Ερευνητική Εργασία Α΄ Λυκείου

«Η κωδικοποίηση της πληροφορίας στην εποχή της τεχνολογίας»

3ο ΓΕΛ Θήβας

Τμήμα Α1

Υπεύθυνη Καθηγήτρια: Μαρία Βασιλείου

Σχολικό Έτος 2017-2018

Β΄ Τετράμηνο

Περιεχόμενα

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ

- Αναγνώστου Ποσειδών
- Αντωνάκη Όλγα
- Αντωνάκης Θεόδωρος
- Βασιλού Ζωή
- Βέλια Σκόντρα Εμαννουέλα
- Δελβενακιώτη Ιωάννα Λουκία
- Ζγούρη Βασίλειος
- Κατσίνα Μαργαρίτα
- Λαϊου Δήμητρα
- Λεχρής Άγγελος
- Μόκκα Χρυσάνθη

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΚΩΔΙΚΟΠΟΙΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ

Οι προσπάθειες για την διατήρηση της μυστικότητας άπτονται της απαρχής της γέννησης της ανθρωπότητας. Η κρυπτογραφία προέκυψε ως ιδεολογική προσέγγιση και έννοια σχεδόν με την επινόηση της γραφής. Η τέχνη για την διατήρηση της μυστικότητας οδήγησε στην κρυπτογραφία. Παρόλο που η κρυπτογραφία ξεκίνησε ως τέχνη (ίσως και ένα παιχνίδι) στη συνέχεια μετεξελίχθηκε σε επιστήμη δηλαδή σε σύγχρονη κρυπτογραφία με στόχο την ασφάλεια των υπολογιστικών, πληροφοριακών και επικοινωνιακών συστημάτων. (https://dspace.lib.uom.gr/bitstream/2159/229/6/Chapter5.pdf)

ΤΑ ΣΤΑΔΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

- **1ο ΣΤΑΔΙΟ** (1900 π.Χ-1900 μ.Χ) : Η έντυπη απεικόνιση σε μελάνι και χαρτί παραδείγματος χάρη ο κρυπτογραφικός αλγόριθμος του Καίσαρα.

- **2ο ΣΤΑΔΙΟ** (1900μ.Χ-1950 μ.Χ): Εισαγωγή μηχανών στην αποκρυπτογράφηση π.χ η γερμανική μηχανή Enigma.

- **3ο ΣΤΑΔΙΟ** (1950-σήμερα): Το σύγχρονο κρυπτογραφικό σύστημα που επέτρεψε την χρήση περιπλοκότερων αλγορίθμων κρυπτογράφησης

Η κρυπτογραφία όμως από τέχνη ίσως και ένα παιχνίδι μετεξελίχθηκε σε επιστήμη δηλαδή σύγχρονη κρυπτογράφηση με στόχο την ασφάλεια τον υπολογιστικών, πληροφοριακών και επικοινωνιακών συστημάτων. Ωστόσο με την μετεξέλιξη της κρυπτογραφίας ο στόχος παραμένει πανομοιότυπος: η ασφάλεια της επικοινωνίας μέσω ενός επικεφαλούς μέσου επικοινωνίας.

Πρώτη Περίοδος Κρυπτογραφίας: Ο Αλγόριθμος του Καίσαρα

Ο Κώδικας του Καίσαρα είναι μία από τις απλούστερες και πιο γνωστές τεχνικές κωδικοποίησης στην κρυπτογραφία. Είναι κώδικας αντικατάστασης στον οποίο κάθε γράμμα του κειμένου αντικαθίσταται από κάποιο άλλο γράμμα με σταθερή απόσταση κάθε φορά στο αλφάβητο. Για παράδειγμα, με μετατόπιση 3, το Α θα αντικαθιστούνταν από το Δ, το Β από το Ε, και ούτω καθεξής. Η μέθοδος πήρε το όνομά της από τον Ιούλιο Καίσαρα, ο οποίος την χρησιμοποιούσε στην προσωπική του αλληλογραφία.

Παράδειγμα:

Ο μετασχηματισμός μπορεί να αναπαρασταθεί με παράλληλη παράθεση δύο αλφαβήτων. Τα αλφάβητο κωδικοποίησης είναι το απλό αλφάβητο περιστρεμμένο δεξιά ή αριστερά κατά κάποιο αριθμό θέσεων. Για παράδειγμα ακολουθεί ένας κώδικας του Καίσαρα που χρησιμοποιεί αριστερή περιστροφή τριών θέσεων (η **παράμετρος μετατόπισης, εδώ 3**, χρησιμοποιείται ως **κλειδί**):

Απλό: ΑΒΓΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩ

Κώδικας: ΔΕΖΗΘΙΚΛΜΝΞΟΠΡΣΤΥΦΧΨΩΑΒΓ

Σπάζοντας τον κώδικα

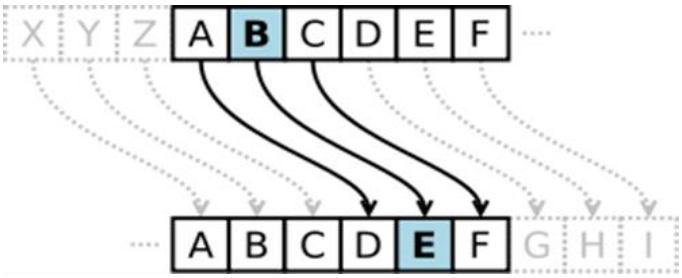
Ο κώδικας του Καίσαρα μπορεί εύκολα να σπάσει ακόμα και με σενάριο κρυπτοκειμένου μόνο (ciphertext-only scenario). Μπορούν να ληφθούν υπόψη δύο περιπτώσεις

ο επιτιθέμενος γνωρίζει (ή υποθέτει) ότι έχει χρησιμοποιηθεί κάποιου είδους κώδικας απλής αντικατάστασης, αλλά όχι ότι πρόκειται για τον κώδικα του Καίσαρα συγκεκριμένα.

ο επιτιθέμενος γνωρίζει ότι πρόκειται για κώδικα του Καίσαρα, αλλά δεν γνωρίζει την τιμή της μετατόπισης.

Στην πρώτη περίπτωση ο κώδικας μπορεί να σπάσει χρησιμοποιώντας τις ίδιες τεχνικές όπως και σε ένα γενικό απλό κώδικα αντικατάστασης, όπως η ανάλυση συχνότητας ή οι λέξεις μοτίβα. Ενώ θα λύνεται, είναι πιθανό ότι το άτομο θα διαπιστώσει σύντομα την κανονικότητα στη λύση και θα συμπεράνει ότι χρησιμοποιείται ο κώδικας του Καίσαρα.

Στη δεύτερη περίπτωση το σπάσιμο του κώδικα είναι ακόμα πιο εύκολο. Καθώς υπάρχει περιορισμένος μόνο αριθμός πιθανών μετακινήσεων (24 στα Ελληνικά), μπορούν να εξεταστούν με τη σειρά σε μία brute force attack. Ένας τρόπος να γίνει αυτό είναι να γραφτεί ένα τμήμα του κρυπτογραφημένου κειμένου σε ένα πίνακα για όλες τις πιθανές μετατοπίσεις - τεχνική που κάποιες φορές ονομάζεται «completing the plain component» (ολοκληρώνοντας το απλό συστατικό)



Δεύτερη Περίοδος Κρυπτογραφίας: ΜΗΧΑΝΗ ENIGMA

Η πρώτη μηχανή Enigma δημιουργήθηκε από τον γερμανό Ηλεκτρολόγο Μηχανικό Arthur Scherbius (20 Οκτωβρίου 1878 – 13 Μαίου 1929), με σκοπό την προστασία των εταιρικών μυστικών μεγάλων επιχειρήσεων της εποχής, κυρίως τραπεζών. Η μηχανή ονομάστηκε Enigma από την ελληνική λέξη «αίνιγμα».

Ο ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ENIGMA

Η βασική αρχή λειτουργίας της Enigma ήταν απλή: Πιέζοντας ένα πλήκτρο από το πληκτρολόγιο της μηχανής (το οποίο περιελάμβανε 26 γράμματα του λατινικού αλφαβήτου), το ηλεκτρικό σήμα που ξεκινούσε από αυτό το πλήκτρο, περνούσε μέσα από τους 3 ρότορες (και στην τροποποιημένη στρατιωτική έκδοση που χρησιμοποιήθηκε από την Ναζιστική Γερμανία πρώτα από το Plugboard = Πίνακας ηλεκτρικών υποδοχών), κατέληγε σε ένα λαμπτήρα, ο οποίος υποδείκνυε ένα «τυχαίο» γράμμα στον πίνακα λυχνιών, ακριβώς από πάνω από το πληκτρολόγιο, το οποίο θα αναμεταδίδοταν μέσω ασυρμάτου σε κώδικα Mors, ένα κρυπτογραφημένο μήνυμα (δηλαδή ο χειριστής της Enigma θα πληκτρολογούσε το μήνυμα που ήθελε να μεταδώσει στην Enigma, και θα σημείωνε κατά σειρά ποιο γράμμα άναβε στον πίνακα με τους λαμπτήρες, και αντίστροφα για να το αποδικοποιήσει). Αυτό βέβαια προϋποθέτει και οι δύο χειριστές να έχουν τις μηχανές τους ρυθμισμένες κατά τον ίδιο τρόπο (ίδια θέση ρότορα, και στην στρατιωτική έκδοση, ίδια συνδεσμολογία στον πίνακα ηλεκτρικών υποδοχών

Η αποκρυπτογράφηση της Enigma

Η αποκρυπτογράφηση της Enigma δεν βασίστηκε τόσο στις αδυναμίες τις μηχανής όσο στην ανθρώπινη αδυναμία. Ο Γερμανός απόστρατος Χανς-Θίλο Σμιντ ήταν ένας κατάσκοπος που, κατά τη διάρκεια της δεκαετίας του 1930, πούλησε μυστικά σχετικά με την Γερμανική Enigma μηχανή στη Γαλλία. Μετά από μια ανεπιτυχή καριέρα στις τάξεις του γερμανικού στρατού έκανε διάφορες εργασίες στο Βερολίνο όπου και διέμενε.

