UNIVERSITÀ DEGLI STUDI
DI MILANO

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

STUDENT'S GUIDE
to the
MASTER DEGREE
in

Computer Science

at CREMA

Academic Year 2011/2012

DISCLAIMER: THE PRESENT STUDENT'S GUIDE IS AN INFORMATIVE SUPPORT THAT DOES NOT SUBSTITUTE THE OFFICIAL DOCUMENTS APPROVED BY THE ACADEMIC ORGANS AND AVAILABLE ON THE UNIVERSITY WEB SITES. THESE DOCUMENTS ARE EFFECTIVELY THE ONLY VALID REFERENCE.

CONTENTS

MASTER DEGREE
IN
COMPUTER SCIENCE

STUDY ORGANISATION OF THE MASTER DEGREE IN COMPUTER SCIENCE[4]

GENERALITIES

Belongs to master degree class: LM-18 Informatica
Granted qualification: Dottore Magistrale (Master Degree)
Active curricula: A
Duration: 2 years
CFUs required to access the degree: 180
CFUs granted by the degree: 120
Degree years activated: 1st and 2nd year
Access limitations: No
Degree code: F94

REFERENCES

Faculty Dean
Prof.ssa Paola Campanelli
President of the Didactics Coordination Council (DCC)
Prof. Mario Ornaghi (Milano), Prof. Nello Scarabottolo (Crema)
Tutors
Prof. Silvio Ghilardi, Prof. Federico Pedersini, Prof. Vincenzo Piuri (Crema), Prof. Marco Trubian
Web sites
http://www.ccdinf.unimi.it - http://www.ccdinfcr.unimi.it
DCC Computer Science and Information Technology (Crema)
Via Bramante 65, Crema (CR), Phone +39 0373/898011-12,
http://www.ccdinfcr.unimi.it, segreteria.studenti.dti@unimi.it
DCC Computer Science and Information Technology (Milano)
Via Comelico 39/41, Phone +39 02 503 16250 / 16326,
http://www.ccdinf.unimi.it, infostudenti@ccdi.unimi.it
Students office
http://www.unimi.it/studenti/segreterie

[4] Please note that this student guide is just an information support, not replacing in any case the official Italian documents of the master degree (ordinamento didattico, regolamento didattico, manifesto didattico) available on the unimi web sites and constituting the only valid regulations.

MASTER DEGREE CHARACTERISTICS

INTRODUCTION

The Master Degree in Computer Science has been activated by the Università degli Studi di Milano since 2009/10 and belongs to the master degree class in Informatics (LM-18).

In the Crema campus, a complete edition of the master degree is available, where **all mandatory and some complementary courses are offered in English language**, starting from year 2011/2012.

GENERAL AND SPECIFIC GOALS

The Master Degree in Computer Science aims at supplying advanced knowledge and at forming professional competences suitable for job positions in research, design and management of systems in the various application areas of computer science, with particular reference to commercial, industrial and scientific environments. Once graduated, the student will be employable in design, development, control and management of complex information systems. Her/his main goals will be the continuous improvement of information systems and the ability to foster innovation in her/his application fields. The Master Degree will thus prepare professionals characterized by high-level analytical and operating competences, but also by an open view of al problems connected with the adoption and usage of ICT.

The Master Degree ensures an advanced and complete knowledge of the main ICT sectors: networks and distributed systems, information management, theoretical informatics, computational intelligence.

The Master Degree also requires the development of a graduation thesis, to be carried on either inside the University or in another public or private Institution and to be discussed in the final graduation exam. The graduation thesis is a written report, structured as a scientific paper, to be prepared under the control of a supervisor and referring an original scientific experience related to ICT.

ACQUIRED COMPETENCES AND SKILLS

Following the European harmonization principles, the competences and skills granted by the Master Degree in Computer Science are here summarized, according to the Dublin descriptors scheme.

Knowledge and understanding

Graduated students will possess advanced theoretical and operating competences in the following fields: information management, knowledge management, distributed systems, distributed algorithms, complex networks, mathematical logics, probability and statistics applied to information processes, automata theory, complexity theory, intelligent systems.

Applying knowledge and understanding

Graduated students will be able to apply acquired competences to analysis, design, implementation and evaluation of complex information systems in various application fields: commerce, industry, public administration, insurances, banks, hospitals, environment management, energy management, research.

They will also be able to evaluate the correctness and the sustainability of their own design choices, as well as the effects of their own decisions regarding information systems, when applied in their professional job positions in: industries, public and private research centers, government bodies, control authorities.

Making judgements

Graduated students will be able to formulate autonomous judgments regarding strategic decisions and design choices of companies and other institutions where they will be employed. They will also acquire the deontological professionalism principles driving the interpersonal relationships in their employment environments.

Communication skills

Graduated students will be able to argument their own opinions and to communicates results of their own analysis and evaluation in a clear, effective way, using the English language and exploiting the possibilities offered by up-to-date computer tools as well as mathematical, statistical, econometrics tools for the analysis and the presentation of data.

Learning skills

The Master Degree aims at gradually bring students to the frontiers of research in its reference disciplines. For this reason, the Degree will also develop student's ability of continuous learning and of undertaking autonomous research activities in line with international standards, in view of a possible prosecution of their studies in the frame of PhD programs in Computer Science or similar fields.

PROFESSIONAL PROFILE AND POSSIBLE JOB POSITIONS

The acquired competences and skills will allow the graduated student in the Master Degree in Computer Science to obtain high responsibility positions in projects requiring consultancy, analysis, design, management, maintenance, marketing of medium-to-large ICT systems.

She/he will be able to operate in a variety of application fields for the design and the management of ICT systems and for the study of new systems and applications.

These activities will take place in all areas of public and private institutions using ICT: banks, insurances, logistics and transportations, health, public administrations, telecommunications and media, service providers, industry. More specifically, roles and positions of graduated students according to the Italian ISTAT coding are listed below.

2114 Informatics and telematics

21141 Specialists in basic informatics research

21142 Analysts and designers of system and application software

21143 System analysts

21144 Information security specialists

21145 Networks and computer communications specialists

26200 Researchers and graduated technicians in mathematical and information sciences

ACCESS REQUIREMENTS

To register for the Master Degree in Computer Science, candidates must have obtained in their previous studies at least:

- 66 CFUs (University Formative Credits) belonging to sectors INF/01, ING-INF/05
- 36 CFUs belonging to sectors MAT/01-09
- 6 CFUs belonging to sectors FIS/01-03

Access of students not complying with the above requirements will be possible only after decision of the Didactics Coordination Council, under delegation of the Faculty Council.

For academic year 2011/12, the Crema Didactics Coordination Council decided to reduce to 24 the minimum number of CFUs belonging to sectors MAT/01-09 necessary to access the Master Degree in Computer Science. Students having less than 36 CFUs belonging to sectors MAT/01-09 will have to compensate their lack using the free choice CFUs planned by the Master Degree.

Other curricular integrations necessary to fulfill the above requirements should be acquired before accessing the Master Degree, by passing exams of the courses of the Bachelor Degree in Computer Science (Laurea in Informatica) indicated by the Didactics Coordination Council.

DEGREE STRUCTURE

Single curriculum.

DEGREE CURRICULUM ORGANIZATION

The standard duration of the Master Degree in Computer Science is two years. To graduate, the students should acquire 120 CFUs. The acquisition of competences and skills by students is quantified in terms of CFUs according to the didactical regulations of the Università degli Studi di Milano.

The CFU is a measurement unit of the amount of learning work required to each student, corresponding to 25 hours of activities, which can include either:

- 8 hours of lectures and 17 hours of individual study;
- 12 hours of exercising and 13 hours of individual study;
- 16 hours of labs and 9 hours of individual study;
- 25 hours of activities related to the preparation of the final graduation exam.

Teaching activities are organized for each course year in two coordinated cycles, conventionally called semesters, having a minimum duration of 12 weeks each, were lectures, exercises and labs take place. It is also planned a stage activity, to be done possibly outside the University, in public or private institutions.

NOTES

Student should verify each year the activation of the courses inserted in her/his study plan.

COURSES LOCATIONS

Computer Science courses are held in: via Comelico n. 39/41 - Milano. Other courses are held in: Settore Didattico, via Celoria - Milano.

Crema courses are held at the Dipartimento di Tecnologie dell'Informazione, via Bramante 65, Crema (CR).

LANGUAGE TESTS

To be admitted to the final graduation exam, the student must demonstrate her/his ability to fluently use the written and oral English language in the technical environment through a pass/fail verification test granting 3 CFUs. Usually, this verification can be done either:

- by presenting a B2-level internationally recognized certification (list of recognized certifications is available at http://www.ccdbiol.unimi.it/it/informazioni/linguaInglese.html);
- by passing a B2-level test (*placement test*) organized during exam sessions;
- by frequenting a specific course provided by the Faculty and by passing the level-B2 test.

For students of the English edition of the Master Degree in Computer Science, such a verification test is substituted by the first passed exam of one of the courses of the Degree.

ATTENDANCE OBBLIGATION

The attendance is not compulsory, but strongly recommended.

PROFICIENCY ASSESSMENT METHODS

The proficiency is assessed through written and oral exams, with an examination results expressed in thirtieths. Some teachers organize *in itinere* examinations, on voluntary base.

GENERAL RULES FOR ENROLMENT AND ADMISSION TO THE EXAMINATIONS

It is mandatory the enrolment to the examination using the SIFA kiosks or the SIFA on-line service at http://www.unimi.it/studenti/servizi_online.htm

GENERAL RULES FOR ENROLMENT TO THE EDUCATIONAL ACTIVITIES AND LABORATORIES

None.

FULFILMENT OF STUDIES/INTERNSHIP ABROAD

The procedure and forms for applying for internships (it is the same for internship in Italy or abroad) can be downloaded from www.dti.unimi.it. For periods of study abroad, the subscription to the Erasmus project is necessary, according to the timing and the procedures established by UniMi and published on www.unimi.it.

FORMULATION AND PRESENTATION OF THE STUDY PROGRAMME

Students must submit their Study Programme, in compliance with the Academic Regulations of the Faculty of Sciences, choosing complementary teachings among those listed in the course programs. The choice can be made from the 1st year and may be modified during the following year. The Study Programme should also indicate how the student intends to obtain the free choice CFUs that can be chosen from courses offered by UniMi, or selected from among those proposed by the Didactics Coordination Council.

The Study Programme must be submitted using the service provided at http://www.unimi.it/studenti/servizi_online.htm, during the periods stated by the Students Officies.

FINAL EXAM ADMISSION CRITERIA

In order to be admitted to the final exam (laurea), the student must have at least 81 CFUs, as stated by the composition rules of the present course program. The final exams agenda, the deadlines for the submission of the graduation application and the required documentation are published on www.dti.unimi.it.

FINAL EXAM PECULIARITIES

Once the required CFU have been acquired, in accordance with the present regulations, the student is admitted to the final exam for graduation, in compliance with the general principles expressed in the Rules of the Faculty, to which reference is made for any other provision on the subject. The final examination for obtaining the Master Degree in Computer Science consists in the presentation and discussion of a master thesis (in English or Italian) in the form of an original work made by the student under the guidance of a supervisor, which involves an organic and complete job, that can demonstrate abilities of researching, processing and synthesis.

LESSONS SCHEDULE

The class schedule for the Milano's edition is available at: http://www.ccdinf.unimi.it/
The class schedule for the Crema's edition is available at: http://www.ccdinfcr.unimi.it/

ADMISSION CONDITIONS: 1ST YEAR OPEN

INFORMATION AND ORGANIZATIONAL ARRANGEMENTS FOR THE REGISTRATION

For information contact the students office at tel. 0373/898011-12 or by e-mail at segreteria.studenti.dti@unimi.it

Registration start date: **15 July 2011**

USEFUL LINK FOR THE REGISTRATION

www.unimi.it

APPLICATION REQUEST

The application request, mandatory for both graduate and final year students, must be electronically submitted from the 15 July 2011 to the 15 September 2011. Graduate and final year students from UniMi or other Universities can submit the application request.

PERSONAL QUALIFICATION VERIFICATION

The personal qualification of the applicants will be verified, for the admission at the Master Degree, through an interview on topics related to the fundamental subjects studied in the Bachelor courses. The interview will be conducted by a committee of teachers designated by the Didactics Coordination Council.

For the academic year. 2011/2012, the interview will be held **at the Dipartimento di Scienze dell'Informazione - Via Comelico 39, Milano** according to the agenda reported on the admission receipt.

The interview can be made even before the achievement of the Bachelor Degree (which must still be obtained on or before 28 February 2012), withstanding the curricular requirements.

Compliance with the requirements will be verified by the Didactics Coordination Council.

The negative results obtained in the interview, for all graduate students and undergraduates, involves the foreclosure to the admission to the Master of Science for the current year.

If successful, the student must indicate the site chosen (Milano or Crema).

REGISTRATION

Students who have successfully passed the interview will be able to enroll after 5 working days from the date of the interview, if already graduated, but no later than 15 March, 2012, if not yet graduated at the time of the interview. To enroll in the Master Degree, students must acquire the Bachelor Degree no later than 28 February 2012.

The University students who graduate between October 2011 and February 2012 will attend the courses and laboratories planned for the Master Degree course and take the exams gaining their CFUs. These CFUs, in excess with respect to the 180 needed for Bachelor Degree, will be validated in order to attain the 120 credits required for the Master of Science, provided that they are achieved before 31 January 2012.

COURSE STRUCTURE

1st YEAR Mandatory educational activities				
Delivering	**Training activity**	**CFU**	**Field**	**Teaching Format**
1st semester	Logica matematica (*)	6	MAT/01	48 hours Lessons
1st semester	Sistemi intelligenti (*)	6	INF/01	48 hours Lessons
2nd semester	Informatica teorica (*)	6	INF/01	48 hours Lessons
2nd semester	Reti wireless e mobili (*)	6	INF/01	48 hours Lessons
2nd semester	Sistemi distribuiti (*)	6	INF/01	48 hours Lessons
	Total mandatory CFUs	**30**		

2nd YEAR Mandatory educational activities				
Delivering	**Training activity**	**CFU**	**Field**	**Teaching Format**
1st semester	Gestione dell'informazione (*)	6	INF/01	48 hours Lessons
2nd semester	Conoscenza della lingua inglese 2 (*)	3	L-LIN/12	24 hours Lessons
	Total mandatory CFUs	**9**		

Optional educational activities				
Delivering	**Training activity**	**CFU**	**Field**	**Teaching Format**
THE STUDENT WILL HAVE TO GAIN 18 CFUs BY CHOOSING FROM THE FOLLOWING COURSES (TABLE 1):				
1st semester	Algoritmi e complessità	6	INF/01	48 hours Lessons
2nd semester	Algoritmi per reti di calcolatori	6	INF/01	48 hours Lessons
1st semester	Architetture digitali	6	INF/01	48 hours Lessons
1st semester	Architetture e programmazione DSP	6	INF/01	48 hours Lessons
1st semester	Architetture software orientate ai servizi (**)	6	INF/01	48 hours Lessons
1st semester	Bioinformatica	6	INF/01	48 hours Lessons
1st semester	Crittografia II	6	INF/01	48 hours Lessons
1st semester	Elaborazione di immagini (**)	6	INF/01	48 hours Lessons
2nd semester	Elaborazione delle immagini I	6	INF/01	48 hours Lessons
2nd semester	Elaborazione delle immagini II	6	INF/01	48 hours Lessons
1st semester	Elaborazione di segnali (**)	6	INF/01	16 hours Lab, 40 hours Lessons
1st semester	Elaborazione numerica dei segnali II	6	INF/01	48 hours Lessons
1st semester	Estrazione e gestione della conoscenza (**)	6	INF/01	48 hours Lessons
not delivered	Gestione dell'informazione nei sistemi mobili e pervasivi	6	INF/01	48 hours Lessons
2nd semester	Gestione e organizzazione dei progetti (**)	6	INF/01	48 hours Lessons
2nd semester	Ingegneria dei processi aziendali (**)	6	INF/01	48 hours Lessons
not delivered	Intelligenza artificiale e laboratorio	6	INF/01	48 hours Lessons

not delivered	Laboratorio di segnali	6	INF/01	48 hours Lessons
2nd semester	Linguaggi e traduttori	6	INF/01	48 hours Lessons
not delivered	Metodi formali dell'informatica	6	INF/01	48 hours Lessons
not delivered	Metodi per il ragionamento automatico	6	INF/01	48 hours Lessons
1st semester	Modelli dei dati e DBMS di nuova generazione	6	INF/01	48 hours Lessons
2nd semester	Ontologie e web semantico	6	INF/01	48 hours Lessons
2nd semester	Progettazione e sviluppo software per sistemi mobili e pervasivi	6	INF/01	48 hours Lessons
2nd semester	Sicurezza informatica	6	INF/01	48 hours Lessons
not delivered	Simulazione	6	INF/01	48 hours Lessons
2nd semester	Sistemi informativi geografici	6	INF/01	48 hours Lessons
2nd semester	Sistemi informativi II	6	INF/01	48 hours Lessons
1st semester	Sistemi intelligenti per il monitoraggio e il controllo (**)	6	INF/01	48 hours Lessons
not delivered	Sistemi organizzativi	6	INF/01	48 hours Lessons
2nd semester	Soft computing	12	INF/01	96 hours Lessons
1st semester	Tecniche speciali di programmazione	6	INF/01	48 hours Lessons
2nd semester	Verifica e convalida del software	6	INF/01	48 hours Lessons
THE STUDENT WILL HAVE TO GAIN 6 CFUs BY CHOOSING ONE OF THE FOLLOWING COURSES:				
2nd semester	Metodi probabilistici (*)	6	MAT/06	48 hours Lessons
2nd semester	Metodi statistici per l'apprendimento	6	MAT/06	48 hours Lessons
2nd semester	Processi stocastici	6	MAT/06	48 hours Lessons
THE STUDENT WILL HAVE TO GAIN 6 CFUs BY CHOOSING FROM THE FOLLOWING COURSES (TABLE 2):				
not delivered	Algebra computazionale	6	MAT/02	48 hours Lessons
2nd semester	Calcolo numerico	6	MAT/08	48 hours Lessons
1st semester	Complementi di ricerca operativa (*)	6	MAT/09	48 hours Lessons
not delivered	Economia e gestione dell'innovazione	6	SECS-P/07,08	48 hours Lessons
1st semester	Elettronica digitale	6	ING-INF/01	48 hours Lessons
1st semester	Fisica II	6	FIS/01,02,03	48 hours Lessons
1st semester	Geometria computazionale	6	MAT/03	48 hours Lessons
1st semester	Logica II	6	MAT/01	48 hours Lessons
2nd semester	Logistica (**)	6	MAT/09	48 hours Lessons
not delivered	Metodi e modelli per le decisioni	6	MAT/09	48 hours Lessons
2nd semester	Organizzazione aziendale (**)	6	SECS-P/10	48 hours Lessons
1st semester	Tecnologie informatiche per la qualità (**)	6	ING-INF/07	48 hours Lessons

(*) Course held **also** at the Crema campus.

