



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



Bollettino Notiziario - A.A. 2021/2022

LAUREA MAGISTRALE IN CYBERSECURITY (ORD. 2020)

Curriculum: Corsi comuni

BIG DATA COMPUTING (NUMEROSIT CANALE 1)

Titolare: Prof. ANDREA ALBERTO PIETRACAPRINA

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Il corso ha i seguenti prerequisiti: competenze relative al progetto e all'analisi di algoritmi e strutture dati, conoscenza delle nozioni fondamentali di calcolo delle probabilità e statistica, e capacità di programmazione in Java o Python.

Conoscenze e abilità da acquisire:

In questo corso gli studenti imparano tecniche algoritmiche fondamentali per l'elaborazione efficiente ed efficace di insiemi di dati di grande dimensione. Inoltre, attraverso alcune attività pratiche, essi acquisiscono abilità relative allo sviluppo di applicazioni in Apache Spark, che è uno dei framework di programmazione più popolari e diffusi per big data computing.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni frontali, uso di piattaforme di students engagement, seminari di esperti selezionati, e attività propedeutiche allo svolgimento degli homework.

Contenuti:

Il corso affronterà i seguenti argomenti: Introduction to the Big Data phenomenon. Programming frameworks: MapReduce, Apache Spark Reducing input size (Case study: clustering) Reducing output size (Case study: frequent itemsets) Streaming framework.

Modalità di esame:

L'esame consiste in alcuni homework di programmazione, assegnati ogni 2-3 settimane e da svolgere in gruppi di 2-3 studenti, e in una prova scritta individuale comprendente domande teoriche ed esercizi.

Criteri di valutazione:

La valutazione finale è basata sugli homework e sulla prova scritta. Gli homework mirano a verificare la capacità degli studenti di programmare applicazioni big data in Apache Spark, mentre la prova scritta mira a verificare la loro conoscenza delle tecniche algoritmiche apprese durante il corso e la loro capacità di problem solving nel contesto big data.

Testi di riferimento:

J. Leskovec, A. Rajaraman and J. Ullman, Mining Massive Datasets. : Cambridge University Press, 2014

Eventuali indicazioni sui materiali di studio:

Il diario delle lezioni, il materiale didattico e le modalità d'esame dettagliate sono resi disponibili sul MOODLE del corso e sul MOODLE esami.

BIG DATA COMPUTING (NUMEROSIT CANALE 2)

Titolare: Prof. FRANCESCO SILVESTRI

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Il corso ha i seguenti prerequisiti: competenze relative al progetto e all'analisi di algoritmi e strutture dati, conoscenza delle nozioni fondamentali di calcolo delle probabilità e statistica, e capacità di programmazione in Java o Python.

Conoscenze e abilità da acquisire:

In questo corso gli studenti imparano tecniche algoritmiche fondamentali per l'elaborazione efficiente ed efficace di insiemi di dati di grande dimensione. Inoltre, attraverso alcune attività pratiche, essi acquisiscono abilità relative allo sviluppo di applicazioni in Apache Spark, che è uno dei framework di programmazione più popolari e diffusi per big data computing.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni frontali, uso di piattaforme di students engagement, seminari di esperti selezionati, e attività propedeutiche allo svolgimento degli homework.

Contenuti:

Il corso affronterà i seguenti argomenti: * Introduction to the Big Data phenomenon; * Programming frameworks: MapReduce/Spark; * Reducing input size (Case study: clustering); * Reducing output size (Case study: frequent itemsets). * Streaming framework.

Modalità di esame:

L'esame consiste in alcuni homework di programmazione, assegnati ogni 2-3 settimane e da svolgere in gruppi di 2-3 studenti, e in una prova scritta individuale comprendente domande teoriche ed esercizi.

Criteri di valutazione:

La valutazione finale è basata sugli homework e sulla prova scritta. Gli homework mirano a verificare la capacità degli studenti di programmare applicazioni big data in Apache Spark, mentre la prova scritta mira a verificare la loro conoscenza delle tecniche algoritmiche apprese durante il corso e la loro capacità di problem solving nel contesto big data.

