Laurea Informatica Corso Triennale – L31
Coorte 2013/2014 - Curriculum unico

I Anno – Corsi Annuali

SSD	Denominazione	Attività	CFU	ambito
MAT/05	Elementi di Analisi Matematica (A-L, M-Z)	affine	12	Affini o integrative
MAT/03	Matematica Discreta	base	12	Formazione matematico-fisica

I Anno I Semestre

SSD	Denominazione	Attività	CFU	ambito
INF/01	Fondamenti di Informatica	base	9	Formazione Informatica di base
INF/01	Programmazione I (A-L, M-Z)	base	9	Formazione Informatica di base

I Anno II Semestre

SSD	Denominazione	Attività	CFU	ambito
INF/01	Architetture degli Elaboratori	car	9	Discipline Informatiche
INF/01	Programmazione II (A-L, M-Z)	car	9	Discipline Informatiche

Totale I anno 60

II Anno – I Semestre

SSD	Denominazione	Attività	CFU	ambito
INF/01	Basi di Dati	car	9	Discipline Informatiche
INF/01	Interazione e Multimedia	car	9	Discipline Informatiche
INF/01	Algoritmi	car	9	Discipline Informatiche
	Inglese		6	

II Anno – II Semestre

SSD	Denominazione	Attività	CFU	ambito
INF/01	Reti di Calcolatori	car	9	Discipline Informatiche
INF/01	Sistemi Operativi	car	9	Discipline Informatiche
INF/01	Ingegneria del Software	car	9	Discipline Informatiche

Totale II anno 60

III anno I Semestre

SSD	Denominazione	Attività	CFU	ambito

MAT/07	Metodi Matematici e Statistici	affine	6	Affini o Integrative
INF/01	Tecniche di programmazione concorrente e distribuita (o Introduzione al Data Mining)	car	9	Discipline Informatiche
INF/01	Computer Grafica (o Internet Security)	car	9	Discipline Informatiche
INF/01	Insegnamento a scelta		6	

III anno II Semestre

SSD	Denominazione	Attività	CFU	ambito
FIS/01	Fisica	base	9	Formazione Matematico-Fisica
	Insegnamento a Scelta	car	6	Discipline Informatiche
	Insegnamento a scelta	car	6	Discipline Informatiche
	Tirocinio		3	
	Prova Finale		6	

Totale III anno 60

Corsi a Scelta

I semestre – Tabella 1

Informatica Musicale	6
Laboratorio Avanzato di Programmazione 1	6
Programmazione Parallela su Architetture GPU	6
Startup d'Impresa e Modelli di Business	6

II semestre – Tabella 2

Computer Forensics	6
Calcolo Numerico	6
Laboratorio Avanzato di Programmazione 2	6
Sviluppo di Giochi Digitali	6
Sistemi Centrali	6

CONTENUTO DI MASSIMA DEGLI INSEGNAMENTI

L31 Informatica

Algoritmi, SSD INF/01, CFU 9

Contenuti di Massima: Il corso offre un'introduzione rigorosa allo studio degli algoritmi e delle strutture dati ponendo particolare enfasi sulle relative metodologie generali di progettazione e le tecniche di analisi. Più specificamente, saranno discussi: fondamenti matematici per la stima della complessità asintotica degli algoritmi; problema dell'ordinamento e della selezione; strutture dati elementari, alberi, heap; problema dell'hashing e algoritmi correlati; alberi RB e statistiche d'ordine dinamiche; programmazione Dinamica; algoritmi Golosi; grafi e algoritmi elementari su grafi.

Modalità di esame: Prova scritta, prova pratica di laboratorio e Progetto SW.

