

Ubuntistas

Το περιοδικό της Ελληνικής Κοινότητας Ubuntu-gr

Τεύχος 11

Ιανουάριος Φεβρουάριος Μάρτιος 2011

Google Search
Tips

Java
Κρυπτογραφία
Finale

Android

Sympy

Συμβολικά Μαθηματικά
με την Python

GIS

Γεωγραφικά Συστήματα
Πληροφοριών

OpenMP

Παράλληλος Προγραμματισμός

Ομάδα Περιοδικού:

- **Κωστάρας Γιάννης (hawk):**
Συντάκτης - jkost@freemail.gr
- **Παπαδόπουλος Δημήτρης (Dimitris):**
Συντάκτης, σελιδοποίηση - chaosdynamics@googlemail.com
- **Πετούμενου Τζένη (jennie):**
Επιμελήτρια κειμένων - epetoumenou@gmail.com
- **Στεφανίδης Φώτης (atermon):**
Συντάκτης - fotis.stefanidis@gmail.com
- **Χατζηπαντελής Παντελής (kalakouentin):**
Σελιδοποίηση - kalakouentin@yahoo.com
- **Δήμος Πούπος (Qdata):**
Επιμελητής κειμένων - demos_w57@hotmail.com

Σημείωμα από τη σύνταξη...

Μόλις πήρατε στα χέρια σας το πρώτο τεύχος του ubuntistas για το 2011. Είμαι σίγουρος ότι ανυπομονείτε να το διαβάσετε. Πριν όμως συνεχίσετε με την ανάγνωση των άρθρων, ας κάνουμε μια σύντομη ιστορική αναδρομή. Το πρώτο τεύχος του ubuntistas κυκλοφόρησε τον Οκτώβριο--Νοέμβριο του 2008. Έχουμε συμπληρώσει δηλαδή 2 χρόνια κυκλοφορίας! Όχι κι άσχημα για ένα περιοδικό που βασίζεται αποκλειστικά και μόνο σε εθελοντές. Παρόλ'αυτά για να συνεχίσει να λειτουργεί αδιάκοπα χρειάζεται και τη συνεισφορά των αναγνωστών, εσάς δηλαδή. Έχετε κάποιο άρθρο που θέλετε να δημοσιεύσετε ή να μοιραστείτε μαζί μας την εμπειρία σας με το ubuntu; Επικοινωνήστε μαζί μας και το άρθρο σας θα δημοσιευτεί στο επόμενο τεύχος του ubuntistas.

Αν ίσως παρατηρήσατε, τα τεύχη δημοσιεύονται πλέον με αρκετή καθυστέρηση. Ο λόγος είναι ότι

χρειαζόμαστε επείγοντως στοιχειοθέτη και σελιδοποιητή. Αν λοιπόν έχετε γνώσεις Latex ή ακόμα και Scribus και θέλετε να αφιερώσετε κάποιο χρόνο για να συνεισφέρετε στην κοινότητα αναλαμβάνοντας τη στοιχειοθέτηση του περιοδικού τότε παρακαλώ όπως να επικοινωνήσετε μαζί μας. Τόσο εμείς όσο και οι αναγνώστες μας θα σας είναι ευγνώμονες.

Σ'αυτό το τεύχος θα βρείτε άρθρα για το android και για τεχνικές αναζήτησης στο google. Η σειρά των άρθρων για κρυπτογραφία με java συνεχίζεται με το 3ο μέρος ενώ υπάρχει εισαγωγή στα γεωγραφικά συστήματα πληροφοριών (GIS). Μια σύντομη περιγραφή της scheme μας δίνει μια πρώτη γεύση από ένα διαφορετικό τρόπο προγραμματισμού, ενώ το άρθρο για sympr μας δείχνει πώς μπορούμε να κάνουμε συμβολικά μαθηματικά με την rython. Τέλος, μια εισαγωγή σε parallel computing με openmp.

Καλή ανάγνωση!

Περιεχόμενα

ΑΠΟΨΕΙΣ

4 Android

8 GIS

ΑΠΟΨΕΙΣ

15 Εισαγωγή στην Κρυπτογραφία με τη γλώσσα Java --- Μέρος 3

18 OpenMP

REVIEW

20 Scheme

21 Sympy

HINTS & TIPS

22 Google Search Tips

Η άδεια διάθεσης του περιεχομένου του ubuntuistas

Τα άρθρα που περιλαμβάνονται στο περιοδικό διατίθενται υπό τη άδεια της **Creative Commons Attribution-By-Share Alike 3.0 Unported license**. Αυτό σημαίνει ότι μπορείτε να προσαρμόσετε, να αντιγράψετε, να διανείμετε και να διαβιβάσετε τα άρθρα, αλλά μόνο υπό τους ακόλουθους όρους: πρέπει να αποδώσετε την εργασία στον αρχικό συντάκτη (π.χ. με **αναφορά ονόματος, email, url**) αλλά και στο περιοδικό, αναφέροντας την ονομασία του (**Ubuntuistas**). **Δεν επιτρέπεται** να αποδίδετε το άρθρο/α με τρόπο που να το/α επικυρώνετε ως δική σας εργασία. Και εάν κάνετε αλλαγές, μεταβολές, ή δημιουργίες πάνω σε αυτήν την εργασία, πρέπει να διανείμετε την προκύπτουσα εργασία **με την ίδια άδεια, παρόμοια ή συμβατή**.

Περίληψη άδειας: <http://tinyurl.com/5nv7kn> - **Πλήρης άδεια:** <http://tinyurl.com/yqontc>

Το ubuntu

Το ubuntu linux είναι ένα λειτουργικό σύστημα. Με περιβάλλον εργασίας gnome το φωνάζουμε ubuntu, με kde το φωνάζουμε kubuntu. Είναι πλήρες(!), τεχνολογικά προηγμένο(!), και εύκολο στην χρήση από οποιονδήποτε(!). Στα αποθετήρια του ubuntu υπάρχουν διαθέσιμες κυριολεκτικά χιλιάδες εφαρμογές σχεδόν για οτιδήποτε(!) ... για επαγγελματική, επιστημονική, εκπαιδευτική, και οικιακή χρήση. Τόσο το ubuntu όσο και οι εφαρμογές του είναι Ελεύθερο Λογισμικό / Λογισμικό Ανοιχτού Κώδικα (ΕΛ/ΛΑΚ), δηλαδή διατίθενται ελεύθερα, και στην Ελλάδα υποστηρίζονται από την άτυπη αλλά πολύ δραστήρια κοινότητα ubuntu-gr. Περισσότερα στο <http://www.ubuntu-gr.org>.

Η κοινότητα ubuntu-gr

Η κοινότητα ubuntu-gr ανήκει στα μέλη της και είναι ανοιχτή σε όλους! Είναι το μέρος όπου έμπειροι και άπειροι(!) χρήστες συζητάνε ό,τι τους απασχολεί, ιδέες, ερωτήματα, πρακτικά ζητήματα, οργανωτικά θέματα, και κυρίως τεχνικά προβλήματα. Αποτελείται από ανθρώπους με εμπειρία στην πληροφορική αλλά κυρίως από απλούς χρήστες, οι οποίοι εθελοντικά συμμετέχουν i) στην δημιουργία-ανάπτυξη του λογισμικού, ii) στην μετάφρασή του στην ελληνική γλώσσα, iii) στην προώθηση-διάδοση του στην Ελλάδα, και κυρίως iv) στην παροχή αμεσότητας(!) και υψηλής ποιότητας(!) τεχνικής υποστήριξης σε άλλους ελληνόφωνους χρήστες. Λειτουργεί με αυτό-οργάνωση και προσπαθούμε οι αποφάσεις να λαμβάνονται όσο το δυνατόν πιο δημοκρατικά από εκείνους που προσφέρουν-δραστηριοποιούνται συστηματικά. Η ελληνική κοινότητα του Ubuntu διαθέτει μέχρι στιγμής φόρουμ, λίστα ηλ. ταχυδρομείου, κανάλι συζητήσεων τύπου IRC, καθώς και το περιοδικό Ubuntuistas. Για όλα αυτά υπάρχουν οδηγίες και links στο <http://www.ubuntu-gr.org>.

Το περιοδικό ubuntuistas

Το Ubuntuistas, το ηλεκτρονικό περιοδικό της ελληνικής κοινότητας του ubuntu (ubuntu-gr), κυκλοφορεί ελεύθερα κάθε δίμηνο, με πρώτο τεύχος του Νοεμβρίου - Δεκεμβρίου 2008. Περιέχει νέα, πληροφορίες, συνεντεύξεις, παρουσιάσεις, οδηγούς, και άρθρα σχετικά με το ubuntu. Το περιοδικό είναι ανοιχτό σε όλους, όπως και το GNU/Linux! Ο καθένας μπορεί να συμμετέχει ενεργά στην δημιουργία του, να αρθρογραφήσει, να προτείνει ιδέες και να κάνει τις επισημάνσεις / παρατηρήσεις του.

Ένα έξυπνο ανδροειδές στην τσέπη σας!

Android

Στα μέσα του 2005 η Google εξαγόρασε την Android Inc., μια μικρή και άγνωστη startup εταιρεία με έδρα το Palo Alto της Καλιφόρνια. Το αντικείμενό της ήταν τότε η ανάπτυξη λογισμικού για κινητά τηλέφωνα. Μέσα σε δύο χρόνια -περίοδο δοκιμών και επαφών με κατασκευαστές- άρχισαν ήδη να κυκλοφορούν οι φήμες για τη δημιουργία "έξυπνου κινητού" από τη google. Στα τέλη του 2007 συστήνεται κοινοπραξία εταιρειών της συγκεκριμένης αγοράς με την ονομασία Open Handset Alliance και σκοπό τη δημιουργία ανοιχτών προτύπων (open standards) για κινητές συσκευές (smartphones). Σύντομα ξεκινά και η ιστορία του ολοκληρωμένου λειτουργικού συστήματος Android, του οποίου η πρώτη έκδοση κυκλοφορεί το Σεπτέμβριο του 2008. Η άδεια διάθεσης του είναι η Apache License, που χαρακτηρίζεται ως ιδιαίτερα προοδευτική συγκρινόμενη με τις υπόλοιπες άδειες ΕΛΛΑΚ. Υπάρχουν βέβαια και μέρηματα κώδικα υπό την GNU/GPLv2.

Η χρήση του Android δεν περιορίζεται μόνο σε κινητά τηλέφωνα, αλλά επεκτείνεται και σε μια ευρεία γκάμα οικιακών συσκευών όπως netbooks, tablets, τηλεοράσεις, φούρνους μικροκυμάτων, ψυγεία. Ο κάθε κατασκευαστής μπορεί δηλαδή να

το προσαρμόσει κατάλληλα στο υλικό που παράγει. Ειδικά όμως στα έξυπνα κινητά, το ανδροειδές έχει σαρώσει ως δούρειος ίππος την παγκόσμια αγορά.

Ας δούμε λίγο το γραφικό περιβάλλον μιας τέτοιας συσκευής. Καταρχάς, υποστηρίζονται πολλαπλές επιφάνειες οθόνης για την τοποθέτηση εικονιδίων - συνδέσμων προς τις εφαρμογές. Σέρνοντας το δάχτυλό μας από τη μια άκρη της οθόνης ως την άλλη μεταφερόμαστε στην επόμενη επιφάνεια, σύμφωνα με την κατεύθυνση της κίνησης. Η γραμμή ειδοποιήσεων πάνω στα δεξιά μας δείχνει την ώρα, την κατάσταση της μπαταρίας και το είδος της τρέχουσας σύνδεσης (GSM, 3G/HSDPA, WiFi). Στα αριστερά εμφανίζονται οι ειδοποιήσεις του συστήματος και κάποιες από τις εφαρμογές που εκτελούνται. Κάτω και στη μέση υπάρχει το κουμπί για άμεση πρόσβαση σε όλες τις εγκατεστημένες εφαρμογές και λειτουργίες, ενώ τα κουμπιά "Τηλέφωνο" και "Διαδίκτυο" () βρίσκονται είτε ακριβώς από πάνω, είτε αριστερά και δεξιά του κουμπιού πρόσβασης. Στην επιφάνεια εργασίας μπορούμε να προσθέσουμε όχι μόνο εικονίδια συντομεύσεων για εφαρμογές, αλλά και μικροεφαρμογές/widgets, όπως ρολόι, καιρό, email, facebook, twitter,

youtube, ημερολόγιο, αναζήτηση. Συνήθως, η προσθαφαίρεση συντομεύσεων και widget γίνεται με παρατεταμένο κράτημα των εικονιδίων. Οι περισσότερες συσκευές της αγοράς έχουν και τρία κουμπιά - σύμβολα εκτός επιφάνειας εργασίας (επιστροφή, αρχική, μενού).

Ο browser του Android βασίζεται στη μηχανή webkit, ενώ η πρόσβαση στο Διαδίκτυο γίνεται είτε μέσω δικτύου κινητής τηλεφωνίας είτε μέσω ασύρματης σύνδεσης WiFi. Πολλοί πάροχοι κινητής τηλεφωνίας διαθέτουν προσφορές για πρόσβαση στο Διαδίκτυο μέσω των δικτύων τους. Στη δικιά μου συσκευή είναι μονίμως ενεργοποιημένο το WiFi και όπου υπάρχει διαθέσιμο δίκτυο συνδέομαι αυτόματα, ειδάλλως χρησιμοποιείται η πρόσβαση μέσω του παρόχου, που έχει όριο τα 250 MB το μήνα, τα οποία δεν έτυχε να ξεπεράσω ακόμη --με προσεκτική χρήση βέβαια. Επειδή όμως το WiFi ξεζουμίζει τη μπαταρία, ο διακαής μου πόθος είναι να άντεχε η ρημάδα η μπαταρία ένα μήνα τουλάχιστον, για να την γέμιζα μαζί με τις άλλες μηνιαίες εκκρεμότητες (λυπητερές συνήθως).

Η προσθαφαίρεση εφαρμογών είναι εφικτή μέσω της προεγκατεστημένης εφαρμογής Android Market της Google

(κλειστού κώδικα). 200.000 εφαρμογές τουλάχιστον είναι διαθέσιμες στο διαδίκτυο για προσθαφαίρεση με ένα κλικ στην οθόνη αφής (που υποστηρίζει παρεμπιπτόντως και τη λειτουργία multi-touch). Προς το παρόν, το τοπίο είναι κάπως άναρχο με άδειες ελεύθερες και μη, επί πληρωμή ή δωρεάν, όπου το δωρεάν να περιλαμβάνει και "λάιτ" δοκιμαστικές εκδόσεις (free lite), συνοδευτικές διαφημίσεις (adware), ή απλές παρακλήσεις για χορηγίες (donationware). Προσωπικά πάντως, χρησιμοποιώ και με καλύπτουν 20 έως 30 εφαρμογές, με τις περισσότερες εξ' αυτών να υπόκεινται σε άδειες ανοιχτού λογισμικού. Επίσης, πολλοί κατασκευαστές διαθέτουν τις δικές τους λύσεις τόσο για εφαρμογές όσο και για βελτιώσεις/τροποποιήσεις της γραφικής διεπαφής των συσκευών τους. Φυσικά, θα βρείτε και εφαρμογές τρίτων εκτός Market.

Η γκάμα των διαθέσιμων εφαρμογών καλύπτει σχεδόν κάθε ανθρώπινη δραστηριότητα. Έχετε την ελευθερία να προσαρμόσετε το κινητό σας στις δικές σας ανάγκες. Μπορείτε να παρακολουθείτε και να ενημερώνετε τα κοινωνικά σας δίκτυα από παντού, ακόμη και με φρέσκο πολυμεσικό περιεχόμενο. Αν χαθείτε στο δρόμο, ενεργοποιήστε το GPS και βρείτε το στίγμα σας στο χάρτη. Ενημερωθείτε για τις τρέχουσες εξελίξεις της υπόθεσης WikiLeaks και του ιδρυτή της άμεσα μέσω ροών RSS. Δείτε τα επαγγελματικά σας ραντεβού για αύριο μέσω κοινόχρηστων ημερολογίων. Πόσες θερμίδες καταναλώσατε σήμερα; Πρέπει να περπατήσετε μισή ωρίτσα ακόμη για να'χετε

την υγεία σας. Υπάρχει διαθέσιμο πρατήριο βενζίνης εδώ στην ερημιά και πόσο πάει το λίτρο αμόλυβδης; Πού βρίσκεται ο αστερισμός της Ανδρομέδας στον ουρανό; Αυτό το ψηφιακά υπογεγραμμένο PDF στα εισερχόμενά μου να το εκτυπώσω στο γραφείο ώστε να προλάβει να το στείλει ταχυδρομικώς και συστημένο η γραμματέας μου (λέμε τώρα); Δεν θα προλάβω να περάσω από εκεί σήμερα. Για να σκανάρω το QR Code του νέου συνεργάτη γιατί βαριέμαι να πληκτρολογώ όλα τα στοιχεία του. Θολώνει η φαντασία μου με όλα αυτά τα απίθανα πράγματα που συμβαίνουν στο κινητό μου και την χρεωκοπημένη χώρα μου. Και βουλιάζουμε και αλλάζουμε, αλλά τώρα μάλλον ήρθε η ώρα για απότομη προσγείωση, γιατί πρέπει να τελειώνουμε με το άρθρο. Α, και μην λησμονείτε ποτέ ότι πλέον ο εντοπισμός της θέσης σας είναι παιχνιδάκι σε αυτές τις (παν)έξυπνες συσκευές, οπότε το νου σας.