Ο δρόμος για την επίλυση του αινίγματος είχε ανοίξει με τον Σμιντ να βλέπει ότι ο μόνος τρόπος για να κερδίσει χρήματα, ήταν να πουλήσει ότι μπορούσε να έχει στα χέρια του, μιας και βασικά πνευματικά αγαθά, έλαμπαν δια της απουσίας τους από την ιδιοσυγκρασία του και ασφαλώς δεν μπορούσαν να του αποφέρουν χρήματα, τουλάχιστον άμεσα.

Τελικά, την 1η Απριλίου 1943 η Γκεστάπο εισέβαλε στο διαμέρισμα του, τον συνέλαβε και τον φυλάκισε. Έμεινε για λίγο καιρό απομονωμένος στην φυλακή μέχρι να επιτραπεί στην κόρη του Γκιζέλα, να τον επισκεφθεί.

Μετά τις πολλαπλές τροποποιήσεις μετά την τελευταία προδοσία του Smid, πίστευαν ότι το μυστικό της Enigma θα ήταν ασφαλές. Όμως ήταν ήδη πολύ αργά.

ALAN TURING

Ο «άνθρωπος-κλειδί ήταν ο Alan Turing. Ο Alan Matheson Turing ήταν βρετανός μαθηματικός, καθηγητής της λογικής, κρυπτογράφος, πρωτοπόρος στην επιστήμη της τεχνητής νοημοσύνης, θεωρείται ότι έθεσε τα θεμέλια για την εφεύρεση των ηλεκτρονικών υπολογιστών. Στο Bletchley Park, ήταν το κεντρικό πρόσωπο στην αποκρυπτογράφηση των Γερμανικών κωδικών, ως προϊστάμενος της ομάδας 8. Η ομάδα αυτήν ήταν που επιφορτίστηκε με την αποκωδικοποίηση της συσκευής Enigma. Η εργασία του Turing κρατήθηκε μυστική μέχρι τη δεκαετία του ’70, αφού ακόμα και οι στενοί φίλοι του δεν την ήξεραν. Στο Bletchley Park ο Turing εργάστηκε από το 1939 ως το 1940 όταν και μετακινήθηκε προς την Ομάδα 8. Ο Turing συνειδητοποίησε ότι δεν ήταν απαραίτητο να εξεταστούν όλοι οι πιθανοί συνδυασμοί για να σπάσουν τους κωδικούς της μηχανής Enigma. Απέδειξε ότι ήταν δυνατό να εξετάσει τις σωστές τοποθετήσεις των διακοπτών (περίπου ένα εκατομμύριο συνδυασμοί) χωρίς να πρέπει να εξεταστούν οι τοποθετήσεις του πίνακα συνδέσεων (περίπου 157 εκατομμύρια συνδυασμοί).Το 1954 πέθανε από δηλητηρίαση από ένα μισοφαγωμένο μήλο που άφησε το οποίο περιείχε κυάνιο.

Πατώντας αυτήν την πηγή, θα δείτε το βίντεο με θέμα την μηχανή Enigma:

Η ταινία μου.mp4

Τρίτη Περίοδος Κρυπτογραφίας:

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon τον ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας ο οποίος καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA.
Χρησιμοποιείται σήμερα σε πολλές εφαρμογές της καθημερινότητάς μας όπως :

Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM	Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
Κινητή τηλεφωνία (TETPA-ΤΕΤΡΑΠΟΛ-GSM)	Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
Σταθερή τηλεφωνία (cryptophones)	Ιδιωτικά δίκτυα
Word Wide Web	Εξυπνες κάρτες
Ηλεκτρονική ψηφοφορία	Συστήματα συναγερμών
Διπλωματικά δίκτυα (Τηλεγραφήματα)	Ηλεκτρονικό γραμματοκιβώτιο
Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)	Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)
Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)	Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)

ΚΩΔΙΚΟΠΟΙΗΣΗ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΣΤΟΝ ΥΠΟΛΟΓΙΣΤΗ

Ας εξηγήσουμε γιατί ο υπολογιστής είναι ψηφιακός. Ο υπολογιστής είναι μια μηχανή που δουλεύει με ηλεκτρικό ρεύμα. Τα ηλεκτρονικά του κυκλώματα, σε απλοποιημένη μορφή, αποτελούντα από καλώδια και «διακόπτες». Για λόγους ευκολίας στην κατασκευή του, ο υπολογιστής μπορεί να αναγνωρίσει μόνο δύο διαφορετικές καταστάσεις, για να εκτελέσει τους υπολογισμούς του, όπως παράδειγμα (Εικόνα 1.3):

- την κατάσταση στην οποία δεν περνάει ρεύμα μέσα από ένα καλώδιο και
- την κατάσταση στην οποία περνάει ρεύμα μέσα από ένα καλώδιο

Ένας υπολογιστής είναι ψηφιακός, επειδή μπορεί να χειριστεί συγκεκριμένο αριθμό καταστάσεων (μόνο δύο). Ανατρέχοντας στην ιστορία βλέπουμε ότι οι πρώτοι υπολογιστές (από τη δεκαετία του 1940) δημιουργήθηκαν, για να εκτελούν αριθμητικές πράξεις. Ωστόσο, οι κατασκευαστές της εποχής εκείνης ήρθαν αντιμέτωποι με ένα μεγάλο πρόβλημα. Τα αριθμητικά ψηφία (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) του δεκαδικού συστήματος δεν μπορούσαν να χρησιμοποιηθούν, αφού η κατασκευή ενός τέτοιου υπολογιστή ήταν εξαιρετικά πολύπλοκη, θα έπρεπε επομένως με κάποιο τρόπο να αναπαρασταθούν τα 10 αυτά ψηφία με συνδυασμούς δύο καταστάσεων, που είναι πιο εύκολο να αναγνωρίζει ο υπολογιστής. Η λύση ήρθε με τη χρησιμοποίηση ενός άλλου συστήματος αρίθμησης: του δυαδικού.
Σύμφωνα με το δυαδικό σύστημα αρίθμησης τα μοναδικά σύμβολα που απαιτούνται για τη γραφή όλων των αριθμών είναι μόνο δύο: το 0 και το 1

Όταν εισάγονται ή αποθηκεύονται χαρακτήρες στον υπολογιστή, χρησιμοποιούνται ειδικοί κώδικες για την παράστασή τους. Η κωδικοποίηση γίνεται με τη χρήση συνδυασμών του 0 και του 1, οπότε κάθε χαρακτήρας αντιστοιχίζεται με μια μοναδική διαφορετική ακολουθία δυαδικών ψηφίων. Παράλληλα η ακολουθία αυτή στο δυαδικό σύστημα παριστάνει μια αριθμητική τιμή. Η τιμή αυτή, που μπορεί να εκφραστεί εκτός από το δυαδικό και στο οκταδικό, στο δεκαδικό ή στο δεκαεξαδικό σύστημα αρίθμησης, λέγεται **τιμή του κωδικού** (code value).
Οι κυριότεροι κώδικες χαρακτήρων που χρησιμοποιούνται είναι:

ASCII	**των 8 bit**
Unicode	**των 16 bit**

ASCII (αμερικανικό πρότυπο κώδικα ανταλλαγής πληροφοριών)

Ο **ASCII** (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange) δημιουργήθηκε χάρη στην υποστήριξη του Εθνικού Αμερικανικού Ινστιτούτου Προτύπων ANSI (**A**merican **N**ational **S**tandard Institute), σε μια προσπάθεια να υπάρξει ένας κοινός κώδικας για την ανταλλαγή των δεδομένων μεταξύ υπολογιστών καθώς και για την αποθήκευσή τους Ο **ASCII** είναι ένα κωδικοποιημένο

σύνολο χαρακτήρων του λατινικού αλφάβητου όπως αυτό χρησιμοποιείται σήμερα στην Αγγλική γλώσσα και σε άλλες δυτικοευρωπαϊκές γλώσσες. Χρησιμοποιείται για αναπαράσταση κειμένου στους υπολογιστές. σε συσκευές τηλεπικοινωνίας, καθώς και σε άλλες συσκευές που δουλεύουν με κείμενο. Οι περισσότερες σύγχρονες κωδικοποιήσεις χαρακτήρων βασίζονται στον ASCII, αν και υποστηρίζουν πολύ περισσότερους χαρακτήρες.

Ο ASCII (αμερικανικός πρότυπος κώδικας για την ανταλλαγή πληροφοριών) είναι η πιο κοινή μορφή για αρχεία κειμένου σε υπολογιστές και στο Internet. Σε ένα αρχείο ASCII, κάθε αλφαβητικός, αριθμητικός ή ειδικός χαρακτήρας αναπαριστάται με έναν **δυαδικό αριθμό 7 δυαδικών ψηφίων** Προσδιορίζονται 128 πιθανοί χαρακτήρες Πρόκειται για έναν κωδικό που αντιπροσωπεύει 128 αγγλικούς χαρακτήρες ως αριθμούς, με κάθε γράμμα να αντιστοιχίζεται ένας αριθμός από 0 έως 127. Για παράδειγμα, ο ASCII κώδικας για κεφαλαία Μ είναι 77. Οι περισσότεροι υπολογιστές χρησιμοποιούν κώδικες ASCII για να αντιπροσωπεύουν κείμενο , το οποίο καθιστά δυνατή τη μεταφορά δεδομένα από έναν υπολογιστή στον άλλο.