Architettura degli Elaboratori, SSD INF/01, CFU 9

Contenuti di Massima: Macchine da calcolo: cenni storici, unità funzionali, architetture. Aritmetica Maya. Rappresentazione binaria dei numeri e dell'informazione. Strutture algebriche, algebre di Boole, logica della commutazione. Porte e circuiti logici, sintesi di reti combinatorie, realizzazione di porte logiche. Circuiti sequenziali, flip-flop, registri. Componenti di chip di memoria e del processore, PLA, FPGA, ALU. Architetture RISC e CISC, modi d'indirizzamento, esempi di ISA reali. Linguaggio assemblativo, direttive di assemblatore, pile e sottoprogrammi. Tipi e formati di istruzioni, esempi di linguaggi assemblativi reali. Modi di indirizzamento complessi, esempi di programmi assemblativi. Operazioni di I/O, controllo e servizio delle interruzioni, eccezioni. Software di supporto, sistema operativo. Struttura del processore, progettazione di microarchitetture cablate, microprogrammazione. Processori ad alte prestazioni, pipelining, tecniche predittive, processori superscalari. Bus e circuiti d'interfaccia, standard d'interconnessione. Dispositivi di memoria principale, DMA, gerarchia delle memorie, memorie cache, miglioramento delle prestazioni, memoria secondaria. Circuiti efficienti per l'aritmetica binaria, aritmetica binaria in virgola mobile, standard IEEE 754. Architetture di sistemi embedded. Chip di calcolo parallelo, multiprocessori, reti e griglie di calcolo.

Modalità di esame: Prova scritta e colloquio orale; progetto di simulatore software (opzionale).

Basi di Dati, SSD INF/01, CFU 9

Contenuti di Massima: Il corso introduce lo studente agli aspetti fondamentali delle basi di dati. Il modello relazionale: Algebra relazionale. SQL: concetti base, caratteristiche evolute. Progettazione di basi di dati, metodologie e modelli per il progetto, progettazione concettuale e logica. Normalizzazione. Gestione delle transazioni Database attivi. Cenni sull'organizzazione fisica delle interrogazioni. Cenni sui noSQL database. DBMS: MySQL, sqlLite, ORACLE.

Modalità di esame: Prova scritta e colloquio orale.

Calcolo Numerico, SSD MAT/08, CFU 6

Contenuti di Massima: il corso offre un'introduzione rigorosa allo studio della risoluzione numerica di problemi matematici, ponendo particolare enfasi sulle relative tecniche numeriche e sviluppo di codici. Più specificamente, saranno discussi: il linguaggio MATLAB come linguaggio di base dei codici da utilizzare per la risoluzione dei problemi numerici su computer; la teoria dell'analisi degli errori; alcuni richiami di elementi di algebra lineare; la risoluzione numerica dei sistemi lineari con metodi diretti ed iterativi; l'interpolazione polinomiale e le splines; la risoluzione numerica delle equazioni non lineari: la risoluzione numerica del calcolo degli integrali

Modalità di esame: Prova scritta e colloquio orale.

Computer Grafica, SSD INF/01, CFU 9

Contenuti di Massima: Il corso introduce lo studente alla intera catena di elaborazione che porta dalla concezione di una immagine alla sua realizzazione mediante procedure algoritmiche, coprendo i seguenti argomenti: mesh 3d e struttura dati per la loro manipolazione, editazione di mesh, curve e superficie spline per la grafica, modelli di illuminazione e loro applicazione, modelli di rendering, controllo della deformazione di una mesh, materiali, UV Mapping, rendering non fotorealistico, raytracing, problematiche di codec.

Modalità di esame: Test scritto a risposta aperta. Test di Laboratorio. Progetto individuale o di gruppo.

Computer Forensics, SSD INF/01, CFU 6

Contenuti di Massima: Il corso mira a favorire l'acquisizione di conoscenze e competenze all'avanguardia in materia di Computer e Image Forensics e a promuovere il riconoscimento e la graduale regolamentazione delle nuove professionalità legate all'informatica forense. Il corso esamina gli aspetti tecnologici (e in parte giuridici) attinenti alla prova digitale in ambito forense. Sono presentate le diverse modalità di investigazione "digitale" alla luce dell'ordinamento giuridico italiano: tecniche di indagine informatica, investigazione difensiva nel campo dei crimini informatici e dei crimini comuni la cui prova sia costituita da dati digitali o veicolati da sistemi informatici. Viene presentato un quadro complessivo dei problemi tecnici, tipicamente informatici, in connessione con le problematiche giuridiche che sottendono a tali tipi di indagini. Ci si sofferma in particolare sulle "best-practice" da utilizzare sul campo per acquisizione, conservazione, analisi e produzione dei dati digitali rinvenuti nei computer e dei flussi telematici per la loro utilizzabilità nell'ambito dei vari tipi di processi, istruttori e/o procedimento amministrativi. Particolare rilievo è dato all'emergente settore dell'Image and Video Forensics e alle relative tecniche investigative.