Για να καταπιαστούμε, εν κατακλείδι, και με τα τεχνολογικά χαρακτηριστικά του λειτουργικού. Η διαχείριση της περιορισμένης επεξεργαστικής ισχύος και η μικρή φυσική μνήμη των συσκευών Android σαφώς παίζει καθοριστικό ρόλο για το λειτουργικό σύστημα. Το Android λοιπόν βασίζεται σε τροποποιημένη έκδοση του πυρήνα Linux 2.6 για την υποστήριξη του κατάλληλου υλικού και σε ένα υποσύνολο κλάσεων και βιβλιοθηκών, επίσης τροποποιημένο, της γλώσσας προγραμματισμού Java, που κάνει χρήση της εικονικής μηχανής Dalvik. Αυτή ακριβώς η ανεξάρτητη υλοποίηση προκάλεσε

πρόσφατα τη δικαστική διαμάχη μεταξύ της Oracle και της Google. Συνοπτικά, οι γλώσσες προγραμματισμού που αποτελούν το σύστημα είναι η C (πυρήνας), ή C++ (βιβλιοθήκες) και η Java - XML (γραφικό περιβάλλον). Τέλος, ας αναφέρουμε εδώ και την υποστήριξη δικτύωσης IPv6 του Android, που επιτρέπει την πλήρη αυτοματοποίηση και τον απομακρυσμένο έλεγχο των συσκευών.

Το ιστορικό εκδόσεων του Android, με τις αντίστοιχες κωδικές ονομασίες επιδορπίων, περιγράφεται στον παρακάτω πίνακα:

Platform	API Level
Android 2.3(Gingerbread)	9
Android 2.2(Froyo)	8
Android 2.1(Eclair)	7
Android 1.6(Donut)	4
Android 1.5(Cupcake)	3

Αν θέλετε να ασχοληθείτε με την ανάπτυξη εφαρμογών για το συγκεκριμένο λειτουργικό σύστημα, καλό είναι να προμηθευτείτε πρώτα ένα σχετικό βιβλίο. Για τα γραφικά περιβάλλοντα ανάπτυξης, τις ιδιαιτερότητες εγκατάστασης και για την πρώτη σας εφαρμογή HelloAndroid θα μιλήσουμε ενδελεχώς στο επόμενο άρθρο. Μείνετε συντονισμένοι λοιπόν στο αξιόλογο κοινοτικό περιοδικό μας!

Βιβλιογραφία

1. <http://developer.android.com/guide/basics/what-is-android.html>
2. <http://www.google.com/mobile/android/>

Γεωγραφικά Συστήματα Πληροφοριών

GIS

Γεωγραφικά Συστήματα Πληροφοριών

Ο όρος Γεωγραφικά Συστήματα Πληροφοριών (Geographic Information Systems – GIS) αναφέρεται σε κάθε σύστημα Η/Υ που έχει τη δυνατότητα να χειρίζεται γεωγραφικά δεδομένα [1]. Δεν περιλαμβάνει μόνο λογισμικό και υλικό, αλλά και ειδικές συσκευές για εισαγωγή και δημιουργία χαρτών, καθώς και τα συστήματα επικοινωνιών που απαιτούνται για να συνδέσουν τα διάφορα συστατικά μεταξύ τους.

Σε σύγκριση με τους απλούς χάρτες, ένα σύστημα GIS έχει το πλεονέκτημα ότι η αποθήκευση των δεδομένων γίνεται χωριστά από την αναπαράστασή τους. Αυτό έχει σαν αποτέλεσμα τα ίδια δεδομένα να μπορούν να αναπαρασταθούν με διαφορετικούς τρόπους. Π.χ. μπορούμε να μεγεθύνουμε τον (ψηφιακό πλέον) χάρτη, να εμφανίσουμε συγκεκριμένες μόνο περιοχές, να κάνουμε υπολογισμούς αποστάσεων μεταξύ τοποθεσιών, να δημιουργήσουμε πίνακες που να δείχνουν τα διάφορα χαρακτηριστικά του χάρτη, να υπερθέσουμε επιπλέον πληροφορία πάνω στο χάρτη, ακόμα και να αναζητήσουμε ποιες είναι οι καλύτερες τοποθεσίες για να ιδρύσουμε τα επόμενα καταστήματά

μας! Επιπλέον, ένα σύστημα GIS έχει όλα εκείνα τα πλεονεκτήματα της χρήσης Η/Υ, όπως διαχείριση μεγάλων ποσοτήτων δεδομένων εύκολα και γρήγορα κλπ. Όλα τα δεδομένα σε ένα σύστημα GIS είναι γεωκαταχωρημένα, δηλαδή συνδεδεμένα με μια συγκεκριμένη γεωγραφική τοποθεσία της επιφάνειας της γης μέσω ενός συστήματος συντεταγμένων. Ένα από τα πιο συνηθισμένα συστήματα γεωγραφικών συντεταγμένων είναι αυτό του γεωγραφικού μήκους και γεωγραφικού πλάτους. Σ' αυτό το σύστημα συντεταγμένων κάθε τοποθεσία προσδιορίζεται σχετικά με τον ισημερινό και τη γραμμή μηδενικού γεωγραφικού μήκους που περνά από το αστεροσκοπείο Greenwich της Αγγλίας. Υπάρχουν πολλά άλλα γεωγραφικά συστήματα συντεταγμένων, και κάθε GIS σύστημα θα πρέπει να μπορεί να μετατρέπει τις συντεταγμένες από το ένα σύστημα στο άλλο. Η χωρική πληροφορία αναπαρίσταται με δυο τρόπους:

- Ως διανυσματικά δεδομένα με τη μορφή σημείων, γραμμών και πολυγώνων, ή
- Ως δικτυωτά (raster) δεδομένα, οργανωμένα συστηματικά σε κελιά (όπως π.χ. μια ψηφιακή εικόνα).

Ιστορία των γεωγραφικών συστημάτων πληροφοριών

Τα γεωγραφικά συστήματα πληροφοριών αναπτύχθηκαν και εξελίχθηκαν στη διάρκεια των αιώνων, μέσω δημιουργίας χαρτών και συλλογής γεωγραφικών πληροφοριών και αποθήκευσής τους σε καταχωρητές. Οι πρώτοι γνωστοί χάρτες σχεδιάστηκαν πάνω σε περγαμινές για να δείξουν τα χρυσωρυχεία του Κοπτής κατά τη διάρκεια της βασιλείας του Ραμσή II της Αιγύπτου (1292-1225 π.Χ.) [1]. Ίσως νωρίτερα, οι Βαβυλώνιοι περιέγραφαν τον τότε γνωστό κόσμο με επιγραφές σφηνοειδούς γραφής. Αργότερα, οι Αρχαίοι Έλληνες συνέταξαν τους πρώτους πραγματικούς χάρτες. Χρησιμοποίησαν ένα ορθογώνιο σύστημα συντεταγμένων γύρω στο 300 π.Χ. Περίπου 100 χρόνια αργότερα, ο Έλληνας μαθηματικός, αστρολόγος και γεωγράφος Ερατοσθένης (276-194 π.Χ.) έβαλε τα θεμέλια της επιστημονικής χαρτογραφίας. Ένας από τους πιο γνωστούς παγκόσμιους χάρτες δημιουργήθηκε από τον Κλαύδιο Πτολεμαίο στην Αλεξάνδρεια (90-168 μ.Χ.).

Οι Ρωμαίοι έριξαν μεγαλύτερο βάρος στην καταγραφή και την καταχώρηση γεωγραφικών δεδομένων. Οι όροι cadastre (ένας επίσημος καταχωρητής ιδιοκτησίας)

και cadastral (ένας χάρτης ή έρευνα που δείχνει τα σύνορα ιδιοκτησίας) προέρχονται από το ελληνικό «κατά στίχον» που σημαίνει «κατά γραμμή, γραμμικός». Οι Ρωμαίοι ήταν οι πρώτοι που εισήγαγαν την έννοια της καταγραφής των ιδιοκτησιών, στο capitum registra (τον καταχωρητή γης). Καθώς οι κοινωνίες οργανώνονταν, π.χ. με την εισαγωγή συστημάτων φορολογίας, η καταχώρηση των ιδιοκτησιών συστηματοποιήθηκε εξ αρχής για να διασφαλίσει το ετήσιο κρατικό εισόδημα. Αργότερα, χάρτες σχεδιάστηκαν για να διευκολύνουν τα εμπορικά ακτοπλοϊκά ταξίδια. Οι Άραβες ήταν οι πρωτοπόροι χαρτογράφοι του Μεσαίωνα. Η Ευρωπαϊκή χαρτογραφία αναγεννήθηκε με την πτώση της Βυζαντινής αυτοκρατορίας και τη μετάφραση τον 15ο αιώνα του έργου Geographia του Κλαύδιου Πτολεμαίου στα Λατινικά, που έγινε η κυρίαρχη εικόνα του τότε γνωστού κόσμου. Παρόλο που η χαρτογραφία παραμελήθηκε, σε πολλές χώρες η καταχώρηση ιδιοκτησιών ευδοκίμησε. Το γνωστότερο παράδειγμα είναι αυτό του Μεγάλου Κτηματολογίου των περιοχών της Αγγλίας που συντάχθηκε το 1086 από τον πρώτο Νορμανδό βασιλιά, τον Γουλιέλμο τον Κατακτητή.

Οι εξερευνήσεις του Μάρκο Πόλο, του Χριστόφορου Κολόμβου, του Βάσκο Ντα Γκάμα κ.ά. είχαν ως αποτέλεσμα, πέραν της ανάπτυξης του εμπορίου, και τη δημιουργία νέων χαρτών. Οι επιτελικοί

χάρτες αποτέλεσαν τις βάσεις τόσο για τοπογραφικούς χάρτες ξηράς όσο και για χάρτες πλοήγησης.

Μέχρι το 19ο αιώνα, η γεωγραφική πληροφορία χρησιμοποιούνταν κυρίως στο εμπόριο, στις εξερευνήσεις, για συλλογή φόρων και από το στρατό. Καθώς οι κοινωνίες έγιναν πολυπλοκότερες, νέες εφαρμογές αναπτύχθηκαν για τις επερχόμενες υποδομές (τηλεφωνικές γραμμές, σιδηροδρόμους κλπ.). Οι αεροφωτογραφίες επιτάχυναν την πρόοδο της χαρτογράφησης. Η φωτογραφική, η τεχνική της μέτρησης των αεροφωτογραφιών, αναπτύχθηκε ταχύτητα στις δεκαετίες του 1920 και του 1930 και κατά το 2ο Παγκόσμιο πόλεμο. Χρησιμοποιείται κυρίως για χάρτες με κλίμακες 1:1500 και 1:50000.

Σήμερα, με τις δυνατότητες που παρέχουν οι Η/Υ, η χαρτογράφηση διατρέχει μια νέα εποχή. Τα δίκτυα Η/Υ, οι εξομοιωτές, η εικονική πραγματικότητα αποτελούν τη τελευταία μόδα στην εξέλιξη των γεωγραφικών συστημάτων.

Περιγραφή Συστήματος GIS

Σε γενικές γραμμές, ένα σύστημα GIS περιλαμβάνει:

- Τεχνικές για εισαγωγή γεωγραφικής πληροφορίας σε ηλεκτρονική μορφή, δηλ. μετατροπή της σε ψηφιακή μορφή,

- Τεχνικές για αποθήκευση αυτής της (μεγάλης σε όγκο) πληροφορίας σε συμπιεσμένη μορφή σε ψηφιακά αποθηκευτικά μέσα,

- Μεθόδους αυτοματοποιημένης ανάλυσης των γεωγραφικών δεδομένων, αναζήτηση προτύπων, συνδυασμό διαφορετικών ειδών δεδομένων, δυνατότητα μετρήσεων, εύρεση των συντομότερων διαδρομών και πολλά άλλα,

- Μεθόδους πρόβλεψης των αποτελεσμάτων πιθανών σεναρίων, όπως της επίδρασης της αλλαγής του κλίματος στη βλάστηση,

- Τεχνικές αναπαράστασης των δεδομένων σε μορφή χαρτών, εικόνων κλπ.

- Δυνατότητες για έξοδο των αποτελεσμάτων σε μορφή αριθμών και πινάκων.

Ένα σύστημα GIS επιτρέπει πράξεις πάνω σε χωρικά δεδομένα, δηλαδή χρησιμοποιώντας γεωγραφικά μήκη και πλάτη [2]. Παράδειγμα μιας τέτοιας πράξης είναι: «Ποιες πόλεις βρίσκονται λιγότερο από 1000 χλμ. η μία από την άλλη;». Επιτρέπει δηλαδή τον προσδιορισμό των χωρικών σχέσεων ανάμεσα στα χαρακτηριστικά ¹ (features) του χάρτη. Επιπλέον, συνδέει χωρικά

¹Ένα χαρακτηριστικό (feature) είναι π.χ. ένας δρόμος, μια λίμνη, τα σύνορα μιας χώρας, κλπ.

δεδομένα με γεωγραφική πληροφορία για ένα συγκεκριμένο χαρακτηριστικό του χάρτη. Η πληροφορία αποθηκεύεται ως ιδιότητες footnote Οι ιδιότητες (attributes) είναι δεδομένα που περιγράφουν ένα σημείο, μια γραμμή, ή ένα πολύγωνο [3]. Οι ιδιότητες αναφέρονται επομένως στα διάφορα χαρακτηριστικά (features) τα οποία αναπαριστώνται στους ψηφιακούς χάρτες ως σημεία, γραμμές και πολύγωνα. Π.χ., οι ιδιότητες ενός ποταμού είναι το όνομά του, το μήκος του, το μέσο βάθος του, ο ρυθμός ροής του, η ποιότητα του ύδατος, πόσα φράγματα ή/και γέφυρες υπάρχουν σ' αυτό, κλπ. [4] (attributes) του γραφικά παρουσιαζόμενου χαρακτηριστικού σε μια Βάση Δεδομένων. Για κάθε χαρακτηριστικό αποθηκεύονται τρεις βασικές πληροφορίες στη ΒΔ: η γεωγραφική πληροφορία, η προβολή (projection) πάνω στην οποία εκφράζεται η γεωγραφική πληροφορία, και οι ιδιότητες του χαρακτηριστικού. Επίσης, για κάθε χαρακτηριστικό του χάρτη αποθηκεύονται στη ΒΔ του GIS οι εξής πληροφορίες: τι χαρακτηριστικό είναι, πού βρίσκεται και πώς σχετίζεται με άλλα χαρακτηριστικά.

Πέραν της δυνατότητας σχεδίασης/χειρισμού χαρτών, ένα σύστημα GIS μπορεί να συνδέει εξωτερικές ΒΔ με αντικείμενα που ανήκουν στο χάρτη [4]. Αυτή η σύνδεση μας επιτρέπει να βλέπουμε αμέσως στο χάρτη όποιες αλλαγές γίνονται στις ΒΔ, καθώς και να κάνουμε ερωτήσεις στη ΒΔ απευθείας από το χάρτη. Επίσης, διαθέτει ένα σύνολο από εργαλεία που μπορούν

να διαχωρίσουν τα διάφορα δεδομένα που είναι αποθηκευμένα στις εξωτερικές ΒΔ, εμφανίζοντας π.χ. αντικείμενα ή περιοχές που ικανοποιούν συγκεκριμένα κριτήρια με διαφορετικά χρώματα ή σχήματα.