(**) Course held **only** at the Crema campus.

Final activities	
Final exam	39
Total mandatory CFUs	**39**

Optional Activities

The student have to gain **12 freely chosen CFUs** from among:

- courses freely chosen by the student from among those provided by UniMi;
- other certified and CFU-quantified academic activities carried out also in other places, provided the Didactics Coordination Council approval;
- additional internships, which can also supplement the final stage, carried out after the Didactics Coordination Council approval.

The EUCIP certification can grant 3 CFUs.

The CISCO certification can grant 5 CFUs.

COURSES SYLLABUS

SYLLABUS OF THE COURSES HELD- A.A. 2011/2012

Affidabilità dei sistemi - Dependability

Docente: Lazzaroni Massimo

Obiettivi (dettagli AF)

Il corso ha lo scopo di illustrare le problematiche inerenti l'affidabilità, la diagnostica e la manutenibilità dei componenti, dei sistemi e del software con particolare riguardo ai casi in cui l'informatica costituisce la parte più importante.

Programma

AFFIDABILITÀ:

- Definizioni di affidabilità. Modi, meccanismi e cause di guasto. Concetti di guasto, avaria e loro classificazione. Modelli matematici di affidabilità: densità di probabilità di guasto, tasso di guasto istantaneo e "curva a vasca", legge fondamentale dell'affidabilità. Parametri statistici di affidabilità e disponibilità. Affidabilità di sistema. *Reliability Block Diagram*. Configurazioni canoniche e miste. Tecniche di calcolo di affidabilità e disponibilità per configurazioni non canoniche. Fenomeni di degradazione nei componenti elettronici (modello di Arrhenius).
- Analisi statistica dei dati di affidabilità: raccolta, classificazione e rappresentazione dei dati.
- Condizioni operative: Modelli di previsione di affidabilità. Condizioni operative. Condizioni ambientali. Climatogrammi. Previsione di affidabilità: calcolo e interpretazione del tasso di guasto ed MTBF di componenti e apparati elettronici. Uso delle banche dati.
- Disponibilità: Metodi induttivi e deduttivi. *Quality Function Deployment* (QFD). Disponibilità di sistema: analisi con il modello di Markov. Analisi dei rischi. Diagnostica. La riprogettazione del sistema, tecniche di incremento della disponibilità. Manutenibilità di sistema e tecniche di manutenzione.
- Cenni sull'analisi dei modi e degli effetti di guasto (FMEA) e della loro criticità (FMECA) e sull'analisi dell'albero delle avarie (FTA).

AFFIDABILITÀ NEL SOFTWARE:

- Fidatezza-Dependability nel software: *Reliability, Availability, Safety, Confidentiality, Integrity, Maintainability*. Il problema della Security. Il problema del servizio di un sistema di calcolo, del comportamento, della percezione dell'utente (umano e non). Requisiti e problematiche dei sistemi dependable: Rapidità di risposta, disponibilità, continuità di servizio, sicurezza nei confronti dell'operatore e dell'ambiente (*safety*), protezione (*security*). Fallimento (*system failure*), errore, guasto.
- Problematiche dei sistemi di calcolo: Prevenzione dai guasti (fault prevention), Tolleranza ai guasti (fault tolerance), Eliminazione del guasto (fault removal), Predizione di guasti (fault forecasting).
- Conseguimento dei requisiti, validazione e valutazione.
- Impedimenti alla dependability: guasti e loro classificazione
- I guasti intenzionali: logic bomb, Trojan horse, trapdoor, virus, worm, zombie, intrusion attempts,
- I fallimenti (fallimenti con blocco e sistemi *fail–stop*, fallimento per omissione, crash, sistemi *fail–silent*.
- *Accountability*, *authenticity*, *non-repudiability*.
- La dependability delle reti (*Survivability*).
- La manutenibilità del software. La documentazione.

SOFTWARE PER L'ANALISI DELL'AFFIDABILITÀ: CENNI

Propedeuticità consigliate

Un corso di Statistica

Materiale di riferimento

Le dispense e i lucidi utilizzati durante le lezioni.
AA.VV. L'affidabilità nella moderna progettazione: un elemento competitivo che collega sicurezza e certificazione, Editore A&T Affidabilità & Tecnologia, Aprile 2008, ISBN: 978-88-903149-0-2.
AA.VV. Reliability Engineering, Springer, 2011, ISBN 978-3-642-20982-6,

Prerequisiti
-

Modalità di esame
Scritto e orale
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-27/

Algoritmi e strutture dati

Docente: De Capitani di Vimercati Sabrina

Obiettivi (dettagli AF)

Il corso ha lo scopo di introdurre i concetti fondamentali riguardanti l'analisi ed il progetto di algoritmi e strutture dati e l'analisi della complessità computazionale degli algoritmi.

Programma

1. *Introduzione*. Nozione di problema e algoritmo. Analisi di algoritmi, complessità in spazio e tempo di algoritmi ricorsivi e non. Notazioni asintotiche. Calcolo dei tempi di esecuzione di un programma.
2. *Tipi di dati astratti di base*. Liste, Stack, Code: definizione ed operazioni. Implementazione (array, puntatori) con esecuzione delle operazioni e vantaggi/svantaggi.
3. *Alberi*. Concetto di albero e definizioni. Tecniche di attraversamento (inorder, preorder, postorder). Operazioni su ADT albero. Tecniche di rappresentazione. Alberi binari di ricerca: definizione, rappresentazione, operazioni. Alberi binari rosso neri: definizione, rappresentazione, operazioni.
4. *Insiemi*. Definizione, operazioni e tecniche di rappresentazione. Dizionari: definizione e operazioni. Code di priorità: concetti, esempi di utilizzo e tecniche di rappresentazione. Heap: realizzazione e esecuzione delle operazioni.
5. *Hashing*. Tavole ad indirizzamento diretto. Tavole hash. Funzioni hash. Indirizzamento aperto.
6. *Tecniche avanzate di progettazione ed analisi*. Programmazione dinamica. Algoritmi greedy.
7. *Grafi.* Grafi orientati e non orientati: definizioni e concetti principali. Tecniche di rappresentazione. Cammino minimo in grafi pesati: problema e soluzioni. Algoritmi di visita in ampiezza (BFS) e profondità (DFS). Esempi di applicazioni della DFS: test di aciclicità, ordinamento topologico, ritrovamento di componenti fortemente connesse. Esempi di applicazioni della BFS: calcolo cammino minimo in grafi non pesati. Minimo albero ricoprente: problema e soluzioni. Punti di articolazione: definizione e ritrovamento. Graph matching.
8. *Ordinamento*. Problema. Limite inferiore di complessità per gli algoritmi di ordinamento. Insertion sort, heapsort, quicksort, mergesort: descrizione ed analisi della complessità.
9. *Gestione dei dati su memoria esterna*. Problemi. B-alberi: definizione, proprietà e vantaggi. Esecuzione delle operazioni di ricerca, inserimento e cancellazione. Operazioni di concatenazione e bilanciamento nella cancellazione. Operazioni di divisione e promozione nell'inserimento.

Propedeuticità consigliate

-

Materiale di riferimento

T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein, "Introduzione agli Algoritmi e Strutture Dati," McGraw-Hill, 2a edizione (2005)

Prerequisiti

Concetti base di programmazione

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-13/

Analisi e gestione del rischio

Docente: Cremonini Marco

Obiettivi (dettagli AF)

L'obiettivo principale del corso di Analisi e Gestione del Rischio è di presentare una panoramica significativa dell'insieme di studi e metodologie relativo all'analisi del rischio quantitativa e qualitativa e alla tematica connessa delle decisioni in condizioni di incertezza.
L'insieme di studi è intrinsecamente interdisciplinare e per la maggior parte sviluppato in discipline diverse dall'Informatica o la Sicurezza Informatica.
Tuttavia, la rilevanza di queste analisi è sempre più riconosciuta come importante per l'Informatica o la Sicurezza Informatica; le implicazioni, dirette e indirette, verranno discusse nel corso.

Programma

1. Breve prospettiva storica e definizione del contesto interdisciplinare
2. Rischio, complessità e ICT
3. Rischio e vulnerabilità nelle organizzazioni.
4. Il Fattore Umano nell'analisi del rischio
5. L'analisi del rischio classica: Teoria dell'Utilità Attesa.
6. Oltre il modello classico: errori sistematici e distorsioni delle valutazioni.
7. Euristiche, Metriche
8. Metodi qualitativi di classificazione e Matrici del Rischio
9. Standard ISO/FDIS 31000, 31010 e 27001
10. Rischi e statistiche

Propedeuticità consigliate
Statistica

Materiale di riferimento
Articoli tecnici e scientifici in inglese disponibili dalla pagina del corso
Dispensa del docente

Prerequisiti
Lettura e comprensione testi in inglese

Modalità di esame
Scritto
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano
Inglese (materiale didattico)

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-31/

Altre informazioni
L'esame si tiene in modalità open-book, ovvero è possibile (molto consigliato) portare tutto il materiale didattico. Le domande d'esame richiedono di presentare analisi e commenti ragionati sulla base di una rielaborazione del contenuti del materiale didattico.

Architettura degli elaboratori I

Docente: Scarabottolo Nello

Obiettivi (dettagli AF)

L'insegnamento ha lo scopo di introdurre i concetti di base dell'architettura hardware e firmware dei sistemi di elaborazione, a partire dai fondamenti della logica digitale fino a descrivere il comportamento e la struttura circuitale dei principali componenti di un calcolatore.
L'insegnamento si articola in 40 ore (5cfu) di lezione e 16 ore (1 cfu) di laboratorio.

Programma

FUNZIONAMENTO DEL CALCOLATORE

- ***Architettura di riferimento***. La macchina di Von Neumann. Struttura funzionale delle componenti principali.
- ***Il linguaggio macchina.*** Il linguaggio *Assembly*. Esercizi.

ARCHITETTURA DEL CALCOLATORE

- ***Principi di funzionamento dei sistemi elettronici digitali***. Codifica digitale delle informazioni. Algebra di commutazione, porte logiche, bistabili. Reti combinatorie e sequenziali.
- ***I principali componenti dell'architettura del microcalcolatore***. Circuiti per la realizzazione delle principali funzioni di memoria. Elementi di memoria (ROM, SRAM, DRAM).
- ***Architettura delle periferiche di I/O (Input/Output)***. Tipi e caratteristiche dei dispositivi di I/O. Il bus: struttura e modalità di connessione. La gestione *software* dell'I/O.
- ***Il processore: progetto del Data Path***. Circuiti per le principali operazioni aritmetiche. Progettazione di un modello di ALU.
- ***Il processore: progetto del Control Path***. Progetto di un'unità di controllo. Unità di controllo cablate e microprogrammate.
- ***Principali direttrici di evoluzione architetturale***. Memorie cache. Memoria virtuale. *Pipelining*.

Propedeuticità consigliate

-

Materiale di riferimento

Dispense e lucidi a cura del docente, disponibili sul sito dell'insegnamento.
Materiale consigliato

- P.Patel, Y.Patt: Introduction to computing systems: from bits and gates to C and beyond, McGraw Hill, 2000.
- V.C.Hamacher, Z.G.Vranesic, S.G.Zaky: Introduzione all'Architettura dei Calcolatori, McGraw Hill, 1997.

Prerequisiti

Si richiede una conoscenza dei concetti base di programmazione e la capacità di leggere un testo in inglese.

Modalità di esame

Scritto + Prova pratica

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-18/

Architettura degli elaboratori II

Docente: Scarabottolo Nello

Obiettivi (dettagli AF)

L'insegnamento ha lo scopo di introdurre i concetti di base relativi al funzionamento e alla struttura dei circuiti elettronici digitali, a partire dai fondamenti della logica digitale fino a descrivere le metodologie di sintesi delle reti logiche.
Si presentano inoltre gli aspetti fondamentali di un linguaggio di descrizione dello *hardware* (il VHDL) che permette la rappresentazione sia in modo funzionale sia strutturale di un qualunque sistema digitale.
L'insegnamento si articola in 48 ore (6cfu) di lezione.

Programma

RETI LOGICHE

- ***Principi di funzionamento dei sistemi elettronici digitali***. Codifica digitale delle informazioni. Algebra di commutazione e suoi teoremi principali. Funzionamento e struttura elettronica delle porte logiche.
- ***Analisi e sintesi di reti combinatorie***. Analisi delle reti combinatorie: le tabelle delle verità. Espressioni logiche. Sintesi di reti combinatorie. Ottimizzazioni della sintesi di reti combinatorie.
- ***Analisi e sintesi di reti sequenziali***. I bistabili e il concetto di stato. Analisi delle reti sequenziali. Classificazione delle reti sequenziali. Sintesi di reti sequeniali. Ottimizzazioni della sintesi di reti sequenziali.
- ***I principali componenti integrati***. Classificazione delle famiglie di circuiti integrati. Circuiti integrati combinatori e sequenziali. Circuiti integrati programmabili (ROM, PROM, EPROM, PLA, PAL, FPGA).

LINGUAGGIO DI DESCRIZIONE DELLO *HARDWARE*

Il linguaggio VHDL. Presentazione del flusso di progettazione circuitale in VHDL. Presentazione dell'ambiente di simulazione, sintesi e *testing*. Entità di un dispositivo elettronico. Architetture: funzionale e strutturale. Funzionamento e rappresentazione di un processo. Assegnamento di valori a segnali e variabili. Assegnamenti sequenziali. Assegnamenti concorrenti.

Propedeuticità consigliate

Nessuna.

Materiale di riferimento

Dispense e lucidi a cura del docente, disponibili sul sito dell'insegnamento.
Materiale consigliato

- R.H.Katz: Contemporary Logic Design, Benjamin/Cummings, 1994.
- E.J.McCluskey: Logic Design Principles, Prentice Hall, 1986.

Prerequisiti

Si richiede una conoscenza dei concetti base di programmazione e la capacità di leggere un testo in inglese.

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-17/

Architetture software orientate ai servizi

Docente: Damiani Ernesto

Obiettivi (dettagli AF)

Scopo del corso è introdurre i concetti base e i principi di progettazione delle SOA, nonché gli aspetti non tecnici come l'impatto delle SOA sulla cultura, l'organizzazione e il governo d'impresa. Vengono trattati anche i vari standard per l'interoperabilità, l'infrastruttura tecnologica e i problemi di sicurezza posti dalle implementazioni SOA.

Programma

Le Architetture Orientate ai Servizi sono un modo di organizzare ed utilizzare servizi distribuiti messi a disposizione da fornitori diversi per eseguire processi aziendali. Le SOA forniscono l'infrastruttura necessaria per offrire e ricercare i servizi, nonché per interagire con loro per produrre effetti compatibili con i requisiti e le precondizioni. Il corso descrive i concetti base sulle SOA, i principi di progettazione, gli standard di interoperabilità , le considerazioni di sicurezza, l'infrastruttura esecutiva e i web services, la tecnologia d'implementazione delle SOA. I temi del corso comprendono:

- Modelli di riferimento e di servizio delle SOA
- Motivazioni aziendali per l'adozione del paradigma SOA
- Principi di progetto dei sistemi
- SOA, SOAP e REST
- WSDL, UDDI
- Infrastruttura SOA
- Governance delle SOA
- Sicurezza dei Web Services
- Fornitori e prodotti SOA
- Argomenti monografici

La nozione di SOA però trascende l'aspetto tecnologico, per mettere l'accento sulla condivisione dei servizi. Quindi, sono previsti argomenti monografici aggiuntivi come l'impatto delle SOA sulla cultura, l'organizzazione e il governo dell'impresa.

Propedeuticità consigliate

Reti di Calcolatori

Materiale di riferimento

Dispense e presentazioni del corso
Per consultazione: Thomas Erl "SOA: Principles of Service Design", Prentice Hall

Prerequisiti

Conoscenza delle tecnologie Web, di XML e dei principali protocolli applicativi

Modalità di esame

Progetto più Esame Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano (con seminari in Inglese)

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-47/

Altre informazioni

L'esame consiste nella presentazione di un progetto o seminario (70% del voto) su tema monografico concordato con il docente . E' possibile svolgere l'attività di progetto in gruppo (fino a 3 studenti). La valutazione è completata da un esame scritto sul programma istituzionale del corso

Automazione e misure industriali

Docente: Lazzaroni Massimo

Obiettivi (dettagli AF)

Il corso si propone di studiare sia i principi dell'automazione industriale e le tecnologie digitali basate su calcolatore per il monitoraggio e il controllo di sistemi complessi sia le metodologie e le tecnologie per l'acquisizione dei segnali e delle grandezze sul campo con particolare riguardo alle grandezze che tipicamente si incontrano in automazione.

Programma

BASI TEORICHE

Presentazione del corso. Unità di misura. Sistema internazionale SI. Multipli e sottomultipli. Conversioni. Il problema delle cifre significative. Rappresentazione di sistemi e grandezze fisiche. Analogie elettromeccaniche.