Modalità di esame: Prova scritta e progetto SW individuale.

Elementi di Analisi Matematica, SSD MAT/05, CFU 12

Contenuti di Massima: Teoria degli insiemi. Numeri reali. Insiemi numerici. Numeri complessi. Successioni e serie numeriche. Limiti di funzioni. Funzioni continue. Calcolo differenziale per le funzioni reali di una variabile. Calcolo integrale. Metodi risolutivi per le equazioni differenziali.

Modalità di esame: Prova scritta e colloquio orale.

Fisica, SSD FIS/01, CFU 9

Contenuti di Massima: il corso si prefigge di formare gli studenti all'applicazione del metodo scientifico e del ragionamento critico e di fornire le nozioni fondamentali per la comprensione dei fenomeni della meccanica e dell'elettromagnetismo. Mediante la risoluzione di esercizi, mira a preparare gli studenti alla risoluzione di problemi concreti riguardanti la cinematica, la dinamica ed i fenomeni elettromagnetici. Gli argomenti principali trattati sono: metodo sperimentale e invarianza delle leggi. Leggi della cinematica e della dinamica. Lavoro, potenza ed energia. Principi di conservazione. Elettrostatica nel vuoto. Condensatori , energia elettrostatica. Conduzione. Legge di Ohm. Circuito RC. Proprietà del campo magnetico. Forza di Lorentz. Legge di Biot-Savart. Legge di Ampere. Induzione. Equazioni di Maxwell.

Modalità di esame: Prova scritta e colloquio orale.

Fondamenti di Informatica, SSD INF/01, CFU 9

Contenuti di Massima: Il corso mira all'acquisizione e allo sviluppo delle capacità dello studente di: comprendere i concetti fondamentali del pensiero informatico, e i principi metodologici che ne ispirano lo sviluppo, mediante una descrizione del suo dizionario, dai concetti di base allo stato dell'arte, nella prospettiva storica della sua evoluzione; apprendere le basi di logica matematica e teoria dei linguaggi formali, propedeutiche allo sviluppo di paradigmi di programmazione e di modelli di calcolo, dai più tradizionali ai più innovativi e non-convenzionali. Più specificamente, dopo un'introduzione storica all'informatica, si trattano i seguenti argomenti: Rappresentazione di algoritmi, strutture di controllo. Principi di progettazione di algoritmi. Elementi di analisi degli algoritmi. Rappresentazione binaria dell'informazione. Dispositivi di memoria fisica dei dati. Compressione e validazione dei dati. Architetture hardware di sistemi di calcolo. Sistemi operativi e macchine virtuali. Reti di calcolatori: Internet e World Wide Web. Linguaggi di programmazione e paradigmi. Traduzione di programmi. Strutture algebriche, Algebre di Boole. Logica predicativa, sintassi e semantica. Logica proposizionale, completezza e compattezza. Completezza e compattezza della logica predicativa. Grammatiche formali e riconoscitori, gerarchia di Chomsky. Automi a stati finiti. Linguaggi regolari. Proprietà dei linguaggi regolari. Pumping lemma per linguaggi regolari. Grammatiche libere e automi a pila. Macchine di Turino. Linguaggi ricorsivamente enumerabili. Modelli di calcolo, Tesi di Church-Turing. Programmazione logica e linguaggi formali Risvolti etici e sociali dell'informatica.

Modalità di esame: Prova scritta e colloquio orale.

Informatica Musicale, SSD INF/01, CFU 6

Contenuti di Massima: Elementi di acustica, il Decibel, Equalizzatori e filtri, Effetti e Processori di Segnali, il Rumore, l'audio digitale, sintesi di segnali sonori, il protocollo Midi, la notazione musicale e l'uso del computer, le macchine virtuali, intelligenza artificiale e musica.