Ένα σύνολο από χαρακτηριστικά (π.χ. όλο το οδικό δίκτυο) θεωρούνται ως ένα στρώμα (layer) [2, 5]. Στην πραγματικότητα, οι ψηφιακοί χάρτες δεν είναι τίποτε άλλο από μια συλλογή στρωμάτων. Φανταστείτε αυτά τα στρώματα ως διαφάνειες, όπου κάθε στρώμα περιέχει ένα διαφορετικό μέρος του χάρτη. Τα στρώματα τοποθετούνται το ένα πάνω στο άλλο και μας επιτρέπουν να δούμε όλες τις όψεις του χάρτη την ίδια χρονική στιγμή. Π.χ. ένα στρώμα θα μπορούσε να περιέχει τα σύνορα των χωρών της γης, ένα άλλο στρώμα να περιέχει σύμβολα που να αναπαριστούν τις πρωτεύουσες, ένα τρίτο στρώμα μπορεί να περιέχει τις εθνικές οδούς, κλπ. Τοποθετώντας αυτές τις διαφάνειες τη μια πάνω στην άλλη δημιουργούμε έναν πλήρη χάρτη. Το GIS σύστημα συνδυάζει διάφορα στρώματα για να απαντήσει σε συγκεκριμένες χωρικές ερωτήσεις. Χαρακτηριστικά που σχετίζονται μεταξύ τους, όπως ποτάμια και κανάλια, μπορούν να εμφανίζονται σε ένα στρώμα, ενώ όλες οι υποδομές, όπως οι δρόμοι, μπορούν να εμφανίζονται σε άλλο στρώμα. Όταν κάποια χαρακτηριστικά δεν ενδιαφέρουν το χρήστη σε κάποια χρονική στιγμή, μπορεί να τα αποκρύπτει εμφανίζοντας μόνο την πληροφορία που τον ενδιαφέρει [3].

Όπως είπαμε, οι χάρτες σ' ένα GIS

σύστημα αποθηκεύονται σε ψηφιακή μορφή σε μια βάση δεδομένων. Σ' αυτή τη ΒΔ αποθηκεύονται δυο είδη πληροφορίας (ή αλλιώς, η πληροφορία που αποθηκεύεται σ' ένα GIS έχει δυο ιδιότητες, χωρικές και περιγραφικές): [2,3]

- Χωρική πληροφορία που περιγράφει την τοποθεσία και το σχήμα των γεωγραφικών χαρακτηριστικών, καθώς και τις χωρικές σχέσεις τους με άλλα χαρακτηριστικά, και
- Περιγραφική πληροφορία που αφορά τα χαρακτηριστικά.

Η χωρική πληροφορία αποθηκεύεται με τη μορφή τριών βασικών χαρακτηριστικών: του σημείου, της γραμμής και του πολυγώνου. Η περιγραφική πληροφορία εμφανίζεται με τη μορφή συμβόλων και ετικετών πάνω στο χάρτη. Η δύναμη του συστήματος βασίζεται στη δυνατότητα που έχει να συνδυάζει αυτά τα δυο είδη πληροφορίας.

Συνοψίζοντας έως εδώ, ένα χαρακτηριστικό (feature) του χάρτη αποτελείται από ιδιότητες (attributes). Ένα GIS αποθηκεύει τα χαρακτηριστικά σε πίνακες [4], έτσι ώστε κάθε γραμμή του πίνακα να αποτελεί ένα χαρακτηριστικό του χάρτη, και κάθε στήλη μια ιδιότητα αυτού του χαρακτηριστικού. Τα χαρακτηριστικά αυτά έχουν τις ίδιες ιδιότητες και επομένως ο πίνακας αποτελεί ένα στρώμα (layer) καθώς είναι ένα σύνολο από ίδια χαρακτηριστικά. Το σύνολο όλων αυτών των πινάκων

(στρωμάτων), από τα οποία αποτελείται ο χάρτης, αποθηκεύεται στην GIS Βάση Δεδομένων.

Ιδιότητα (attribute)			
	Αρ. δρόμου	Μήκος	Αρ. Οχημάτων
Χαρακτηριστικό (feature)	E1	210	100000
	E2	169	59000

Σχήμα 1: GIS ΒΔ.

Όποιος έχει δουλέψει με ΒΔ θα είναι οικείος με την ιδέα της εγγραφής. Μια εγγραφή είναι ένα σύνολο από στήλες που περιέχουν σχετική πληροφορία. π.χ., μια ΒΔ πελατών περιέχει μια εγγραφή για κάθε πελάτη και επίσης περιέχει στήλες για το όνομα, τη διεύθυνση κλπ. του πελάτη. Ένα χαρακτηριστικό είναι απλά μια εγγραφή που συνδυάζει δεδομένα σε μορφή πίνακα και γεωγραφική πληροφορία. Κάθε εγγραφή περιλαμβάνει αρκετές στήλες με δεδομένα καθώς και μια αναφορά σε γεωμετρική πληροφορία που περιγράφει το σχήμα και την τοποθεσία κάθε χαρακτηριστικού. Τα δεδομένα σε μορφή πίνακα ονομάζονται ιδιότητες και τα γεωμετρικά δεδομένα γεωμετρία. Αυτοί οι δυο τύποι δεδομένων αποτελούν το χαρακτηριστικό.

Μία άλλη σημαντική έννοια είναι αυτή της τοπολογίας. Τοπολογία ονομάζεται η μαθηματική διαδικασία βάση της οποίας ορίζονται χωρικές σχέσεις. Προσδιορίζονται δηλαδή οι σχέσεις μεταξύ των διαφόρων χαρακτηριστικών. Τρεις τοπολογικές έννοιες είναι: ο σύνδεσμος (κόμβος), ο ορισμός της περιοχής (το πολύγωνο) και η γειτνίαση.

Τα θέματα (themes) μας επιτρέπουν να αλλάξουμε προγραμματιστικά την εμφάνιση ορισμένων ή όλων των χαρακτηριστικών ενός στρώματος βασιζόμενοι σε συγκεκριμένα κριτήρια. Πρότυπα και τάσεις που είναι σχεδόν αδύνατο να ανιχνευθούν σε λίστες δεδομένων αποκαλύπτονται ξεκάθαρα όταν χρησιμοποιείται θεματική σκίαση για αναπαράστασή τους στο χάρτη. Ένας χάρτης σκιάζεται θεματικά χρησιμοποιώντας δεδομένα από ένα στρώμα. Το πιο κοινό παράδειγμα θεματικού χάρτη είναι ο χάρτης καιρού. Οι κόκκινες περιοχές δηλώνουν ζέστη, οι μπλε κρύο. Οι θεματικοί χάρτες αναπαριστούν τα δεδομένα με χρωματικές αποχρώσεις, πρότυπα, σύμβολα ή γεμίσματα και μπορεί κάποιος να δημιουργήσει διαφορετικούς θεματικούς χάρτες με αυτά τα αντικείμενα, βασιζόμενος στα δεδομένα του.

Η αναζήτηση, τέλος, είναι μια από τις πιο σημαντικές δυνατότητες ενός GIS. Επιτρέπει την ανάκτηση συγκεκριμένων δεδομένων με βάση τη γεωγραφική πληροφορία.

Ένα GIS σύστημα μπορεί να απαντήσει στους παρακάτω τύπους ερωτήσεων: [2]

- Τοποθεσίας, π.χ.: Τι βρίσκεται σε μια συγκεκριμένη τοποθεσία;
- Συνθηκών, π.χ.: Ποια τοποθεσία ικανοποιεί συγκεκριμένα κριτήρια;
- Τάσεων, π.χ.: Τι θα αλλάξει μετά από κάποιο χρονικό διάστημα;

- Μοτίβων (patterns), π.χ.: Ποια θα είναι η χρονική καθυστέρηση αν κυριαρχούν συγκεκριμένες εδαφικές συνθήκες;
- Μοντελοποίησης, π.χ. ερωτήσεις του τύπου: Τι θα συνέβαινε εάν ... ;

Συστήματα Συντεταγμένων και Γεωαναφορές

Προτού ανόμοια γεωγραφικά δεδομένα χρησιμοποιηθούν σε ένα GIS, θα πρέπει να αναχθούν σε ένα κοινό σύστημα. Υπάρχουν πολλά συστήματα γεωαναφορών που περιγράφουν τον πραγματικό κόσμο με διαφορετικούς τρόπους και με διαφορετική ακρίβεια. Ως γεωαναφορά (georegistration) ορίζεται η τοποθέτηση των αντικειμένων στον δισδιάστατο ή τρισδιάστατο χώρο [1]. Όπως φαίνεται και στο σχήμα 2, υπάρχουν δυο βασικές μέθοδοι γεωαναφοράς:

- Τα συνεχή συστήματα γεωαναφοράς και
- Τα διακριτά συστήματα γεωαναφοράς.

Στα συνεχή συστήματα γεωαναφοράς γίνεται συνεχής μέτρηση της θέσης των αντικειμένων σε σχέση με ένα σημείο αναφοράς χωρίς απότομες αλλαγές ή διακοπές. Τα δεδομένα χαρακτηρίζονται από την ανάλυσή τους (resolution) και την ακρίβειά τους (precision). Τα συνεχή συστήματα γεωαναφοράς χωρίζονται με τη σειρά τους σε άμεσα και σχετικά. Τα άμεσα περιλαμβάνουν:

- Τα συστήματα συντεταγμένων στην καμπύλη επιφάνεια της γης
- Τις γεωκεντρικές συντεταγμένες και
- Τις ορθογώνιες συντεταγμένες

Τα σχετικά περιλαμβάνουν:

- Πολικές συντεταγμένες,
- Οριζόντιες αποστάσεις, και
- Μετρήσεις κατά μήκος οδικών δικτύων

Βασικές έννοιες των άμεσων συστημάτων γεωαναφοράς είναι:

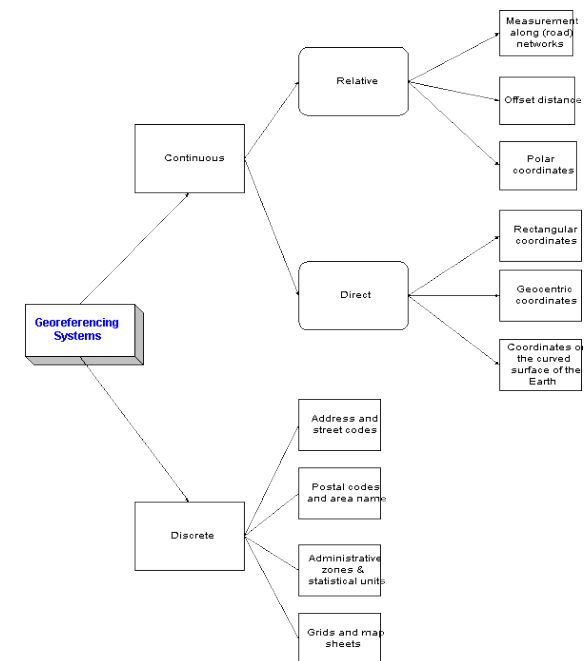
- Το χωροσταθμικό σημείο (datum). Όπως γνωρίζουμε, η γη δεν είναι σφαιρική αλλά περισσότερο ελλειψοειδής. Διάφορα ελλειψοειδή συστήματα έχουν προταθεί, με διαφορετική ακρίβεια περιγραφής του μεγέθους της γης. Ένα χωροσταθμικό σημείο είναι ένα μοντέλο (ελλειψοειδές) της γης που χρησιμοποιείται για γεωδαιτικούς υπολογισμούς. Το πιο ευρέως χρησιμοποιούμενο χωροσταθμικό σημείο σήμερα είναι το WGS84 (World Geodetic System 1984).
- Η προβολή χάρτη (projection). Τα διάφορα γεωαναφορικά δεδομένα μπορούν να αποτυπωθούν πάνω στο χάρτη μόνο όταν αναφέρονται στο επίπεδο και όχι στην καμπύλη

επιφάνεια της γης. Διάφορες προβολές της σφαιρικής επιφάνειας της γης στο επίπεδο έχουν προταθεί, και χωρίζονται σε τρεις κατηγορίες: κυλινδρικές (π.χ Mercator, UTM κ.ά.), κωνικές και αζιμουθιακές προβολές. Κάθε προβολικό σύστημα εισάγει λάθη στις αποστάσεις, το σχήμα των περιοχών κλπ.

- Το σύστημα συντεταγμένων. Οι γεωγραφικές συντεταγμένες της επιφάνειας της γης είναι το γεωγραφικό μήκος και το γεωγραφικό πλάτος. Σ' αυτό το σύστημα συντεταγμένων οι αποστάσεις υπολογίζονται χρησιμοποιώντας σφαιρική γεωμετρία και την ακτίνα της γης. Πολλές χώρες έχουν εθνικά συστήματα συντεταγμένων που τους επιτρέπουν να περιγράφουν τις περιοχές με μονάδες μήκους σε σχέση με ένα σημείο αναφοράς. Τα συνηθέστερα χρησιμοποιούν ορθογώνιες συντεταγμένες με μειονέκτημα την αναπόφευκτη εισαγωγή λάθους. Για να περιοριστεί το λάθος τα συστήματα αυτά περιορίζονται σε μικρές περιοχές. Για μεγαλύτερες περιοχές χρησιμοποιούνται πολλά τέτοια συστήματα μετατοπισμένα το ένα σε σχέση με τα άλλα. Πολλά συστήματα GIS προσφέρουν δυνατότητες μετατροπής από ένα σύστημα συντεταγμένων σε άλλο, με βάση

κοινά σημεία στα δυο συστήματα. Το πιο γνωστό σύστημα συντεταγμένων είναι το UTM (Universal Transverse Mercator Grid).

- Τέλος, το γεωειδές, η επιφάνεια που περνά από τα σημεία της γης με μηδενικό υψόμετρο (το μέσο επίπεδο θαλάσσης). Το γεωειδές επηρεάζεται από τη μάζα της γης και επομένως ακολουθεί τις υψομετρικές καμπύλες.



Σχήμα 1: GIS ΒΔ.

GPS (Global Positioning System) και ECDIS

Το GPS είναι ένα στρατιωτικό δορυφορικό σύστημα πλοήγησης που

αναπτύχθηκε από το υπουργείο άμυνας των Η.Π.Α. Το GPS ελέγχει 24 δορυφόρους μεγάλης ακριβείας που μπορούν να εκπέμπουν ραδιοσήματα με μεγάλη ακρίβεια. Η θέση στην επιφάνεια της γης προσδιορίζεται με λήψη και σύγκριση των σημάτων τριών τέτοιων δορυφόρων, η οποία μεταφράζεται στον υπολογισμό της μοναδικής τομής τριών κώνων, των οποίων οι κορυφές είναι οι τρεις δορυφόροι. Η τυπική ακρίβεια μέτρησης του GPS είναι $\pm 100\text{m}$ και μπορεί να φθάσει τα $\pm 10\text{m}$ με τη βοήθεια διαφορικού GPS. Το GPS επιτρέπει τον προσδιορισμό της θέσης σημείων σ' όλο τον κόσμο 24 ώρες το εικοσιτετράωρο κάτω από οποιοσδήποτε καιρικές συνθήκες.

Το GPS μπορεί να συνδυαστεί άμεσα με συστήματα GIS καθώς και με συστήματα ηλεκτρονικών χαρτών και πληροφοριακών συστημάτων ECDIS (Electronic Chart Display and Information System). Η ακρίβεια που παρέχεται από το GPS είναι καλύτερη από αυτή των ναυτικών χαρτών και άρα χρησιμότερη και ακριβέστερη για εισαγωγή σε ένα ECDIS. Ένα ECDIS αποτελείται από τρία πληροφοριακά υποσυστήματα:

- Έναν ηλεκτρονικό χάρτη πλοήγησης (ENC – Electronic Navigation Chart) που συνδυάζει ναυτική με υδρογραφική πληροφορία για απεικόνιση στον ψηφιακό χάρτη.
- Πληροφορία τοποθεσίας από το ραντάρ του πλοίου και το GPS.
- Πληροφορία κατεύθυνσης από το σύστημα κατεύθυνσης του πλοίου.

