πιο γνωστή. Το Bitcoin είναι ένα ψηφιακό νόμισμα που λειτουργεί μέσω ενός αποκεντρωμένου δικτύου υπολογιστών που συντηρούν το Blockchain χωρίς την ανάγκη για έναν κεντρικό διαμεσολαβητή, όπως μια τράπεζα. Όλες οι συναλλαγές στο δίκτυο Bitcoin είναι δημόσια διαθέσιμες και καταγεγραμμένες στο Blockchain, εξασφαλίζοντας διαφάνεια και ακεραιότητα, όχι όμως ιδιωτικότητα.



Δραστηριότητα 2

Κρυπτογραφήστε τη φράση «ΑΥΤΟΚΙΝΗΤΟ» χρησιμοποιώντας κρυπτογράφηση του Καίσαρα με ολίσθηση δύο (2) θέσεων δεξιά.

6.5 Ερωτήσεις

Ε.1: Ερωτήσεις

1. Τί εννοούμε με τον όρο «κυβερνοασφάλεια»;
2. Τί εννοούμε με τον όρο «κρυπτογράφηση»;
3. Να αναζητήσετε πληροφορίες για την κρυπτογραφία Δημόσιου/Ιδιωτικού κλειδιού.