AUTOMAZIONE INDUSTRIALE

Trasformata di Laplace. Esempi di sistemi di controllo. Elementi di teoria dei sistemi (stato di un sistema, descrizione analitica dei sistemi, funzione di trasferimento, risposta all'impulso, traiettoria di stato, studio della stabilità, transitori, diagramma di Bode, diagramma di Nyquist. Criteri di Nyquist e di Bode per lo studio della stabilità). Elementi di teoria della regolazione (retroazione, descrizione analitica di sistemi retroazionati, studio della risposta al gradino e alla rampa, implicazioni sul transitorio e sul regime, rappresentazione dei sistemi retroazionati nel dominio del tempo e delle frequenze, parametri critici). Introduzione ai sistemi numerici (influenza della rappresentazione digitale dei segnali, descrizione discreta dei sistemi, transitorio e regime, controllabilità e stabilità, evoluzione dinamica dei sistemi, regime e transitorio, componenti di un sistema di controllo digitale). L'hardware (sensori, attuatori, sistemi di trasmissione, regolatori, PLC).
Misura dei segnali (acquisizione e trattamento dei segnali, procedure di misura, incertezza, confidenza, ambienti distribuiti di misura). Il Software (caratteristiche di base del software per controllo di processo, test di software per il controllo di processo, algoritmi di base (PID). Software di mercato e software dedicato: criteri di scelta ed effetti su tempi e costi).

MISURE INDUSTRIALI

Metrologia: misura di una grandezza fisica o di un segnale, i campioni e le unità di misura, grandezze fondamentali, gli istituti metrologici, il SIT, errore e incertezza, il concetto della riferibilità. I sistemi di misura automatici: rappresentazione dei segnali, i segnali tempo discreti, il teorema del campionamento, l'aliasing, formula di ricostruzione di Shannon, analisi nel dominio della frequenza, struttura di un sistema automatico di misura, sistemi multicanale, banda passante, multiplexing, il filtro antialiasing, gli strumenti virtuali.
Convertitori A/D: struttura, caratteristica di conversione, errori, dithering, il sample & hold, bit effettivi. La struttura dei sistemi di elaborazione numerica dei segnali: la struttura a microcalcolatore, memoria, bus, i bus industriali. Sistemi a DSP e a microcontrollore.
Interfacciamento: IEEE 488, RS 232, RS 422, RS 485, IEEE 1394, USB.
Sensori e trasduttori: principio di funzionamento, specifiche e loro utilizzo. Websensor.
Sistemi di visualizzazione e presentazione dei dati: LED, CRT e display a LCD.

Propedeuticità consigliate

-

Materiale di riferimento

Dispense, lucidi e articoli messi a disposizione dal docente durante il corso.

Prerequisiti

-

Modalità di esame
Scritto e orale
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-B/F67-22/

Basi di dati

Docente: Samarati Pierangela

Obiettivi (dettagli AF)

Il corso ha l'obiettivo di introdure i concetti fondamentali delle basi di dati relazionali e dei sistemi di gestione, le metodologie di progettazione delle basi di dati, la struttura interna di un sistema di gestione delle base di dati, la gestione delle transazione e delle architetture distribuite. Il corso inoltre illustra alcune direzioni di evoluzione della tecnologia delle basi di dati quali la gestione dei dati semistrutturati, le basi di dati attive e le basi di dati per il supporto alle decisioni.

Programma

1. *Introduzione alle basi di dati.* Sistemi Informativi, sistemi organizzativi e sistemi informatici. Concetto di informazione e dato. Introduzione a basi di dati e DBMS, modello dei dati, concetto di schema ed istanza. Indipendenza logica e fisica dei dati, tipologia di linguaggi per basi di dati, entità coinvolte nella gestione delle basi di dati.
2. *Modello relazionale.* Modelli logici. Modello relazionale: relazioni vs tabelle; relazioni con attributi; notazioni; informazione incompleta e valori nulli. Vincoli di integrità: vincoli di tupla; chiavi e valori nulli; vincoli di integrità referenziale.
3. *Algebra relazionale.* Operatori di base (unione, intersezione, differenza, selezione e proiezione) ed operatori derivati (natural join, theta join, semi-join). Interrogazioni in algebra relazionale ed equivalenza di espressioni algebriche. Idiomi di interrogazione.
4. *SQL.* Data Definition Language: i domini elementari, definizione di schema, tabelle e di domini. Vincoli intrarelazionali ed interrelazionali. Interrogazioni in SQL: interrogazioni semplici, operatori aggregati, clausola di GROUP BY, interrogazioni di tipo insiemistico e nidificate. Operazioni di inserimento, modifica e cancellazione. Definizione di vincoli di integrità generici, asserzioni e viste. Controllo dell'accesso.
5. *Progettazione di basi di dati.* Ciclo di vita dei sistemi informativi. Raccolta e analisi dei requisiti. Metodologia di progettazione. Fasi della progettazione. Il modello Entità-Relazione: costrutti (entità, relazione, attributo, cardinalità, identificatori, gerarchie); documentazione di schemi; regole. Strategie di progetto: top-down, bottom-up, inside-out, mista. Qualità di uno schema concettuale. Progettazione logica: ristrutturazione di schemi E-R (eliminazione delle gerarchie; scelta degli identificatori principali; partizionamento/accorpamento di entità e relazione); traduzione verso il modello relazionale; documentazione di schemi logici. Cenni alla progettazione fisica.
6. *Organizzazione fisica delle basi di dati.* Moduli per l'accesso ai dati. Memoria principale, memoria secondaria e buffer. Gestore del buffer e sue primitive. Organizzazione dei file: struttura sequenziale (seriale, ad array, ordinata), ad accesso calcolato (hash-based), ad indici (alberi). Alberi B e B+. Gestione delle tuple nelle pagine. Progettazione fisica e definizione degli indici.
7. *Gestione delle transazioni.* Definizione di transazione. Proprietà ACIDe delle transazioni. Transazioni e moduli di sistema. Gestore dell'affidabilità. Memoria stabile. Log: organizzazione, record e gestione. Guasti e loro gestione: ripresa a caldo e a freddo. Controllo della concorrenza. Anomalie delle transazioni concorrenti. Schedule seriali e serializzabili. View-equivalenza e conflict equivalenza. Locking a due fasi e sue varianti. Timestamp (monoversione e multiversione). Lock e loro gestione. Locking e livelli di isolamento in SQL. Deadlock e sua gestione. Livelock e starvation.
8. *Architetture distribuite.* Paradigmi per la distribuzione dei dati. Tipologie di architetture. Proprietà dei sistemi distribuiti. Architettura client-server. Basi di dati distribuite. Frammentazione e allocazione dei dati. Livelli di trasparenza. Transazioni in basi di dati distribuite: classificazione e gestione delle proprietà ACIDe. Ottimizzazione di query distribuite. Metodo di Lamport. Deadlock distribuiti: definizione e gestione. Protocolli di commit distribuito: commit a due fasi e sue varianti.
9. *Dati semistrutturati.* XML. Definizione di dati semistrutturati in XML. Interrogazione di dati XML: XQuery e XPath; espressioni FLOWR.
10. *Basi di dati attive.* Regole E-C-A. Trigger. Livelli e modalità di esecuzione. Caratteristiche evolute delle regole attive. Proprietà delle regole attive: terminazione, confluenza, determinismo delle osservazioni. Analisi di terminazione. Applicazioni delle regole attive.
11. *Basi di dati per il supporto alle decisioni.* OLTP vs OLAP. Basi di dati per il supporto alle decisioni (OLAP). Data warehouse: caratteristiche e architettura. Rappresentazione multidimensionale dei dati. Operazioni su dati multidimensionali. Realizzazione di un data warehouse. Progettazione di un

data warehouse: schema a stella e a fiocco di neve. Operazioni su ROLAP. Aggregazione in SQL. Data mining: regole di associazione e di classificazione.

Propedeuticità consigliate
-

Materiale di riferimento
- P. Atzeni, S. Ceri, S. Paraboschi, R. Torlone, *Basi di Dati: Modelli e Linguaggi di Interrogazione*, 2 ed., McGraw-Hill Italia, 2006
- P. Atzeni, S. Ceri, P. Fraternali, S. Paraboschi, R. Torlone, *Basi di Dati: Architetture e Linee di Evoluzione*, 2 ed., McGraw-Hill Italia, 2007
- S. Foresti, E. Pedrini, S. De Capitani di Vimercati, *Eserciziario di Basi di Dati*, Pitagora ed., 2006
- Slide disponibili sul sito web del corso

Prerequisiti
Concetti di informatica di base

Modalità di esame
Scritto
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-12/

Calcolo delle probabilità e statistica matematica

Docente: Gianini Gabriele

Obiettivi (dettagli AF)

Il corso si propone di introdurre lo studente ai concetti di base del Calcolo delle Probabilità e della Statistica inferenziale e di indicare le principali applicazioni di queste discipline in ambito informatico.

Programma

Definizione di probabilità di un evento. Probabilità dell'evento complementare e dell'unione di eventi di due o più eventi.
Probabilità condizionata: eventi dipendenti e indipendenti; legge del prodotto; verifica dell'indipendenza.
Struttura della dipendenza a 2 e a più eventi: le copule.
Legge della somma. Valore atteso di una quantità. Teorema di Bayes e probabilità inversa; aggiornamento e forecasting.
Variabili Aleatorie. Distribuzioni e densità di probabilità elementari. Funzione cumulativa e anticumulativa. Moda, mediana e media. Quartili. Intervallo interquartile. Percentili. Quantili. Funzione Quantile. Momenti di ordine superiore. Momenti centrali. Varianza. Deviazione standard. Cenni al concetto di Informazione; l'Entropia di Shannon.
Processo Bernoulliano, processo Poissoniano. Distribuzioni dei tempi d'attesa: dalla Geometrica all'esponenziale negativa. Mancanza di memoria. Dalla Binomiale alla Poissoniana. Merging and splitting di processi di Poisson. La distribuzione Multinomiale.
Gaussiana o Normale. Legge tre sigma. Uso delle tabelle per Normale standard.
Somma di variabili aleatorie indipendenti. Funzioni generatrici. La distribuzione Binomiale Negativa.
Il teorema del limite centrale. Cenni ai cammini aleatori.
La densità di Cauchy. Il teorema generalizzato del limite centrale.
Le distribuzioni campionarie di minimo e massimo, media e mediana. Campionamento da uniforme e da gaussiana.
Teorema di Bayes e metodi Bayesiani.
Probabilità inversa per Gaussiana.
Ruolo della Lilkelihood e della prior.
Stima Maximum Likelihood.
Distribuzione ipergeometrica. Sistemi con memoria.
Cenni alle Catene di Markov. Cenni agli Hidden Markov Models (HMM).
Variabili aleatorie in 2D e 3D: distribuzioni congiunte. Probabilità condizionata e dipendenza per distribuzioni e densità: distribuzioni condizionate. Valore atteso condizionale.
Trasformazioni di coordinate 1D, 2D, 3D.

Propedeuticità consigliate

Matematiche del discreto, Matematiche del continuo

Materiale di riferimento

Sito Web del Corso

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-7/

Complementi di matematica

Docente: Zampieri Elena

Obiettivi (dettagli AF)

Proporre, sviluppare, analizzare e implementare in linguaggio MATLAB metodi numerici per l'approssimazione di alcuni problemi di analisi matematica, geometria e algebra lineare.

Programma

1. Introduzione al corso. Scopo del Calcolo Numerico. Generazione e propagazione degli errori in un processo di calcolo. Condizionamento e stabilità nei problemi matematici, numerici e negli algoritmi. Rappresentazione dei numeri sul calcolatore.
2. Risoluzione numerica di equazioni non lineari. Metodi di bisezione, secanti, Newton, punto fisso. Analisi di convergenza. Test d'arresto.
3. Risoluzione numerica di sistemi lineari. Analisi dell'errore e condizionamento di un sistema lineare. A) Metodi diretti. Sistemi triangolari. Metodo di eliminazione di Gauss. Fattorizzazione LU. Pivoting. Altre fattorizzazioni. B) Metodi iterativi. Metodi di Jacobi, Gauss-Seidel, SOR. Introduzione ai metodi di tipo gradiente. Splitting. Convergenza e criteri di arresto.
4. Interpolazione e approssimazione di funzioni e di dati. Interpolazione polinomiale: unicità del polinomio di interpolazione, forma di Lagrange e di Newton (con algoritmo di Horner). Stima dell'errore di interpolazione. Interpolazione nei nodi di Chebyshev. Splines lineari e cubiche. Approssimazione di dati nel senso dei minimi quadrati.
5. Integrazione numerica. Formule di quadratura interpolatorie. Formule di Newton-Cotes. Errore di quadratura e grado di precisione. Formule di quadratura composite. Formule di quadratura di Gauss.
6. Approssimazione di autovalori e autovettori. Localizzazione. Il metodo delle potenze.
7. Approssimazione numerica di ODE. Metodi di Eulero, Crank-Nicolson, Runge-Kutta 2 e 4. Concetti di consistenza, convergenza, zero-stabilità, assoluta stabilità.

Propedeuticità consigliate

Matematica del continuo. Matematica del discreto.

Materiale di riferimento

- Appunti sulle pagine web del corso.
- A. Quarteroni, F. Saleri: Introduzione al calcolo scientifico: esercizi e problemi risolti con MATLAB. Milano, Springer 2004, seconda edizione.
- A. Quarteroni, R. Sacco, F. Saleri: Matematica Numerica. Milano, Springer 2000.
- V. Comincioli: Analisi numerica: metodi, modelli, applicazioni. Milano, McGraw-Hill Libri Italia 1995.
- G. Naldi, L. Pareschi: MATLAB Concetti e progetti. Milano, Apogeo 2002.

Prerequisiti

Numeri reali e complessi. Polinomi. Vettori e matrici. Limiti, derivate e integrali. Studio di funzioni da $\mathbb{R}$ in $\mathbb{R}$. Successioni numeriche. Funzioni da $\mathbb{R}^2$ in $\mathbb{R}$. Derivate parziali. Equazioni differenziali ordinarie.

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-3/

Altre informazioni
Lezioni ed esercitazioni in aula e in laboratorio informatico. L'esame consta di una prova scritta con l'ausilio del software MATLAB. Sono previsti anche quesiti teorici. La prova orale è facoltativa per gli studenti con scritto sufficiente (maggiore o uguale di 18/30).

Complementi di ricerca operativa (Operations research complements)

Professor: Righini Giovanni

Goals

The course aims at presenting some of the classical algorithmic techniques in Operations Research, both for solving problems of polynomial complexity and for NP-hard problems.

Syllabus

EFFICIENT ALGORITMS FOR GRAPH OPTIMIZATION PROBLEMS:

- Graphs, definitions and properties.
- Problems of minimum cost connectivity. Minimum cost spanning tree: Kruskal, Prim, Boruvka algorithms. Minimum cost spanning arborescence: Edmonds algorithm.
- Shortest path problems. Unweighted graphs: BFS algorithm. Weighted acyclic graphs: Critical Path Method. Graphs without negative cost cycles: Bellman-Ford algorithm. Graphs without negative cost arcs: Dijkstra algorithm. Floyd-Warshall algorithm for the computation of the all-pairs shortest paths matrix on a weighted digraph.
- Optimal flow problems. Ford-Fulkerson algorithm for the maximum flow problem and its implementations. Algorithms for the maximum flow minimum cost problem. Duality: max flow - min cut theorem. Gomory and Hu algorithm for the minimum cut in a weighted graph.
- Matching problems. Transformation of matching problems into flow problems. Hungarian algorithm.
- Minimum cost transportation problems. Transformation into minimum cost flow problems. Dantzig algorithm.

OPTIMIZATION ALGORITHMS FOR NP-HARD PROBLEMS:

- Branch-and-bound. Techniques for dual bounds computation: linear relaxation, Lagrangean relaxation, surrogate relaxation, combinatorial relaxations. Heuristics for the computation of primal bounds. Tree search policies. Branching methods. Implementation of branch-and-bound algorithms.
- Dynamic programming. Illustration and examples. Data-structures and space an dtime complexity of dynamic programming algorithms. State space relaxation. Implementation of dynamic programming algorithms.

APPROXIMATION ALGORITHMS FOR NP-HARD PROBLEMS:

- Definitions. Approximation error, approximation schemes.
- Algorithms with constant approximation error.
- Algorithms with approximation error depending on the size of the instance.
- Algorithms with data-dependent approximation error.
- Combination of approximation algorithms.
- Polynomial approximation schemes. The knapsack problem.

Recommended preparatory courses

-

Course materials

F. S. Hillier, G. J. Lieberman: “Introduction to operations research”, McGraw-Hill, 1995.
R. K. Ahuja, T. L. Magnanti, J. B. Orlin: “Network flows”, Prentice Hall, 1993.
Slides available on the course website.

Prerequisites

Operations Research, Computer programming, Algorithms and Data-structures, English.

Course assessments
Written and oral exams
Lecture attendance
Recommended
Teaching format
In presence learning
Language
English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-28/

Other information
Under the supervision of the teacher the students will implement some of the algorithms learned during the course.

Crittografia

Docente: Cimato Stelvio

Obiettivi (dettagli AF)

Il corso si propone di introdurre gli studenti alla conoscenza dei concetti fondamentali e delle applicazioni pratiche della crittografia moderna. A partire dalle tecniche classiche di cifratura, verranno presentati durante il corso i principali algoritmi crittografici per la cifratura simmetrica e asimmetrica, per la creazione ed utilizzo di funzioni hash e mac, per la firma digitale, per lo scambio di chiavi crittografiche e per la condivisione di segreti.

Programma

1. *Crittografia Classica.* Tecniche di crittografia classiche e crittoanalisi. Cifrari di Cesare, Playfair e Hill. Cifrari a sostituzione polialfabetica. Cifrario di Vigenere e crittoanalisi. Macchine cifranti. One-time pad. Steganografia.
2. *Crittografia Simmetrica*. Principi della cifratura a blocchi. Strutture di Feistel. DES e modalita' operative. Crittoanalisi lineare e differenziale. AES. Altri cifrari simmetrici:Blowfish, RC5 e RC4.
3. *Crittografia Asimmetrica*. Principi dei crittosistemi a chiave pubblica. RSA. Sicurezza e aspetti computazionali. Test di primalita'. Crittosistema di El-Gamal. Crittografia a curva ellittica.
4. *Funzioni Hash e MAC.* Funzioni hash: attacco del compleanno, funzioni hash iterate, MD4, MD5, SHA-1, funzioni hash basate su cifrari a blocchi. Message Authentication Code: CBC-MAC, MAC basati su funzioni hash, HMAC.
5. *Firme Digitali.* RSA, Digital Signature Standard.
6. *Gestione delle chiavi e altre applicazioni.* Gestione e scambio di chiavi: Diffie-Hellmann. PKI e Certificati. Sistemi di condivisione del segreto. Crittografia visuale.