Το ECDIS παρέχει ένα πλήρες σύστημα πλοήγησης και προειδοποίησης που απεικονίζει τη θέση του πλοίου και άλλη πληροφορία απαραίτητη για την ασφαλή πλοήγησή του. Το σύστημα παρέχει ακόμα ακουστικά και οπτικά σήματα προειδοποίησης στην περίπτωση που το πλοίο ξεφεύγει της πορείας του, περνά από αβαθή νερά, κινδυνεύει να συγκρουστεί, κλπ. Αν εισαχθούν και εικόνες από το ραντάρ, το σύστημα μπορεί να απεικονίσει και άλλα πλοία και τις κινήσεις τους στην περιοχή. Το ECDIS μπορεί να ακολουθήσει την πορεία του αυτόματου πιλότου. Τέλος, όπως και στο GIS, ο χρήστης του ECDIS μπορεί να χτίσει μια Βάση Δεδομένων με τα χαρακτηριστικά όλων των αντικειμένων που φαίνονται στους ψηφιακούς χάρτες.

Άλλη εφαρμογή του GPS είναι στις επίγειες μεταφορές. Τα συστήματα πλοήγησης αυτοκινήτων, που ήδη χρησιμοποιούνται σε αρκετές Ευρωπαϊκές χώρες, χρησιμοποιούν απλές GIS λειτουργίες με ψηφιακούς χάρτες και παρεμφερή πληροφορία. Σε περιοχές με αυξημένο κυκλοφοριακό πρόβλημα, τέτοια συστήματα παρέχουν στους οδηγούς τις απαραίτητες πληροφορίες για να αποφύγουν τα μποτιλιαρίσματα και να οδηγούν με ασφάλεια. Αποτελούν ένα σύνολο από ερευνητικά προγράμματα σε Ευρώπη και Η.Π.Α., γνωστά ως Έξυπνα Συστήματα Μεταφοράς (Intelligent Information Systems - ITSs).

Συμπερασματικά

Τα συστήματα GIS έχουν μια ευρεία περιοχή εφαρμογών. Τυπικές εφαρμογές τους είναι στη διαχείριση του περιβάλλοντος και των πόρων του, στο σχεδιασμό και ανάπτυξη νέων υποδομών των πόλεων (π.χ. δρόμων), στις θαλάσσιες και επίγειες μεταφορές, στην ασφάλεια στη θάλασσα, στις βιομηχανίες τηλεπικοινωνιών, ύδατος και ηλεκτρισμού, όπου η έμφαση ρίχνεται στη συντήρηση και λειτουργία των δικτύων τους, ακόμα και σε στρατιωτικές εφαρμογές. Τα συστήματα GIS είναι μια ενεργή περιοχή της ψηφιακής τεχνολογίας με ετήσια ανάπτυξη 20% και πωλήσεις της τάξης των \$500 εκατομμυρίων. Η ικανότητα των συστημάτων αυτών να αποθηκεύουν σχέσεις ανάμεσα στα χαρακτηριστικά, πέρα από τα ίδια τα χαρακτηριστικά και τις ιδιότητές τους, είναι ένα από τα πιο σημαντικά χαρακτηριστικά ισχύος και ευελιξίας αυτής της τεχνολογίας. Τέλος, υπάρχει μια πολύ δραστήρια κοινότητα στην Ελλάδα, που μπορείτε να επισκεφθείτε στο <http://www.gistech.gr>.

Πηγές:

1. Bernhardsen T., Geographic Information Systems - An Introduction, 2nd Edition, John Wiley: 1999.
2. ESRI, Understanding GIS - The ARC/INFO Method, Environmental Systems Research Institut Inc.: 1990.

(συνεχίζεται στη σελίδα 25)

Εισαγωγή στην Κρυπτογραφία με τη γλώσσα Java – Μέρος 3ο

Αυθεντικοποίηση

Στο τρίτο και τελευταίο μέρος της σειράς άρθρων για την Κρυπτογραφία θα μιλήσουμε για την αυθεντικοποίηση, τις ψηφιακές υπογραφές, τις Αρχές Πιστοποίησης, και φυσικά θα δούμε υλοποιήσεις σε Java, χρησιμοποιώντας τις βιβλιοθήκες Java Cryptography Extension (JCE).

Αυθεντικοποίηση

Κάθε φορά που πηγαίνετε σε ένα αυτόματο τραπεζικό μηχάνημα (ATM) για να πραγματοποιήσετε μια συναλλαγή, απαιτείται ν' αποδείξετε ότι είστε όντως εσείς για να σας δοθεί πρόσβαση στο λογαριασμό σας. Με την τραπεζική κάρτα σας γίνεται η ταυτοποίησή σας (identification) από την τράπεζα, ενώ με τον προσωπικό αριθμό αναγνώρισης (PIN) γίνεται η αυθεντικοποίησή σας (authentication), δηλαδή διαπιστώνεται ότι η κάρτα είναι όντως δική σας. Το PIN είναι ένα κοινό μυστικό που γνωρίζετε μόνο εσείς και η τράπεζά σας.

Άλλο παράδειγμα αυθεντικοποίησης είναι η σύνδεση σ' ένα σύστημα πελάτη/διακομιστή (client/server). Ο διακομιστής ζητά ένα όνομα χρήστη κι έναν κωδικό από τον πελάτη για να μπορέσει

να συνδεθεί με το σύστημα. Στέλνοντας τα χωρίς κρυπτογράφηση, υπάρχει ο κίνδυνος κάποιος που “κρυφακούει” τη γραμμή να αποκτήσει την παραπάνω πληροφορία. Ένας τρόπος αντιμετώπισης είναι, αντί να στείλουμε τον κωδικό, να στείλουμε ένα ψηφιακό αποτύπωμά του. Ο διακομιστής με τη σειρά του, παράγει κι αυτός το ψηφιακό αποτύπωμα του κωδικού του χρήστη που έχει αποθηκευμένο και στη συνέχεια συγκρίνει τα δυο αποτυπώματα. Αν αυτά είναι ίδια, τότε ο χρήστης αυθεντικοποιείται.

Ωστόσο, η παραπάνω μέθοδος εξακολουθεί να μην είναι ασφαλής, καθώς είναι ευάλωτη στις επιθέσεις επανεκτέλεσης (replay attacks) ή ενδιάμεσου (man-in-the-middle attacks). Ο ενδιάμεσος που “κρυφακούει” χρησιμοποιεί ο ίδιος το κρυπτογραφημένο ψηφιακό αποτύπωμα για να συνδεθεί στο διακομιστή ως ο πελάτης. Για να αποφευχθεί κι αυτό το πρόβλημα, απαιτείται να προστεθεί στο αποτύπωμα κάποια πληροφορία που είναι μοναδική για τη διάρκεια της συνεδρίας, π.χ. ένα χρονικό αποτύπωμα κι ένας μοναδικός (τυχαίος) αριθμός, όπως κάνουν οι τράπεζες που μας δίνουν μια συσκευή για ηλεκτρονικές τραπεζικές συναλλαγές. Κάθε φορά που ο πελάτης στέλνει το ψηφιακό αποτύπωμα του συνθηματικού του,

στέλνει μαζί κι ένα μοναδικό ψευδοτυχαίο αριθμό ο οποίος χρησιμοποιείται για τη συγκεκριμένη μόνο συναλλαγή και δεν μπορεί να ξαναχρησιμοποιηθεί. Το χρονικό αποτύπωμα και ο τυχαίος αριθμός στέλνονται χωρίς κρυπτογράφηση στο διακομιστή για να μπορέσει να παράγει το ψηφιακό αποτύπωμα. Στη συνέχεια θα μιλήσουμε για τους τρεις τρόπους αυθεντικοποίησης που μπορείτε να χρησιμοποιήσετε στις ηλεκτρονικές συναλλαγές σας:

- Ψηφιακά αποτυπώματα μηνυμάτων (message digest)
- Ψηφιακές υπογραφές ως αποδεικτικά της εγκυρότητας των δεδομένων
- Πιστοποιητικά (certificates) ως θησαυροφυλάκια δημοσίων κλειδιών

Ψηφιακά αποτυπώματα

Οι πιο γνωστοί αλγόριθμοι παραγωγής ψηφιακών αποτυπωμάτων είναι οι εξής:

- MD5
- SHA

Το Java Security API διαθέτει την κλάση `java.security.MessageDigest` για τη

δημιουργία ψηφιακών αποτυπωμάτων. Μπορείτε να κατεβάσετε τον κώδικα από [εδώ](#).

```
/* *
 * Returns the digest of
 * <code>message</code>.
 * @param message a string to generate
 * its digest
 * @param algorithm algorithm to use,
 * e.g. SHA or MD5
 * @return digest of the message
 * @throws NoSuchAlgorithmException if
 * an unrecognized algorithm string is
 * passed
 */ String messageDigest(final String
message, final String algorithm)
throws
NoSuchAlgorithmException {
    MessageDigest md =
    MessageDigest.getInstance(algorithm);
    byte[] digest =
    md.digest(message.getBytes());
    Base64 encoder = new Base64();
    return encoder.encodeToString(digest);
}
```

Η έξοδος της παραπάνω μεθόδου:

```
Plain text input: This is a long
message!
Message digest:
neWNgutfQkbyB/5Hlfk1TEii6w0= }
```

MAC

Ίδια δουλειά με το ψηφιακό αποτύπωμα κάνει και ο Κώδικας Αυθεντικοποίησης Μηνύματος ή Message Authentication Code (MAC). Ο MAC παράγεται όπως και το ψηφιακό αποτύπωμα, με τη διαφορά ότι χρησιμοποιείται κι ένα κλειδί για την παραγωγή του αποτυπώματος, ώστε να προστατεύεται η ακεραιότητα των δεδομένων. Το Java Security API διαθέτει την κλάση `java.security.Mac` για τη δημιουργία MAC.

```
/* *
 * Generates a random secret key.
 * @param algorithm to use,
 * e.g. HmacSHA1, SHA etc.
 * @throws NoSuchAlgorithmException
 * if the algorithm string passed as a
 * parameter is not recognized */
private SecretKey generateKey(final
String algorithm) throws
NoSuchAlgorithmException {
    KeyGenerator keygen =
    KeyGenerator.getInstance(algorithm);
    keygen.init(new SecureRandom());
    return keygen.generateKey();
}
/* *
 * Returns the MAC of
 * <code>message</code>.
 * @param message a string to generate
 * its MAC
 * @param algorithm algorithm to use,
 * e.g. HmacSHA1
 * @return MAC of the message
```

```
* @throws NoSuchAlgorithmException if
an unrecognized algorithm string is
passed
* @throws InvalidKeyException if an
invalid key is used
*/
String Mac(final String message,
final String algorithm) throws
NoSuchAlgorithmException,
InvalidKeyException {
    SecretKey key =
    generateKey(algorithm);
    Mac mac =
    Mac.getInstance(algorithm);
    mac.init(key);
    byte[] digest =
    mac.doFinal(message.getBytes());
    Base64 encoder = new Base64();
    return
    encoder.encodeToString(digest);
} }
```

Θα πάρετε κάτι παρόμοιο με το παρακάτω:

```
Plain text input: This is a long
message!
MAC: xvyCTHc4IIdxng6z72TQEKpJBL0=
```

Ένας άλλος τρόπος παραγωγής του κλειδιού φαίνεται παρακάτω:

```
SecureRandom sr = new
SecureRandom();
byte[] keyBytes = new byte[20];
sr.nextBytes(keyBytes);
SecretKey key = new
SecretKeySpec(keyBytes, algorithm);
```

Εδώ χρησιμοποιείται η `SecretKeySpec` αντί της `KeyGenerator`. Η `SecureRandom` γεμίζει έναν πίνακα με τυχαία bytes και αυτός περνιέται στην `SecretKeySpec` για την παραγωγή του κλειδιού.

Ψηφιακές υπογραφές

Ας υποθέσουμε ότι θέλετε να στείλετε μια επιστολή στην τράπεζά σας στην Ελβετία, ζητώντας τους να κάνουν μια μεταφορά χρημάτων για την αγορά του νέου κότερου που αγοράσατε. Πώς μπορεί η τράπεζα να επιβεβαιώσει ότι όντως είστε εσείς αυτός που έστειλε την επιστολή κι όχι κάποιος επιτήδειος που θέλει να τραβήξει χρήματα απ' το λογαριασμό σας; Με τη 'χάρτινη' επιστολή, ο τραπεζίτης συγκρίνει την υπογραφή που βρίσκεται στην επιστολή με μια γνήσια υπογραφή που έχει στη διάθεσή του από τότε που ανοίξατε το λογαριασμό.

Πώς μπορούμε να προσομοιώσουμε την παραπάνω λειτουργία ηλεκτρονικά, με το ηλεκτρονικό ταχυδρομείο; Μα με τη χρήση ψηφιακών υπογραφών. 'Υπογράφοντας' ψηφιακά ένα κείμενο, επιβεβαιώνουμε ότι είμαστε εμείς αυτός που έστειλε την επιστολή κι όχι κάποιος τρίτος. Επίσης, απ' τη στιγμή που στείλαμε μια ψηφιακά υπογεγραμμένη επιστολή, δεν μπορούμε μετά ν' αρνηθούμε την αποστολή της, καθώς έχει τη δική μας ψηφιακή υπογραφή.

Πώς δουλεύουν οι ψηφιακές υπογραφές; Πολύ εύκολα. Είναι το ακριβώς ανάποδο της κρυπτογραφίας δημοσίου κλειδιού που περιγράψαμε στο προηγούμενο τεύχος. Αντί να κρυπτογραφήσουμε το μήνυμα με

το δημόσιο κλειδί, το κρυπτογραφούμε με το ιδιωτικό μας κλειδί. Έτσι, όποιος έχει στη διάθεσή του το δημόσιο κλειδί μας, μπορεί να επιβεβαιώσει ότι το μήνυμα προήλθε από εμάς και μόνο.

Μια ψηφιακή υπογραφή παρέχει δυο υπηρεσίες ασφαλείας: *αυθεντικοποίηση* και *ακεραιότητα* (integrity). Έτσι, όχι μόνο επιβεβαιώνει ότι ένα μήνυμα δεν έχει αλλάξει, αλλά και ότι ο αποστολέας είναι αυτός που λέει ότι είναι. Μια ψηφιακή υπογραφή δεν είναι τίποτ' άλλο από ένα ψηφιακό αποτύπωμα το οποίο κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα. Μόνο όποιος διαθέτει το δημόσιο κλειδί του αποστολέα μπορεί να αποκρυπτογραφήσει την ψηφιακή υπογραφή (αυθεντικοποίηση του αποστολέα). Αν το ψηφιακό αποτύπωμα του μηνύματος είναι το ίδιο με την αποκρυπτογραφημένη ψηφιακή υπογραφή τότε έχουμε και ακεραιότητα δεδομένων. Οι ψηφιακές υπογραφές δεν παράγουν όμως εμπιστευτικότητα (confidentiality) – ο οποιοσδήποτε μπορεί να διαβάσει το μήνυμα που συνοδεύει την ψηφιακή υπογραφή, αν αυτό δεν είναι κρυπτογραφημένο.

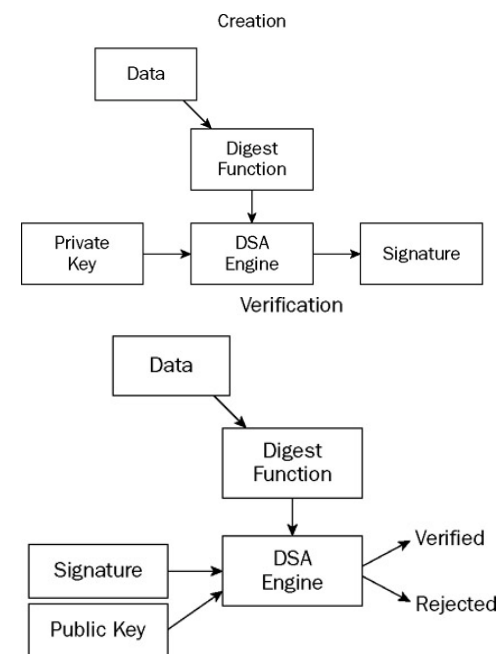
Το Java Security API διαθέτει την κλάση `java.security.Signature` για τη δημιουργία και την επαλήθευση ψηφιακών υπογραφών. Μπορείτε να κατεβάσετε το πρόγραμμα `DigitalSignatureExample` από [εδώ](#). Μια έξοδος του προγράμματος φαίνεται παρακάτω:

Plain text input: This is a long message!