Το τυπικό σύνολο χαρακτήρων ASCII χρησιμοποιεί μόνο 7 bits για κάθε χαρακτήρα. Υπάρχουν πολλά μεγαλύτερα σύνολα χαρακτήρων που χρησιμοποιούν 8 bits, τα οποία τους προσφέρουν 128 επιπλέον χαρακτήρες(8 bits ή 1 byte για να κωδικοποιηθεί, γι' αυτό το byte ονομάζεται και χαρακτήρας). Το bit αυτό ονομάστηκε ψηφίο ισοτιμίας (parity bit). Με την κωδικοποίηση αυτή δίνεται η δυνατότητα να παραστήσουμε 128 ($=2^7$) διαφορετικούς χαρακτήρες, ως αποτέλεσμα των 128 διαφορετικών συνδυασμών από 0 και 1. Με την πάροδο του χρόνου και εξαιτίας της διεύρυνσης της χρήσης των υπολογιστών που δημιούργησε την ανάγκη για περισσότερα σύμβολα, χρησιμοποιήθηκε και το 8ο bit για την παράσταση χαρακτήρων, οπότε έγινε δυνατό να παρασταθούν 256 ($=2^8$) διαφορετικοί χαρακτήρες. Οι διάφοροι κατασκευαστές χρησιμοποίησαν τη νέα περιοχή (128-255) για την κωδικοποίηση ειδικών συμβόλων και γραφικών χαρακτήρων ή για την παράσταση γραμμάτων άλλων αλφαβήτων, διαφορετικών του λατινικού, π.χ. ελληνικού, σλαβικού, κ.ά. Οι επιπλέον χαρακτήρες χρησιμοποιούνται για την αναπαραγωγή μη αγγλικών χαρακτήρων, συμβόλων γραφικών και μαθηματικών συμβόλων. Ο νέος κώδικας που προέκυψε ονομάστηκε **επεκτεταμένος κώδικας ASCII (Extended ASCII) ή ASCII - 8.**

0 - 31
χαρακτήρες ελέγχου (μη εκτυπώσιμοι)
32 - 63
αριθμοί, κενό, σημεία στίξης, σύμβολα πράξεων
64 - 95
κεφαλαία λατινικά γράμματα και ειδικά σύμβολα
96 - 127
πεζά λατινικά γράμματα και ειδικά σύμβολα

ΧΑΡΑΚΤΗΡΑΣ	ΣΥΜΒΟΛΙΣΜΟΣ	ΧΑΡΑΚΤΗΡΑΣ	ΣΥΜΒΟΛΙΣΜΟΣ
0	00000000	A	01000001
1	00000001	B	01000010
2	00000010	C	01000011
3	00000011	D	01000100
4	00000100	E	01000101
5	00000101	F	01000110

Στο παρακάτω πίνακα παραθέτουμε τρία τυχαία παραδείγματα αριθμών των 1,3,5 όπου κάθε

αριθμός αναλύεται στον συμβολισμό του. Οι οκτώ χαρακτήρες κάθε συμβολισμού υψώνονται στον αντίστοιχο εκθέτη.

Εκθέτης:	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
1→	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**
3→	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**
5→	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**

- Κάθε χαρακτήρας του συμβολισμού πολλαπλασιάζεται με τον αριθμό 2 στον αντίστοιχο εκθέτη

π.χ $1=0*2^7+0*2^6+0x2^5+0*2^4+0*2^3+0*2^2+0*2^1+1*2^0$
$3=0*2^7+0*2^6+0*2^5+0*2^4+0*2^3+0*2^2+1*2^1+1*2^0$
$5=0*2^7+0*2^6+0*2^5+0*2^4+0*2^3+1*2^2+0*2^1+0*2^0$

UNICODE

Το συμβολικό όνομα Unicode (**Uni**code) χρησιμοποιήθηκε για να εκφράσει τις τρείς βασικές ιδιότητές του:
α) Παγκόσμιος - οικουμενικός (**Uni**versal). Σχεδιάστηκε για να καλύψει όλες τις γλώσσες του κόσμου.
β) Μοναδικός (**Uni**que). Κάθε χαρακτήρας έχει ακριβώς μία τιμή.
γ) Ομοιόμορφος - ενιαίος (**Uni**form). Κάθε χαρακτήρας έχει σταθερό μήκος (16 bit).

Το **Unicode** είναι μια κωδικοποίηση γραμματοσειράς που αντιστοιχεί τους χαρακτήρες ως ακέραιους αριθμούς κώδικα μηχανής. Αυτό το πρότυπο είναι παρόμοιο με το ASCII αλλά διαφέρει σε κάποια σημεία και ως προς τον αριθμό των χαρακτήρων που μπορεί να αναπαραστήσει.Το Unicode χρησιμοποιεί **δύο bytes** (16 bits) για να αναπαραστήσει τον κάθε χαρακτήρα αντί του ενός byte (8 bits) που χρησιμοποιεί το ASCII. Με αυτόν τον τρόπο το Unicode μπορεί να αντιπροσωπεύσει **περισσότερους από 65.000 χαρακτήρες** σε αντίθεση με τους 256 που μπορεί να χειριστεί το ASCII, καθιστώντας το ικανό να περιλαμβάνει σχεδόν όλα τα συστήματα γραφής που είναι σε χρήση σήμερα. Εκτός από χαρακτήρες όλων των γλωσσών του κόσμου το Unicode περιλαμβάνει και άλλα ιστορικά και εξαφανισμένα αλφάβητα όπως τα Αιγυπτιακά κυρίως για ακαδημαϊκούς σκοπούς αλλά και σύμβολα για την μουσική και τα μαθηματικά. Τα τελευταία χρόνια επίσης περιλαμβάνει και εικονίδια όπως τα emoji.

Ο κώδικας **Unicode** είναι ένας διεθνής κώδικας που χρησιμοποιείται για την παράσταση των χαρακτήρων στους υπολογιστές. Επειδή ο αριθμός των χαρακτήρων που μπορούμε να παραστήσουμε με τον κώδικα ASCII και τους άλλους κώδικες των 8 bit είναι περιορισμένος ήταν επιτακτική η ανάγκη να δημιουργηθεί ένας κώδικας ο οποίος να δίνει τη δυνατότητα για την παράσταση των γραμμάτων όλων των γλωσσών. Έτσι σχεδιάστηκε ο κώδικας Unicode, στον οποίο χρησιμοποιούνται 16 bit για την παράσταση των χαρακτήρων, οπότε μπορούν να παρασταθούν 65.536 ($=2^{16}$) διαφορετικοί χαρακτήρες. (βλέπε εικόνα 2)
Με τον κώδικα αυτό είναι δυνατόν να παρασταθούν οι χαρακτήρες που χρησιμοποιούνται σε όλα τα αλφάβητα του κόσμου -Λατινικό, Ελληνικό, Εβραϊκό, Κυριλλικό, Αραβικό, κ.ά.-, ακόμη και τα ιδεογράμματα που χρησιμοποιούνται στην Κορεατική, την Κινεζική και την Ιαπωνική γλώσσα. Το

πρότυπο Unicode περιλαμβάνει ακόμα διάφορα διακριτικά, μαθηματικά και τεχνικά σύμβολα, βέλη, σημεία στίξης, κ.ά. Δίνει επίσης τη δυνατότητα να παρασταθούν τονούμενα γράμματα. Με το Unicode ένα και μόνο προϊόν ή μία και μόνη τοποθεσία Διαδικτύου μπορεί να επικοινωνεί με διάφορα λειτουργικά συστήματα, σε διάφορες γλώσσες και χώρες, χωρίς την ανάγκη επαναπρογραμματισμού. Γίνεται έτσι δυνατή η μεταφορά δεδομένων ανάμεσα σε πλήθος διαφορετικών συστημάτων δίχως κίνδυνο αλλοίωσης.