Testi di riferimento:

J. Leskovec, A. Rajaraman and J. Ullman, Mining Massive Datasets. : Cambridge University Press, 2014

Eventuali indicazioni sui materiali di studio:

Il diario delle lezioni, il materiale didattico e le modalità d'esame dettagliate sono resi disponibili sul MOODLE del corso e sul MOODLE esami.

BIOMETRICS

Titolare: Prof. SIMONE MILANI

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

La frequentazione del corso richiede la conoscenza di elementi di base di calcolo e teoria della probabilità. Gli studenti potranno valutare il loro livello di competenza tramite un test online. Viene richiesta una conoscenza minima del software Matlab. Possono essere utili (ma non strettamente necessarie) alcune conoscenze preliminari di visione computazionale e di machine learning (presentate nei corsi di "Computer Vision" e "Machine Learning").

Conoscenze e abilità da acquisire:

Il corso è strutturato in modo da fornire agli studenti una buona conoscenza sia pratica sia teorica sulle tecnologie e gli algoritmi connessi alle misure biometriche. In dettaglio, il corso porterà gli studenti ad acquisire e sviluppare le seguenti conoscenze. 1. Conoscenza generale delle principali misure biometriche. 2. Conoscenza dei sensori utilizzati in diversi sistemi biometrici. 3. Conoscenza dei principali modelli matematici che regolano le diverse tecniche di identificazione biometrica. 4. Conoscenza dei principali scenari applicativi. 5. Conoscenza degli aspetti procedurali rilevanti da un punto di vista legale. Gli studenti svilupperanno le seguenti abilità. 1. Capacità di utilizzo dei vari dispositivi di acquisizione presentati nel corso. 2. Capacità di utilizzo delle tecniche di analisi studiate nel corso. 3. Capacità di implementazione dei principali algoritmi presentati nel corso. 3. Capacità di identificare la metodologia più adatta ad uno scenario specifico. 4. Capacità di identificare eventuali situazioni critiche o attacchi ad un sistema di identificazione biometrica (ed attuare delle contromisure). Gli studenti avranno inoltre l'opportunità di testare alcuni dispositivi di acquisizione e sviluppare alcuni sistemi di identificazione biometrica tramite esperienze di laboratorio.

Attività di apprendimento previste e metodologie di insegnamento:

Le conoscenze da acquisire possono essere divise in due parti: a) I sensori di acquisizione biometrica b) I sistemi e gli algoritmi per l'identificazione biometrica. Nell'ambito del corso, le attività e le metodologie di insegnamento prevedono lezioni frontali in aula dove su supporto informatico (powerpoint) e alla lavagna vengono presentati i contenuti del corso. Le lezioni frontali saranno intervallate da 4 lezioni in laboratorio in cui ogni studente potrà applicare alcune tecnologie analizzate nell'ambito del corso.

Contenuti:

Introduzione ai sistemi biometrici Part a: Sensori utilizzati in biometria a.1 Sensori per l'acquisizione di impronte digitali a.1.1 Sensori ottici a.1.2 Sensori capacitivi a.1.3 Sensori termici a.1.4 Sensori RF a.1.5 Sensori ad ultrasuoni a.2 Sensori per il riconoscimento facciale/iride a.2.1 Fotocamere digitali a.2.2 Fotocamere a infrarossi a.2.3 Camere termiche a.2.4 Sensori di profondità 3D a.2.5 Scanner 3D a.2.6 Scanner retinali a.3 Altri sensori a.3.1 Sensori iperspettrali a.3.2 Sistemi di analisi del movimento a.3.3 Sistemi per il rilevamento del DNA Part b: Sistemi di identificazione biometrica b.1 Riconoscimento facciale b.1.1 Schema generale di un sistema di riconoscimento facciale b.1.1 Allineamento e normalizzazione b.1.2 Estrazione delle feature facciali b.1.3 Tecniche di identificazione e verifica b.1.4 Problematiche e attacchi ad un sistema di riconoscimento facciale b.2 Identificazione tramite impronte digitali b.1.1 Schema generale di un sistema di riconoscimento impronte b.1.2 Rilevamento delle minutiae b.1.3 Allineamento dell'impronta b.1.4 Problematiche e attacchi ad un sistema di riconoscimento impronte b.3 Sistemi di riconoscimento dell'iride b.3.1 Identificazione dell'iride b.3.2 Compensazione dell'orientamento, posa, ingrandimento b.3.3 Confronto dell'iride b.4 Riconoscimento vocale b.5 Analisi di sequenze DNA b.6 Analisi della camminata b.7 Altre misure biometriche