Signature:

MCwCFHA49354heCfHhDmRINN2MR49UjIAhRsFuQOX53Eb0ajlPuJtASWEHWrcQ==

Verified: true Το πρόγραμμα διαθέτει δυο βασικές μεθόδους, την `createSignature(message, privateKey, algorithm)` και τη `verifySignature(message, signature, publicKey, algorithm)`. Η πρώτη δημιουργεί την ψηφιακή υπογραφή, χρησιμοποιώντας το ιδιωτικό κλειδί που παράχθηκε από την `generatePKI(algorithm)`, ενώ η δεύτερη ελέγχει τη γνησιότητα της ψηφιακής υπογραφής, χρησιμοποιώντας το δημόσιο κλειδί. Η λειτουργία του αλγορίθμου φαίνεται στο ακόλουθο σχήμα:



Σχήμα 1: Λειτουργία του αλγορίθμου

δημόσιου κλειδιού

Οι πιο γνωστοί αλγόριθμοι ψηφιακής υπογραφής, οι οποίοι βασίζονται στον RSA, είναι οι:

- DSA – Digital Signature Algorithm
- SHA with RSA
- PSS

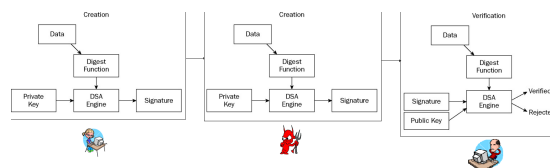
Χάρης στις βιβλιοθήκες JCE, οι αλλαγές που χρειάζεται να κάνετε στο παραπάνω πρόγραμμα είναι ελάχιστες. Κάντε τις εξής αλλαγές:

```
final String algorithm =
"SHA1withRSA"; /* OR SHA224withRSA OR
SHA256withRSA OR SHA1withRSAandMGF1
OR SHA256withRSAandMGF1 */
KeyPair keypair =
digitalSignature.generatePKI("RSA");
```

και προσθέστε τον πάροχο **BouncyCastle** όπως περιγράψαμε στο προηγούμενο τεύχος (αφήνεται ως άσκηση για τον αναγνώστη), για να δείτε τη χρήση των υπόλοιπων αλγορίθμων.

Πώς μπορούμε όμως να είμαστε σίγουροι ότι το δημόσιο και το ιδιωτικό κλειδί είναι όντως από το πρόσωπο που ισχυρίζονται ότι είναι κι όχι από κάποιον επιτήδειο; Ας δούμε την περίπτωση που φαίνεται στο παρακάτω σχήμα. Η Αλίκη υπογράφει τα δεδομένα της με το ιδιωτικό κλειδί της και τα στέλνει στο Βασίλη. Ο Βασίλης χρειάζεται το δημόσιο κλειδί της Αλίκης για να ελέγξει τη γνησιότητα της υπογραφής της Αλίκης. Η κακιά

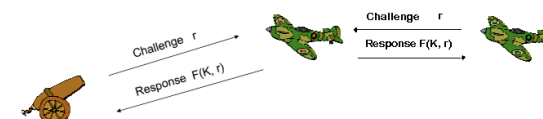
Εύα όμως, διανέμει το δημόσιο κλειδί της κάνοντας τον Βασίλη να νομίζει ότι είναι το κλειδί της Αλίκης. Όταν η Αλίκη στέλνει το υπογεγραμμένο μήνυμά της, η Εύα το αντιγράφει, το τροποποιεί όπως αυτή θέλει, το υπογράφει με το δικό της ιδιωτικό κλειδί και το στέλνει στο Βασίλη. Ο Βασίλης επιβεβαιώνει τη γνησιότητα της ψηφιακής υπογραφής της Εύας, νομίζοντας ότι πρόκειται για την ψηφιακή υπογραφή της Αλίκης και πείθεται ότι το μήνυμα είναι ένα γνήσιο μήνυμα που προέρχεται από την Αλίκη.



Σχήμα 2 Man-in-the-middle (ενδιάμεσος)

Άλλο παράδειγμα ενδιάμεσου φαίνεται στο ακόλουθο σχήμα. Η χώρα Α επιτίθεται στη χώρα Β. Η χώρα Β διαθέτει ένα σύγχρονο αντιαεροπορικό σύστημα το οποίο στέλνει μια ερώτηση-πρόκληση r σε κάθε αεροσκάφος που στοχεύει. Αν το IFF του αεροσκάφους απαντήσει σε εύλογο χρονικό διάστημα με τη σωστή απάντηση $F(K, r)$ τότε το αντιαεροπορικό αντιλαμβάνεται ότι πρόκειται για φίλο αεροσκάφος και δεν το καταρρίπτει, διαφορετικά βάλλει κατ' αυτού. Χωρίς όμως η χώρα Β να το γνωρίζει, η χώρα Α έχει εξοπλιστεί κι αυτή με το ίδιο σύστημα ανταπόκρισης στις προκλήσεις r . Ένα αεροσκάφος της χώρας Α, παρόλο

που δεν γνωρίζει τι ν' απαντήσει στις προκλήσεις της χώρας Β, στέλνει την ερώτηση πρόκληση r ένα αεροσκάφος της χώρας Β, το οποίο, νομίζοντας ότι είναι ερώτηση του αντιαεροπορικού, στέλνει ευχαρίστως τη σωστή απάντηση την οποία το αεροσκάφος της χώρας Α αναμεταδίδει στο αντιαεροπορικό κι έτσι αποφεύγει την κατάρριψη. Έτσι, στην ουσία αχρηστεύεται το αντιαεροπορικό σύστημα της χώρας Β.



Σχήμα 3 Man-in-the-middle

Πιστοποιητικά και Αρχές Πιστοποίησης

Πώς λοιπόν μπορούμε να αντιμετωπίσουμε το πρόβλημα του ενδιάμεσου; Το πρόβλημα που είχαμε με τη συμμετρική κρυπτογραφία ήταν αυτό της ασφαλούς διανομής του μυστικού κλειδιού. Με την κρυπτογραφία δημόσιου κλειδιού το παραπάνω πρόβλημα μετατράπηκε σε πρόβλημα αυθεντικοποίησης, δηλαδή διαπίστωσης του αν το δημόσιο κλειδί που διαθέτουμε ανήκει όντως στην οντότητα που ισχυρίζεται ότι ανήκει.

Όπως είπαμε, για να αποκρυπτογραφήσουμε μια ψηφιακή υπογραφή χρειαζόμαστε το δημόσιο κλειδί του αποστολέα. Πώς μπορούμε όμως να διανεύουμε δημόσια κλειδιά με ασφαλή τρόπο; Ακόμα κι αν είχαμε τη δυνατότητα να κατεβάσουμε το κλειδί από την ιστοσελίδα

του αποστολέα, πώς μπορούμε να είμαστε σίγουροι ότι δεν είναι πλαστό; Η απάντηση είναι η χρήση πιστοποιητικών. Ένα πιστοποιητικό είναι μια επιβεβαίωση ενός τρίτου προσώπου ότι το δημόσιο κλειδί ενός προσώπου είναι έγκυρο. Για να συμβεί αυτό, θα πρέπει το τρίτο πρόσωπο που υπογράφει την επιβεβαίωση να εμπιστεύεται το άλλο πρόσωπο.

Στην κρυπτογραφία, ένα πιστοποιητικό συσχετίζει μια οντότητα ή αλλιώς, ένα υποκείμενο μ' ένα δημόσιο κλειδί. Η οντότητα που υπογράφει το πιστοποιητικό είναι ο υπογράφων. Το πιστοποιητικό περιέχει πληροφορίες για τον υπογράφοντα, το υποκείμενο και το δημόσιο κλειδί του υποκειμένου. Υπογράφεται κρυπτογραφικά και η υπογραφή αυτή συμπεριλαμβάνεται επίσης στο πιστοποιητικό. Με άλλα λόγια, σ' ένα πιστοποιητικό περιλαμβάνονται:

- πληροφορίες για το υποκείμενο (το πρόσωπο)
- το δημόσιο κλειδί του υποκειμένου
- πληροφορίες για τον εκδότη
- η ψηφιακή υπογραφή του εκδότη

Αυτό επιτυγχάνεται με τη χρήση των Αρχών Πιστοποίησης ή Certification Authorities (CA). Πρόκειται για έμπιστους οργανισμούς που αναλαμβάνουν τη διαχείριση των δημόσιων κλειδιών. Η πιο γνωστή τέτοια αρχή είναι η **Verisign**. Η Αρχή Πιστοποίησης εκδίδει ένα πιστοποιητικό για το δημόσιο κλειδί κάθε πιστοποιημένου χρήστη της. Πώς ακριβώς δουλεύει αυτό; Κάθε χρήστης

που θέλει να πιστοποιηθεί, στέλνει το δημόσιο κλειδί του στην CA μαζί με ιδιωτικές πληροφορίες, όπως π.χ. το όνομά του, την ημερομηνία λήξης του πιστοποιητικού κλπ. Η CA χρησιμοποιεί όλες αυτές τις πληροφορίες για να εκδώσει το πιστοποιητικό, το οποίο και στέλνει στο χρήστη. Παλιότερα η υπηρεσία αυτή ήταν δωρεάν, σήμερα, νομίζω ότι δεν υπάρχει οργανισμός πιστοποίησης που να παράγει πιστοποιητικά χωρίς κάποια χρέωση. Αν λοιπόν θέλετε να μάθετε αν το δημόσιο κλειδί του χρήστη X είναι γνήσιο, αρκεί να λάβετε το δημόσιο κλειδί της CA η οποία έχει παράγει το πιστοποιητικό του δημόσιου αυτού κλειδιού, και ,να επιβεβαιώσετε ότι το δημόσιο κλειδί του χρήστη X ανήκει όντως σ' αυτόν. Η όλη φιλοσοφία δουλεύει ως εξής: αν εμπιστεύεστε το κλειδί της CA, τότε εμπιστεύεστε κι όλα τα κλειδιά που έχουν εκδοθεί από τη CA. Βέβαια ο προσεκτικός αναγνώστης θα διερωτηθεί, τι ελέγχους κάνει η CA για να ελέγξει ότι όντως είναι ο χρήστης X αυτός που ζητάει το πιστοποιητικό του δημόσιου κλειδιού του χρήστη X κι όχι κάποιος επιτήδειος; Απ' όσο γνωρίζω, για μεγάλες εταιρίες και οργανισμούς, γίνεται όντως έλεγχος κι άρα το παραγόμενο πιστοποιητικό έχει αξία. Για ιδιώτες όμως, όπως εγώ κι εσείς, δεν γίνεται κάποιος έλεγχος. Οπότε, εν τέλει, ούτε αυτό το δίκτυο αρχών πιστοποίησης είναι εντελώς ασφαλές. Π.χ., η Verisign διαθέτει πιστοποιητικά κλάσεων 1, 2 και 3, όπου μόνο στο 3 γίνεται εξονυχιστικός έλεγχος του αιτούντος του πιστοποιητικού. Οι περιηγητές διαθέτουν πιστοποιητικά από

πολλές αρχές πιστοποίησης. Π.χ., στον Firefox πηγαίνετε στο μενού Επεξεργασία > Προτιμήσεις > Για προχωρημένους > καρτέλα Κρυπτογράφηση και πατήστε το κουμπί Προβολή πιστοποιητικών για να δείτε μια λίστα από CA. Τελευταία, έχει δημιουργηθεί μια ανεξάρτητη αρχή, η **CACert**, η οποία παράγει πιστοποιητικά για ιδιώτες. Βασίζεται σ' ένα δίκτυο εμπιστοσύνης που χτίζετε γύρω σας. Η Java, από το JDK 1.2 και μετά, υποστηρίζει την εισαγωγή και πιστοποίηση πιστοποιητικών X.509v3 αλλά όχι τη δημιουργία τους. Ήδη μιλήσαμε για τις αρχές πιστοποίησης που σκοπός τους είναι η διαχείριση των πιστοποιητικών των χρηστών. Άλλοι τρόποι παραγωγής πιστοποιητικών είναι οι παρακάτω:

- SSL – Secure Socket Layer
- PGP – Pretty Good Privacy
- SPKI – Simple Public Key Infrastructure
- IBC – Identity Based Cryptography

Επίλογος

Στο τρίτο και τελευταίο μιας σειράς άρθρων για την κρυπτογραφία, μιλήσαμε για τους τρόπους αυθεντικοποίησης, τις ψηφιακές υπογραφές και τις Αρχές Πιστοποίησης.

Ελπίζω ότι τόσο οι έννοιες όσο και τα προγράμματα θα σας φανούν χρήσιμα στις δικές σας εφαρμογές.

(συνεχίζεται στη σελίδα 25)

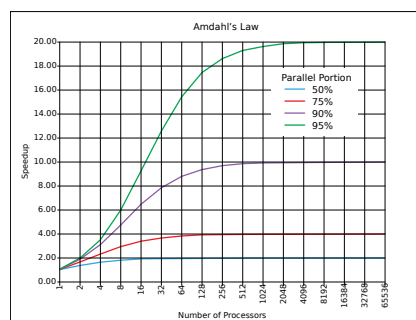
Parallel computing

OpenMP.

Όλο και πιο συχνά ακούγεται στις μέρες μας ο όρος parallel computing, ή «παράλληλοι υπολογισμοί», και έχει γίνει πλέον πραγματικότητα και στους προσωπικούς υπολογιστές, με επεξεργαστές διπλών και τρίδιπλων (όπως το λαϊκό) πυρήνων. Αλλά ποιος ο λόγος, και υπάρχει πράγματι κέρδος από τους επεξεργαστές με δύο πυρήνες ή είναι απλώς ένα εμπορικό παιχνίδι των εταιριών για να αυξήσουν τα κέρδη τους; Σε αυτήν την ερώτηση δυστυχώς αδυνατώ να απαντήσω, αλλά θα σας δώσω μια απλή γεύση του πώς μπορούμε να εκμεταλλευτούμε τις δυνατότητες αυτών των επεξεργαστών. Με τον όρο παράλληλοι υπολογισμοί εννοούμε ότι ένας μεγάλος όγκος υπολογισμών χωρίζεται σε επιμέρους υπολογισμούς οι οποίοι πραγματοποιούνται παράλληλα, δηλαδή ταυτόχρονα [1]. Υπάρχουν πολλές διαφορετικές μορφές παράλληλων υπολογισμών, ανάλογα με το επίπεδο στο οποίο πραγματοποιείται η παραλληλοποίηση, πχ. σε επίπεδο δεδομένων, διεργασιών, κ.α.

Όποιος κι αν είναι ο τρόπος παραλληλοποίησης, το βασικό δομικό στοιχείο στους υπολογιστές είναι ο επεξεργαστής. Όπως θα έχετε

συνειδητοποιήσει, συνεχώς βγαίνουν καλύτεροι επεξεργαστές. Μάλιστα, η βελτίωση αυτή έχει ποσοτικοποιηθεί. Ο νόμος του Amdahl [2], προς τιμή του αρχιτέκτονα υπολογιστών Gene Amdahl, περιγράφει ακριβώς αυτή τη βελτίωση στην ταχύτητα των επεξεργασιών, βλ. Εικόνα 1.

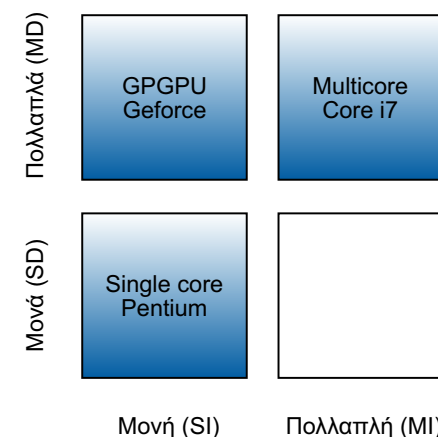


Εικόνα 1: Ο νόμος του Amdahl.

Πριν εμφανιστούν οι πρώτοι πολυπύρρηνοι (multi-core) επεξεργαστές ο νόμος προέβλεπε αύξηση στην ταχύτητα, αλλά η φυσική απέκλειε περαιτέρω μειώσεις στο μέγεθος των επεξεργασιών. Κι όμως η ανθρώπινη δημιουργικότητα βρήκε τρόπο να εξελιχθεί κι έτσι εμφανίστηκαν οι πρώτοι πολυπύρρηνοι επεξεργαστές.

Όπως είπαμε στην αρχή, υπάρχουν διάφορα είδη παραλληλοποίησης. Τα δύο βασικά αφορούν δεδομένα (data) και

οδηγίες (instructions). Σύμφωνα με αυτή την κατηγοριοποίηση υπάρχουν 4 δυνατοί συνδυασμοί [3], όπως φαίνεται και στην Εικόνα 2.



Εικόνα 2: Κατηγοριοποίηση των σύγχρονων επεξεργασιών.