ΔΕΚΑΕΞΑΔΙΚΟΣ ΠΙΝΑΚΑΣ UNICODE

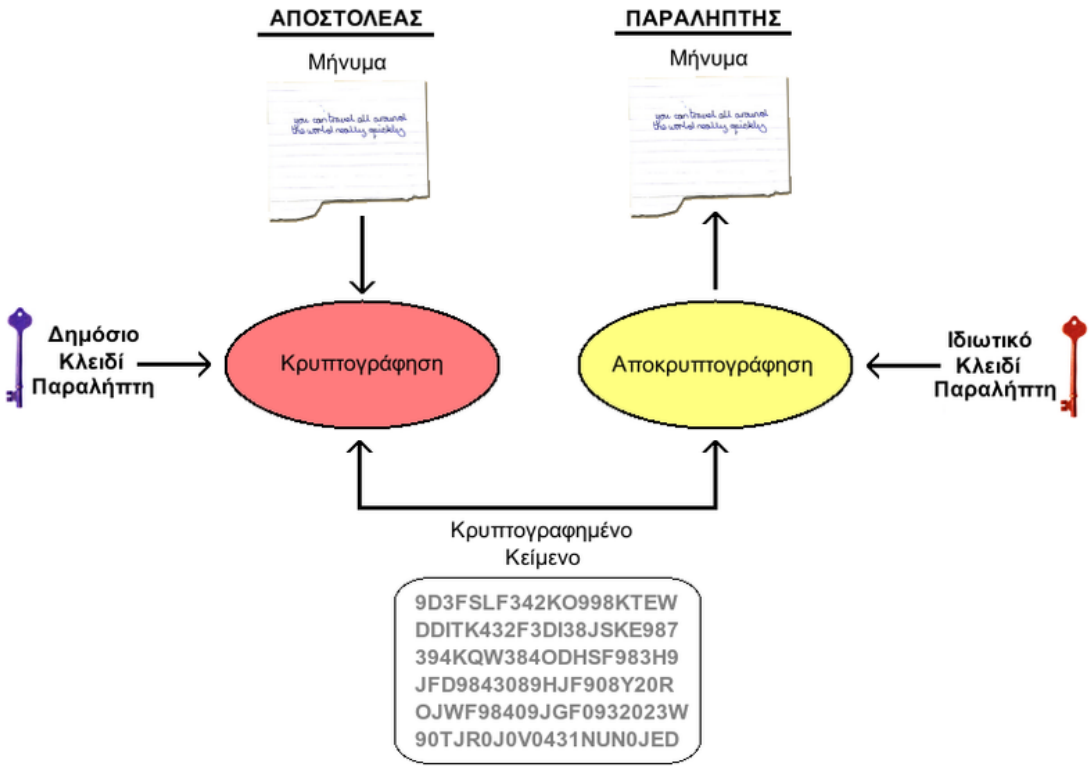
0020	0 0030	@ 0040	P 0050	` 0060	p 0070	00A0	° 00B0	À 00C0	Ð 00D0	à 00E0	ð 00F0
! 0021	1 0031	A 0041	Q 0051	a 0061	q 0071	¡ 00A1	± 00B1	Á 00C1	Ñ 00D1	á 00E1	ñ 00F1
" 0022	2 0032	B 0042	R 0052	b 0062	r 0072	¢ 00A2	² 00B2	Â 00C2	Ò 00D2	â 00E2	ò 00F2
# 0023	3 0033	C 0043	S 0053	c 0063	s 0073	£ 00A3	³ 00B3	Ã 00C3	Ó 00D3	ã 00E3	ó 00F3
$ 0024	4 0034	D 0044	T 0054	d 0064	t 0074	¤ 00A4	´ 00B4	Ä 00C4	Ô 00D4	ä 00E4	ô 00F4
% 0025	5 0035	E 0045	U 0055	e 0065	u 0075	¥ 00A5	µ 00B5	Å 00C5	Õ 00D5	å 00E5	õ 00F5
& 0026	6 0036	F 0046	V 0056	f 0066	v 0076	¦ 00A6	¶ 00B6	Æ 00C6	Ö 00D6	æ 00E6	ö 00F6
' 0027	7 0037	G 0047	W 0057	g 0067	w 0077	§ 00A7	· 00B7	Ç 00C7	× 00D7	ç 00E7	÷ 00F7
(0028	8 0038	H 0048	X 0058	h 0068	x 0078	¨ 00A8	¸ 00B8	È 00C8	Ø 00D8	è 00E8	ø 00F8
) 0029	9 0039	I 0049	Y 0059	i 0069	y 0079	© 00A9	¹ 00B9	É 00C9	Ù 00D9	é 00E9	ù 00F9
* 002A	: 003A	J 004A	Z 005A	j 006A	z 007A	ª 00AA	º 00BA	Ê 00CA	Ú 00DA	ê 00EA	ú 00FA
+ 002B	; 003B	K 004B	[005B	k 006B	{ 007B	« 00AB	» 00BB	Ë 00CB	Û 00DB	ë 00EB	û 00FB
, 002C	< 003C	L 004C	\ 005C	l 006C	| 007C	¬ 00AC	¼ 00BC	Ì 00CC	Ü 00DC	ì 00EC	ü 00FC
- 002D	= 003D	M 004D	] 005D	m 006D	} 007D	- 00AD	½ 00BD	Í 00CD	Ý 00DD	í 00ED	ý 00FD
. 002E	> 003E	N 004E	^ 005E	n 006E	~ 007E	® 00AE	¾ 00BE	Î 00CE	Þ 00DE	î 00EE	þ 00FE
/ 002F	? 003F	O 004F	_ 005F	o 006F	007F	¯ 00AF	¿ 00BF	Ï 00CF	ß 00DF	ï 00EF	ÿ 00FF

Εικόνα 2

SSL (Secure Sockets Layer)

Το **πρωτόκολλο SSL (Secure Sockets Layer)** αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης.

.



ΕΛΟΤ

Για το Ελληνικό αλφάβητο έχει υιοθετηθεί από τον Ελληνικό Οργανισμό Τυποποίησης (ΕΛΟΤ) ο κώδικας **ΕΛΟΤ 928** ο οποίος αποτελεί επέκταση του ASCII στα 8 bit. Στον κώδικα αυτό οι πρώτοι 128 χαρακτήρες είναι σχεδόν όμοιοι με τους αντίστοιχους του ASCII, ενώ στους επόμενους 128 έχουν τοποθετηθεί τα γράμματα του Ελληνικού αλφαβήτου (κεφαλαία, πεζά, τονούμενα) και άλλα σύμβολα.

ΚΩΔΙΚΟΠΟΙΗΣΗ ΣΤΗ ΜΕΤΑΔΟΣΗ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Πρόλογος

Η κωδικοποίηση δεδομένων στο διαδίκτυο επιτελείται με διάφορους τρόπους και διαφοροποιείται ανάλογα με τη χρήση της. Ενδεικτικά μερικοί τρόποι είναι :

- το **HTTPS**
- το **FTP**
- το **SSL**
- η **ψηφιακή υπογραφή**

Κρυπτογράφηση Δεδομένων

Σε έναν κόσμο χωρίς κρυπτογράφηση δεδομένων, θα ήταν αδύνατον να έχουμε ένα προσωπικό email, έναν προσωπικό λογαριασμό στο facebook, ή να χρησιμοποιήσουμε μια πιστωτική κάρτα για αγορές στο Internet. Η κρυπτογράφηση δεδομένων χρησιμοποιείται παντού, και είναι η "κλειδαριά" που κρατάει την ψηφιακή μας ζωή ασφαλή.

Τι είναι η κρυπτογράφηση

Κρυπτογράφηση (**encryption**) είναι ο μετασχηματισμός των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί από κανένα παρά μόνο από αυτόν που διαθέτει ένα κατάλληλο κλειδί. Υπάρχουν δύο μεγάλες οικογένειες αλγόριθμων κρυπτογράφησης:

- οι **συμμετρικοί αλγόριθμοι (ή αλγόριθμοι ιδιωτικού κλειδιού) και**
- **οι ασύμμετροι (ή αλγόριθμοι δημόσιου κλειδιού).**

Κατά την ανταλλαγή δεδομένων, οι πληροφορίες κρυπτογραφούνται, ώστε να μη μπορεί μία τρίτη πηγή χωρίς την απαιτούμενη εξουσιοδότηση, να τα υποκλέψει ή να τα διαβάσει.
Η τεράστια ανάπτυξη των δικτύων υπολογιστών και η επικοινωνία πληροφοριών κάθε μορφής έφερε ένα τεράστιο πρόβλημα στην επιφάνεια, την ανάγκη για προστασία αυτής της πληροφορίας.
Οι **πέντε βασικές υπηρεσίες ασφαλείας** που μπορούν να υποστηριχθούν σε ανοικτά συστήματα είναι:

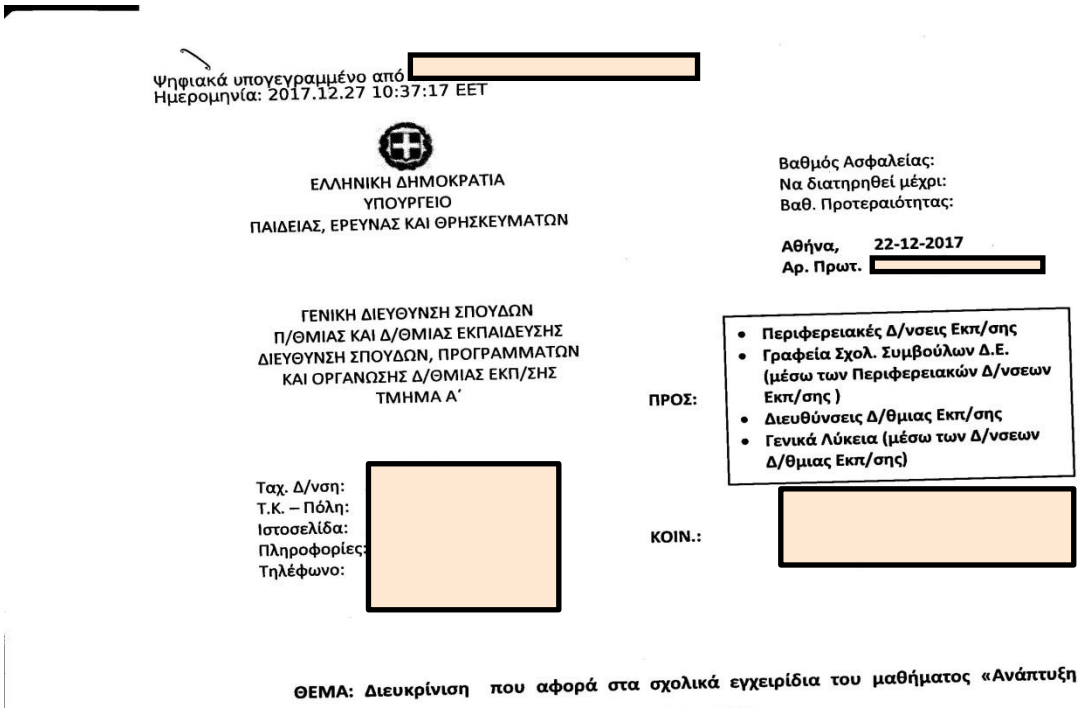
1. η γνησιότητα χρηστών και πληροφοριών (authentication)
2. ο έλεγχος πρόσβασης (access control)
3. η εμπιστευτικότητα (confidentiality)
4. η ακεραιότητα των δεδομένων (data integrity)
5. η μη δυνατότητα αποκήρυξης γεγονότων που έχουν συμβεί (non-repudiation)

Αυτές οι υπηρεσίες παρέχονται από διάφορους μηχανισμούς. Οι υπηρεσίες (1), (3), (4) και (5) μπορούν να υποστηριχθούν από κρυπτογραφικές μεθόδους ενώ η υπηρεσία (2) προϋποθέτει προσθετικά και την χρήση φυσικών μεθόδων.