Propedeuticità consigliate

Matematica discreta, Calcolo probabilità e statistica

Materiale di riferimento

Slide del corso

W. Stallings, "Crittografia e Sicurezza delle Reti", McGrawHill, 2004"

Douglas Stinson - *Cryptography: Theory and Practice (Second Edition)*, Chapman 2002

B. Menezes, P. van Oorschot, S. A. Vanstone - *Handbook of Applied Cryptography*, CRC Press 1996

Prerequisiti

-

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-B/F68-12/

Altre informazioni

E' possibile integrare il voto con un progetto facoltativo.

Diritto penale dell'informatica

Docente: Salvatore Davide

Obiettivi (dettagli AF)

Al termine del corso lo studente sarà in grado di comprendere gli elementi essenziali dell'ordinamento penale italiano ed avrà sviluppato una conoscenza dettagliata relativa ai reati informatici in esso presenti.

Programma

Diritto penale: principi del diritto penale (principi di legalità, irretroattività e colpevolezza); elementi del reato; principali categorie di reati (reati di condotta e di evento, reati di danno e reati di pericolo, reati commissivi e omissivi); cause di giustificazione; colpevolezza; il sistema della sanzione penale.
Diritto penale dell'informatica: introduzione ai reati informatici; frode informatica (art. 640-ter c.p.); abuso di carte di pagamento (art. 12 l. 197/1991); danneggiamento informatico (art. 635-bis, art. 635-ter, art. 635-quater e art. 635-quinquies c.p.); diffusione di programmi finalizzati a danneggiare un sistema informatico (art. 615-quinquies c.p.); accesso abusivo ad un sistema informatico (art. 615-ter c.p); possesso e diffusione di codici di accesso (art 615-quater c.p.).

Propedeuticità consigliate

-

Materiale di riferimento

C. Pedrazzi, Introduzione al diritto penale, Cusl, 2003
C. Pecorella, Il diritto penale dell'informatica, CEDAM, 2006, cap. I, cap. II, cap. IV e cap. V sez. seconda e terza
Un'edizione aggiornata del codice penale.

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F68/default/F68-8/

Altre informazioni

Gli studenti frequentanti potranno sostenere una prova intermedia relativa alla parte generale del diritto penale.

Elaborazione dei segnali e delle immagini

Docente: Pizzi Rita

Obiettivi (dettagli AF)

Il corso si pone l'obiettivo di presentare la teoria della trasmissione a partire dal concetto di informazione, che viene esaminata in chiave sia classica che quantistica, introducendo alle applicazioni più importanti.

Programma

Introduzione al concetto di informazione classica. Studio del concetto di sorgente di informazione (discreta senza memoria e con memoria), del concetto di canale di trasmissione, dei teoremi di Shannon. Introduzione a teoria della trasmissione, teorema del campionamento, analisi spettrale del segnale e criterio di Nyqvist. Introduzione dei principali metodi di codifica compresa quella convoluzionale, ed elementi di crittografia. Si introducono infine le prime nozioni di informazione quantistica ed i concetti necessari per comprendere il funzionamento dei sistemi di crittografia quantistica.

Propedeuticità consigliate

Almeno 12 crediti di corsi di Matematica

Materiale di riferimento

Documentazione sul sito web di riferimento
E. Angeleri, Informazione: Significato e Universalità, UTET 2000.
David J.C. MacKay, A short Course in Information Theory, http://www.cs.toronto.edu/~mackay/info-theory/course.html

Prerequisiti

Nozioni di analisi matematica

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-4/

Elaborazione di immagini (Image Processing I)

Professor: Ferrari Stefano

Goals

The aim of this course is to provide the general principles on the acquisition, the representation, and the improvement of digital images and the processing techniques for extracting information from images of real scenes.

Syllabus

The course concerns the funding concepts of the digital image processing. The lectures will introduce the principles of the processing of digital signals, the sampling, and encoding, the techniques generally used in image processing: geometrical operations, features extraction, equalization, filtering, transforms, image encoding and compression. Laboratory sessions will also take place in which numeric simulation software will be used.

- **Introduction**: introduction to the image processing, image basic concepts.
- **Digital images fundamentals**: light, vision and perception; acquisition and digitalization of images.
- **Image representation**: formats for the representation of digital images, pixel relations, basic mathematical operations.
- **Intensity transforms and spatial filtering**: intensity transforms, histograms, equalization, spatial domain filtering, equalization, image improvement in spatial domain.
- **Filtering in the frequency domain**: Discrete Fourier Transform, extension to 2D functions, filtering and improvement of images in the frequency domain.
- **Morphological image processing**: dilation, erosion, opening, closing, extraction of connected components, convex hull, thinning, thickening, contour extraction.
- **Image segmentation**: edge detection and linking, region based processing.
- **Image compression**: redundancy, image encoding.

Recommended preparatory courses

Fundamentals of probability and statistics, signal processing, and programming.

Course materials

R.C. Gonzalez and R.E. Woods, Digital Image Processing, (3 ed.), Prentice Hall, 2008. ISBN 9780131687288.

Prerequisites

-

Course assessments

Written and oral exams

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-45/

Elaborazione di segnali (Digital signal processing)

Professor: Sassi Roberto

Goals

The course will cover the basis for digital signal processing at an advance undergraduate / graduate level. While rigorously covering the theoretical foundations of the discipline, the course will also include several laboratory sessions where the students will practice writing their own codes (MATLAB).

Syllabus

- **Introduction**. Continuous-time and discrete-time signals. Sequences. Analysis of continuous-time signals in the frequency domain: the Fourier transform. Convolution and correlation.
- **Digital signals: sampling and quantization**. Sampling of continuous-time signals and the sampling theorem. Sampling of periodical signals. Aliasing. Reconstruction of continuous-time signals from samples and interpolation. Quantization.
- **Analysis of discrete-time signals in the frequency domain**. Discrete-time Fourier Transform (DTFT), Discrete Fourier Transform (DFT) and FFT algorithm. Spectral characterization of sampled signals.
- **Linear time**-invariant systems (LTI). Impulse response. Stability and causality. Systems interconnection (series, parallel, feedback). Finite-difference equations as representation of LTI systems.
- **Zeta transform**. Definition and principal properties. Region of convergence. Analysis of LTI systems via Zeta transform. Transfer functions, poles and zeros. Frequency response. Stability condition in the Zeta domain
- **FIR filters**. Linear phase and LTI filter with symmetrical impulse response. FIR filters design with the window method.
- **IIR filters**. Design of digital IIR filters starting from their analog counterparts. Sensitivity to quantization of the filter coefficients.
- **Wavelet transform**. Definition and main properties of the wavelet transform.

Recommended preparatory courses

Courses of "matematica del continuo" (continuous mathematics and "calcolo delle probabilità e statistica matematica" (probability and mathematical statistics)

Course materials

Material freely available from the course's web page.

A. V. Oppenheim & R. W. Schafer, "Discrete-Time Signal Processing" (3rd ed.), Prentice Hall, 2009. (Main textbook in English).

Massimiliano Laddomada e Marina Mondin, "Elaborazione Numerica dei Segnali", Pearson Education Italia, 2007. (Main textbook in Italian).

John G. Proakis, Dimitris G. Manolakis, "Digital signal processing" (4th ed.), Pearson Prentice Hall, 2007. (Reading material).

Prerequisites

-

Course assessments

Written and oral exams

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-44/

Other information

Course breakdown: 20 lectures (40 hours, 5 CFU) and 8 laboratory sessions (16 hours, 1CFU).

Elementi di sicurezza e privatezza

Docente: Braghin Chiara

Obiettivi (dettagli AF)

L'insegnamento ha lo scopo di introdurre i concetti di base relativi alle problematiche di sicurezza e privatezza dei sistemi informatici.

Programma

1. Introduzione. Descrizione dei crimini informatici. Modelli di sicurezza.
2. Politiche e modelli per il controllo dell'accesso: politiche discrezionarie, mandatorie e basate sui ruoli.
3. Diversi livelli di sicurezza: Sicurezza dei sistemi operativi, Sicurezza delle reti, Programmi sicuri.
4. Protocolli di Sicurezza. Meccanismi di identificazione e autenticazione.
5. Un nuovo trend: metodi formali per la sicurezza.
6. Sicurezza nel Web.

Propedeuticità consigliate

Comprensione di un testo scientifico in inglese

Materiale di riferimento

Slide del corso, appunti presi a lezione e articoli in inglese che sono parte integrante del programma del corso.

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-5/

Elettronica

Docente: Liberali Valentino

Obiettivi (dettagli AF)

L'insegnamento illustra i concetti di base dell'elettronica, partendo dai concetti di base della teoria dei circuiti, descrivendo i principi di fuzionamento dei dispositivi a semiconduttore e presentando alcuni semplici esempi di circuiti elettronici per l'elaborazione di segnali analogici e digitali. L'insegnamento è completato da una introduzione alla simulazione circuitale.

Programma

INTRODUZIONE: Grandezze elettriche. Definizione delle grandezze elettriche. Unità di misura del Sistema Internazionale.

CIRCUITI IN CONTINUA: Bipoli elettrici. Resistore. Caratteristica tensione-corrente. Legge di Ohm. Generatori. Generatori indipendenti e dipendenti. Analisi dei circuiti elettrici in continua. Leggi di Kirchhoff. Nodi e maglie. Teoremi di Thévenin e di Norton. Principio di sovrapposizione degli effetti. Teorema della massima potenza. Amplificatore operazionale. Amplificatore operazionale ideale. Retroazione. Stabilità.

CIRCUITI CON GRANDEZZE VARIABILI NEL TEMPO: Caratteristiche dipendenti dal tempo. Induttore. Condensatore. Energia immagazzinata. Potenza istantanea e potenza media. Analisi nel dominio del tempo. Circuito integratore. Circuito derivatore. Costante di tempo.

DISPOSITIVI E CIRCUITI ELETTRONICI: Semiconduttori. Semiconduttori intrinseci. Drogaggio. Proprietà elettriche di un semiconduttore drogato. Diodo. Giunzione p-n. Diodo a giunzione. Relazione tensione-corrente nel diodo. Risoluzione di circuiti con diodi. Transistore a giunzione. Transistore bipolare a giunzione. Regioni di funzionamento. Porte logiche con transistori bipolari. Transistore MOS. Struttura metallo-ossido-semiconduttore (MOS). Transistore MOS a svuotamento. Transistore MOS ad arricchimento. Regioni di funzionamento e relazione tensione-corrente. Tecnologia CMOS. Porte logiche in tecnologia CMOS.

CIRCUITI ELETTROMAGNETICI: Circuiti con trasformatori. Trasformatore. Raddrizzatore a semionda. Raddrizzatore a doppia semionda.

SIMULAZIONE CIRCUITALE: SPICE. Descrizione in SPICE di un circuito elettrico. Tipi di analisi. Simulazione di circuiti con SPICE.

Propedeuticità consigliate

Analisi matematica; Fisica

Materiale di riferimento

L.S. Bobrow: Fundamentals of Electrical Engineering - 2nd edition, Oxford University Press, Oxford, 1996.

Prerequisiti

Conoscenze di base di analisi matematica e di elettromagnetismo

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-B/F67-23/

Estrazione e gestione della conoscenza (Knowledge extraction and management)

Professor: Tettamanzi Andrea Giovanni Battista

Goals

This class is a continuation of the teaching on Information Management.

Syllabus

There is no detailed program. The class is structured around individual student projects under the supervision of the teacher.

Recommended preparatory courses

Information Management

Course materials

Jiawei Han, Micheline Kamber. Data Mining: Concepts and techniques (2nd ed.). Morgan Kauffman, 2006.

Prerequisites

English proficiency, knowledge of discrete mathematics, calculus, probability and statistics, and data bases.

Course assessments

Oral exam

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-50/

Fisica

Docente: Fornili Sandro

Obiettivi (dettagli AF)

Scopo del corso è di proporre allo studente una introduzione al metodo scientifico attraverso il modeling fisico della realtà. Data la scarsità del tempo a disposizione si è scelto di priviligiare lo studio della meccanica in quanto ideale per far acquisire concetti e metodi operativi della fisica e l'elettromagnetismo in quanto settore più naturalmente vicino ad un corso di studi basato sull'uso di computer.

Programma

Il corso introduce il metodo scientifico e nozioni di teoria della misura. Si sviluppa quindi attraverso lo studio della meccanica attraverso una serie di applicazioni che coprono in modo esaustivo, anche se necessariamente elementare, lo studio della cinematica, della dinamica e della statica dei modelli punto materiale e corpo rigido. La seconda parte del corso esamina fenomeni elettrici e magnetici evidenziando dettagli che sono di interesse per la formazione di un informatica.

Propedeuticità consigliate

Matematica del continuo.

Materiale di riferimento

D.C. Giancoli "Physics: Principles with Apllications", Pearson Prentice Hall; D.C. Giancoli "Fisica Principi e Applicazioni", C.E.A.
Materiale on line in formato ppt

Prerequisiti

Matematica elementare; elementi di trigonometria

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Mista

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-19/

Gestione degli incidenti informatici

In fase di assegnazione

Obiettivi (dettagli AF)

Fornire agli Studenti gli strumenti necessari, teorici, metodologici e tecnologici, per effettuare operazioni di Gestione e Risposta agli Incidenti di sicurezza, e contestualizzare i fondamentali della disciplina della Computer Forensics.

Programma

La gestione degli incidenti, generalità
RFC di riferimento - Request for Comments
Le best practices nella acquisizione ed analisi delle prove digitali
Aspetti organizzativi e legali della disciplina dell'incident managament
L'offerta tecnologica, commerciale ed open source.
Sessioni pratiche di laboratorio

Propedeuticità consigliate

Si consiglia una conoscenza adeguata dei princìpi dell'information security, Elementi di programmazione, TCP/IP, FileSystem.

Materiale di riferimento

Lucidi del corso
RFC di riferimento
Software. the PTK Forensic Project (Gratuito)

Prerequisiti

La conoscenza dell'inglese è altamente consigliata.

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale
A distanza

Lingua in cui è tenuto l’insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-B/F68-11/

Gestione dell'informazione (Information management)

Professor: Tettamanzi Andrea Giovanni Battista

Goals

The aim of this class is to illustrate several advanced information management techniques that are collectively known as data mining. These techniques are oriented toward the automatic or semi-automatic extraction of knowledge from huge volumes of data.

Syllabus

INTRODUCTION

- Motivations and definitions: purposes, tools, applications.

DATA PREPARATION

- Description: statistical tools, visualization.
- Data cleaning: missing values, noise, cleaning as a process.
- Transformation and Reduction: integration, transformation, attribute selection, dimensionality reduction, discretization and conceptual hierarchy generation.
- Data warehouses and OLAP: differences with databases, purposes and function, multidimensional model, architectures.

CLASSIFICATION AND PREDICTION

- Main models: fuzzy logic, decision trees, Bayesian classification, rules, neural networks, SVM, k-nearest neighbor.
- Model induction techniques: linear regression, quadratic optimization, evolutionary algorithms.
- Model evaluation: error and accuracy, information-theoretic measures, validation, bootstrap, confidence interval estimation, ROC curve.
- Cluster analysis: partitioning, hierarchic methods, density-based methods, model-based methods.
- TIME SERIES ANALYSIS
- Specificities: sequence analysis, pattern extraction, clustering, phase space.
- Financial time series: markets and financial instruments, technical analysis, modeling, prediction.

Recommended preparatory courses

-

Course materials

Jiawei Han, Micheline Kamber. Data Mining: Concepts and techniques (2nd ed.). Morgan Kauffman, 2006.

Prerequisites

English proficiency, knowledge of discrete mathematics, calculus, probability and statistics, and data bases.

Course assessments

Oral exam

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-9/

Gestione dei processi aziendali

Professor: Damiani Ernesto

Goals

The goal of the course is the study and design of Business Processes and of the role of information systems and technologies that support them. The course will focus on the analysis, design, and implementation of Business Processes, also discussing the issues of workflow management. A number of real case studies will be presented to students during the lectures to get students used to main organizational processes, fostering an applied knowledge on Business Process modeling.

Syllabus

The program of the course is focused on the following main points:

- Learn how to analyze, model, and design a process.
- Understand the role of workflow and process analysis in the context of Business Process Management (BPM).
- Learn the basic principles of process and workflow analysis and management.
- Study in deep the techniques and tools for process modeling and learn how to exploit them in the workflow management.

The subjects treated during the course include:

- Course Introduction
  - Introduction to Business Process
  - Introduction to process analysis and modeling
  - Introduction to BPMN
  - Use of BPMN for process modeling
- Process Modeling
  - Diagrams and swimlanes
  - Event-Driven Process Chain (EPC)
- Workflow Implementation Technologies
  - Technologies for process automation
  - Collaborative organization
  - Workflow base concepts
- Business Process Automation – Workflow Interoperability and Integration
  - Creation of Tasks, Cycles, and logic operator
  - Process and contract interoperability
  - Business workflow – deadlines, reports, tests, and process logs
- Business Process Management from an integration viewpoint
  - Migration of process model towards the implementation platform
  - Analysis of Enterprise and Business Management Tools

Recommended preparatory courses

Course of "Architetture orientate ai servizi" (Service-oriented architectures)

Course materials

Slide and notes of the course.
Reference: A. Grosskopf, G. Decker, and M. Weske, "The process: Business Process Modeling using BPMN," Meghan-Kiffer Press, 2009. ISBN-13: 978-0929652269.

Prerequisites

Web technologies, XML, and main application protocols.

Course assessments
Exercises during the course + final project
Lecture attendance
Recommended
Teaching format
In presence learning
Language
English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-49/

Other information
COURSE EVALUATION

- Written examination: 30.00%
- Team Design Project and presentation: 70.00%
- Extra points will be given during lessons with specific homeworks.
- Assignments: Readings and Research Papers – Besides the reading list given below, each student will be encouraged to search the web and find current journal articles related to the course.

Gestione di progetti
Docente: Gianini Gabriele

Obiettivi (dettagli AF)
Il corso presenta metodi e tecniche di pianificazione, organizzazione, controllo e documentazione di un progetto software. L'obiettivo del corso è quello di fornire una visione chiara dei problemi, dei rischi e dei fattori critici associati ai progetti tecnologici, di introdurre gli studenti al ruolo e alle funzioni del project manager, di illustrare il ciclo di vita del progetto, di presentare le varie tecniche di pianificazione e gestione, di rivedere le varie metodologie di progettazione, sviluppo e collaudo del software, di introdurre alle varie tecniche di gestione del team di processo, degli utenti e delle loro aspettative.
Il corso si propone di introdurre lo studente ai concetti di base del Calcolo delle Probabilità e della Statistica inferenziale e di indicare le principali applicazioni di queste discipline in ambito informatico.