Modalità di esame: Prova scritta e colloquio orale.

Ingegneria del Software, SSD INF/01, CFU 9

Contenuti di Massima: Il corso tratta ciascuna delle fasi dello sviluppo del software di grandi dimensioni ed i più noti processi di sviluppo, inclusi i processi a cascata, RUP, spirale e XP. Si forniranno tecniche per la gestione dei requisiti del software; per la progettazione del software, tramite le linee guida del paradigma ad oggetti, stili architetturali e design pattern più usati, compresi Observer, Composite, Decorator, Factory Method, etc.; per la documentazione tramite diagrammi UML; per la gestione della qualità del codice, tramite metriche, tecniche di test e tecniche di refactoring.

Modalità di esame: Prova scritta e colloquio orale.

INTERNET Security SSD INF/01, CFU 9

Il corso di Internet Security è finalizzato alla conoscenza delle fondamentali minacce alla sicurezza di Internet, all'apprendimento delle essenziali proprietà di sicurezza digitale, nonché alla competenza sull'uso delle principali tecnologie per garantire tali proprietà. Il corso affronterà quindi i metodi per violare (nel gergo, "bucare") una macchina e per proteggerla. Tratterà altresì l'utilizzo e la configurazione degli attuali strumenti per mettere in sicurezza una rete, quali antivirus intelligenti di ultimissima generazione, protocolli crittografici di uso comune in Internet come SSL/TLS, sistemi per il rilevamento di intrusioni come Snort, e firewall come IPTables.

Modalità di esame: Prova scritta e colloquio orale.

Interazione e Multimedia, SSD INF/01, CFU 9

Contenuti di Massima: L'occhio umano e il suo funzionamento. La percezione dei colori. I coni e i bastoncelli. L'equazione lente sottile e le sue applicazioni. Il Bayer pattern nelle macchine fotografiche digitali. Operazioni affini sulle immagini immagini. Il campionamento. La quantizzazione. L'interpolazione. Il PSNR e le tecniche per la valutazione della qualità delle immagini. Gli spazi di colore: HSV, RGB, CMY, YUV, YCbCr Operazioni puntuali e Lut. Operazioni lineari e invarianti per traslazione La convoluzione. Filtri di media, mediano, noise reduction, edge enhancement. Trasformata di Fourier. Teorema della convoluzione. Filtri nel dominio della trasformata. Compressione e teorema di Shannon sulla compressione. Codifica di Huffman. Compressione Lossy e Lossless. Codifica Jpeg. Interfacce in Matlab.

Modalità di esame: Prova scritta e progetto Software.

Introduzione all'analisi dei dati, SSD INF/01, CFU 9 (Introduzione al Data Mining, SSD INF/01, CFU 9)

Contenuti di Massima: Il corso presenta un'introduzione al campo del data mining e del knowledge discovery. Questo rappresenta uno dei campi applicativi più richiesti dalle aziende. I metodi algoritmici e le tecniche sono presentate nella prospettiva delle basi di dati. Il focus delle lezioni sarà sui concetti di base del data mining per la scoperta di pattern nascosti all'interno di grandi quantità di dati.

Modalità di esame: Prova scritta e progetto Software.

Laboratorio avanzato di programmazione 1, SSD INF/01, CFU 6

Contenuti di Massima: Linguaggio C. Sintassi base; dichiarazioni; costrutti condizionali e iterativi; funzioni; array e puntatori; allocazione statica e dinamica; stringhe e funzioni sulle strighe; strutture; gestione dei file. Linguaggio C++. Sintassi base; dichiarazione di classe; metodi e attributi; visibilità; creazione statica e dinamica di un oggetto; overloading; ereditarietà multipla; overloading degli operatori; template. Programmazione microcontrollori; architettura di un microcontrollore; periferiche speciali (linee digitali, convertitore analogico/digitale, timer, uart, bus I2C); esempi di programmazione delle periferiche.