Ψηφιακή Υπογραφή

Η Ψηφιακή υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το

υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά.
Σε μερικές χώρες όπως οι ΗΠΑ και κάποιες χώρες της Ευρωπαϊκής ένωσης, οι ψηφιακές υπογραφές έχουν και νομική υπόσταση. Οι ψηφιακές υπογραφές σε ψηφιακά έγγραφα είναι παρόμοιες με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Όταν οι ψηφιακές υπογραφές υλοποιούνται - εφαρμόζονται σωστά (με χρήση ασφαλών κρυπτογραφικών αλγορίθμων), είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες χειρόγραφες. Επίσης το φυσικό πρόσωπο που ψηφιακά υπογράφει το ψηφιακό έγγραφο δεν μπορεί να ισχυριστεί ότι δεν το υπόγραψε (όσο το ιδιωτικό κλειδί που χρησιμοποίησε δεν υποκλάπηκε). Κάποιες υλοποιήσεις των ψηφιακών υπογραφών προσθέτουν και την ημερομηνία υπογραφής του εγγράφου, ώστε και το ιδιωτικό κλειδί να υποκλαπεί, η ψηφιακή υπογραφή να είναι έγκυρη. Η ψηφιακή υπογραφή μπορεί να προστεθεί σε οποιαδήποτε σειρά από bits (δηλαδή δεδομένα): παραδείγματα χρήσης είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, μηνύματα που στέλνονται στο Διαδίκτυο κλπ. Πολλοί οργανισμοί υιοθετούν την χρήση των ψηφιακών υπογραφών ώστε να αποφεύγεται η αποστολή τυπωμένων εγγράφων (επικυρωμένα με χρήση σφραγίδων και υπογραφών).


Ψηφιακά υπογεγραμμένο από [redacted]
Ημερομηνία: 2017.12.27 10:37:17 EET

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ

Βαθμός Ασφαλείας:
Να διατηρηθεί μέχρι:
Βαθ. Προτεραιότητας:

Αθήνα, 22-12-2017
Αρ. Πρωτ. [redacted]

ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΣΠΟΥΔΩΝ
Π/ΘΜΙΑΣ ΚΑΙ Δ/ΘΜΙΑΣ ΕΚΠΑΙΔΕΥΣΗΣ
ΔΙΕΥΘΥΝΣΗ ΣΠΟΥΔΩΝ, ΠΡΟΓΡΑΜΜΑΤΩΝ
ΚΑΙ ΟΡΓΑΝΩΣΗΣ Δ/ΘΜΙΑΣ ΕΚΠ/ΣΗΣ
ΤΜΗΜΑ Α΄

ΠΡΟΣ:
- Περιφερειακές Δ/νσεις Εκπ/σης
- Γραφεία Σχολ. Συμβούλων Δ.Ε. (μέσω των Περιφερειακών Δ/νσεων Εκπ/σης)
- Διευθύνσεις Δ/θμιας Εκπ/σης
- Γενικά Λύκεια (μέσω των Δ/νσεων Δ/θμιας Εκπ/σης)

Ταχ. Δ/νση:
Τ.Κ. – Πόλη:
Ιστοσελίδα:
Πληροφορίες:
Τηλέφωνο:

ΚΟΙΝ.:

ΘΕΜΑ: Διευκρίνιση που αφορά στα σχολικά εγχειρίδια του μαθήματος «Ανάπτυξη

Εικόνα 1 ψηφιακή υπογραφή

Δημόσιο κλειδί - Ιδιωτικό κλειδί

Αν και τα Δημόσια κλειδιά και τα Ιδιωτικά κλειδιά αναφέρονται και τα δύο ως κλειδιά, βοηθά να τα σκεφτείτε ως λίγο διαφορετικά. **Προσπαθήστε να σκεφτείτε ένα Δημόσιο κλειδί ότι είναι σαν ένα λουκέτο και ότι ένα Ιδιωτικό κλειδί ότι είναι σαν ένα κλειδί που ξεκλειδώνει το λουκέτο.**

Συμμετρικοί αλγόριθμοι ή ιδιωτικό κλειδί

Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί

που χρησιμοποιείται για την αποκρυπτογράφηση και το ανάποδο. Μάλιστα στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγόριθμων βασίζεται στην μυστικότητα αυτού του κλειδιού. Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό. Παραδείγματα συμμετρικών αλγορίθμων είναι οι DES, IDEA, RC5 και SAFER.
Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. απωλέσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

Παράδειγμα χρήσης ιδιωτικού κλειδιού

Στην κρυπτογράφηση δεδομένων με symmetric key, ουσιαστικά η Alice κλειδώνει το μήνυμα σε ένα κουτί, με ένα λουκέτο (αλγόριθμος κρυπτογράφησης) για το οποίο έχει μόνο εκείνη το κλειδί (κλειδί κρυπτογράφησης). Ύστερα, στέλνει το κλειδωμένο κουτί με το ταχυδρομείο στον Bob. Και, αναγκαστικά, του στέλνει σε ένα ξεχωριστό φάκελο, μέσω ταχυδρομείου, ένα αντίγραφο του μοναδικού κλειδιού.

Ασύμμετροι αλγόριθμοι ή δημόσιο κλειδί

Οι ασύμμετροι αλγόριθμοι ή αλγόριθμοι δημόσιου κλειδιού είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση. Πέρα από αυτό, το κλειδί αποκρυπτογράφησης δεν μπορεί να υπολογιστεί από το κλειδί κρυπτογράφησης. Οι αλγόριθμοι αυτοί καλούνται και "δημόσιου κλειδιού" γιατί το κλειδί κρυπτογράφησης μπορεί να δημοσιοποιηθεί. Ο καθένας μπορεί να κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί αλλά μόνο αυτός που διαθέτει το αντίστοιχο ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει.
Παραδείγματα ασύμμετρων αλγορίθμων είναι οι RSA, ElGamal και DSA.

Παράδειγμα χρήσης δημόσιου κλειδιού

Έστω λοιπόν πως η Alice θέλει να στείλει ένα μυστικό μήνυμα στον Bob μέσω του δημόσιου ταχυδρομείου, και περιμένει μια επίσης μυστική απάντηση από τον Bob.
Στην κρυπτογράφηση δεδομένων με Public/Asymmetric key, η Alice και ο Bob έχουν ξεχωριστά λουκέτα και ξεχωριστά κλειδιά. Ο Bob στέλνει το λουκέτο του ανοιχτό (Public key) με το ταχυδρομείο στην Alice, αλλά κρατάει εκείνος το κλειδί (Private key).Η Alice χρησιμοποιεί αυτό το λουκέτο για να κλειδώσει το κουτί με το μήνυμα, και στέλνει το κλειδωμένο κουτί στον Bob, που το ανοίγει με το κλειδί του. Αντίστοιχα, αν θέλει ο Bob να στείλει μήνυμα, θα πρέπει να του στείλει η Alice το δικό της λουκέτο πρώτα. Αυτή η μέθοδος έχει το τεράστιο πλεονέκτημα πως δεν χρειάζεται να ανταλλάξουν κλειδιά ο Bob και η Alice, ώστε να μην υπάρχει η πιθανότητα να γίνει υποκλοπή κατά την ανταλλαγή. Όμως, στην κρυπτογράφηση symmetric key, χρειάζεται μία μόνο φορά να σταλεί το κλειδί κρυπτογράφησης.

HTTPS

Το **HTTPS** (Hypertext Transfer Protocol Secure) χρησιμοποιείται στην πληροφορική για να δηλώσει μία ασφαλή δικτυακή σύνδεση http. Ένας σύνδεσμος (URL) που αρχίζει με το πρόθεμα https υποδηλώνει ότι θα χρησιμοποιηθεί κανονικά το πρωτόκολλο HTTP, αλλά η σύνδεση θα γίνει σε διαφορετική πόρτα και τα δεδομένα θα ανταλλάσσονται κρυπτογραφημένα. Το σύστημα αυτό σχεδιάστηκε αρχικά από την εταιρία Netscape Communications Corporation για να χρησιμοποιηθεί σε ιστοσελίδες όπου απαιτείται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Σήμερα χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες (πχ αριθμοί πιστωτικών καρτών, passwords κοκ).