Programma
Aspetti di base: persone, processi, prodotti, strumenti e tecnologie. Processi di sviluppo software e processi di gestione: rilevanza della gestione di progetto. Differenza tra i progetti software e altri tipi di progetto. Modelli di processo software. Le fasi di progetto software. Le strutture organizzative e le responsabilità: l'organigramma, i ruoli, le comunicazioni, le riunioni e il coordinamento. Planning, Estimation, e Scheduling. Istanzazione del processo e scomposizione delle attività (WBS). Definizione delle attività e delle dipendenze. Stime di impegno e durata delle attività, diagrammi GANTT e calendario di progetto, allocazione delle risorse. Economia del software. Gestione del Rischio. Monitoraggio di progetto. Controllo di progetto.

Propedeuticità consigliate
-

Materiale di riferimento
Sito Web del Corso

Prerequisiti
-

Modalità di esame
Scritto
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-28/

Gestione e organizzazione di progetti

Docente: Gianini Gabriele

Obiettivi (dettagli AF)

Il corso presenta metodi e tecniche di pianificazione, organizzazione, controllo e documentazione di un progetto software. L'obiettivo del corso è quello di fornire una visione chiara dei problemi, dei rischi e dei fattori critici associati ai progetti tecnologici, di introdurre gli studenti al ruolo e alle funzioni del project manager, di illustrare il ciclo di vita del progetto, di presentare le varie tecniche di pianificazione e gestione, di rivedere le varie metodologie di progettazione, sviluppo e collaudo del software, di introdurre alle varie tecniche di gestione del team di processo, degli utenti e delle loro aspettative.
Il corso si propone di introdurre lo studente ai concetti di base del Calcolo delle Probabilità e della Statistica inferenziale e di indicare le principali applicazioni di queste discipline in ambito informatico.

Programma

Aspetti di base: persone, processi, prodotti, strumenti e tecnologie. Processi di sviluppo software e processi di gestione: rilevanza della gestione di progetto. Differenza tra i progetti software e altri tipi di progetto. Modelli di processo software. Le fasi di progetto software. Le strutture organizzative e le responsabilità: l'organigramma, i ruoli, le comunicazioni, le riunioni e il coordinamento. Planning, Estimation, e Scheduling. Istanzazione del processo e scomposizione delle attività (WBS). Definizione delle attività e delle dipendenze. Stime di impegno e durata delle attività, diagrammi GANTT e calendario di progetto, allocazione delle risorse. Economia del software. Gestione del Rischio. Monitoraggio di progetto. Controllo di progetto.

Propedeuticità consigliate

-

Materiale di riferimento

Sito Web del Corso

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-28/

Informatica teorica (Theory of computation)

Professor: Trucco Gabriella

Goals

This course is about the part of theoretical computer science that studies the limits of what can be done with computing machines.
The course introduces the basics of the theory of computability and complexity. We deal with the concepts of problem algorithmically solvable and problems that do not allow algorithmic resolution. Then we analyze the classification of problems in complexity classes, defined in terms of limits on the amount of available resources.

Syllabus

- Automata and languages: deterministic and non-deterministic finite automata, regular languages, context-free languages, pushdown automata.
- Theory of computability: Turing machine, decidability, reducibility.
- Complexity theory: time and space complexity.

Recommended preparatory courses

-

Course materials

- Lectures slides
- M. Sipser, Introduction to the theory of computation

Prerequisites

-

Course assessments
Written exam
Lecture attendance
Recommended
Teaching format
In presence learning
Language
English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-8/

Ingegneria dei processi aziendali (Business process engineering)

Professor: Damiani Ernesto

Goals

The goal of the course is the study and design of Business Processes and of the role of information systems and technologies that support them. The course will focus on the analysis, design, and implementation of Business Processes, also discussing the issues of workflow management. A number of real case studies will be presented to students during the lectures to get students used to main organizational processes, fostering an applied knowledge on Business Process modeling.

Syllabus

The program of the course is focused on the following main points:

- Learn how to analyze, model, and design a process.
- Understand the role of workflow and process analysis in the context of Business Process Management (BPM).
- Learn the basic principles of process and workflow analysis and management.
- Study in deep the techniques and tools for process modeling and learn how to exploit them in the workflow management.

The subjects treated during the course include:

- Course Introduction
  - Introduction to Business Process
  - Introduction to process analysis and modeling
  - Introduction to BPMN
  - Use of BPMN for process modeling
- Process Modeling
  - Diagrams and swimlanes
  - Event-Driven Process Chain (EPC)
- Workflow Implementation Technologies
  - Technologies for process automation
  - Collaborative organization
  - Workflow base concepts
- Business Process Automation – Workflow Interoperability and Integration
  - Creation of Tasks, Cycles, and logic operator
  - Process and contract interoperability
  - Business workflow – deadlines, reports, tests, and process logs
- Business Process Management from an integration viewpoint
  - Migration of process model towards the implementation platform
  - Analysis of Enterprise and Business Management Tools

Recommended preparatory courses

Course of "Architetture orientate ai servizi" (Service-oriented architectures)

Course materials

Slide and notes of the course.
Reference: A. Grosskopf, G. Decker, and M. Weske, "The process: Business Process Modeling using BPMN," Meghan-Kiffer Press, 2009. ISBN-13: 978-0929652269.

Prerequisites

Web technologies, XML, and main application protocols.

Course assessments
Exercises during the course + final project
Lecture attendance
Recommended
Teaching format
In presence learning
Language
English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-49/

Other information
COURSE EVALUATION

- Written examination: 30.00%
- Team Design Project and presentation: 70.00%
- Extra points will be given during lessons with specific homeworks.
- Assignments: Readings and Research Papers – Besides the reading list given below, each student will be encouraged to search the web and find current journal articles related to the course.

Linguaggi di programmazione
Docente: Ceselli Alberto

Obiettivi (dettagli AF)
Il corso intende fornire la capacità di
- analizzare in modo critico ogni linguaggio di programmazione,
- valutare le implicazioni che ha la scelta di un particolare linguaggio nei costi e nei tempi di sviluppo di un'applicazione
- scegliere il linguaggio giusto in contesti differenti
- sviluppare strategie per apprendere rapidamente nuovi linguaggi di programmazione.

Programma
Nella prima metà del corso è presentata una panoramica storica dell'evoluzione dei linguaggi di programmazione, delle loro caratteristiche comuni e della loro classificazione. Vengono brevemente presentati anche i fondamenti teorici alla base dell'equivalenza tra linguaggi di programmazione, del problema del rilevamento automatico di errori nei programmi e dell'indecidibilità algoritmica.
Poi, insieme a richiami di programmazione con stile imperativo, vengono approfondite le tecniche di programmazione secondo paradigma funzionale, dichiarativo e logico.

La seconda metà del corso, invece, analizza i cardini comuni a qualsiasi linguaggio di programmazione:
- descrizione formale della sintassi e della semantica di un linguaggio di programmazione
- scope, binding ed il sistema dei tipi
- programmazione strutturata, sottoprogrammi ed encapsulation
- abstract data types, tipi parametrici, overloading, polimorfismo
- supporto alla programmazione ad oggetti e generic programming
- supporto alla programmazione concorrente ed alla gestione delle eccezioni

Durante tutto il corso vengono presentati esempi e proposti piccoli esercizi di programmazione utilizzando diversi linguaggi di programmazione reali.

Propedeuticità consigliate
Programmazione, Sistemi Operativi, Algoritmi e strutture dati.

Materiale di riferimento
R. Sebesta “Concepts of Programming Languages”, ottava edizione, Pearson International Edition, 2009.
Dispense e materiale fornito dal docente durante il corso.

Prerequisiti
Il corso assume come pre-requisiti la capacità di programmazione in un linguaggio qualsiasi (ad esempio C, Java o C#) e la capacità di comprendere un testo in inglese.

Modalità di esame
Progetto e orale
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l’insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-6/

Linguaggi formali ed automi

Docente: De Capitani di Vimercati Sabrina

Obiettivi (dettagli AF)

Il corso ha lo scopo di introdurre la teoria dei linguaggi formali e di illustrarne l'applicazione nelle tecniche per la compilazione e l'interpretazione dei linguaggi di programmazione.
Il corso è suddiviso in due parti: la prima parte descrive le principali proprietà dei linguaggi formali e delle loro rappresentazioni; la seconda parte analizza la struttura dei compilatori, esaminando le diverse fasi del processo di traduzione, le problematiche associate a ciascuna di esse e le relative tecniche di soluzione.

Programma

1. *Introduzione*. Linguaggi e compilatori.
2. *Teoria dei linguaggi formali*. Concetti di base. Grammatiche. Classificazione di Chomsky. Automi e macchine di Turing.
3. *Linguaggi regolari*. Grammatiche regolari. Espressioni regolari. Automi a stati finiti.
4. *Linguaggi liberi dal contesto*. Grammatiche libere dal contesto. Automi a pila.
5. *Compilatori*. Struttura dei compilatori. Fasi di lavoro di un compilatore.
6. *Analisi lessicale*. Token e loro codifica.
7. *Analisi sintattica*. Gestione degli errori. Ottimizzazione del codice. Gestione degli errori.
8. *Analisi semantica*. Grammatiche ad attributi.

Propedeuticità consigliate

-

Materiale di riferimento

- S. Crespi Reghizzi, "Linguaggi formali e compilazione," Pitagora editrice, 2006.
- Slide disponibili sul sito web del corso

Prerequisiti

Concetti di informatica di base

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F67-9/

Logica

Docente: Ciriani Valentina

Obiettivi (dettagli AF)

Gli obiettivi principali del corso sono:

- lo sviluppo dell'attitudine a formalizzare problemi utilizzando la logica proposizionale e del primo ordine;
- la comprensione e l'uso del calcolo logico e degli strumenti logici in alcuni ambiti dell'Informatica;
- l'acquisizione di concetti fondamentali legati alla logica matematica, tra cui la semantica formale della logica proposizionale e del primo ordine.

Programma

La prima parte dell'insegnamento descrive i concetti di base della logica classica: la logica proposizionale e la logica predicativa. La seconda parte fornisce alcuni esempi di applicazioni della logica all'Informatica: linguaggi di programmazione logici, verifica formale di programmi, logiche modali, logica fuzzy, logica di BAN e strutture dati per la rappresentazione di funzioni booleane (OBDD).

INTRODUZIONE. La logica linguistica, filosofica (studio dei paradossi) e matematica.
LOGICA PROPOSIZIONALE. Sintassi e semantica della logica proposizionale. Sistemi deduttivi del calcolo proposizionale: deduzione naturale e calcolo dei sequenti. Forme normali congiuntive e disgiuntive. Cenni di complessità computazionale di alcuni problemi di logica proposizionale.
LOGICA PREDICATIVA. Sintassi e semantica della logica dei predicati. Sistemi deduttivi del calcolo predicativo: deduzione naturale e calcolo dei sequenti. Forma normale prenessa e forma di Skolem. Semidecibilità della logica predicativa. Traduzione dal linguaggio naturale.
RISOLUZIONE. Algoritmo di unificazione. Metodi di risoluzione proposizionale e predicativa. Clausole di Horn e programmazione logica.
LOGICA FUZZY. Insiemi fuzzy. Sintassi e semantica della logica fuzzy: cenni.
BINARY DECISION DIAGRAMS (OBDD). La rappresentazione di funzioni booleane con OBDD. Riduzione di un OBDD. Operatori logici e la funzione `Apply`.
VERIFICA FORMALE DI PROGRAMMI. Triple di Hoare. Regole di calcolo per la correttezza parziale di programmi. Regole di calcolo per la correttezza totale di programmi.
LOGICHE MODALI. Sintassi e semantica delle logiche modali. Esempi di logiche modali. Modello di Kripke.
LOGICA PER LA SICUREZZA. Sintassi e semantica della logica di BAN. Analisi del Protocollo di Needham-Schroeder .

Propedeuticità consigliate

-

Materiale di riferimento

- Andrea Asperti, Agata Ciabattoni, *Logica a Informatica* McGraw-Hill, 1997.
- Michael Huth , Mark Ryan. *Logic in Computer Science: modelling and reasoning about systems* (2nd edition), Cambridge University Press, 2004.
- Mordechai Ben-Ari. *Mathematical Logic for Computer Science* (2nd edition) , Springer, 2001.
- Lucidi ed altro materiale disponibile sul sito web del corso.

Prerequisiti

-

Modalità di esame
Scritto
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-35/

Logistica (Logistics)

Professor: Righini Giovanni

Goals

The course describes the supply chains operations and functions and the problems related to planning and management of logistic systems, with particular emphasis on optimization problems and on computational techniques to solve them.

Syllabus

THE SUPPLY CHAIN:

- Terminology and definitions. Description of the supply chain and its main components.

FORECASTING:

- The problem of demand foreccatsing. Models and algorithms for demand forecasting. Least squares and simple linear regression.

INVENTORY MANAGEMENT:

- Models of inventory systems. Inventory systems with continuous and discrete replenishment. Single-product and multi-product systems. Single-depot and multi-depot systems. Economic order quantity. Scale economies and discount policies.

PRODUCTION LOGISTICS:

- Lot sizing problems. Mathematical models and algorithms.
- Scheduling problems. Mathematical models and algorithms.

DISTRIBUTION LOGISTICS:

- Packing problems. Mathematical models and approximation algorithms: first-fit and best-fit.
- Exact solution via spreadsheet.
- Routing problems. Vehicle routing with additional constraints and heuristic algorithms.

QUEUING THEORY:

- Definitions and properties of queuing systems. Modeling, analysis and synthesis of queuing systems. Use of software for queuing systems optimization.

Recommended preparatory courses

Operations Research

Course materials

Ghiani, Gianpaolo, Gilbert Laporte, Roberto Musmanno. 2004. Introduction to Logistics Systems Planning and Control. John Wiley and Sons, New York.

Prerequisites

-

Course assessments

Written exam

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-42/

Matematica del continuo

In fase di assegnazione

Obiettivi (dettagli AF)

Il corso si propone di presentare argomenti classici dell'analisi matematica indispensabili per affrontare qualunque corso di carattere scientifico: campi numerici, successioni e serie numeriche, calcolo differenziale ed integrale per funzioni reali di variabile reale, serie di funzioni e di potenze, e cenni sulle equazioni differenziali.

Programma

Elementi di teoria degli insiemi

- Insiemi, applicazioni, operazioni sui sottoinsiemi, relazioni di equivalenza.
- Insiemi ordinati, massimo, minimo, estremi superiore ed inferiore.
- Numeri interi e numeri razionali.
- Il sistema dei numeri reali, struttura, operazioni, ascissa di un punto.
- Il principio di induzione.
- Insiemi finiti ed infiniti, numerabilita', potenza del continuo.

Numeri complessi

- Definizioni, forma algebrica, trigonometrica ed esponenziale.
- Rappresentazione geometrica.
- Operazioni, radici e logaritmi.

Successioni

- Successioni reali, definizioni.
- Limiti e teoremi fondamentali. Le forme di indecisione.
- piccolo, O grande, asintoticita', ordini di grandezza, proprieta'.
- Successioni monotone, il numero e.
- Criterio di Cauchy.
- Successioni non regolari, massimo e minimo limite.
- Successioni definite per ricorrenza.

Funzioni reali di variabile reale

- Limiti, criterio di Cauchy, monotonia e proprieta'.
- Continuita' e prime proprieta'.
- Teoremi sulle funzioni continue in un intervallo chiuso.
- Continuta' della funzione inversa.
- Infiniti ed infinitesimi.
- Derivata: definizione e significato geometrico.
- Regole di derivazione, derivata delle funzioni elementari.
- Derivata delle funzioni composte e della funzione inversa.
- Derivate successive.
- Teoremi fondamentali del calcolo differenziale e loro applicazioni (Rolle, Lagrange, Cauchy, Hôpital).
- La formula di Taylor.
- Punti di crescenza e di decrescenza, di massimo e di minimo relativo.
- Convessita'.

Serie numeriche

- Definizioni, criterio generale di convergenza.
- Serie a termini positivi, criteri del confronto, della radice e del rapporto.
- Serie a termini di segno qualunque, convergenza assoluta.
- Serie a termini a segno alterno.
- Proprieta' associativa e commutativa, operazioni sulle serie.

Integrazione

- Definizioni e considerazioni geometriche.
- Integrale di una funzione continua, proprieta'.
- Integrali definiti.

- Teorema fondamentale del calcolo integrale.
- Integrali indefiniti.
- Integrali impropri.
- Integrazione delle funzioni elementari, integrali immediati, per decomposizione in somme, per sostituzione e per parti.
- Integrazione delle funzioni razionali fratte e di alcune trascendenti elementari.
- Calcolo degli integrali definiti.
- Cenni sull'integrale di Riemann.

Serie di funzioni (cenni)

- Successioni di funzioni.
- Serie di Funzioni.
- Serie di Taylor.
- Serie di potenze, con applicazione alle funzioni generatrici e alla risoluzione di equazioni di ricorrenza.

Equazioni differenziali (cenni)

- Definizioni.
- Equazioni a variabili separabili.
- Equazioni lineari di primo ordine.

Propedeuticità consigliate

-

Materiale di riferimento

J.P. Cecconi, G. Stampacchia, Analisi matematica. I° volume : funzioni di una variabile, Liguori Editore

Prerequisiti

-

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-20/

Matematica del discreto

In fase di assegnazione

Obiettivi (dettagli AF)

Il corso si propone di presentare una visione assiomatica di quanto studiato nelle scuole precedenti. In particolare vengono presentati vari tipi di strutture algebriche, con varie applicazioni interessanti per i corsi di laurea che hanno l'informatica come base.

Programma

Teoria dei numeri elementare: induzione, congruenze, classi di equivalenza e numeri razionali, rappresentazione dei numeri in varie basi.
Strutture algebriche; gruppi, anelli, campi e spazi vettoriali. Applicazioni a matrici, sistemi lineari, geometria lineare del piano e dello spazio.