Modalità di esame: Prova scritta in C++ ;Progetto in C su un microcontrollore.

Laboratorio avanzato di programmazione 2, SSD INF/01, CFU 6

Contenuti di Massima: Il corso introduce alla programmazione per dispositivi con Sistemi Operativi Android e iOS.

Modalità di esame: Prova scritta e progetto Software.

Matematica Discreta, SSD MAT/03, CFU 12

Contenuti di Massima: Insiemi ed operazioni su di essi. Cardinalità di un insieme. Applicazioni. Relazioni di equivalenza e di ordinamento parziale. Operazioni algebriche binarie. Strutture algebriche: gruppi, campi. Matrici. Operazioni fra matrici. Matrici notevoli. Determinanti. Proprietà del determinante. Rango di una matrice. Sistemi lineari e matrici ridotte per righe. Calcolo della matrice inversa. Teoremi di Cramer e di Rouché-Capelli.. Vettori e geometria lineare nel piano e nello spazio. Spazi Vettoriali. Applicazioni lineari e matrici. Autovalori ed autovettori. Teoria dei numeri. Congruenze. Calcolo combinatorio e probabilità discrete. Grafi e proprietà.

Modalità di esame: Prova scritta e colloquio orale.

Metodi Matematici e Statistici, SSD MAT/07, CFU 6

Contenuti di Massima: L'obiettivo del corso è di fornire allo studente gli strumenti di base della statistica e del calcolo delle probabilità, per poi applicarli in problematiche informatiche. Più specificamente, saranno discussi i seguenti argomenti: Statistica descrittiva, Elementi di probabilità, Stime di parametri, Verifiche di ipotesi, Generazione di numeri casuali e metodo Monte Carlo, Introduzione alle Catene di Markov, Sistemi a coda.

Modalità di esame: Prova di Laboratorio e colloquio orale.

Programmazione I, SSD INF/01, CFU 9

Contenuti di Massima: Il corso presenta i fondamenti della programmazione procedurale ed i concetti di base della programmazione orientata agli oggetti (OOP) adottando C++ come linguaggio di riferimento. Più specificamente, saranno discussi i seguenti argomenti: Introduzione alla programmazione (Problemi; Algoritmi; Diagrammi di flusso; Variabili; Espressioni; Assegnazioni; Notazione lineare strutturata; Teorema di Bohm-Jacopini). Linguaggi di programmazione (Compilazione ed interpretazione; Installazione e funzionamento di un IDE: Editing, Compiling, Running, Debugging). Nozioni di base del C/C++ (Tipi di dato primitivi; Operatori predefiniti; Conversioni di tipo; Gestione dell'I/O; Puntatori e loro aritmetica; Controllo del flusso: costrutti di selezione e di iterazione; Reference; Array; Stringhe). Algoritmi notevoli (Algoritmi di Ricerca: lineare in una sequenza ordinata e non, ricerca con sentinella, ricerca del massimo/minimo, ricerca dicotomica; Algoritmi di Ordinamento: Bubblesort, Selectionsort, Insertionsort; Algoritmo di Natural-merge). Ricorsione (Gestione delle chiamate ai metodi mediante stack delle attivazioni; Metodi ricorsivi; Ricorsione di coda e non di coda; Efficienza della ricorsione). Introduzione alla OOP (Oggetti: stato e comportamento; Classi: attributi ed operazioni; Messaggi; Istanziazione di oggetti: costruttori e distruttori; Relazione di composizione per gli oggetti; Modificatori di accesso; Allocazione di memoria per i tipi primitivi e non-primitivi; Implementazione di metodi: valore di ritorno, passaggio di parametri per valore e per riferimento; Regole di visibilità; Riferimento "this"; Overloading; Attributi e metodi statici; Metodi "friend": Principi di progettazione orientata agli oggetti: astrazione, encapsulation, information hiding). Nozioni avanzate di OOP (Ereditarietà; Relazione ISA; Gerarchie ereditarie di classi; Overriding; Late-binding; Metodi virtual; Polimorfismo; Classi astratte; Ereditarietà multipla; Diagrammi UML per le classi; Classi e metodi "template").