Τρόπος λειτουργίας

Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο όπως μερικοί νομίζουν, αλλά αναφέρεται στον συνδυασμό του απλού HTTP πρωτοκόλλου και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο Secure Sockets Layer (SSL). Η κρυπτογράφηση που χρησιμοποιείται διασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα μπορούν να υποκλαπούν από άλλους κακόβουλους χρήστες. Για να χρησιμοποιηθεί το HTTPS σε έναν server, θα πρέπει ο διαχειριστής του να εκδώσει ένα **πιστοποιητικό δημοσίου κλειδιού**. Πολλοί χρήστες πιστωτικών καρτών θεωρούν ότι το HTTPS προστατεύει ολοκληρωτικά τον αριθμό της πιστωτικής τους κάρτας από κατάχρηση. Αυτό όμως δεν ισχύει: Το HTTPS χρησιμοποιεί την κρυπτογράφηση για να μεταδώσει τον αριθμό από τον υπολογιστή του πελάτη προς τον server. Η μετάδοση είναι ασφαλής και τα δεδομένα φτάνουν στον server χωρίς κανείς να μπορέσει να τα υποκλέψει. Παρόλα αυτά υπάρχει το ενδεχόμενο διάφοροι χάκερ να έχουν επιτεθεί στον server και από εκεί να έχουν υποκλέψει τα ευαίσθητα προσωπικά δεδομένα.
Τον Μάρτιο του 2017, το 21,13% του συνόλου των καταχωρισμένων Ελληνικών τομέων χρησιμοποιούσε το HTTPS.

File Transfer Protocol (FTP)

Το **File Transfer Protocol (FTP)**, (ελληνικά: **Πρωτόκολλο Μεταφοράς Αρχείων**) είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP (δίκτυα όπως internet ή intranet). Ο υπολογιστής που τρέχει εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server, μετονομασία ή διαγραφή αρχείων από τον server κ.ο.κ. Το πρωτόκολλο είναι ένα ανοιχτό πρότυπο. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου, ακόμη και εάν ο δεύτερος διαθέτει διαφορετικό λειτουργικό σύστημα.

Το FTP αφορά στη μεταφορά αρχείων μέσω διαδικτύου. Πρόκειται για μια από τις παλαιότερες υπηρεσίες του Διαδικτύου που χρησιμοποιείται ακόμη και σήμερα, πολύ συχνά χωρίς να το αντιλαμβάνεται ο τελικός χρήστης. Υπάρχουν προγράμματα που αξιοποιούν πλήρως τις δυνατότητες του FTP, όπως το Filezilla, το οποίο είναι λογισμικό δωρεάν και ανοιχτού κώδικα, με γραφικό περιβάλλον. Επίσης, όλα τα σύγχρονα προγράμματα πλοήγησης υποστηρίζουν το FTP για μεταφορά αρχείων. Για την πρόσβαση σε έναν άλλο υπολογιστή με FTP απαιτούνται κωδικοί πρόσβασης. Μόνο στην περίπτωση ελεύθερης πρόσβασης , που ονομάζεται «ανώνυμο ftp» (anonymous ftp) ο υπολογιστής επιτρέπει τη σύνδεση σε οποιονδήποτε χρήστη.

Τρόπος λειτουργίας

Αρχικά ο FTP server ανοίγει την θύρα (port) περιμένοντας έναν FTP client να συνδεθεί. Στη συνέχεια ο client ξεκινά μια νέα σύνδεση από μια τυχαία θύρα προς την θύρα του server. Μόλις γίνει η σύνδεση παραμένει ανοιχτή για όλη τη διάρκεια της συνόδου FTP. Η συγκεκριμένη σύνδεση ονομάζεται σύνδεση ελέγχου (control connection).
Ακολουθεί η δημιουργία (data connection), της σύνδεσης με την οποία μεταφέρονται τα δεδομένα. Υπάρχουν δύο τρόποι για να δημιουργηθεί, με χρήση της ενεργητικής λειτουργίας (active mode) ή με χρήση της παθητικής λειτουργίας (passive mode).

Χρήση

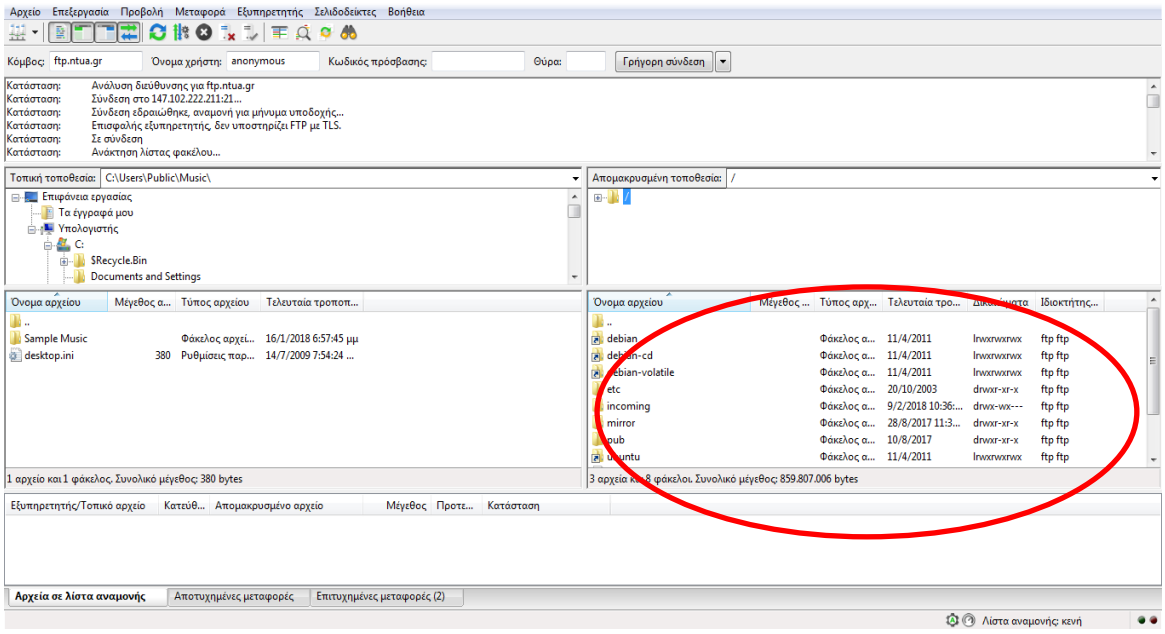
Το FTP είναι ένα πρωτόκολλο πελάτη-εξυπηρετητή 8-bit, ικανό να χειρίζεται οποιονδήποτε τύπο αρχείου χωρίς περαιτέρω επεξεργασία. Ωστόσο το FTP έχει εξαιρετικά υψηλή καθυστέρηση (latency). Αυτό σημαίνει ότι ο χρόνος μεταξύ του αιτήματος και της διαδικασίας παραλαβής του είναι αρκετά μεγάλος και για αυτό μερικές φορές απαιτείται μεγάλη διαδικασία σύνδεσης.

Προγράμματα FTP

Παρακάτω είναι ένας κατάλογος από FTP προγράμματα που μπορείτε να χρησιμοποιήσετε για να συνδεθείτε σε ένα FTP Server.

FileZilla – Ένα ελεύθερο FTP και SFTP, με ότι χρειάζονται οι περισσότεροι χρήστες.

Κατεβάσαμε από το διαδίκτυο το πρόγραμμα FileZilla. Μπήκαμε στα αρχεία ενός άλλου υπολογιστή και πήραμε κάποιες πληροφορίες από αυτόν. Στην δεξιά πλευρά βρίσκονται τα αρχεία του άλλου υπολογιστή που πήραμε τις πληροφορίες (κυκλωμένα). Ενώ, στην αριστερή πλευρά είναι τα αρχεία του δικού μας υπολογιστή.



Εικόνα 2 πρόγραμμα FileZilla

WinSCP - Ένα άλλο ελεύθερο FTP, SFTP, SCP βοήθημα το οποίο υποστηρίζει και scripting.

SmartFTP – Ένα πρόγραμμα FTP με ότι χρειάζονται οι περισσότεροι χρήστες.
CuteFTP – Ένα άλλο δημοφιλές και ευρέως χρησιμοποιούμενο πρόγραμμα FTP.
Internet Explorer – Οι χρήστες που έχουν Microsoft Internet Explorer στους υπολογιστές τους, μπορούν να τον χρησιμοποιήσουν για να συνδεθούν σε FTP εξυπηρετητές.