Propedeuticità consigliate

-

Materiale di riferimento

BIANCHI- GILLIO: Introduzione alla Matematica Discreta – McGraw-Hill
DOLCHER: Algebra Lineare – Zanichelli
ALZATI, BIANCHI, CARIBONI: Matematica Discreta: Esercizi, CittàStudi Edizioni.
Dispense del corso

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.dti.unimi.it/corsi/matematica_discreto

Metodi probabilistici (Probabilistic Methods)

Professor: Pizzi Rita Maria Rosa

Goals

The course aims to complete and integrate the mathematical skills of the student using as a reference frame the classical probability theory and its main application methods.

Syllabus

Introduction to the probability calculus
Theory of random variables
Models of discrete and continuous rtandom variables
Estimation theory
Statistical hypothesis tests
Random processes and Markov chains
Autoregressive methods

Recommended preparatory courses

Mathematics: at least 12 credits
Probability Calculus and Statistics

Course materials

Course website documentation
Introduction to the theory of statistics. Mood, Alexander Mcfarlane
New York, NY, US: McGraw-Hill. (1950). xiii, 433 pp.

Prerequisites

Mathematics: foundations
Probability calculus and Statistics

Course assessments

Written and oral exams

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-4/

Modellazione ed analisi di sistemi

Docente: Riccobene Elvinia Maria

Obiettivi (dettagli AF)

Il corso presenta le fondamentali metodologie e tecniche per la specifica e l' analisi formale di sistemi HD/SW. Lo studente imparerà i fondamenti teorici delle metodologie di modellazione astratta sia di tipo operazionale che dichiarativo, e delle tecniche di validazione e verifica formale basate su simulazione, testing, e model checking. Alla fine del corso lo studente sarà in grado di usare specifici linguaggi di specifica che consentono di descrivere un sistema da analizzare e le proprietà da provare, nonché gli strumenti automatici (tool) che consentono la verifica ((semi-)automatica e/o interattiva) delle proprietà di un sistema.

Programma

Introduzione: Cosa sono ed a cosa servono i Metodi Formali. Applicazione dei Metodi Formali alla progettazione ed all'analisi di sistemi.
Modellazione ed analisi ad alto livello di astrazione. Le Abstract State Machines (ASM). Tecniche di raffinamento di modelli. Tecniche di astrazione. Il tool-set *ASMETA* per modelli ASM. Casi di studio di specifica di sistemi.
Modellazione ed analisi a basso livello di astrazione. Automi di Kripke e Logica Temporale CTL: sintassi, semantica, pattern di specifica. Algoritmi di model checking. Simbolic Model Checking con rappresentazione mediante OBDD. Verifica di proprietà temporali: proprietà di raggiungibilità, di safety, di liveness, di fairness, assenza di deadlock. Astrazione di modelli: fusione degli stati; astrazione di variabili, riduzione di variabili, observer automata. Raffinamenti di modelli: mappatura di modelli ad alto livello di astrazione verso modelli temporali. Tool: NuSMV e AsmetaSMV.

Propedeuticità consigliate

Linguaggi di Programmazione per la Sicurezza, Logica.

Materiale di riferimento

- Egon Boerger, Robert Staerk. **Abstract State Machines. A Method for High-Level System Design and Analysis.** Springer Verlag, 2003.
- Michael Huth , Mark Ryan. **Logic in Computer Science: modelling and reasoning about systems** (2nd edition). Cambridge University Press, 2004.
- B. Berard et al., **System and Software Verification** Model-Checking Techniques and Tools, Springer Verlag, 2001.

Prerequisiti

Concetti di informatica di base e quelli forniti nei corsi di "Progettazione del Software" e di "Logica".

Modalità di esame

Scritto e prova pratica

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-36/

Altre informazioni

La prova scritta d'esame precede la prova pratica .

Organizzazione aziendale
In fase di assegnazione

Obiettivi (dettagli AF)
Il corso si pone l'obiettivo di fornire agli studenti conoscenze relative alla progettazione dell'organizzazione aziendale, e gli strumenti per interpretare casi empirici di realtà aziendali.

Programma in italiano
Il contesto istituzionale in cui operano le imprese.
Gli elementi costitutivi di un'impresa e la gestione d'impresa.
Il sistema organizzativo. Le variabili di sistema e quelle organizzative.
Elementi di progettazione organizzativa.
Stili di direzione.

Propedeuticità consigliate
-

Materiale di riferimento
Daft R.L., Organizzazione Aziendale, Apogeo, Milano

Prerequisiti
-

Modalità di esame
Scritto e orale
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.dti.unimi.it/corsi/organizzazioneaziendale

Privatezza e protezione dei dati

Docente: Samarati Pierangela

Obiettivi (dettagli AF)

Viviamo oggi nella cosi detta società dell'informazione, sempre più basata sulla pubblicazione, condivisione e rilascio di dati. In tale contesto diventa cruciale proteggere la privacy degli utenti e delle informazioni che li riguardano sia nell'interazione con altre parti sia nella gestione e nel rilascio dei dati. L'obiettivo di questo corso consiste nel fornire una analisi dei principali problemi legati alla privatezza dei dati nella società dell'informazione e nell'offrire una panoramica dei recenti approcci per assicurare il rispetto della privacy nella gestione e nel rilascio dei dati nelle moderne applicazioni.

Programma

- Modelli avanzati per il controllo dell'accesso
- Modelli e linguaggi per il controllo sull'uso secondario delle informazioni
- Composizione di politiche di controllo dell'accesso
- Privacy nel web
- Protezione dei dati di locazione
- Protezione dei dati in outsourcing
- Protezione di dati in sistemi distribuiti
- Protezione di macrodati e microdati.
- Metriche e tecniche di protezione; k-anonymity, l-diversity

Propedeuticità consigliate

Articoli e slide disponibili sul sito web del corso

Materiale di riferimento

Articoli e slide disponibili sul sito web del corso

Prerequisiti

Concetti di base di: sicurezza e privatezza; basi di dati

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-33/

Progettazione del software

Docente: Riccobene Elvinia Maria

Obiettivi (dettagli AF)

Il corso presenta i principi, i processi e le tecniche per la progettazione e lo sviluppo di applicazioni software. Il corso è organizzato in due parti tra loro complementari: i principi dell'ingegneria del software e la progettazione model-driven. L'obiettivo della prima parte è quello di fornire le conoscenze necessarie per la progettazione di software e per l'analisi del codice prodotto attraverso test e tecniche di analisi statica e dinamica del flusso esecutivo. La finalità della seconda parte è quella di introdurre le più moderne tecniche di progettazione basate sull'uso di modelli, a diversi livelli di astrazione sia PIM (platform independent model) che PSM (platform specific model), l'uso delle trasformazioni di modelli per la codifica, e design pattern architetturali per un design a componenti.

Programma

1. **CICLO DI VITA DEL SOFTWARE.** Proprietà del software. Fasi di sviluppo del software. Modelli di ciclo di vita. La sicurezza nel ciclo di vita del software. Ciclo di vulnerabilità.
2. **ARCHITETTURE SOFTWARE.** Principi di architetture. Linee guida e principi per architetture sicure.
3. **SPECIFICA E PROGETTAZIONE DI SOFTWARE**. Proprietà di specifiche di software. Metodi di specifica. Macchine a stati finiti. Communicating Machines. Design by contract. JML.
4. **IMPLEMENTAZIONE**. Linee guida per la programmazione sicura. Tipici errori. Sicurezza dei linguaggi di programmazione. Alcune violazioni di sicurezza in C. Programmi sicuri in C. Introduzione al linguaggio Java. Java sandbox. Dalla specifica al codice: macchine a stati finiti in Java.
5. **TESTING**. Il testing nel ciclo di vita del software. Tipi di testing. Tecniche per la validazione e verifica. I limiti del testing. Testing basato sui programmi. Grafo di flusso di un programma. Copertura delle istruzioni e degli archi. Copertura delle decisioni e delle condizioni. I metodi MCC e MCDC. Valutare la copertura con Emma. Il tool JUnit.
6. **MODEL-DRIVEN ENGINEERING**. Principi dell' MDE. Modello e meta modello. Contesti di applicazione dell' MDE: MDA (model-driven architecture), Profili UML per la specifica di Domain-Specific Languages.
7. **MODELLAZIONE UML: SPECIFICA STRUTTURALE**. Modellare con le classi (diagramma delle classi, diagramma degli oggetti). Specifica dei vincoli: OCL. Uso dei Design pattern.
8. **MODELLAZIONE UML: SPECIFICA COMPORTAMENTALE**. Modellare interazioni e comportamento (diagrammi di interazione, macchine di stato, diagrammi di attività).
9. **PROCESSO UP (UNIFIED PROCESS) E SPECIFICA DI ARCHITETTURE SW**. Il processo UP. Principi guida per lo sviluppo di architetture SW. Modellazione UML dell' architettura (diagramma delle componenti, digramma di dislocamento)

Propedeuticità consigliate

Programmazione, Algoritmi e Strutture Dati

Materiale di riferimento

- Ghezzi Carlo, Jazayeri Mehdi, Mandrioli Dino. Ingegneria del software. Fondamenti e principi. Pearson Education Italia, 2004, 2ª ed.
- Glenford J. Myers, Corey Sandler, Tom Badgett, Todd M. Thomas. The Art of Software Testing. John Wiley & Sons; 2 edition, 2004.
- Timothy C. Lethbridge and Robert Laganière. Object-Oriented Software Engineering: Practical Software Development using UML and Java. Second Edition. McGraw Hill.
- Mark G. Graff, Kenneth R. van Wyk. Secure Coding: Principles and Practices. O'Reilly, 2003.
- Craig Larman. Applying UML and Patterns. An Introduction to Object-Oriented Analysis and Design and Iterative Development (3rd Edition) - Prentice Hall (2004).

Prerequisiti

Le conoscenze ed i concetti forniti dai corsi di *Programmazione*, Algoritmi e Strutture Dati

Modalità di esame
Scritto e prova pratica
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-10/

Progettazione di software sicuro

Docente: Riccobene Elvinia Maria

Obiettivi (dettagli AF)

Il corso si propone di presentare i principi architetturali e le principali tecniche di progettazione per lo sviluppo di applicazioni software. L'obiettivi è quello di fornire le conoscenze necessarie per la progettazione di software sicuro e per l'analisi di sicurezza del codice sorgente attraverso test e tecniche di analisi statica e dinamica del flusso esecutivo.

Programma

1. **SICUREZZA DEL SOFTWARE.** Proprietà del software. Proprietà del software sicuro. Ciclo di vita del software: fasi di sviluppo del software, modelli di ciclo di vita. La sicurezza nel ciclo di vita del software. Ciclo di vulnerabilità. Attacchi a livello di progettazione, di implementazione ed di funzionalità.
2. **ARCHITETTURE E TECNOLOGIE SICURE.** Principi di architetture sicure. Linee guida e principi per architetture sicure. Criteri di scelta di tecnologie sicure. Il caso di studio di Java sandbox.
3. **SPECIFICA E PROGETTAZIONE DI SOFTWARE SICURO**. Proprietà di specifiche di software sicuro. Metodi di specifica. Macchine a stati finiti. Communicating Machines. Macchine di stato UML. Design by contract. Il tool JML.
4. **IMPLEMENTAZIONE**. Linee guida per la programmazione sicura. Tipici errori. Sicurezza dei linguaggi di programmazione. Alcune violazioni di sicurezza in C. Programmi sicuri in C. Introduzione al linguaggio Java. Dalla specifica al codice: macchine a stati finiti in Java.
5. **TESTING**. Il testing nel ciclo di vita del software. Tipi di testing. Tecniche per la validazione e verifica. I limiti del testing. Testing basato sui programmi. Grafo di flusso di un programma. Copertura delle istruzioni e degli archi. Copertura delle decisioni e delle condizioni. I metodi MCC e MCDC. Valutare la copertura con Emma. Il tool JUnit.

Propedeuticità consigliate

Programmazione, Tecnologie per la sicurezza e la privatezza

Materiale di riferimento

- Mark G. Graff, Kenneth R. van Wyk. Secure Coding: Principles and Practices. O'Reilly, 2003.
- John Viega, Gary McGraw. Building secure software : how to avoid security problems the right way. Addison-Wesley, 2002.
- John C. Mitchell. Concepts in programming languages. Cambridge University Press, 2003.
- Ghezzi Carlo, Jazayeri Mehdi, Mandrioli Dino. Ingegneria del software. Fondamenti e principi. Pearson Education Italia, 2004, 2ª ed.
- Glenford J. Myers, Corey Sandler, Tom Badgett, Todd M. Thomas. The Art of Software Testing. John Wiley & Sons; 2 edition, 2004.
- Broy, M.; Jonsson, B.; Katoen, J.-P.; Leucker, M.; Pretschner, A. (Eds.). Model-Based Testing of Reactive Systems. Springer, LNCS 3472, 2005.

Prerequisiti

Le conoscenze ed i concetti forniti dai corsi di *Programmazione*, di *Tecnologie per la sicurezza e la privatezza*

Modalità di esame

Scritto e prova pratica

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F68/default/F68-10/

Progetto e ottimizzazione di reti (Network design and optimization)

Professor: Ceselli Alberto

Goals

The course aims at giving both theoretical and practical tools for solving complex decision problems, arising in the design and optimization of telecommunication network infrastructures and services.
Issues related to the design of infrastructures and services offering robustness and efficiency guarantees will be analyzed in depth during the course, together with the problem of protection against failures.
The course is aimed at students in both Computer Science and Information Security.

Syllabus

Part I: overview on main graph optimization problems; models and algorithms for flow problems, min cost flow and multicommodity flow; models and algorithms for network routing.
Part II: design and optimal dimensioning of network infrastructures.
Part III: models and algorithms for the protection and the design of networks with robustness guarantees.

Recommended preparatory courses

Computer programming, algorithms and data structures (suggested: operations research).

Course materials

M. Pioro, D. Medhi "Routing, Flow, and Capacity Design in Communication and Computer Networks", Morgan Kauffman, 2004
R.K. Ahuja, T.L. Magnanti, J.B. Orlin "Network Flows: Theory, Algorithms, and Applications", Prentice Hall, 1993

Prerequisites

Good coding skills, good attitude to mathematical modeling, and design and analysis of algorithms.

Course assessments

Oral exam + Exam project

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-59/

Programmazione

Docente: Tettamanzi Andrea Giovanni Battista

Obiettivi (dettagli AF)

Questo è un corso introduttivo alla programmazione, ai suoi principi ed alle sue tecniche. Il suo scopo è quello di familiarizzare lo studente, che potrebbe non essere mai stato esposto alla programmazione, con questa disciplina e fornirgli quella comprensione e gli strumenti necessari ad affrontare tutti i corsi che ne presuppongono la conoscenza.

Programma

NOZIONI DI BASE

- Nozione di algoritmo.
- Fasi della programmazione.
- Strumenti di modellazione.
- Documentazione.
- Breve storia della programmazione.

PROGRAMMAZIONE ELEMENTARE

- Rappresentazione di informazione numerica e simbolica
- La macchina MIX e il suo linguaggio assembly MIXAL
- Organizzazione dei dati: il concetto di variabile, mappa della memoria e tabelle, strutture dati dinamiche.
- Alcune tecniche fondamentali di programmazione: sottoprogrammi, ricorsione, interpreti, automi.

PROGRAMMAZIONE STRUTTURATA

- Principi della programmazione strutturata.
- Linguaggio C: espressioni e assegnamenti, costrutti di controllo, tipi predefiniti, vettori, matrici e stringhe, tipi strutturati, puntatori e gestione della memoria, funzioni e passaggio di parametri, main e parametri al main, libreria standard, gestione dei file.
- Eliminazione dei Salti: teorema di Böhm-Jacopini, trasformazione di Ashcroft e Manna.
- Correttezza del codice: elementi di validazione e verifica della correttezza, logica di Hoare.

Propedeuticità consigliate

-

Materiale di riferimento

Dispense e lucidi a cura dei docenti, disponibili sul sito dell'insegnamento.

Prerequisiti

-

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

A distanza

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-16/

Reti di calcolatori

Docente: Damiani Ernesto

Obiettivi (dettagli AF)

L'insegnamento ha come obiettivo principale l'analisi delle tecnologie, dei modelli, dei principi di funzionamento e dei principali protocolli alla base delle reti di calcolatori. Verranno inoltre analizzati i principali protocolli applicativi, e relativi servizi, della rete IP e presentate alcune tecniche di programmazione distribuita.

Programma

L'insegnamento presenterà le tecnologie ed i protocolli alla base del funzionamento delle reti di calcolatori. Nella prima parte dell'insegnamento verranno discussi i fondamenti dei sistemi di rete, le reti locali, la rete Internet, con particolare riferimento ai protocolli di rete e di trasporto (IP).

1. Introduzione. Struttura e tipologie dei sistemi di elaborazione dell'informazione. Infrastrutture di calcolo e di servizi. Standard multilivello: l'esempio di ISO/OSI.
2. Introduzione alle reti locali. Motivazioni. Reti private e pubbliche; storia e filosofia di progetto. Tipi e architetture di reti private: LAN, MAN, WAN. Topologie: reti parzialmente o completamente connesse, gerarchiche, ad anello, a stella, a bus. Comunicazione: i concetti di instradamento, connessione, contesa. Il livello 1: cablaggi e proprietà fisiche della comunicazione in guida. Il livello 2: MAC e LLC. Gli standard IEEE.
3. Protocolli. Generalità. Il livello 3: Protocolli e caratteristiche di progetto. Organizzazione interna. Il livello 4: servizi offerti al livello trasporto. Confronto tra reti basate su circuito virtuale e reti basate su datagrammi.
4. Caso di studio: Internet Protocol. Il livello rete di IPv4. Indirizzi IP. Subnetting e Supernetting. Protocolli di controllo. ICMP. ARP, RARP. IPv6. Il preambolo IPv6 principale. Preamboli di estensione.
5. Algoritmi di Routing. Routing lungo il cammino minimo. Flooding. Routing basato sui flussi. Routing basato su vettori di distanza. Routing basato sullo stato dei canali. Broadcast routing. Multicast routing. Routing IP: OSPF. BGP. Internet multicasting.
6. Internetworking IP. Circuiti virtuali concatenati. Internetworking senza connessioni. Tunneling e gestione della frammentazione. Firewall. NAT.
7. Il servizio di trasporto. Elementi del protocollo di trasporto. Trasporto TCP/IP: Il modello di servizio TCP. Il protocollo TCP. Il protocollo UDP. Il preambolo del segmento TCP. Il preambolo UDP. Qualità del servizio. Primitive del servizio di trasporto.