Ο απλός Pentium πραγματοποιεί μία οδηγία σε ένα μόνο δεδομένο, αντίθετα η κάρτα γραφικών GeForce πραγματοποιεί μία οδηγία σε πολλά δεδομένα, τα οποία αντιστοιχούν, χοντρικά, στα pixels της οθόνης. Ο δε επεξεργαστής Core i7 μπορεί να πραγματοποιεί πολλαπλές οδηγίες σε πολλαπλά δεδομένα. Τέλος, ακόμη δεν υπάρχει καμία εφαρμογή για επεξεργαστές που εφαρμόζουν πολλαπλές

οδηγίες σε ένα μόνο δεδομένο. Ίσως στο όχι και τόσο μακρινό μέλλον. Κάποιος θα μπορούσε εδώ να πει «Ωραία, τότε γιατί δε φτιάχνουμε μόνο core i7 ακόμη και για κάρτες γραφικών;» Η απάντηση είναι απλή: το πλήθος των δεδομένων διαφέρει. Υπάρχει βέβαια και το αντίστροφο ερώτημα, «Γιατί δε χρησιμοποιούμε κάρτες γραφικών όπως η NVIDIA Tesla για να κάνουμε τους υπολογισμούς μας αφού είναι τόσο καλές;» Η αλήθεια είναι ότι οι κάρτες γραφικών νέας γενιάς έχουν τη δυνατότητα να εφαρμόζουν μία οδηγία σε ένα μεγάλο πλήθος δεδομένων. Ο νέος υπερυπολογιστής που βρίσκεται πρώτος στη λίστα των 500 γρηγορότερων υπολογιστών παγκοσμίως [4] χρησιμοποιεί κάρτες γραφικών NVIDIA. Ο λόγος που δεν τις χρησιμοποιούμε κι εμείς στους προσωπικούς υπολογιστές, εκτός από το κόστος, είναι ότι χρειάζονται ειδικό προγραμματισμό σύμφωνα με το API CUDA [5] ή OpenCL.

Αφήνοντας τις κάρτες γραφικών προς το παρόν, οι παράλληλοι υπολογιστές χωρίζονται σε δύο βασικές κατηγορίες: shared και distributed μνήμης υπολογιστές. Οι πρώτοι, με shared memory, είναι αυτοί που έχουμε στους υπολογιστές μας, όπου ο κάθε επεξεργαστής (στο σημείο αυτό δε θα τους ξεχωρίσω από τους πυρήνες) μοιράζεται την ίδια μνήμη με όλους τους υπόλοιπους. Οι distributed memory υπολογιστές έχουν ο καθένας δική του μνήμη και επικοινωνούν μέσω δικτύου [6]. Προφανώς, αν έχουμε 100

επεξεργαστές είναι λίγο δύσκολο να τους καλωδιώσουμε ώστε να μοιράζονται την ίδια μνήμη, ίσως στο μέλλον. Η δημιουργία, ο προγραμματισμός και η χρήση distributed memory είναι αρκετά προχωρημένα θέματα και δε θα ασχοληθώ εδώ καθόλου.

Ας συνεχίσουμε λοιπόν με shared memory υπολογιστές, δηλαδή τους πολυπύρηνους επεξεργαστές που έχουμε στους υπολογιστές μας. Για τα παρακάτω θα χρειαστεί να εγκαταστήσουμε τα πακέτα:

```
sudo apt-get install build-essential
sudo apt-get install libgomp
```

Το build-essential περιέχει όλα τα απαραίτητα πακέτα για προγραμματισμό και ανάπτυξη κώδικα, ενώ το libgomp περιέχει τη βιβλιοθήκη για shared memory parallel programming. Αναλυτικές οδηγίες για την gnu openMP μπορούν να βρεθούν στην ιστοσελίδα της [7].

Θα ξεκινήσω με ένα απλό hello world πρόγραμμα σε C. Δημιουργούμε καταρχάς ένα φάκελο mkdir /testgomp cd /testgomp Ανοίγουμε μέσα στο φάκελο testgomp με το gedit το αρχείο hello.c και εισάγουμε τα παρακάτω:

```
#include <stdio.h>
int main()
{
    printf("Hello world\n");
}
```

Το μεταγλωττίζουμε και δημιουργούμε το εκτελέσιμο με:

```
gcc -c hello.c
gcc -o serialtest hello.o
```

Εκτελούμε το πρόγραμμα που δημιουργήθηκε με ./serialtest και βλέπουμε ότι εκτυπώνεται στην οθόνη Hello world μόνο μία φορά.

Τώρα προσθέτουμε τη γραμμή #pragma omp parallel. Δηλαδή, το αρχείο γίνεται:

```
#include <omp.h>
#include <stdio.h>
int main()
{
    #pragma omp parallel
    printf("Hello world\n");
}
```

Το μεταγλωττίζουμε (τώρα χρειάζεται επίσης να συνδέσουμε την αντίστοιχη βιβλιοθήκη) και δημιουργούμε το εκτελέσιμο με:

```
gcc -c -fopenmp hello.c
gcc -o paralleltest hello.o
```

Εκτελούμε τώρα το παράλληλο πρόγραμμα με ./paralleltest και βλέπουμε να τυπώνεται δύο φορές ενώ υπάρχει μόνο μία φορά στον κώδικά μας, και φυσικά δεν υπάρχει κανένας βρόχος. (Βέβαια, αν έχουμε επεξεργαστή με ένα μόνο πυρήνα δε θα δούμε διαφορά) Η γραμμή #pragma omp parallel γίνεται αντιληπτή από το μεταγλωττιστή gcc σαν σχόλιο αν δεν υπάρχει η επιλογή -fopenmp κατά τη μεταγλώττιση, πράγμα που καθιστά αρκετά portable τα προγράμματα που γράφουμε.

Προφανώς, αυτό το πρόγραμμα δεν είναι και πολύ χρήσιμο γιατί επαναλαμβάνει

την ίδια δουλειά δύο φορές. Εμείς χρειαζόμαστε κάτι που να μοιράζει το φόρτο εργασίας στους δύο επεξεργαστές. Ας δημιουργήσουμε λοιπόν ένα άλλο αρχείο hello2.c που θα περιέχει τα εξής:

```
#include <omp.h>
#include <stdio.h>

#define N 100000
int main()
{
    int i, a[N];
    #pragma omp parallel for
    for (i=0;i<N;i++)
        a[i]= 2*i;
    return 0;
}
```

Η μεταγλώττιση γίνεται όπως πάντα με:

```
gcc -c -fopenmp hello2.c
gcc -o parallelttest2 hello2.o
```

Το συγκεκριμένο παράδειγμα μοιράζει αυτόματα το array a[N] στα δύο threads που δημιουργούνται. Τα αποτελέσματα είναι σωστά γιατί το δεξί μέλος της ισότητας δεν εξαρτάται από το αριστερό.

Έστω όμως ότι είχαμε αυτήν την περίπτωση:

```
#include <omp.h>
#include <stdio.h>

#define N 100000
int main()
{
    int i, a[N];
```

```
    a[0]=0;
    #pragma omp parallel for
    for (i=1;i<N;i++)
        a[i]= a[i-1]+1;
    return 0;
}
```

Εδώ ο κώδικας δεν θα λειτουργούσε γιατί κάθε επόμενο στοιχείο του a εξαρτάται από το προηγούμενο. Άρα για να υπολογιστεί το στοιχείο 50000 στο δεύτερο thread απαιτείται το 49999 από το πρώτο thread, το οποίο δεν έχει υπολογιστεί ακόμη.

Φυσικά, μπορούμε να ορίσουμε μεταβλητές οι οποίες φαίνονται μόνο μέσα σε κάθε thread, σε αντίθεση με το a στο προηγούμενο παράδειγμα. Στο παρακάτω παράδειγμα η μεταβλητή th_id είναι ιδιωτική, δηλαδή σε κάθε thread έχει διαφορετική τιμή. Επίσης, εδώ έχουμε μια barrier, δηλαδή κάθε thread περιμένει μέχρι όλα τα υπόλοιπα threads να φτάσουν στο ίδιο σημείο και μετά συνεχίζει την εκτέλεση. Κάτι τέτοιο μπορεί να χρειάζεται όταν δεδομένα από τα υπόλοιπα threads είναι απαραίτητα για τη συνέχιση του προγράμματος.

```
#include <omp.h>
#include <stdio.h>
#include <stdlib.h>

int main (int argc, char *argv[]) {
    int th_id, nthreads;
    #pragma omp parallel private(th_id)
    {
        th_id = omp_get_thread_num();
        printf("Hello World from thread %d\n",
            th_id);
```

```
    #pragma omp barrier
    if ( th_id == 0 ) {
        nthreads = omp_get_num_threads();
        printf("There are %d threads\n",
            nthreads);
    }
    return EXIT_SUCCESS;
}
```

Περισσότερες πληροφορίες σχετικά με προγραμματισμό για shared memory μπορούν να βρεθούν στους συνδέσμους [7,8,9].

Βιβλιογραφία

1. http://en.wikipedia.org/wiki/Parallel_computing
2. http://en.wikipedia.org/wiki/Amdahl's_law
3. Linux Magazin, Τεύχος 07/10.
4. <http://www.top500.org/>
5. <http://en.wikipedia.org/wiki/CUDA>
6. http://en.wikipedia.org/wiki/Distributed_computing
7. <http://openmp.org/wp/>
8. <http://gcc.gnu.org/onlinedocs/libgomp/>
9. <http://en.wikipedia.org/wiki/OpenMP>

Scheme

Μια πολύ σύντομη εισαγωγή στο συναρτησιακό προγραμματισμό.

Στον προγραμματισμό υπάρχουν διάφορες τεχνικές (paradigms στα Αγγλικά), όπως π.χ. δομικός προγραμματισμός, αντικειμενοστραφής προγραμματισμός και συναρτησιακός προγραμματισμός. Στο συναρτησιακό προγραμματισμό το βασικό στοιχείο είναι η συνάρτηση. Η ιδέα του συναρτησιακού λογισμού βασίζεται στην λάμδα ανάλυση, ένα μαθηματικό εργαλείο που αναπτύχθηκε για τη μελέτη συναρτήσεων και αναδρομικών ορισμών. Η πρώτη γλώσσα προγραμματισμού που βασίστηκε στο συναρτησιακό προγραμματισμό ήταν η lisp, η οποία είναι και η δεύτερη αρχαιότερη γλώσσα προγραμματισμού. Άλλες γλώσσες συναρτησιακού προγραμματισμού είναι η scheme (μια από τις διαλέκτους της lisp), η haskell, η erlang, η OCaml, καθώς και κάποιες οι οποίες περιέχουν στοιχεία συναρτησιακού προγραμματισμού.

Ένα από τα βασικά χαρακτηριστικά της lisp και της scheme είναι το prefix notation (προθεματική σημειογραφία). Ενώ στις συνήθεις γλώσσες προγραμματισμού ο τελεστής είναι μεταξύ των δύο αντικειμένων, για παράδειγμα $1 + 2$, σύμφωνα με το prefix notation αυτό γράφεται $+ 1 2$. Για να αποφεύγονται παρανοήσεις χρησιμοποιούνται παρενθέσεις $(+ 1 2)$. Επίσης, η scheme είναι interpreted γλώσσα,

οπότε μπορούμε να ανοίξουμε (αφού φυσικά τον εγκαταστήσουμε) τον scheme interpreter, scsh, και να γράψουμε:

```
> (+ 1 2)
3
```

Ο τελεστής εφαρμόζεται σε όλα τα στοιχεία μέσα στην παρένθεση διαδοχικά, δηλαδή:

```
> (+ 1 2 3)
6
```

Η χρήση παρενθέσεων οδηγεί σε μια ωραία γενίκευση του prefix notation, όπως στο παράδειγμα:

```
> (+ (* 3 5) (- 10 6))
19
```

Ο ορισμός των μεταβλητών στη scheme γίνεται με χρήση του τελεστή define. Π.χ.:

```
(define size 2)
```

Αυτή η έκφραση δίνει στη μεταβλητή size την τιμή 2. Την τιμή της μεταβλητής μπορούμε να την ελέγξουμε πληκτρολογώντας size.

Με τη χρήση του define μπορούμε να ορίσουμε και συναρτήσεις. Π.χ.:

```
> (define (square x) (* x x))
```

Έτσι ορίζεται μια συνάρτηση η οποία επιστρέφει το τετράγωνο ενός αριθμού.

```
> (square 2)
4
```

Για να υπολογίσουμε τον τύπο $x^2 + y^2$ θα γράψουμε:

```
> (define (sum-of-squares x y)
  (+ (square x) (square y)))
> (sum-of-squares 3 4)
25
```

Απλό και ωραίο, σωστά;

Ας υποθέσουμε τώρα ότι θέλουμε να τυπώσουμε κάτι στην οθόνη. Ας δούμε το πολυσυζητημένο πρόγραμμα «hello world»:

```
> (define (hello) (display "hello world")
  (newline))
> (hello)
hello world
```

Όπως και προηγουμένως, ορίζουμε μια συνάρτηση, αυτή τη φορά χωρίς κανένα όρισμα, η οποία δείχνει στην οθόνη το hello world και μια καινούρια γραμμή.

Βιβλιογραφία

1. http://en.wikipedia.org/wiki/Functional_programming
2. [http://en.wikipedia.org/wiki/Scheme_\(programming_language\)](http://en.wikipedia.org/wiki/Scheme_(programming_language))

Sympy

Συμβολικά μαθηματικά με την python.

Ποιος είπε ότι η python δεν ενδείκνυται για συμβολικά μαθηματικά; Σίγουρα υπάρχουν πολλά πακέτα για συμβολικά μαθηματικά, αλλά αν μπορεί κανείς να συνδυάσει μια σύγχρονη γλώσσα προγραμματισμού, τις αριθμητικές δυνατότητες που προσφέρουν τα πακέτα numpy και scipy, και τα συμβολικά μαθηματικά, τότε δε λείει όχι.

Το πακέτο sympy, αφού εγκατασταθεί, μπορεί να χρησιμοποιηθεί μέσα από την python πολύ απλά:

```
>>>from sympy import *
```

Το πρώτο που πρέπει να κάνουμε είναι να ορίσουμε τα σύμβολα που θα χρησιμοποιήσουμε, για παράδειγμα:

```
>>>x = Symbol('x')
```

Έπειτα μπορούμε να υπολογίσουμε αναλυτικά όρια συναρτήσεων, π.χ:

```
>>>limit(sin(pi*x)/x, x, 0)
pi
```

Ακόμη, μπορούμε να ολοκληρώσουμε συναρτήσεις:

```
>>>integrate(x + sinh(x), x)
(1/2*x**2 + cosh(x))
```

Ή και να τις παραγωγίσουμε:

```
>>>diff(_, x)
x + sinh(x)
```

Το `_` αναφέρεται στο αποτέλεσμα της προηγούμενης πράξης.

Επίσης, μπορούμε να ορίσουμε πίνακες με σύμβολα ως στοιχεία και να υπολογίσουμε τις ιδιοτιμές του πίνακα. Για παράδειγμα:

```
>>>var('mu')
mu
>>>M = Matrix(4, 4, lambda i,j: i*j + mu)
>>>M
[mu mu mu mu ]
[
[mu 1+mu 2+mu 3+mu]
[
[mu 2+mu 4+mu 6+mu]
[
[mu 3+mu 6+mu 9+mu]
>>>M.eigenvalues()
{7+2*mu+(-80*mu+(14+4*mu)**2)**(1/2)/2: 1,
7+2*mu-(-80*mu+(14+4*mu)**2)**(1/2)/2: 1,
0: 2}
```

Αλγεβρικές εξισώσεις μπορούν να επιλυθούν εξίσου απλά. Η 4ου βαθμού εξίσωση $x^4 - 1 = 0$ μπορεί να λυθεί:

```
>>>solve(x**4-1,x)
[i, 1, -1, -i]
```

Όπως βλέπετε, η παραπάνω εξίσωση έχει 2 πραγματικές και 2 φανταστικές λύσεις.