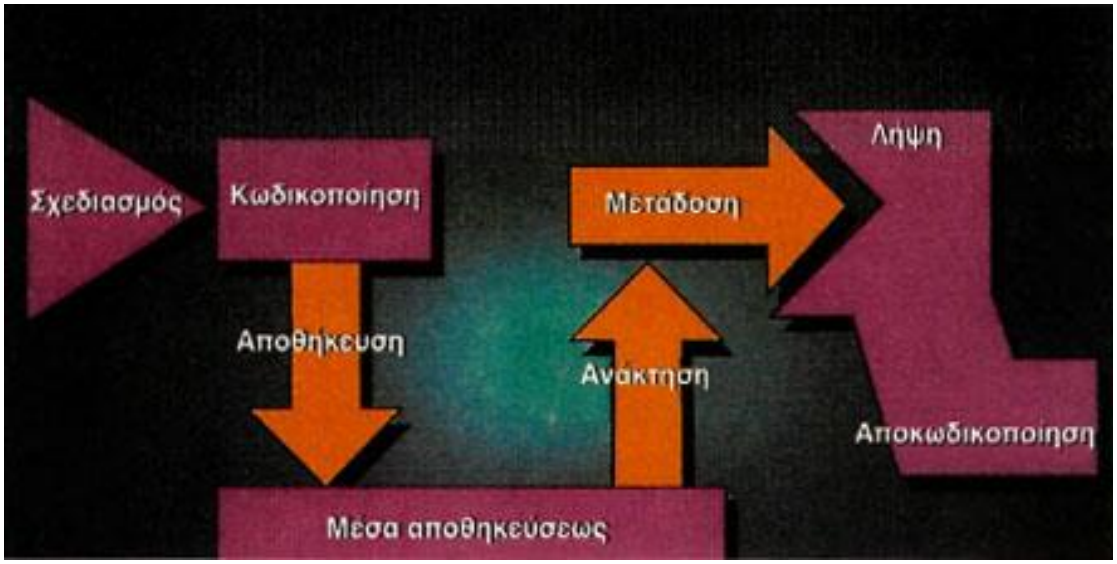
Πρωτόκολλο SSL

Το **πρωτόκολλο SSL** (**Secure Sockets Layer**) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. **Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.**
Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

ΚΩΔΙΚΟΠΟΙΗΣΗ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Τι είναι η κωδικοποίηση

Στις επικοινωνίες **κώδικα** ονομάζουμε έναν κανόνα για μετατροπή ενός τμήματος πληροφορίας π.χ. ένα γράμμα, λέξη, ή φράση σε μια άλλη μορφή αναπαράστασης όχι απαραίτητα του ίδιου τύπου. Στις επικοινωνίες και στην επεξεργασία πληροφοριών **κωδικοποίηση** είναι η διαδικασία με την οποία μια πηγή (αντικείμενο) εκτελεί αυτήν την μετατροπή πληροφορίας σε δεδομένα, τα οποία στέλνονται μετά στον παραλήπτη (παρατηρητή), όπως ένα σύστημα επεξεργασίας δεδομένων. **Αποκωδικοποίηση** είναι η αντίστροφη διαδικασία της μετατροπής δεδομένων, τα οποία έχουν σταλεί από μια πηγή , σε πληροφορία κατανοητή από τον παραλήπτη. Ένας κωδικοποιητής/αποκωδικοποιητής είναι μια υλοποίηση αυτού του κανόνα (η αλγόριθμος) . Ένας λόγος για χρήση της κωδικοποίησης είναι η ύπαρξη περιπτώσεων όπου με χρήση της συνηθισμένης προφορικής ή γραπτής γλώσσας δεν μπορείς να επιτύχεις αξιόπιστη και αποτελεσματική επικοινωνία. Για παράδειγμα όταν η απόσταση μεταξύ των ατόμων που προσπαθούν να επικοινωνήσουν είναι μεγάλη τότε πρέπει αναπαραστήσουμε το μήνυμα σε μια μορφή που μπορεί να μεταφερθεί σε μεγάλες αποστάσεις (π.χ. με ηλεκτρικά σήματα). Στην ιστορία της κρυπτογραφίας οι κώδικες χρησιμοποιούνταν συχνά για να εξασφαλίσουν το απόρρητο της επικοινωνίας.



http://ebooks.edu.gr/modules/ebook/show.php/DSGL-B110/93/737,2749/

Τι είναι τα Barcodes

Οι **Γραμμωτοί Κώδικες - barcodes** είναι ένα σύγχρονο εργαλείο για την ακριβή και γρήγορη εισαγωγή δεδομένων σε Ηλεκτρονικούς Υπολογιστές. Αντικαθιστούν την παραδοσιακή πληκτρολόγηση η οποία συνήθως οδηγεί σε λάθη και καθυστερήσεις. Χαρακτηριστικά αναφέρεται ότι **η πιθανότητα λάθους πληκτρολόγησης είναι 1 πρός 300 ενώ η πιθανότητα λάθους ανάγνωσης ενός σωστά εκτυπωμένου barcode είναι περίπου 1 ανά 3.000.000 αναγνώσεις.** Τα barcodes αποτελούν κλάδο του γενικότερου τομέα τεχνολογιών Αυτόματης Συλλογής Δεδομένων (Automatic Data Capture Technologies). Είναι τυποποιημένα σύμβολα, ένα είδος αλφαβήτου, που απεικονίζουν με συνδυασμούς από γραμμές διαφορετικού πλάτους και "είδους"

("σκοτεινές" και "φωτεινές"), μια συγκεκριμένη πληροφορία (π.χ. τον κωδικό ενός προϊόντος)· "διαβάζονται" από μηχανήματα ηλεκτρονικής οπτικής ανάγνωσης (scanners).

Περνώντας ο scanner πάνω από μία μπάρα, καταλαβαίνει το είδος της (φωτεινή ή σκοτεινή) καθώς και το πλάτος της. Μ' αυτόν τον τρόπο αποκωδικοποιείται το σύμβολο και μεταφέρεται στον Η/Υ η «πληροφορία» η οποία περιέχεται μέσα στο barcode. Ο Η/Υ με τη σειρά του χρησιμοποιώντας αυτόν τον κωδικό, ανατρέχει στη βάση δεδομένων του όπου και βρίσκονται όλες οι πληροφορίες που αντιστοιχούν στον συγκεκριμένο κωδικό. Έτσι επιτυγχάνεται η ομαλή και απροβλημάτιστη διακίνηση και διαχείριση προϊόντων και υπηρεσιών.

Τα πλεονεκτήματα των barcodes

Τα πλεονεκτήματα των barcodes, μπορούν να συνοψισθούν στα εξής:

- Μείωση σφαλμάτων που προκύπτουν από την πληκτρολόγηση δεδομένων
- Εξασφάλιση ποιοτικών πληροφοριών
- Τυποποιημένες διαδικασίες διαχείρισης μεταξύ όλων των εμπλεκομένων στην εφοδιαστική αλυσίδα
- Αυξημένη παραγωγικότητα
- Αποτελεσματικότερη διαχείριση αποθεμάτων και διαδικασιών αποθήκευσης
- Παρακολούθηση πωλήσεων και αποθεμάτων σε πραγματικό χρόνο
- Δυνατότητα εντοπισμού και παρακολούθησης των εμπορευμάτων σε όλα τα σημεία της εφοδιαστικής αλυσίδας
- Άμεσοι χρόνοι παραγγελίας και παράδοσης
- Μείωση κόστους κ.α.

Το σύστημα GS1

Ο GS1 είναι ένας διεθνής μη κερδοσκοπικός οργανισμός που ιδρύθηκε το 1977, εδρεύει στις Βρυξέλλες και εκπροσωπείται σε περισσότερες από 100 χώρες στον κόσμο. Ασχολείται αποκλειστικά με το σχεδιασμό και την εφαρμογή διεθνών προτύπων με σκοπό την αποτελεσματικότερη λειτουργία της εφοδιαστικής αλυσίδας σε παγκόσμιο επίπεδο και ποικίλους τομείς. Προσφέροντας μία πλήρη σειρά προϊόντων, υπηρεσιών και λύσεων, εξασφαλίζονται τυποποιημένες διαδικασίες και επιτυγχάνονται αποτελεσματικότερες εμπορικές συναλλαγές προς όφελος επιχειρήσεων και καταναλωτών. Τα πρότυπα GS1 είναι τα πλέον διαδεδομένα στον κόσμο.

Οι εταιρείες που χρησιμοποιούν το σύστημα GS1 μπορούν να επιλέξουν μεταξύ πολλών τύπων γραμμωτού κώδικα, ανάλογα με την εφαρμογή. Κι’ αυτό γιατί ο κάθε τύπος γραμμωτού κώδικα έχει διαφορετικά πλεονεκτήματα και αδυναμίες.

Οι τύποι των barcodes που χρησιμοποιούνται από τα πρότυπα GS1 διαχωρίζονται σε:

Γραμμικά (linear- 1D) :

i) EAN/UPC

•Προορίζονται για χρήση στα σημεία λιανικής πώλησης (POS).

•Όταν χρησιμοποιείται τόσο σε περιβάλλον POS όσο και σε περιβάλλον logistics, το σύμβολο θα πρέπει να είναι εκτυπωμένο σε μέγεθος μεγαλύτερο του κανονικού.

•Η χρήση του περιορίζεται για την απεικόνιση Διεθνών Κωδικών Αναγνώρισης GS1, καθώς και Ειδικών Κωδικών Αναγνώρισης για συγκεκριμένες εφαρμογές όπως η κωδικοποίηση Μονάδων Εμπορίας Μεταβλητής Μέτρησης και η εσωτερική κωδικοποίηση.

ii) GS1 DataBar (παλαιότερα γνωστό ως RSS)

•Αποτελούν μια οικογένεια συμβόλων που μπορούν να αναγνωσθούν στα σημεία λιανικής πώλησης (POS), είναι μικρότερα από τα σύμβολα EAN/UPC και μπορούν να απεικονίσουν και πρόσθετες πληροφορίες όπως αύξοντες αριθμούς, αριθμούς παρτίδας και ημερομηνίες λήξης.

•Έχει ήδη εγκριθεί σε παγκόσμιο επίπεδο η χρήση των συμβόλων GS1 για τη σήμανση υγειονομικών προϊόντων που δεν πωλούνται στα σημεία λιανικής πώλησης (POS).

iii) GS1-128 (παλαιότερα γνωστό ως UCC/EAN-128 ή EAN-128)

•Τα σύμβολα GS1-128 (UCC/EAN-128) μπορούν να απεικονίσουν όλους τους Κωδικούς Αναγνώρισης GS1 μαζί με πρόσθετες πληροφορίες, αλλά δεν μπορούν να χρησιμοποιηθούν για τη σήμανση αντικειμένων που πωλούνται στα σημεία λιανικής πώλησης (POS).