Modalità di esame: Prova scritta, prova pratica di laboratorio e Progetto SW.

Programmazione II, SSD INF/01, CFU 9

Contenuti di Massima: Il corso ha lo scopo di fornire gli strumenti per la risoluzione di semplici problemi connessi all'uso di alcune strutture dati elementari attraverso l'utilizzo della programmazione ad oggetti. In particolare il corso parte dall'introduzione del concetto di modello dei dati astratto per poi introdurre ed approfondire diversi modelli dei dati quali: pile, code, liste, alberi e grafi. In connessione alle strutture dati saranno dati i concetti di base relativi alla complessità computazionale. Infine verranno trattati i principali algoritmi di ordinamento, tra cui shellsort, quicksort e mergesort. Il linguaggio C++ verrà usato come strumento per presentare le implementazioni delle strutture dati e degli algoritmi.

Modalità di esame: Prova scritta, prova pratica di laboratorio e Progetto SW.

Programmazione Parallela su Architetture GPU, SSD INF/01, CFU 6

Contenuti di Massima: Il corso ha lo scopo di introdurre gli studenti all'uso delle schede grafiche come hardware computazionale ad alte prestazioni: fondamenti del GPGPU (General-Purpose Programming on GPU); architettura CUDA e sue interfacce di programmazione di alto (runtime API) e basso (driver API) livello; strumenti di benchmarking e principali elementi di ottimizzazione e debugging; introduzione all'OpenCL ed alla programmazione GPGPU eterogenea; cenni sul multi-GPU.

Modalità d'esame: esame di laboratorio (individuale), progetto implementativo (individuale o in coppia) concordato con il docente.

Reti di Calcolatori, SSD INF/01, CFU 9

Contenuti di Massima: Architettura di una rete di Calcolatori Il sistema a livelli, servizi e funzionalità. I livelli del TCP/IP. Reti broadcast, multicast, punto-punto, PAN, LAN, MAN e WAN. Il livello fisico e i mezzi trasmissivi. Tecniche di modulazione dei segnali. Il DLL. Framing dei dati, rilevazione e correzione degli errori. Protocolli per l'accesso ai mezzi condivisi - CSMA/CD Ethernet, Fast Ethernet, GigaEthernet. Algoritmi di routing Il protocollo IPv4. Modello Client-Server - Indirizzamento a livello di trasporto Il livello di Trasporto in IP: UDP e TCP. Controllo della congestione in TCP. Comunicazione tra processi Protocolli applicativi: HTTP, FTP , SMTP, DNS.

Modalità di esame: Prova scritta, prova pratica di laboratorio e Progetto SW.

Sistemi Centrali, SSD INF/01, CFU 6

I Sistemi centrali , noti nel mercato come Mainframe, rappresentano tutt'ora il cuore informatico di un gran numero di imprese, Banche ed Enti Governativi che ad essi si affidano per elaborare in modo sicuro grandi volumi di dati, caratterizzati da grande frequenza di accesso da parte di un gran numero di utenti concorrenti. Il 'Manframe' di oggi è molto diverso dai Sistemi degli anni settanta, coi i quali tuttavia mantiene completa compatibilità : esso si presenta infatti come il 'servente' per dati ed applicazioni, in grado di aderire a tutti i modelli applicativi piu' moderni pur mantenendo la continuità con le applicazioni del passato in maniera 'Ibrida' e virtualizzata cioe' supportando diversi sistemi operativi nella stessa 'box'.La conoscenza del Mainframe è quindi oggi ancora un elemento di valore nel curriculum del laureato in Informatica . Il corso si pone l'obiettivo di descrivere ambienti operativi, Hardware, Sistemi Operativi e caratteristiche dei Sistemi Centrali, copre i concetti di Piattaforma Informatica , Infrastruttura Informatica ed Ambiente operativo con particolare risalto sui concetti di Cluster, Sistema Ibrido e Sistema Ottimizzato per un Tipo di lavoro . Offre inoltre una trattazione completa del tema della 'virtualizzazione' delle risorse. Nella parte pratica vengono illustrati i concetti di dimensionamento di Sistemi Virtualizzati e di dimensionamento di Sistemi Ibridi e di dimensionamento di Sistemi Eterogenei, attraverso esercitazioni pratiche di calcolo. La parte finale del corso viene dedicata ai metodi di ''selezione della piattaforma informatica" e della

ottimizzazione della infrastruttura attraverso la valutazione dei costi e della convenienza economica con l'analisi di un gran numero di casi pratici provenienti dalla realtà di mercato.