Εάν θέλουμε να μεταβούμε από τα συμβολικά μαθηματικά σε αριθμητικά αποτελέσματα, δεν έχουμε παρά να τα υπολογίσουμε. Για παράδειγμα, το άθροισμα $\sum_{i=1}^{\infty} 1/n * *n$ υπολογίζεται αριθμητικά:

```
>>>Sum(1/n**n, (n, 1, oo)).evalf()
1.29128599706266
```

Οι δυνατότητες του sympy δεν περιορίζονται σε απλές συναρτήσεις και πράξεις, αλλά επεκτείνονται και σε συναρτήσεις θεωρίας αριθμών, στην άλγεβρα πολυωνύμων, τον υπολογισμό σειρών, την επίλυση αλγεβρικών εξισώσεων, τις κατανομές πιθανότητας, τις διαφορικές εξισώσεις, κ.α. Παράλληλα με το sympy έχουν αναπτυχθεί και άλλα πακέτα που βασίζονται στο sympy, π.χ. για χρήση τανυστών. Τέλος, να μη ξεχνάμε ότι τα αποτελέσματα μπορούν να αποθηκευτούν κατευθείαν και ως τύποι latex.

Βιβλιογραφία

1. <http://code.google.com/p/sympy/>

του Κωστήρα Γιάννη

Χρήσιμα «κόλπα» αναζήτησης που δεν ξέρατε

Google Search Tips

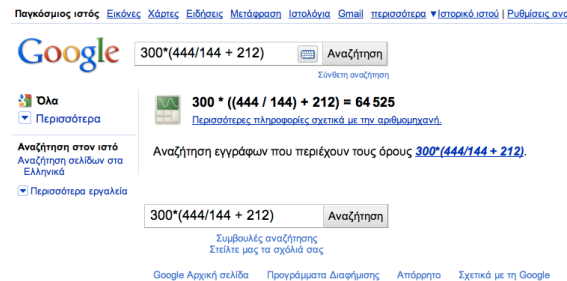
Πριν από λίγο καιρό έλαβα ένα email με «κόλπα» αναζήτησης της μηχανής Google. Ο συγγραφέας του email δυστυχώς άγνωστος. Το παρακάτω άρθρο βασίζεται σ' εκείνο το email, του άγνωστου συγγραφέα, εμπλουτισμένο με μερικά ακόμα «κόλπα», στον οποίο αφιερώνεται και τον ευχαριστούμε.

Η μηχανή αναζήτησης της Google είναι ίσως η ισχυρότερη και πιο διαδεδομένη στο διαδίκτυο. Έχει γίνει μάλιστα μέρος της καθημερινότητάς μας, αφού ακόμα και για σχετικά απλές απορίες, ερωτήσεις και αναζητήσεις στο Google καταφεύγουμε πλέον.

Δεν είναι τυχαίο άλλωστε που η έκφραση «Google it» έχει περάσει ακόμα και στα λεξικά της αμερικανικής και αγγλικής γλώσσας.

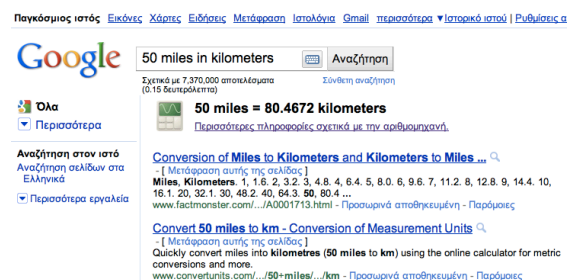
Δείτε λοιπόν μερικά χρήσιμα «κόλπα» που μπορείτε να χρησιμοποιήσετε στην βασική μηχανή αναζήτησης της Google για να έχετε καλύτερα αποτελέσματα.

1. Το πεδίο αναζήτησης είναι και αριθμομηχανή. Πληκτρολογήστε οποιαδήποτε πράξη με τον ίδιο τρόπο που θα το κάνετε και στον υπολογιστή σας και θα δείτε απευθείας το αποτέλεσμα.



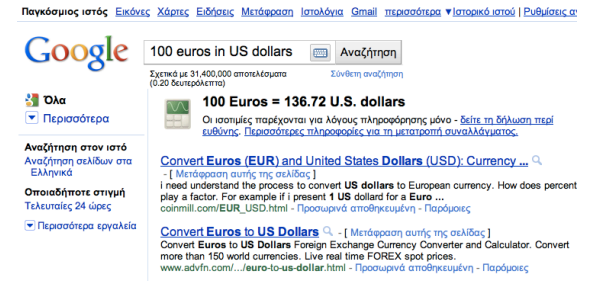
Αριθμομηχανή

2. Δοκιμάστε να μετατρέψετε μονάδες μέτρησης από το ένα σύστημα στο άλλο, πληκτρολογώντας ολογράφως αυτό που ψάχνετε.



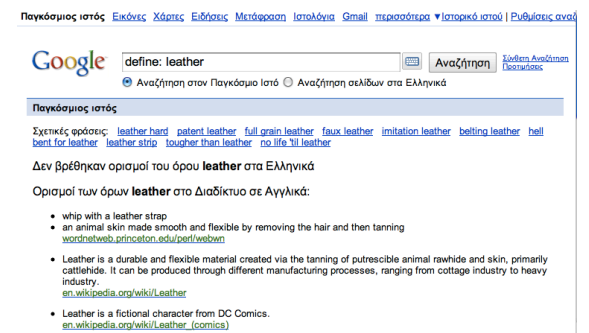
Μετατροπή μονάδων μέτρησης

3. Εκτός από μετατροπές μονάδων μέτρησης, το πεδίο αναζήτησης του Google μπορεί να χρησιμοποιηθεί και για μετατροπές νομισμάτων.



Μετατροπή ισοτιμιών νομισμάτων

4. Χρησιμοποιήστε το πεδίο αναζήτησης ως διαδικτυακό λεξικό. Για να βρείτε τον ορισμό μιας λέξης, πληκτρολογήστε «define:» και τη λέξη που θέλετε.



Λεξικό

5. Μπορείτε, αν επιθυμείτε, να περιορίσετε τα αποτελέσματα της αναζήτησής σας σε εκείνα που προκύπτουν από ένα και μόνο site. Πληκτρολογήστε τη λέξη/φράση που ψάχνετε, αφήστε ένα κενό

και μετά γράψτε «site:» και το όνομα του site.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστοί Ρυθμίσεις α

Google ubuntu site:in.gr Αναζήτηση

Σχετικά με 733 αποτελέσματα (0.39 δευτερόλεπτα)

in.gr - Διαθέσιμο για κατέβασμα το **Ubuntu 9.10 - Τεχνολογία - Ειδήσεις** 29 Οκτ. 2009 ... Το πιο φιλικό λειτουργικό σύστημα στον κόσμο φιλοδοξεί να καταστήσει το **Ubuntu** η Canonical. Η νέα έκδοση είχε προγραμματιστεί να διατεθεί ... tech.in.gr/news/article?aid=103140 - Προσωρινά αποθηκευμένη

in.gr - Wubi, το νέο πρόγραμμα εγκατάστασης των **Ubuntu** ... To Wubi είναι ένα πρόγραμμα εγκατάστασης των **Ubuntu** για τους χρήστες των Windows που θα τους φέρει πιο κοντά στον κόσμο του Linux με έναν κλικ ... tech.in.gr/news/article?aid=100286 - Προσωρινά αποθηκευμένη

in.gr - Διαθέσιμο για κατέβασμα το **Ubuntu 9.10** ... Μορφή αρχείου: PDF/Adobe Acrobat 3 Δεκ. 2009 ... Το πιο φιλικό λειτουργικό σύστημα στον κόσμο φιλοδοξεί να καταστήσει το **Ubuntu** η Canonical. Η νέα έκδοση είχε προγραμματιστεί να διατεθεί ... tech.in.gr/ajax.aspx?m=Common.Pdf&Name=Article&id=1&aid=...

Αναζήτηση στον ιστό
Αναζήτηση σε άλλους στα
Ελληνικά

Κανονικά αποτελέσματα
Ιστοτόπο με εικόνες

▼ Περισσότερα εργαλεία

Περιορισμός αναζήτησης σ' ένα μόνο site

6. Για να δείτε αποτελέσματα αναζήτησης για συγκεκριμένη χρονική περίοδο, πληκτρολογήστε το κάτω (X) και άνω όριο (Y) αυτής της χρονικής περιόδου μετά την λέξη/φράση, ως εξής: «X..Y» (ή «numrange:X-Y»).

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστοί Ρυθμίσεις α

Google US presidents 1950..1970 Αναζήτηση

Σχετικά με 11,700,000 αποτελέσματα (0.19 δευτερόλεπτα)

Dwight D. Eisenhower | **The White House** - [Μετάφραση αυτής της σελίδας] In 1953, the signing of a truce brought an armed peace along the border of South Korea ... The President proposed that the **United States** and Russia exchange ... www.whitehouse.gov/.../presidents/dwighteisenhower - Προσωρινά αποθηκευμένη - Παράνομος

Presidents of the United States (POTUS) - [Μετάφραση αυτής της σελίδας] Attorney for U.S. Office of Emergency Management, 1942; Member of U.S. House of Representatives, 1947-51; **United States Senator**, 1951-53; Vice President, ... www.jpil.org/div1/jmixon.html - Προσωρινά αποθηκευμένη - Παράνομος

POTUS -- **Presidents of the United States** - [Μετάφραση αυτής της σελίδας] 19 Jan 2009 ... POTUS: **Presidents of the United States** ... Harry S. Truman, 1945-1953; Dwight David Eisenhower 1953-1961 - John Fitzgerald Kennedy, 1961- ... www.potus.com/ - Προσωρινά αποθηκευμένη - Παράνομος

American President: John Fitzgerald Kennedy - [Μετάφραση αυτής της σελίδας] Term: 35th **President of the United States (1961-1963)**. Born: May 29, 1917, Brookline, MA. Nickname: "JFK" "Jack". Education: Harvard College graduated ... millercenter.org/.../americanpresident/kennedy - Προσωρινά αποθηκευμένη - Παράνομος

List of **Presidents of the United States** - Wikipedia, the free ...

Αναζήτηση στον ιστό
Αναζήτηση σε άλλους στα
Ελληνικά

Οποιοδήποτε στιγμή
Τελευταίος 2 ημέρες

▼ Περισσότερα εργαλεία

Αποτελέσματα χρονικής περιόδου

7. Για να βρείτε αποτελέσματα ενός συγκεκριμένου τύπου αρχείου (όπως αρχεία τύπου PowerPoint, Excel, Word κλπ.) πληκτρολογήστε μετά τη βασική λέξη/φράση αναζήτησης, « filetype: » ή « ext: » και τον τύπο αρχείου που επιθυμείτε.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστοί Ρυθμίσεις α

Google american history filetype:ppt Αναζήτηση

Σχετικά με 29,600 αποτελέσματα (0.10 δευτερόλεπτα)

Archived: **Teaching American History Technical Assistance Overview** - [Μετάφραση αυτής της σελίδας] Μορφή αρχείου: Microsoft PowerPoint - Quick View The **Teaching American History (TAH)** program provides school districts with resources to create high quality professional development projects for American ... www2.ed.gov/programs/teachinghistory/overview.ppt - Παράνομος

Teaching **American History Forum** - [Μετάφραση αυτής της σελίδας] Μορφή αρχείου: Microsoft PowerPoint - Προβολή ως HTML Teaching **American History Forum**. Peopling the American Past: A Collaboration of 7 School Districts. What do I use the forum for? ... chinn.gmu.edu/7tah/documents/foruminstructions.ppt

Session 3: **Sports and Race in American History** - [Μετάφραση αυτής της σελίδας] Μορφή αρχείου: Microsoft PowerPoint - Προβολή ως HTML Session 3: **Sports and Race in American History**. I. Welcome, and three major themes. II. Do the Right Thing: sports' possibilities and limitations. III. ... community.learnc.org/weblogs/partners/phe/Session%203.ppt - Παράνομος

California **Native American History** - [Μετάφραση αυτής της σελίδας]

Συγκεκριμένος τύπος αρχείου

8. Εάν επιθυμείτε στα αποτελέσματα μιας αναζήτησής σας να μην εμφανίζονται εκείνα που περιέχουν μια συγκεκριμένη παράμετρο, τότε μετά τη λέξη/φράση που αναζητάτε, πληκτρολογήστε το σύμβολο της αφαίρεσης (-) και την παράμετρο που επιθυμείτε να μην περιληφθεί στα αποτελέσματα. Στο παρακάτω παράδειγμα, βλέπετε μια σύνθετη αναζήτηση για «διαρροή πετρελαίου» χωρίς να συμπεριλαμβάνονται στα αποτελέσματα όσα αφορούν την εταιρεία BP.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστοί Ρυθμίσεις α

Google oil spill -bp Αναζήτηση

Σχετικά με 20,900,000 αποτελέσματα (0.18 δευτερόλεπτα)

Bίντεο για oil spill -bp

1999 World Seaside Nurburgina - The Oil Spill

20 Years After Exxon Valdez Oil Spill, Alaska

24 Mar. 2009 democracynow.org

date τη διεύθυνση σας εδώ >

Oil Spill Equipment - [Μετάφραση αυτής της σελίδας] Manufacturer of oil spill equipment skimmers, booms & related equipment www.elastec.com/oilspill/

Oil Spills | Emergency Management | US EPA - [Μετάφραση αυτής της σελίδας] Information about programs for preventing, preparing for, and responding to oil spills that occur in and around inland waters of the United States, ... www.epa.gov/oilspill/ - Προσωρινά αποθηκευμένη - Παράνομος

ITOPF - About Marine Spills - Effects of **Oil Spills** - [Μετάφραση αυτής της σελίδας] Oil spills can have serious effects on marine life, as highlighted

Αφαίρεση παραμέτρου

9. Αντίστοιχα το σύμβολο της πρόσθεσης

(+) μαζί με την παράμετρο που επιθυμείτε να περιληφθεί στα αποτελέσματα ταξινομεί τα αποτελέσματα ανάλογα με τη συχνότητα εμφάνισης της παραμέτρου. Π.χ. στο παρακάτω παράδειγμα τα αποτελέσματα ταξινομούνται ανάλογα με τη συχνότητα εμφάνισης της παραμέτρου BP στα κείμενα που επιστρέφονται σε αύξουσα σειρά.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστοί Ρυθμίσεις α

Google oil spill +bp Αναζήτηση

Σχετικά με 8,930,000 αποτελέσματα (0.29 δευτερόλεπτα)

BP Global | BP - [Μετάφραση αυτής της σελίδας] Welcome to BP. Our products and services provide the freedom to move, to heat and to ... in the response to the accident and oil spill in the Gulf of Mexico ... Careers - Investors - Contact us - Gulf of Mexico response www.bp.com/ - Προσωρινά αποθηκευμένη - Παράνομος

Gulf of Mexico response | Oil spill | BP - [Μετάφραση αυτής της σελίδας] BP announced today that it has pledged certain Gulf of Mexico assets as ... www.bp.com/content/dam/assets/genericarticle.do?... - Προσωρινά αποθηκευμένη

BP - Gulf of Mexico Response - [Μετάφραση αυτής της σελίδας] Information on the company's response with pictures, videos (including live ... www.bp.com/.../bp_.../gov_stream.html - Προσωρινά αποθηκευμένη

✱ Περισσότερα αποτελέσματα από bp.com

Deepwater Horizon oil spill - Wikipedia, the free encyclopedia - [Μετάφραση αυτής της σελίδας] "2010 oil spill" and "BP oil spill" redirect here. For other oil spills in 2010, see 2010 oil spill (disambiguation). For the 2006 oil spill involving BP, ... en.wikipedia.org/.../Deepwater_Horizon_oil_spill - Προσωρινά αποθηκευμένη

BP Oil Spill: 7 Secrets BP Doesn't Want You To Know (PHOTOS) - [Μετάφραση αυτής της σελίδας]

Ταξινόμηση ανάλογα με τη συχνότητα εμφάνισης της παραμέτρου

10. Πληκτρολογώντας το σύμβολο " " πριν από τη λέξη/φράση που αναζητάτε, θα δείτε αποτελέσματα σχετικού περιεχομένου εκτός από τα βασικά αποτελέσματα που θα έδινε η αναζήτηση. Στο παράδειγμα βλέπετε τα σχετικά αποτελέσματα για τη λέξη "space" (διάστημα), που περιέχουν σχετικές παραμέτρους όπως "satellite" (δορυφόρος) και "NASA".