Nella seconda parte dell'insegnamento verranno analizzati i livelli superiori del modello ISO/OSI, discutendo i principali protocolli applicativi e servizi per la rete Internet, e le tecniche per la programmazione distribuita.

1. Protocolli e sistemi applicativi client-server. Struttura dei servizi applicativi basati su TCP e UDP.
2. Protocolli applicativi per il funzionamento della rete IP. Protocolli BOOTP, DHCP. Modalità di assegnamento degli indirizzi IP. DNS. Naming. Concetto di dominio. Risoluzione dei nomi di dominio.
3. Applicazioni e servizi Internet. WWW, Electronic Mail, File Transfer, Remote Login. Descrizione ed analisi dei protocolli HTTP, FTP, Telnet, SMTP, POP3.
4. Amministrazione di rete. Descrizione del protocollo SMNP per la gestione della rete.
5. Programmazione distribuita. Socket. Interfacce standard a livello socket e stream per Unix e Windows. Socket TCP e UDP. Socket C e Java. Socket concorrenti. Tecniche di integrazione tramite middleware. Remote Procedure Call (RPC).
6. Fondamenti delle architetture peer-to-peer.

Propedeuticità consigliate

-

Materiale di riferimento

- D.E. Comer, "Internetworking with TCP/IP: Principles, protocols, and architectures", Volume I, Prentice Hall. Disponibile anche in edizione italiana (edizioni Pearson Education)
- Testo alternativo: Jim Kurose, Keith Ross, "Computer Networking: A Top down Approach featuring

the Internet", 3rd ed. Addison Wesley
- Dispense e slide disponibili alle pagina web dell'insegnamento

Prerequisiti
Si richiede una conoscenza dei concetti base sulle architetture di calcolo

Modalità di esame
Scritto
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-11/

Altre informazioni
L'esame consiste in due compitini e nella presentazione (facoltativa) di un progetto. Ulteriori informazioni possono essere reperite sui siti personali dei docenti
- http://www.dti.unimi.it/ardagna/
- http://sesar.dti.unimi.it/

Reti wireless e mobili (Wireless and mobile networks)

Professor: Agazzi Simone

Goals

The Course deals with mobile and wireless networks by a technological and architectural point of view. The main current technologies for communication on radio channel will be analyzed, with particular reference to cellular network and to technologies for wireless networks ad hoc, as Bluetooth, IEEE 802.11, ZigBee. We will identify for each solution the architecture of protocols and services and we will point out the most relevant algorithmic aspects. An important course part will be kept for routing protocols on wireless networks, with a hint also to the case of mobile knots, and for the impact on TCP protocol generated by radio channels.

Syllabus

- Introducing Personal and Local Wireless Networks
- Bluetooth
  - Configuration and architecture
  - Protocol and service in basic band
  - Protocol and L2CAP service
  - SDP protocol
- IEEE 802.11
  - Configuration and architecture
  - Protocol and under-level MAC service
- Introducing sensor networks
  - MAC energy-aware protocol (S-MAC)
  - ZigBee
- Cellular Networks
  - WCDMA politics
  - UMTS
  - High Speed Downlink Packet Access (HSDPA)
- Routing on wireless networks
  - Mobile IP and WAP
  - Networks ad hoc (AODV, geographic routing, epidemic routing)
- TCP on wireless channel
  - TCP Reno e TCP New Reno
  - End-to-end approaches
  - Link Layer approaches
- Conclusions and exercises

Recommended preparatory courses

-

Course materials

- **UMTS. Tecniche e architetture per le reti di comunicazioni mobili multimediali**
  - Author: Columpsi Gennaro ; Leonardi Marco; Ricci Alessio
  - Editor: Hoepli
- **Wi-Fi, Bluetooth, Zigbee and WiMAX**
  - Author: Di Houda Labiod,Afifi Hossam,Costantino De Santis
  - Editor: Springer
- **Slides given by the teacher.**

Prerequisites

Theoretical knowledge about networks

Course assessments
Oral exam
Lecture attendance
Recommended
Teaching format
In presence learning
Language
English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-7/

Ricerca operativa

Docente: Righini Giovanni

Obiettivi (dettagli AF)

Il corso si propone di introdurre lo studente alla Ricerca Operativa, ossia allo studio scientifico dei metodi per risolvere problemi decisionali complessi con l'aiuto del calcolatore. In particolare l'enfasi del corso è posta sulla modellizzazione matematica e sulla formulazione e classificazione dei problemi di ottimizzazione. Una consistente parte del corso viene svolta in laboratorio, dove gli studenti apprendono l'uso di linguaggi di modellizzazione e di solutori *general-purpose*.

Programma

INTRODUZIONE:

- ***Introduzione alla Ricerca Operativa***. Origini, applicazioni, relazioni con altre discipline.
- ***Modelli matematici***. Dati, variabili, vincoli, funzioni obiettivo, decisori.

PROGRAMMAZIONE LINEARE (PL):

- ***Applicazioni.*** Esempi di problemi di programmazione lineare.
- ***Definizioni e proprietà.*** Forma generale dei problemi di PL, forma alle disuguaglianze con relativa interpretazione geometrica, forma standard. Soluzioni di base e teorema fondamentale della PL.
- ***Dualità.*** Teorema della dualità in forma debole ed in forma forte. Teorema degli scarti complementari. Interpretazione economica della PL.
- ***Algoritmi.*** Forme canoniche. Algoritmo del simplesso primale e duale.
- ***Analisi post-ottimale.*** Analisi di sensitività e analisi parametrica.

PROGRAMMAZIONE A MOLTI OBIETTIVI (PMO):

- ***Applicazioni.*** Esempi di problemi di programmazione a molti-obiettivi.
- ***Definizioni e proprietà.*** Dominanza, soluzioni di Pareto, regione Pareto-ottima, punto-utopia.
- ***Criteri per la scelta della soluzione.*** Criterio degli standard, criterio delle curve di indifferenza, criterio del punto-utopia, criterio della massima curvatura.
- ***Algoritmi per la determinazione della regione Pareto-ottima.*** Metodo dei pesi. Metodo dei vincoli. Interpretazione geometrica. Soluzione di esercizi di programmazione lineare a due obiettivi tramite analisi parametrica.

PROGRAMMAZIONE LINEARE INTERA (PLI):

- ***Applicazioni.*** Esempi di problemi di programmazione lineare intera e di ottimizzazione combinatoria. Uso delle variabili binarie per la modellizzazione di condizioni logiche.
- ***Definizioni e proprietà.*** Rilassamento continuo, *gap* di integralità. Altri tipi di rilassamento.
- ***Algoritmi.*** Branch-and-bound.

PROGRAMMAZIONE NON LINEARE (PNL):

- ***Applicazioni.*** Esempi di problemi di programmazione non lineare.
- ***Definizioni e proprietà.*** Vettore gradiente, matrice Hessiana. Convessità e programmazione convessa.
- ***Algoritmi.*** Algoritmi per l'ottimizzazione mono-dimensionale. Metodi analitici, metodi iterativi, algoritmo del gradiente.

Propedeuticità consigliate

Fondamenti di Matematica del continuo e del discreto. Algoritmi e strutture-dati.

Materiale di riferimento

C. Vercellis: "Modelli e Decisioni", Ed. Esculapio, Bologna 1997.
R.Tadei, F. Della Croce: "Ricerca Operativa e Ottimizzazione", Ed. Esculapio, Bologna 2002
Hillier & Lieberman, "Introduction to Operations Research"

Prerequisiti
-

Modalità di esame
Scritto e orale
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-2/

Sicurezza dei sistemi e delle reti

Docente: Monga Mattia

Obiettivi (dettagli AF)

- Discutere e progettare la sicurezza dei sistemi in rete
- Rivedere i protocolli TCP/IP in un'ottica di sicurezza
- Conoscere le minacce più diffuse
    - A livello di rete locale, A livello infrastrutturale
- Saper analizzare il traffico e riconoscere gli attacchi
- Saper utilizzare le maggiori tecnologie di difesa
    - Firewall, network intrusion detection system
- Saper difendere la privatezza delle operazioni in reti untrusted

Programma

L'insegnamento si propone di analizzare le principali tematiche della sicurezza dei sistemi in rete.

- Concetti generali
- La pila protocollare e le minacce più comuni
    - Ethernet, IP, ARP, TCP, UDP, Problemi di sicurezza intrinseci
- Port scanning
- Analisi del traffico
- Sicurezza perimetrale
    - Stateless filtering, Stateful filtering, Deep packet inspection, Effetti di un firewall, Proxy, NAT
- Rilevamento delle intrusioni
    - Misuse detection, Anomaly detection, Falsi allarmi, Aspetti architetturali, Zero Day, Polimorfismo degli attacchi
- Botnet
- Protezione dell'infrastruttura
- VPN
- Protezione di servizi critici
    - DNS, DNSSEC
- L'autenticazione in rete
- Specificità delle reti Wireless
- Protezione degli utenti all'interno di una rete untrusted

Propedeuticità consigliate

Reti di Calcolatori, Sistemi Operativi

Materiale di riferimento

Inside Network Perimeter Security, 2nd Edition Northcutt, Zeltser, Winters, Kent, Ritchey SAMS ed., 2005
The Tao of Network Security Monitoring - Beyond Intrusion Detection R. Beytlich Pearson Education Inc., 2004
Silence on the Wire
A Field Guide to Passive Reconnaissance and Indirect Attacks, M. Zalewski, No Starch Press, 2005
Articoli della letteratura scientifica indicati a lezione

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-34/

Sicurezza delle architetture orientate ai servizi

Docente: Damiani Ernesto

Obiettivi del corso (dettagli AF)

Il corso di Sicurezza delle Architetture Orientate ai Servizi fornisce agli studenti una conoscenza di base delle tecniche di sicurezza XML. Inoltre presenta gli studenti le implementazioni di sicurezza e gestione dell'identità usando due standard emergenti: OpenID e XACML per esprimere autorizzazioni a granularità fine. Gli studenti apprenderanno comunque tutti gli standard di sicurezza dei servizi Web, compresi WS-Security, WS-Trust, WS-Secure Conversation, e WS-Security Policy. Il corso si occuperà inoltre dei problemi di certificazione delle proprietà non-funzionali dei servizi, comprese quelle di sicurezza e privatezza.

Programma

Il programma del corso di Sicurezza delle Architetture Orientate ai Servizi è focalizzato sui seguenti punti principali:

- Apprendere le basi della sicurezza XML, compresa crittografia e firma elettronica di dati XML
- Capire il ruolo degli standard basati su XML nella gestione delle identità e nella sicurezza dei servizi Web
- Conoscere approfonditamente le tecniche e gli strumenti per l'assurance e la certificazione dei servizi

Gli argomenti trattati durante il corso includono:

- Introduzione al Corso
  - Introduzione a XML
  - Crittografia e firma digitale su dati XML
- Sicurezza dei Web Service
  - WS-Security, WS-Trust
  - WS-Secure Conversation, WS-Security Policy
- Tecnologie per la gestione dell'identità
  - Concetti di base sull'identità
  - Piattaforme di identity management
  - Open ID
- Linguaggi di autorizzazione a granularità fine
  - Concetti di base delle architetture di valutazione e decisione
  - XACML e SAML
  - Profili XACML per settori applicativi
- Certificazione dei servizi
  - Concetti generali di assurance
  - Certificazioni di sicurezza
  - Certificazione dei servizi

Propedeuticità consigliate

Gestione dei Processi Aziendali
Architetture Orientate ai Servizi

Materiale di riferimento

Dispense e presentazioni del corso
Per consultazione: C.Ardagna, E. Damiani, N. El Ioini "Open Source Systems Security Certification," Springer, 2008.

Prerequisiti

Conoscenza delle tecnologie Web, di XML e dei principali protocolli applicativi

Modalità di esame
Progetto più esercizi durante il corso
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano (con seminari in Inglese)

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-32/

Altre informazioni
La valutazione dell'esame avverrà secondo il seguente schema:

- Partecipazione e discussion durante le lezioni: 20.00%
- Discussione di articoli scientifici : 30.00%
- Presentazione del progetto: 50.00%
- Compiti: Lettura di articoli scientifici – ogni studente sarà incoraggiato a fare ricerche nel Web per ricercare articoli su riviste attinenti al corso.

Sicurezza delle reti

Docente: Monga Mattia

Obiettivi (dettagli AF)

- Discutere e progettare la sicurezza dei sistemi in rete
- Rivedere i protocolli TCP/IP in un'ottica di sicurezza
- Conoscere le minacce più diffuse
    - A livello di rete locale, A livello infrastrutturale
- Saper analizzare il traffico e riconoscere gli attacchi
- Saper utilizzare le maggiori tecnologie di difesa
    - Firewall, network intrusion detection system
- Saper difendere la privatezza delle operazioni in reti untrusted

Programma

L'insegnamento si propone di analizzare le principali tematiche della sicurezza dei sistemi in rete.

- Concetti generali
- La pila protocollare e le minacce più comuni
    - Ethernet, IP, ARP, TCP, UDP, Problemi di sicurezza intrinseci
- Port scanning
- Analisi del traffico
- Sicurezza perimetrale
    - Stateless filtering, Stateful filtering, Deep packet inspection, Effetti di un firewall, Proxy, NAT
- Rilevamento delle intrusioni
    - Misuse detection, Anomaly detection, Falsi allarmi, Aspetti architetturali, Zero Day, Polimorfismo degli attacchi
- Botnet
- Protezione dell'infrastruttura
- VPN
- Protezione di servizi critici
    - DNS, DNSSEC
- L'autenticazione in rete
- Specificità delle reti Wireless
- Protezione degli utenti all'interno di una rete untrusted

Propedeuticità consigliate

Reti di Calcolatori, Sistemi Operativi

Materiale di riferimento

Inside Network Perimeter Security, 2nd Edition Northcutt, Zeltser, Winters, Kent, Ritchey SAMS ed., 2005
The Tao of Network Security Monitoring - Beyond Intrusion Detection R. Beytlich Pearson Education Inc., 2004
Silence on the Wire
A Field Guide to Passive Reconnaissance and Indirect Attacks, M. Zalewski, No Starch Press, 2005
Articoli della letteratura scientifica indicati a lezione

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-34/

Sistemi biometrici

Docente: Scotti Fabio

Obiettivi (dettagli AF)

Il Corso di Sistemi Biometrici si propone di portare lo studente a conoscere ed utilizzare correttamente le principali tecniche e i dispositivi ed algoritmi di riconoscimento di identificatori biometrici, con particolare riferimento a quelli della mano, del volto, delle impronte digitali, della retina e dell'iride dell'occhio.

Programma

L'uso di dispositivi automatici di identificazione basati su identificatori biometrici sta ricevendo sempre più attenzione da parte di istituzioni pubbliche e organizzazioni private. Le tecnologie biometriche, dopo un lungo periodo di evoluzione, sono ora pronte a giocare un ruolo importante nel panorama tecnologico. Ci sono però varie preoccupazioni relative ai rischi che l'uso su larga scala di dispositivi biometrici puo' porre alle liberta' civili e alla privacy; queste preoccupazioni hanno portato a un'intensa attività legislativa e normativa sull'argomento. Il Corso di Sistemi Biometrici si propone di portare lo studente a conoscere ed utilizzare correttamente le principali tecniche e i dispositivi ed algoritmi di riconoscimento di identificatori biometrici, con particolare riferimento a quelli della mano, del volto, delle impronte digitali, della retina e dell'iride dell'occhio. Saranno svolti anche cenni sulle tecniche multimodali, sul riconoscimento della voce e su quello di caratteristiche dinamiche quali lo stile di battitura e la postura del corpo. Infine, verranno trattate la struttura e la messa in opera di architetture centralizzate e distribuite per la memorizzazione e la trasmissione di dati biometrici, con particolare riferimento alle tecniche per la difesa della privacy.

Programma del corso:

- *introduzione alla biometria*;
- *terminologia, struttura e caratteristiche di un sistema biometrico;*
- sistemi biometrici basati su impronte digitali;
- sistemi biometrici basati sull'iride;
- sistemi biometrici basati sul volto;
- sistemi biometrici basati su caratteristiche comportamentali e DNA;
- sistemi biometrici multimodali;
- progettazione, valutazione e confronto di sistemi biometrici.

Propedeuticità consigliate

-

Materiale di riferimento

Biometrics: Personal Identification in Networked Society, Anil K Jain, Sharath Pankanti, Ruud Bolle, Springer.
Slide del corso

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-34/

Sistemi distribuiti (Distributed systems)

Professor: Tettamanzi Andrea Giovanni Battista

Goals

The aim of this class is to present the basic distributed system technologies. The class discusses the main issues and design choices of a distributed system, the architectural principles, with a particular focus on interconnection networks, communication among processes, remote method invocation and remote procedure call mechanisms. In addition, basic methods and algorithms for controlling concurrency are introduced.

Syllabus

PRINCIPLES

- Architectures.
- Communication.
- Processes.
- Naming.
- Synchronization.
- Consistency and Replication.
- Fault Tolerance.
- Security.

PARADIGMS

- Object-based Systems.
- Distributed File Systems.
- Document-based Systems.
- Coordination-based Systems.

Recommended preparatory courses

-

Course materials

A. S. Tannenbaum, M. van Steen. Distributed Systems. Pearson Education 2006.

Prerequisites

-

Course assessments

Project

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-11/

Sistemi intelligenti (Intelligent systems)

Professor: Piuri Vincenzo

Goals

The course presents methodologies and techniques to implement intelligent systems for processing information and knowledge, i.e., systems which behaves like the human brain by employing computational intelligence approaches. In particular, the following main approaches will be studied: neural networks, fuzzy systems, and evolutionary computing.