Modalità di esame: Prova scritta e colloquio orale.

Sistemi Operativi, SSD INF/01, CFU 9

Contenuti di Massima: Il corso propone una completa introduzione ai concetti legati alla progettazione dei moderni sistemi operativi. E' inoltre prevista una parte integrata di laboratorio in cui sono curati gli aspetti implementativi attinenti il corso. I principali argomenti trattati sono: struttura di un Sistema Operativo; gestione dei processi e thread; schedulazione; sincronizzazione dei processi; gestione della memoria centrale, memoria virtuale; interfaccia con il file-system, problematiche di implementazione di un file-system; gestione dell'I/O; comandi UNIX, shell, scripting; gestione dei processi e dei thread; comunicazione inter-processo (code di messaggi, memoria condivisa, semafori).

Modalità di esame: Prova scritta, Colloquio Orale.

Startup d'impresa e Modelli di Business, SECS/P08, CFU 6

Contenuti di Massima: Il corso affronta le principali tematiche relative ai processi di nascita delle nuove imprese e agli aspetti economico-manageriali connessi all'integrazione delle ICT nelle funzioni e nei processi aziendali. L'insegnamento intende fornire le conoscenze di base necessarie per la comprensione delle dinamiche di nascita e sviluppo di nuove imprese nei settori tradizionali, high-tech e internet-based, dei modelli e degli strumenti di analisi, pianificazione e adattamento legati alla gestione d'impresa. Il corso vuole altresì fornire conoscenze e competenze di dettaglio nell'ambito della programmazione dell'attività d'impresa attraverso le applicazioni del business planning e del business modeling con particolare riferimento alle imprese operanti nei settori internet based e ad alta tecnologia. Nel corso, il passaggio dall'idea all'impresa o meglio dalla business idea alla start-up, analizzato in dettaglio, viene affiancato da case studies e progetti di didattica partecipativa che consentono di comprendere al meglio la fasi e gli elementi di criticità dello start-up, il ruolo delle competenze informatiche e gestionali, l'importanza dei modelli di business nella creazione di valore e di vantaggi competitivi.

Modalità di esame: Prova scritta, Colloquio Orale.

Sviluppo di giochi digitali, SSD INF/01, CFU 6

Contenuti di Massima: Il corso con struttura ampiamente seminariale coinvolgerà esperti e sviluppatori professionali di video-game che copriranno differenti moduli relativi allo stato dell'arte attuale nello sviluppo di giochi digitali.

Modalità di esame: Prova scritta, prova pratica di laboratorio e Progetto SW.

Tecniche di Programmazione Concorrente e Distribuita, SSD INF/01, CFU 9

Contenuti di Massima: Il corso presenta le principali tecnologie correnti per lo sviluppo di applicazioni concorrenti e distribuite, incluse: la programmazione multi-threaded in ambiente Java e Linux; la programmazione di rete mediante socket (in linguaggio C e Java); le chiamate di procedura remota (Sun RPC in ambiente Linux e Java Remote Method Invocation - RMI); la costruzione di applicazioni Web (con elementi di HTML e JavaScript) attraverso tecnologie "lato server" quali servlet Java, php, Java Server Pages (JSP); i Web Service per le architetture orientate ai servizi (SOA), con tecnologie Java e .NET.

Modalità di esame: Prova scritta, prova pratica di laboratorio e colloquio orale.