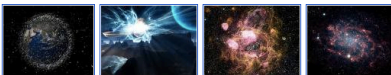
Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστού | Ρυθμίσεις α

Google Αναζήτηση

Σχετικά με 1,050,000,000 αποτελέσματα (0.16 δευτερόλεπτα) Συνθετή αναζήτηση

Συμβουλή: Αναζήτηση αποτελεσμάτων μόνο στα Ελληνικά. Μπορείτε να επιλέξετε τη γλώσσα αναζήτησης στη σελίδα Προτιμήσεις

Εικόνες για ~space - Αναφορά εικόνων



Learn More at Space.com. From Satellites to Stars, NASA ...
[Μετάφραση αυτής της σελίδας]
Space.com provides information on everything Space - satellites, stars, astronomy, the Sun, planets, NASA and more.
NightSky - News - Wallpapers - Videos
www.space.com/ - Προσωρινά αποθηκευμένη - Παρόμοιες
SPACE.com: Space News, NASA News, News Space ...
[Μετάφραση αυτής της σελίδας]
Includes launches, landings, sightings, new projects, scientific discoveries ...
www.space.com/news/ - Προσωρινά αποθηκευμένη - Παρόμοιες

Αναζήτηση στον ιστό
Αναζήτηση σελίδων στα Ελληνικά

Κανονικά αποτελέσματα
Ιστοστοιαι με εικόνες
▼ Περισσότερα εργαλεία

Αποτελέσματα σχετικού περιεχομένου

11.Αν θέλετε να αναζητήσετε επακριβώς μια φράση, κι όχι μόνο μια λέξη, τότε συμπεριλάβετε τη φράση σας μέσα σε εισαγωγικά.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστού | Ρυθμίσεις α

Google Αναζήτηση

Σχετικά με 6,860,000 αποτελέσματα (0.19 δευτερόλεπτα) Συνθετή αναζήτηση

Συμβουλή: Αναζήτηση αποτελεσμάτων μόνο στα Ελληνικά. Μπορείτε να επιλέξετε τη γλώσσα αναζήτησης στη σελίδα Προτιμήσεις

Bruce Willis - IMDb ... [Μετάφραση αυτής της σελίδας]
Bruce Willis, Actor. The Sixth Sense. German born, New Jersey raised US actor and musician well known for his film appearances as wise cracking or hard ...
Biography - Awards - Photo gallery - Genre
www.imdb.com/.../nm0000246/ - Προσωρινά αποθηκευμένη - Παρόμοιες

Bruce Willis - Wikipedia, the free encyclopedia ...
[Μετάφραση αυτής της σελίδας]
Walter Bruce Willis (born March 19, 1955), better known as Bruce Willis, is an American actor, producer, and musician. His career began in television in the ...
Emma Henning - Die Hard - Stargates - 12 Monkeys
en.wikipedia.org/.../Bruce_Willis - Προσωρινά αποθηκευμένη - Παρόμοιες

BruceWillis.com ... [Μετάφραση αυτής της σελίδας]
www.brucewillis.com/ - Προσωρινά αποθηκευμένη - Παρόμοιες

Εικόνες για "bruce willis" - Αναφορά εικόνων

Αναζήτηση στον ιστό
Αναζήτηση σελίδων στα Ελληνικά

Οποιαδήποτε στιγμή
Τελευταίες 2 ημέρες

Κανονικά αποτελέσματα
Ιστοστοιαι με εικόνες
▼ Περισσότερα εργαλεία

Αποτελέσματα αναζήτησης φράσης

12.Η μηχανή αναζήτησης υποστηρίζει ακόμα και χαρακτήρες μπαλαντέρ, όπως την τελεία (.) για αντικατάσταση ενός μόνο χαρακτήρα και το αστεράκι (*) για αντικατάσταση περισσότερων χαρακτήρων. Επίσης, ο χαρακτήρας | δηλώνει το λογικό Ή.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστού | Ρυθμίσεις α

Google Αναζήτηση

Σχετικά με 379,000,000 αποτελέσματα (0.24 δευτερόλεπτα) Συνθετή αναζήτηση

Συμβουλή: Αναζήτηση αποτελεσμάτων μόνο στα Ελληνικά. Μπορείτε να επιλέξετε τη γλώσσα αναζήτησης στη σελίδα Προτιμήσεις

Oceans (2009) - IMDb ... [Μετάφραση αυτής της σελίδας]
★★★★ Αξιολόγηση: 7.6/10 - από 1,992 χρήστες
Σκηνοθεσία Jacques Perrin, Jacques Cluzaud. Πρωταγ.: Pierce Brosnan, Jacques Perrin, Pedro Amendiaiz Jr. ... An ecological drama/documentary, filmed throughout the globe. Part thriller, part meditation on the vanishing wonders of the sub-aquatic world.
www.imdb.com/title/tt0765128/ - Προσωρινά αποθηκευμένη - Παρόμοιες

Ocean - Wikipedia, the free encyclopedia ... [Μετάφραση αυτής της σελίδας]
An ocean (from Greek **Ὠκεανός**, "okeanos" Oceanus) is a major body of saline water, and a principal component of the hydrosphere. Approximately 70.9% of the ...
Pacific Ocean - Indian Ocean - Atlantic Ocean - Southern Ocean
en.wikipedia.org/wiki/Ocean - Προσωρινά αποθηκευμένη - Παρόμοιες

Ωκεανός - Βικιπαίδεια ...
Ωκεανός αποκαλείται η πολύ μεγάλη θαλάσσια επιφάνεια. Ο όρος καθιερώθηκε ...
at.wikipedia.org/wiki/Ωκεανός - Προσωρινά αποθηκευμένη - Παρόμοιες

Περισσότερα αποτελέσματα από wikipedia.org

Εικόνες για oceans | ωκεανός - Αναφορά εικόνων

Αναζήτηση στον ιστό
Αναζήτηση σελίδων στα Ελληνικά

Οποιαδήποτε στιγμή
Τελευταίες 2 ημέρες

Κανονικά αποτελέσματα
Ιστοστοιαι με εικόνες
▼ Περισσότερα εργαλεία

Χαρακτήρες μπαλαντέρ

13.Αν ψάχνετε κάποια λέξη ή λέξεις στον τίτλο των ιστοσελίδων των αποτελεσμάτων αναζήτησης, τότε χρησιμοποιήστε είτε «intitle:» ακολουθούμενη από μια μόνο παράμετρο είτε «allintitle:» αν θέλετε περισσότερες από μια παραμέτρους. Στο παράδειγμα γίνεται αναζήτηση για τη λέξη Java στον τίτλο των ιστοσελίδων που επιστρέφονται ως αποτέλεσμα.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστού | Ρυθμίσεις α

Google Αναζήτηση

Σχετικά με 25,000 αποτελέσματα (0.38 δευτερόλεπτα) Συνθετή αναζήτηση

Think Ruby - Conditionals and Recursion ... [Μετάφραση αυτής της σελίδας]
Chapter 4: Conditionals and Recursion. 4.1 The modulus operator ... 4.9 Stack diagrams for recursive methods. 4.10 Convention and divine law. 4.11 Glossary ...
mysite.vietcon.net/.../thinkruby/.../ch04.html - Προσωρινά αποθηκευμένη - Παρόμοιες

Software Development: Recursion in Ruby ... [Μετάφραση αυτής της σελίδας]
20 Jun 2007 ... I never understood recursion. The interviewer skillfully provided some clues for me to figure this one out myself. ...
brunjan.blogspot.com/.../recursion-in-ruby.html - Προσωρινά αποθηκευμένη - Παρόμοιες

RubyRecursion - Meshplex ... [Μετάφραση αυτής της σελίδας]
9 Oct 2008 ... "In mathematics and computer science, recursion is a particular way of specifying (or constructing) a class of objects (or an object from a ...
www.meshplex.org/.../RubyRecursion - Προσωρινά αποθηκευμένη - Παρόμοιες

ruby recursion and blocks - CodingForums.com ...
[Μετάφραση αυτής της σελίδας]
2 θρονονήσεις - 1 συντάκτης. Τέλευταία καταχώρηση: 8 Aug. 2009.
Is there a certain restriction in ruby when it comes to using code blocks and recursion ?
rosharien is offline ...
www.codingforums.com/showthread.php?... - Προσωρινά αποθηκευμένη

Αναζήτηση στον ιστό
Αναζήτηση σελίδων στα Ελληνικά

Οποιαδήποτε στιγμή
Τελευταία 3 μήνες

Κανονικά αποτελέσματα
Ιστοστοιαι με εικόνες
▼ Περισσότερα εργαλεία

Αναζήτηση στον τίτλο των ιστοσελίδων

14.Αντίστοιχα, υπάρχουν και οι εντολές «inurl:» και «allinurl:» που ψάχνουν τη λέξη ή τις λέξεις στο URL των αποτελεσμάτων.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστού | Ρυθμίσεις α

Google Αναζήτηση

Σχετικά με 245 αποτελέσματα (0.14 δευτερόλεπτα) Συνθετή αναζήτηση

How do I "decompile" Java class files? - Stack Overflow ... [Μετάφραση αυτής της σελίδας]
7 Nov 2010 ... On Java performance questions on this site I often see responses ... The art of "decompiling" can also be thought upon as reverse engineering. ...
stackoverflow.com/.../how-do-i-decompile-java-class-files - Προσωρινά αποθηκευμένη - Παρόμοιες

free java decompile jar download ...
[Μετάφραση αυτής της σελίδας]
JNC - JavaNativeCompiler 1.1 - free JNC - JavaNativeCompiler download (jnc.mtsystems.ch). is a Java to native compiler. It allows AOT (ahead of time) ...
3d2f.com > ... > Java - Προσωρινά αποθηκευμένη - Παρόμοιες

free java decompile jar file download ...
[Μετάφραση αυτής της σελίδας]
SPAMfighter Pro 7.1.99 new! Spam/phishing filter for Outlook/Express and ...
3d2f.com > Development Tools > Java - Προσωρινά αποθηκευμένη

Περισσότερα αποτελέσματα από 3d2f.com

Αναζήτηση στον ιστό
Αναζήτηση σελίδων στα Ελληνικά

Οποιαδήποτε στιγμή
Τελευταία 3 μήνες

Κανονικά αποτελέσματα
Ιστοστοιαι με εικόνες
▼ Περισσότερα εργαλεία

Αναζήτηση στη διεύθυνση των ιστοσελίδων

15.Επίσης υπάρχουν και οι εντολές «inanchor:» και «allintext:» που αναζητούν την παράμετρο στο κείμενο του URL και στο καθαυτό κείμενο των ιστοσελίδων αποτελεσμάτων.

Παγκόσμιος ιστός Εικόνες Χάρτες Ειδήσεις Μετάφραση Ιστολόγια Gmail περισσότερα ▼ Ιστορικά ιστού | Ρυθμίσεις α

Google Αναζήτηση

Σχετικά με 3,130,000 αποτελέσματα (0.16 δευτερόλεπτα) Συνθετή αναζήτηση

Συμβουλή: Αναζήτηση αποτελεσμάτων μόνο στα Ελληνικά. Μπορείτε να επιλέξετε τη γλώσσα αναζήτησης στη σελίδα Προτιμήσεις

How to:python programming under Ubuntu ... [Μετάφραση αυτής της σελίδας]
If you are new to python programming & you're having ubuntu linux as your ... Ubuntu community develops its own tools and scripts under python,so you can ...
www.onecore.net/how-topython-programming-under-ubuntu.html - Προσωρινά αποθηκευμένη - Παρόμοιες

Python Recipes - Community Ubuntu Documentation ...
15 Aug 2009 ... The good news is that Ubuntu has excellent support for Python right out of the box. The great news is that you can get started right away ...
https://help.ubuntu.com/.../PythonRecipes - Προσωρινά αποθηκευμένη - Παρόμοιες

PackagingGuide/Python - Ubuntu Wiki ...
rochu/Emilio Pozuelo Monfort) and Starti co-hosted the Python Apps Packaging ...
https://wiki.ubuntu.com/.../Python - Προσωρινά αποθηκευμένη - Παρόμοιες

Ubuntu - Details of package python in hardy ... [Μετάφραση αυτής της σελίδας]
Python, the high-level, interactive object oriented language, includes an ...
packages.ubuntu.com/.../python - Προσωρινά αποθηκευμένη - Παρόμοιες

Περισσότερα αποτελέσματα από ubuntu.com

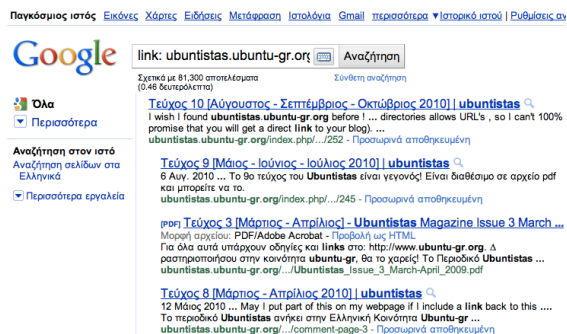
Αναζήτηση στον ιστό
Αναζήτηση σελίδων στα Ελληνικά

Οποιαδήποτε στιγμή
Τελευταία 3 μήνες

Κανονικά αποτελέσματα
Ιστοστοιαι με εικόνες
▼ Περισσότερα εργαλεία

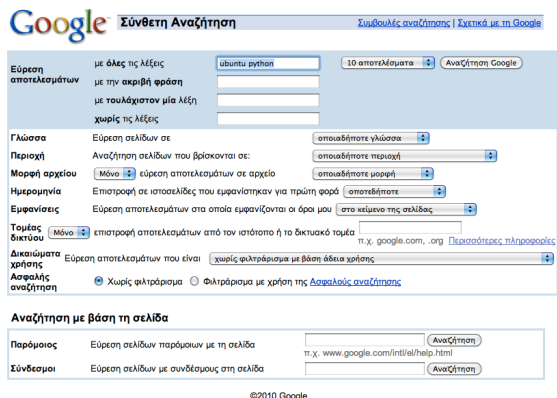
Αναζήτηση στο κείμενο των ιστοσελίδων

16.Αν θέλετε να δείτε πόσες ιστοσελίδες αναφέρουν με τη μορφή υπερσυνδέσμου την ιστοσελίδα σας, χρησιμοποιήστε την εντολή «link:».



Ιστοσελίδες που «δείχνουν» σε μια ιστοσελίδα

17. Αν δε θυμάστε όλα τα παραπάνω κόλπα, τότε η Σύνθετη Αναζήτηση του Google σας παρέχει μια σύνθεση φόρμα για σύνθετες αναζητήσεις.



Σύνθετη αναζήτηση

Στο ακόλουθο σχήμα επιχειρείται μια επεξήγηση των παραπάνω.



Επεξήγηση των «κόλπων» αναζήτησης

Καλή αναζήτηση!

Αναφορές:

1. <http://www.google.com/intl/el/help/features.html>
2. Piotrowski M. (2005), «Dangerous Google – Searching for Secrets», hakin9, τεύχος 4/2005.
3. Grala P. (2006), Google™ Search and Tools in a Snap, Sams.
4. 100+ Google Tricks That Will Save You Time in School, <http://www.onlinecolleges.net>
5. Clever Google Tricks Worth Knowing, <http://www.marcandangel.com>
6. <http://programmerworld.net/articles/tips/google.php>

(συνέχεια από σελ. 11)

- Gillings M. et al., GIS Guide to Good Practice, <http://ahds.ac.uk>:1998.
- Babcock H., Geographic Information Systems - A Resource Guide For Using GIS as a Tool For Your Data, Tahoe Center for a Sustainable Future, <http://ceres.ca.gov/tcsf/gis.html>.
- MapInfo Corporation, MapXtreme Guide, <http://www.mapxtreme.com>, MapInfo Corporation: 1999.

(συνέχεια από σελ. 16)

Πηγές:

1. Menezes A., van Oorschot P., Vanstone S. (1997), Handbook of Applied Cryptography, CRC Press.
2. Schneier B. (1996), Applied Cryptography, John Wiley & Sons.
3. Anderson R. (2001), Security Engineering, John Wiley & Sons.
4. Stallings W. (2005), Cryptography and Network Security, Prentice Hall.
5. Hook D. (2005), Beginning Cryptography with Java, Wrox.
6. Knudsen J. (1998), Java Cryptography, O' Reilly.
7. <http://el.wikipedia.org/wiki/>

Το ubuntistas σε χρειάζεται*

Αλλά δεν έχω το χρόνο να ασχοληθώ...

Όποιος έχει θέληση, λύση βρίσκει

Και πώς μπορώ να συνεισφέρω;

Άρθρα γράφοντας,
εξώφυλλα σχεδιάζοντας,
στη σελιδοποίηση βοηθώντας

Ας είναι το ελεύθερο λογισμικό μαζί σου

* στείλε μας το άρθρο σου για το ελεύθερο λογισμικό για να εμφανιστεί στο επόμενο τεύχος του ubuntistas