Syllabus

- **Neural networks**: Definitions. Neurons: structures, perceptrons, RBF. Neural topologies: feed-forward, feedback, SOM. Learning: supervised, unsupervised. Performance. Optimization. Classification and clustering. Associative memories. Prediction. Function approximation. Applications.
- **Fuzzy logic and systems:** Fuzzy sets. Membership functions. Fuzzy rules. Defuzzification. Fuzzy reasoning. Fuzzy systems. Rough sets. Performance. Applications.
- **Evolutionary computing:** Genomic representation. Fitness functions. Selection. Genetic algorithms. Genetic programming. Evolutionary programming. Evolutionary strategies. Differential evolution. Swarm intelligence. Artificial immune systems.
- **Hybrid systems**

Recommended preparatory courses

Concepts of computing foundations, computer programming, calculus, and English reading.

Course materials

Simon Haykin, Neural Networks: A Comprehensive Foundation, Prentice Hall
Timothy Ross, Fuzzy Logic with Engineering Applications, Wiley
A.E. Eiben, J.E. Smith, Introduction to Evolutionary Computing, Sprinter
Course slides published in the course's website

Prerequisites

Concepts of computing foundations, computer programming, calculus, and English reading.

Course assessments

Oral exam and project

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-10/

Sistemi intelligenti per il monitoraggio e il controllo (Intelligent Systems for Monitoring and Control)

Professor: Piuri Vincenzo

Goals

The course presents methodologies and techniques to implement intelligent systems for monitoring and control in industrial and environmental applications, typically based on computational computational intelligence approaches.

Syllabus

- **Intelligent sensors:** Heterogeneous multi-sensor systems. Sensor data analysis. Diagnosys. Fault tolerance. Self-calibration. Adaptivity. Management.
- **Sensor networks:** Structure. Functions. Adaptivity. Management. Distributed data analysis. Fault tolerance. Diagnosys.
- **Measurements:** Acquisition and processing of sensor measurement in advanced adaptive infrastructures.
- **Sensor signal and image processing:** Feature extraction. Multi-sensorial data fusion. Adaptivity of measurement representation, operations and functions to the application needs. Virtual sensors. Information compression.
- **Classification and clustering:** Classification and clustering of sensor signals. Sensitività analysis. Class robustness.
- **Data mining and knowledge extraction:** Adaptive knowledge extraction from sensor data and system information. Knowledge representation.
- **Monitoring:** Applications of intelligent system sto complex system monitoring. Applications to industrial process monitoring. Qualità monitoring. Applications to environmental monitoring.
- **Prediction:** Applications of intelligent system sto prediction in the industry and the environment. Quality prediction.
- **Control:** Applications of intelligent system sto control of industrial processes, industrial automation, robotic systems, complex products, power distribution grids, automotive and transport systems.

Recommended preparatory courses

Concepts of computing foundations, computer programming, calculus, intelligent systems, industrial automation and measurements, and English reading.

Course materials

Papers in English, distributed by the lecturer and made available through the course's web page.

Prerequisites

Concepts of computing foundations, computer programming, calculus, intelligent systems, industrial automation and measurements, and English reading.

Course assessments

Oral exam and project

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-43/

Sistemi operativi I

Docente: Piuri Vincenzo

Obiettivi (dettagli AF)

Il corso si propone di fornire le conoscenze sui fondamenti teorici, gli algoritmi e le tecnologie riguardanti l'architettura complessiva e la gestione del processore nei sistemi operativi per le principali tipologie di architetture di elaborazione, incluse le architetture distribuite.

Programma

Il corso analizza comparativamente architetture, funzionalità, meccanismi, politiche e gestione dei sistemi operativi relativamente alle varie strutture dei sistemi operativi stessi e alla gestione del processore per le varie architetture dei sistemi di elaborazione (monoprocessore, multiprocessore, cluster, distribuiti, embedded) orientati alle principali aree applicative (sistemi transazionali, interattivi, gestionali, multimediali, d'automazione d'ufficio, per telecomunicazioni, di controllo industriale, robotici, embedded). Il corso approfondisce poi gli aspetti progettuali e di gestione dei sistemi operativi, con riferimento a tecniche di progettazione, configurazione, ottimizzazione, e manutenzione relativamente all'architettura del sistema e alla gestione del processore.

- **Architetture dei sistemi operativi**: tipi e struttura, funzioni caratteristiche, meccanismi e politiche di gestione.
- **Virtualizzazione del processore**: schedulazione di processi, allocazione, riallocazione statica e dinamica, pipelining, deadlock, starvation; meccanismi e politiche per la gestione concorrente, per la sincronizzazione e per la comunicazione tra processi; thread; aspetti di tempo reale; tolleranza ai guasti; progettazione di algoritmi e strutture dati per la virtualizzazione del processore; valutazione delle alternative progettuali.

Propedeuticità consigliate

Concetti di informatica di base, architetture dei calcolatori e programmazione.

Materiale di riferimento

Silbershatz, Galvin, Gagne, Sistemi Operativi, Apogeo, 2005
Lucidi sul sito web del corso

Prerequisiti

Concetti di informatica di base, architetture dei calcolatori e programmazione.

Modalità di esame
Scritto
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-15/

Sistemi operativi II

Docente: Piuri Vincenzo

Obiettivi (dettagli AF)

Il corso si propone di fornire le conoscenze sui fondamenti teorici, gli algoritmi e le tecnologie riguardanti la gestione della memoria centrale, dei dispositivi di ingresso/uscita, del file system, dell'interfaccia utente e dei sistemi operativi distribuiti nei sistemi operativi per le principali tipologie di architetture di elaborazione, incluse le architetture distribuite.

Programma

Il corso analizza comparativamente architetture, funzionalità, meccanismi, politiche e gestione dei sistemi operativi relativamente alla gestione della memoria centrale, dei dispositivi di ingresso/uscita, del file system, dell'interfaccia utente e dei sistemi operativi distribuiti per le varie architetture dei sistemi di elaborazione (monoprocessore, multiprocessore, cluster, distribuiti, embedded) orientati alle principali aree applicative (sistemi transazionali, interattivi, gestionali, multimediali, d'automazione d'ufficio, per telecomunicazioni, di controllo industriale, robotici, embedded). Il corso approfondisce poi gli aspetti progettuali e di gestione dei sistemi operativi, con riferimento a tecniche di progettazione, configurazione, ottimizzazione, e manutenzione relativamente alla gestione della memoria centrale, dei dispositivi di ingresso/uscita, del file system, dell'interfaccia utente e dei sistemi operativi distribuiti.

- **Virtualizzazione della memoria centrale**: politiche e meccanismi di gestione della memoria centrale; supporti architetturali; consistenza; tolleranza ai guasti e agli errori software; sicurezza e protezione; progettazione di algoritmi e strutture dati per la virtualizzazione della memoria centrale; valutazione progettuale.
- **Virtualizzazione dei dispositivi di ingresso/uscita**: meccanismi e politiche di gestione delle tipologie dispositivi e interfacciamento; orologio, ordinamento temporale degli eventi in sistemi distribuiti, coordinamento; dischi; terminali; stampanti; periferiche speciali, supporto di sistema operativo per reti informatiche; aspetti di tempo reale, tolleranza ai guasti e agli errori software, sicurezza e protezione; progettazione di algoritmi e strutture dati per la virtualizzazione del dei dispositivi di ingresso/uscita; valutazione delle alternative progettuali.
- **Astrazione della rappresentazione delle risorse informative e fisiche**: file, file system, file system di rete e distribuito, politiche di identificazione delle risorse; consistenza, caching, backup; tolleranza ai guasti e agli errori software; protezione e sicurezza degli accessi; progettazione di algoritmi e strutture dati per l'astrazione delle risorse; valutazione delle alternative progettuali.
- **Interfaccia utente: tipi di interpreti e interfacce utente** (programmativo, testuale, grafico, multimediale, distribuito, agenti mobili); meccanismi e politiche di gestione dell'interfaccia utente; gestione e sicurezza degli accessi; tolleranza ai guasti e agli errori software; progettazione di algoritmi e strutture dati per l'interfaccia utente; valutazione delle alternative progettuali.
- **Sistemi operativi per architetture distribuite**: esecuzione di processi, sincronizzazione e comunicazione tra processi, gestione del deadlock, gestione delle periferiche, gestione del file system.

Propedeuticità consigliate

Concetti di informatica di base, architetture dei calcolatori e programmazione.

Materiale di riferimento

Silbershatz, Galvin, Gagne, Sistemi Operativi, Apogeo, 2005
Lucidi sul sito web del corso

Prerequisiti

Concetti di informatica di base, architetture dei calcolatori e programmazione.

Modalità di esame
Scritto
Modalità di frequenza
Fortemente consigliata
Modalità di erogazione
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-14/

Tecnologie e linguaggi per il Web

Docente: Ceravolo Paolo

Obiettivi (dettagli AF)

- Comprensione dei principi sui quail si fonda il WWW e degli elementi che si sono consolidati durante la sua evoluzione.
- Comprensione dei principi fondamentali di progettazione di una applicazione web.
- Conoscenza delle principali tecnologie disponibili per lo sviluppo di applicazioni web.

Programma

L'insegnamento ha lo scopo di analizzare i concetti fondamentali delle architetture e delle applicazioni per il World Wide Web; e di fornire una panoramica sulle tecnologie più rappresentative di questo ambiente.
Il Web ha saputo imporsi negli anni quale ambiente universale per l'interazione con servizi informativi di vario genere. La generalità di questo ambiente è determinata da un'architettura semplice e scalabile. Allo stesso tempo, la necessità di supportare le più svariate applicazioni ha richiesto che le tecnologie per il Web evolvessero nella direzione di supportare processi informativi maturi: capaci di gestire in modo efficiente la portabilità, l'interrogazione e l'elaborazione dei dati.
Studiare le tecnologie per il Web, comprenderne i fondamenti, l'evoluzione storica, e l'attualità, costituisce un formidabile campo di comprensione delle implicazioni e degli effetti che a vari livelli l'informatica opera sulla società attuale.

- INTRODUZIONE
  Storia del WWW - Architettura del WWW - Topologia del WWW
- RAPPRESENTAZIONE DEI DATI
  HTML – CSS – XHTML – XML
- LINGUAGGI DI PROGRAMMAZIONE
  Principi di CGI – JSP – JSTL
- MODELLI ARCHITETTURALI WEB 2.0
  AJAX – HTML5 – JSON
- MODELLI DI BUSINESS PER IL WEB
  Principi di usabilità e modelli business

Propedeuticità consigliate

Laboratorio di Informatica Applicata, nozioni di programmazione, fondamenti di reti di calcolatori, concetti di basi di dati e linguaggio SQL

Materiale di riferimento

- HTML 5 e CSS 3 / Gabriele Gigliotti, Milano : Apogeo, c2011
- HTML e CSS / Andrew, Rachel - Shafer, Dan. Segrate : Mondadori Informatica, 2007
- Ajax : per applicazioni Web / Romagnoli, Andrea - Salerno, Pasquale - Guidi, Andrea. Milano : Apogeo, c2007
- Creare siti web multimediali : fondamenti per l'analisi e la progettazione / Brajnik, Giorgio - Toppano, Elio [Milano] : Pearson Addison Wesley, 2007

Prerequisiti

-

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale (disponibili mp3 delle lezioni)

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-B/F67-1/

Tecnologie informatiche per la qualità (Information technology for quality control)

Professor: Lazzaroni Massimo

Goals

The aim of the course is the study of the Quality Control with particular attention on methodologies based on Statistical Process Control (SPC).

Syllabus

INTRODUCTION

Introduction to Quality. Historical evolution. Software for Quality Control. Quality assurance. Quality characteristic, traceability, conformity, nonconformity, defect, requirement, grade, Upper Specification Limits, Lower Specification Limits.

STATISTICAL PROCESS CONTROL

Introduction to Statistical Process Control. Data representation. Observing processes over time. Charts. Dot diagram. Time plot. Stem and Leaf diagrams. Frequency distribution and histograms. Cumulative distribution plot. Box Plots. Pareto chart. Control charts. Mean. Standard Deviation, Variance, Range. Ishikawa chart. Electronic sheets.

QUALITY SYSTEMS

Quality systems and certification. UNI EN ISO 9000 (Quality management systems - Fundamentals and vocabulary), UNI EN ISO 9001 (Quality management systems - Requirements standard), UNI EN ISO 9004 (Quality management systems - Guidelines for performance improvements). Total Quality. Software for Quality management.

MEASUREMENTS VS QUALITY SYSTEMS

Metrology. Measurement unceratinty. Uncertainty evaluation and propagation. Uncertainty due to hardware and software.

QUALITY AND IT

Software for Quality Control and Assurance. Information system in laboratory. Test management. Documentation.

Recommended preparatory courses

-

Course materials

MONTGOMERY DOUGLAS C., STATISTICAL QUALITY CONTROL, ISBN-13: 9780470233979, Ed. 6, 2009.

Prerequisites

-

Course assessments

Written and oral exams

Lecture attendance

Recommended

Teaching format

In presence learning

Language

English

Course web page http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F94/default/F94-46/

Tecnologie per la sicurezza e privatezza

Docente: Braghin Chiara

Obiettivi (dettagli AF)

L'insegnamento ha lo scopo di introdurre i concetti di base relativi alle problematiche di sicurezza e privatezza dei sistemi informatici.

Programma

1. Introduzione. Descrizione dei crimini informatici. Modelli di sicurezza.
2. Politiche e modelli per il controllo dell'accesso: politiche discrezionarie, mandatorie e basate sui ruoli.
3. Diversi livelli di sicurezza: Sicurezza dei sistemi operativi, Sicurezza delle reti, Programmi sicuri.
4. Protocolli di Sicurezza. Meccanismi di identificazione e autenticazione.
5. Un nuovo trend: metodi formali per la sicurezza.
6. Sicurezza nel Web.

Propedeuticità consigliate

Comprensione di un testo scientifico in inglese

Materiale di riferimento

Slide del corso, appunti presi a lezione e articoli in inglese che sono parte integrante del programma del corso.

Prerequisiti

-

Modalità di esame

Scritto

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F68/default/F68-7/

Teoria dell'informazione e della trasmissione

Docente: Pizzi Rita

Obiettivi (dettagli AF)

Il corso si pone l'obiettivo di presentare la teoria della trasmissione a partire dal concetto di informazione, che viene esaminata in chiave sia classica che quantistica, introducendo alle applicazioni più importanti.

Programma

Introduzione al concetto di informazione classica. Studio del concetto di sorgente di informazione (discreta senza memoria e con memoria), del concetto di canale di trasmissione, dei teoremi di Shannon. Introduzione a teoria della trasmissione, teorema del campionamento, analisi spettrale del segnale e criterio di Nyqvist. Introduzione dei principali metodi di codifica compresa quella convoluzionale, ed elementi di crittografia. Si introducono infine le prime nozioni di informazione quantistica ed i concetti necessari per comprendere il funzionamento dei sistemi di crittografia quantistica.

Propedeuticità consigliate

Almeno 12 crediti di corsi di Matematica

Materiale di riferimento

Documentazione sul sito web di riferimento
E. Angeleri, Informazione: Significato e Universalità, UTET 2000.
David J.C. MacKay, A short Course in Information Theory, http://www.cs.toronto.edu/~mackay/info-theory/course.html

Prerequisiti

Nozioni di analisi matematica

Modalità di esame

Scritto e orale

Modalità di frequenza

Fortemente consigliata

Modalità di erogazione

Tradizionale

Lingua in cui è tenuto l'insegnamento

Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F67/F67-A/F67-4/

Trattamento dati sensibili

Docente: Bonavita Simone

Obiettivi (dettagli AF)

L'obiettivo principale del corso è fornire strumenti giuridici di base all'esperto di sicurezza informatica che, nell'adempimento della professione, tratta dati sensibili. Il Corso avrà ad oggetto il trattamento di dati sensibili, nelle sue più ampie declinazioni. Nel coro delle lezioni verranno messe a disposizione degli studenti nel corso delle lezioni dispense riportanti le principali normative applicabili al trattamento di dati sensibili, bozze contrattuali che comportano criticità in merito al trattamento di dati sensibili e policy aziendali relative all'utilizzo degli strumenti informatici. L'insegnamento sarà diviso in più moduli.

Programma

Modulo I - Il trattamento di dati sensibili.
Il Codice della Privacy;
Il dato sensibile;
Le Garanzie previste per il trattamento di dati sensibili;
Il diritto della sicurezza informatica;
La Giurisprudenza del Garante relativa a trattamenti di dati sensibili;
Geolocalizzazione e trattamento dei dati sensibili;
L'attività di profilazione dei dati sensibili: limiti e diritti;
Gli obblighi di distruzione del dato sensibile;
Il diritto all'oblio e gli strumenti di tutela delle informazioni all'interno della Rete;
La responsabilità degli intermediari nel trattamento di dati sensibili;
Casi di studio: Google vs Vividown, Google vs Viacom.

Modulo II – Policy e trattamento di dati sensibili all'interno dell'azienda.
Internet e posta elettronica sul luogo di lavoro;
Il corretto utilizzo dei dati personali;
Policy relative ai compiti degli amministratori di sistema;
Policy di trattamento dei dati relativi a segreti industriali;
I contratti ad oggetto informatico relativi ai servizi critici che comportano trattamento di dati sensibili.

Modulo III- Computer Crimes, computer forensics e trattamento di dati sensibili
Introduzione alla sistematica dei delitti informatici nell'ambito del diritto penale;
I cybercrime;
I modelli organizzativi ex 231/01.

Propedeuticità consigliate

-

Materiale di riferimento

Il testo obbligatorio per tutti gli studenti ai fini della preparazione dell'esame è il seguente:
P. Perri, Protezione dei dati e nuove tecnologie, Milano, Giuffrè , 2007.
In alternativa potrà essere adottato il seguente testo:
P. Perri, Privacy, diritto e sicurezza informatica, Milano, Giuffrè, 2007.
Si consiglia altresì la lettura del seguente testo:
G. Ziccardi, Hacker. Il richiamo delle libertà, Marsilio, Venezia, 2011.

Prerequisiti

-

Modalità di esame:
Orale. Scritto per i soli frequentanti (si considera frequentante chi abbia presenziato ad almeno il 70% delle lezioni).
Modalità di frequenza:
Fortemente consigliata
Modalità di erogazione:
Tradizionale
Lingua in cui è tenuto l'insegnamento
Italiano

Pagina web del corso http://www.ccdinfcr.unimi.it/it/corsiDiStudio/2012/F2Y/F2Y-A/F2Y-30/

Altre informazioni
Ulteriori informazioni disponibili nella pagina ufficiale del corso.