Teoria della Computabilità, SSD INF/01, CFU 9

Contenuti di Massima: Il corso verte sulla formalizzazione di alcuni modelli di calcolo e sullo studio delle loro principali proprietà al fine di evidenziarne alcuni limiti intrinseci. Più in particolare, verranno presentati i seguenti argomenti: macchina URM e funzioni URM-computabili, problemi e predicati decidibili, metodo diagonale di Cantor, teorema s-m-n, programmi universali e applicazioni, decidibilità, indecidibilità e parziale decidibilità, problema della fermata, problemi dell'input e dell'output, ecc., teoremi di Rice e di Rice-Shapiro, insiemi ricorsivi e insiemi ricorsivamente enumerabili, teorema di ricorsione, cenni su complessità e classi di complessità (NP-completezza).

Modalità di esame: Prova scritta, Colloquio Orale.

Teoria dell'informazione e crittografia CFU 9

Contenuti di Massima: Informazione e incertezza. Modello per la trasmissione dell'informazione. Ridondanza e codifica di sorgente. Rumore e codifica di canale. Quantità di informazione. Entropia. Relazione tra entropia e mutua informazione. Il primo teorema di Shannon (o della codifica di sorgente). Teoria dei codici di sorgente. Tipi di sorgente: discrete senza memoria, stazionarie ed ergodiche. Entropia di una sorgente discreta con memoria. Il concetto di codifica, codici univocamente decodificabili. Codici istantanei. Codice di Huffman, ottimalità dei codici di Huffman. Codici aritmetici. Codifica universale di Ziv-Lempel. Notazioni e definizioni. Il canale binario simmetrico e altri canali notevoli. Capacità di canale e sue proprietà. Trasmissione su canali rumorosi. Regole di decisione. Distanza di Hamming. Il secondo teorema di Shannon (o della codifica di canale). Cifrari Storici e One Time Pad. Nozione di Sicurezza Perfetta. Dimostrazione che One-Time Pad garantisce perfetta sicurezza. Introduzione ai Cifrari a Blocchi. DES e AES. Famiglie di Funzioni. Funzioni e Permutazioni Casuali. Funzioni pseudo-casuali (frf) e Permutazioni pseudo-casuali (prf). Applicazioni delle Funzioni e Permutazioni Pseudo Casuali ai cifrari a Blocchi. Cifrari Simmetrici. Cifrari a Stati e Cifrari Randomizzati. Modi di Operazione: ECB, CBC$,CTR$,CTRC. Definizione di Sicurezza contro avversari di tipo CPA. Prova formale che nessun cifrario simmetrico deterministico e senza stati puo' essere sicuro. Sicurezza dei Cifrari CTRC, CTR$, CBC$. Attacchi a crittotesto scelto Definizione di Indistinguibilità relativamente ad attacchi a crittotesto scelto. Funzioni Hash -- Descrizione della funzione SHA1. Definizioni di funzioni hash crittografiche: funzioni universali, funzioni universali unidirezionali, funzioni resistenti alle collisioni. Attacchi generici alle funzioni hash. Cenni ad attacchi specifici contro le funzioni MD4, MD5 e SHA1. La trasformazione Merkle-Damgard. Message Authentication -- Il problema dell'autenticita': introduzione e motivazioni. Autenticita' vs Privacy. Message Authentication Codes (MAC). Verso una definizione di sicurezza. Tipi di attacchi. Definizione di sicurezza (autenticita'). Il paradigma PRF-as-a-MAC. CBC MAC. Introduzione alla crittografia asimmetrica. Elementi di teoria dei numeri computazionale Il problema del Logaritmo discreto. Il

problema Diffie Hellman computazionale. Il problema decisionale Diffie Hellman. Il problema della fattorizzazione. RSA. Il problema RSA e il problema della fattorizzazione. Implementare RSA: primalita', cenni sull'algoritmo Miller Rabin, algoritmo Square and Multiply. Definizioni di sicurezza per i cifrari asimmetrici. Il cifrario El Gamal e sue proprieta'. Cifrari sicuri contro attacchi attivi. Il cifrario RSA-OAEP. Firme digitali. Firme RSA. Perche' le firme RSA di base sono insicure. Il paradigma hash and sign. Full domain hash.

Modalità di esame: Prova scritta, Colloquio Orale.