Composite Component

•Το σύμβολο CompositeComponent (Σύνθετο Στοιχείο) είναι το μόνο «γραμμικό 2-διάστατο» σύμβολο που περιλαμβάνεται στο σύστημα GS1.

•Ονομάζεται “Σύνθετο Στοιχείο”, επειδή χρησιμοποιείται μόνο σε συνδυασμό με ένα γραμμικό σύμβολο όπως το GS1-128 ή το GS1 DataBar (RSS).

iv) ITF-14

Τα σύμβολα ITF-14 μπορούν να χρησιμοποιηθούν μόνο για την απεικόνιση Κωδικών Αναγνώρισης GTIN, μπορούν να εκτυπωθούν απευθείας σε χαρτοκιβώτια από κυματοειδές χαρτόνι, αλλά δεν μπορούν να χρησιμοποιηθούν για τη σήμανση αντικειμένων που πωλούνται στα σημεία λιανικής πώλησης (POS).

1. δισδιάστατα (2D) :

i) GS1 DataMatrix

•Το σύμβολο GS1 DataMatrix είναι το μόνο "2-διάστατο" σύμβολο που περιλαμβάνεται στο Σύστημα GS1 και με την πάροδο του χρόνου είναι αυτό που επιλέγεται όλο και περισσότερο για εφαρμογές του Τομέα Υγείας.

• Επειδή το σύμβολο GS1 DataMatrix απαιτεί τη χρήση σαρωτών τύπου κάμερας, για την ώρα χρησιμοποιείται μόνο για τη σήμανση υγειονομικών προϊόντων που δεν πωλούνται στα σημεία λιανικής πώλησης (POS).

(01)07612345678900(17)100503

(10)AC3453G3

ii) GS1 QR Code

Το QRCode είναι ένα "2-διάστατο" σύμβολο barcode που δίνει τη δυνατότητα απεικόνισης πολλών πληροφοριών σε περιορισμένη επιφάνεια. Διαβάζεται από imagescanners και σύγχρονα κινητά τηλέφωνα (smartphones). Χρησιμοποιείται κυρίως για λόγους marketing και με σκοπό να απεικονίσει ένα URL, ώστε ο καθένας να αντλεί με εύκολο και άμεσο τρόπο επιπρόσθετες πληροφορίες για μία εταιρία, ένα προϊόν, κλπ.Η συμβολογία GS1 QRCode απεικονίζει το GTIN ενός συγκεκριμένου προϊόντος μαζί με έναν νέο Δείκτη Εφαρμογής (ExtendedPackagingInformation) που περιέχει ένα URL με περαιτέρω πληροφορίες για το συγκεκριμένο προϊόν. Απαιτεί και αυτό imagescanners για να διαβαστεί, δεν αντικαθιστά το barcodeEAN-13 του προϊόντος καθώς δεν διαβάζεται στο POS με την τρέχουσα υποδομή, και υπάρχει μόνο συμπληρωματικά.

Ειδικές Δομές Κωδικών

Ένα προϊόν, του οποίου το κόστος εξαρτάται από μέτρηση η οποία είναι διαρκώς μεταβαλλόμενη, μπορεί να κωδικοποιηθεί είτε με ένα κωδικό GTIN, ο οποίος θα σημανθεί με ένα barcode GS1 DataBar, είτε με τους **Εθνικούς Κωδικούς προϊόντων Μεταβλητής Μέτρησης**. Ο όρος αυτός χρησιμοποιείται για να περιγράψει προϊόντα που πωλούνται, παραγγέλνονται ή παράγονται σε ποσότητες οι οποίες μεταβάλλονται συνεχώς, όπως φρούτα και λαχανικά, κρέας, τυρί, σχοινιά, αλυσίδες, υφάσματα, μοκέτες, κλπ.

i) Μονάδες Εμπορίας Μεταβλητής Μέτρησης που προορίζονται για Λιανική Πώληση

Σε αντίθεση με τα προϊόντα σταθερής μέτρησης, τα μεταβλητής μέτρησης έχουν κάποιο (-α) χαρακτηριστικό (-α) το (-α) οποίο (-α) είναι μεταβαλλόμενο (-α) ενώ τα υπόλοιπα είναι σταθερά. Μεταβαλλόμενα χαρακτηριστικά μπορεί να είναι το βάρος, η ποσότητα, το πλήθος των περιεχόμενων τεμαχίων, ή ο όγκος. Παραδείγματα τέτοιων προϊόντων είναι φρούτα και λαχανικά, κρέας, γαλακτοκομικά, σχοινιά, αλυσίδες, υφάσματα, χαλιά, ρολά διαφόρων ειδών κλπ.

ii) Κωδικός GTIN σε Σύμβολο Barcode GS1 DataBar

Εάν πρόκειται να χρησιμοποιηθεί κωδικός GTIN για την αναγνώριση του προϊόντος μεταβλητής μέτρησης τότε το σύμβολο GS1 DataBar και οι εκδοχές Expanded ή Expanded Stacked προτείνονται για χρήση επί φρέσκων προϊόντων. Ο συνδυασμός του GS1 DataBar και των Δεικτών Εφαρμογής προσφέρει μια διεθνή λύση για τα προϊόντα μεταβλητής μέτρησης. Σε αντίθεση με τους Εθνικούς Κωδικούς Περιορισμένης Κυκλοφορίας (Restricted Circulation Numbers – RCNs) οι Κωδικοί GTIN και το σύμβολο barcode GS1 DataBar μπορούν να χρησιμοποιηθούν σε διεθνές επίπεδο. Η διεθνής υιοθέτηση των συμβόλων GS1 DataBar είναι μια τρέχουσα διαδικασία, ειδικά στον τομέα των φρέσκων τροφίμων.

iii) Εθνικοί Κωδικοί Περιορισμένης Κυκλοφορίας σε Σύμβολο Barcode EAN/UPC

Όταν χρησιμοποιούνται οι Εθνικοί Κωδικοί Περιορισμένης Κυκλοφορίας (Restricted Circulation Numbers – RCNs) δεδομένα ποσότητας ή τιμής θα πρέπει να περιλαμβάνονται στον κωδικό ώστε να «διαβάζονται» στα σημεία λιανικής πώλησης.Ένας Εθνικός Κωδικός RCN γενικά αποτελείται από ένα Ειδικό Πρόθεμα GS1, έναν κωδικό αναφοράς και ψηφία τα οποία σχετίζονται με το βάρος, την ποσότητα ή την τιμή.

Η μέτρηση ή η τιμή μπορεί να είναι 4 ή 5 ψηφία και μπορεί να περιλαμβάνει ένα ειδικό ψηφίο ελέγχου εσωτερικά, επιπλέον του τελευταίου ψηφίου ελέγχου του κωδικού όπως ισχύει στους Κωδικούς GS1. Η ακριβής δομή καθορίζεται από τους Εθνικούς Οργανισμούς GS1 για τις χώρες ευθύνης τους.

Ο κωδικός προϊόντων μεταβλητής μέτρησης μπορεί να αποδοθεί κατά περίπτωση από:

- Τον Λιανέμπορο (από τη δυναμικότητα που έχει διαθέσιμη ο Εθνικός Οργανισμός GS1)
- Τον Προμηθευτή από ένα εύρος αριθμών που του αποδίδεται από το Εθνικό Γραφείο GS1
- Τον Εθνικό Οργανισμό GS1 εφόσον κάποιος γενικός αριθμός έχει αποδοθεί για συγκεκριμένο είδος προϊόντων

Το Ειδικό Πρόθεμα των Εθνικών Κωδικών Περιορισμένης Κυκλοφορίας RCN επιλέγεται από τα Εθνικά Γραφεία GS1 και το εύρος προθεμάτων 02 και 20 έως 29.
Εάν πρόκειται να χρησιμοποιηθούν Κωδικοί RCN η απεικόνισή τους πρέπει να γίνεται με σύμβολα barcodes EAN/UPC.

ΠΗΓΕΣ

- Εφαρμογές Πληροφορικής, Πανσεληνάς Γ., Αγγελιδάκης Γ., Μιχαηλήδη Α., Μπλάτσιος Χ., Παπαδάκης Σ., Παυλίδης Γ., Τζαγκαράκης Ε., Τζωρμπατζάκης Α., ΙΤΥΕ Διόφαντος, 2014
- http://kryptografies.blogspot.gr
- http://teachers.teicm.gr/chilas/files/D_III/public_key_cryptography.pdf
- http://www.image.ntua.gr/meleti172KTP/?q=node/23
- http://www.piraeusbank.gr/el/Idiwtes/Trapezikes-Ypiresies/e-Banking/Asfaleia-Synallagon/Asfaleia-Ypiresion-Winbank-Webbanking
- http://www.triklopodia.gr
- https://el.wikipedia.org/
- https://el.wikipedia.org/wiki/%CE%A8%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CE%AE_%CF%85%CF%80%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AE
- https://el.wikipedia.org/wiki/File_Transfer_Protocol#%CE%A5%CF%80%CE%BF%CF%83%CF%84%CE%AE%CF%81%CE%B9%CE%BE%CE%B7_%CE%B1%CF%80%CF%8C_Web_Browser
- https://el.wikipedia.org/wiki/HTTPS
- https://el.wikipedia.org/wiki/SSL
- https://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html