Modalità di esame:

La verifica delle conoscenze e delle abilità attese verrà effettuata tramite una prova scritta e lo sviluppo di un report finale (riguardante una delle esperienze di laboratorio scelta dallo studente). I report andranno consegnati almeno un giorno prima dell'esame finale. La valutazione finale sarà costituita dalla media pesata della valutazione della prova scritta (60%) e dei report (40%). Gli argomenti di valutazione della prova scritta verranno chiaramente indicati nel materiale fornito e durante la lezione. Qualora non fosse possibile effettuare una valutazione scritta in presenza a causa dell'emergenza sanitaria Covid-19, la prova scritta potrà essere sostituita da una prova orale a distanza.

Criteri di valutazione:

La valutazione finale sarà determinata in base al livello di conoscenza dello studente degli argomenti del corso e alla capacità di applicare alcune tecniche di analisi. Gli argomenti di valutazione verranno chiaramente indicati nel materiale fornito e durante la lezione. In dettaglio, i criteri di valutazione sono: 1. Completezza delle conoscenze acquisite riguardanti i dispositivi di acquisizione. 2. Accuratezza delle conoscenze acquisite sugli algoritmi e sugli schemi di funzionamento dei principali sistemi di identificazione biometrica. 3. Capacità di implementare e utilizzare diversi sistemi di identificazione biometrica. 4. Proprietà di linguaggio tecnico-legale. 5. Conformità ed efficacia nell'identificazione della tecnica biometrica più opportuna rispetto allo scenario applicativo considerato. 5. Abilità di programmazione. Il giudizio finale terrà conto sia dei risultati raggiunti sia dell'impegno e dell'interesse dello studente nella materia trattata.

Testi di riferimento:

Watt, Jeremy; Borhani, Reza, Machine learning refined - risorsa elettronica-Foundations, algorithms, and applications, Jeremy Watt, Reza Borhani, Aggelos Katsaggelos. New York: Cambridge University Press, 2016 Jain, Anil K.; Ross, Arun A.; Nandakumar, Karthik, Introduction to Biometrics. London: Springer, 2011 Klette, Reinhard, Concise computer vision - risorsa elettronica-An introduction into theory and algorithms, Reinhard Klette. London: Springer, 2014 Ratha, Nalini K.; Govindaraju, Venu, Advances in biometricssensors, algorithms and systems Nalini K. Ratha, Venu Govindaraju. London: Springer, 0

Eventuali indicazioni sui materiali di studio:

Il materiale di studio è costituito da lucidi e appunti sulle lezioni forniti dal docente prima di ogni lezione. Gli appunti sono generati da diversi articoli scientifici e testi sull'argomento. L'attività didattica frontale utilizzerà lucidi, appunti alla lavagna, ed esempi di programma che potranno essere verificati a casa. Tutto il materiale presentato a lezione sarà disponibile sulla piattaforma <http://elearning.dei.unipd.it>. Gli studenti potranno usufruire della licenza MATLAB fornita dall'Università di Padova per lo svolgimento delle esercitazioni e per la programmazione.

COGNITION AND COMPUTATION

Titolare: Prof. MARCO ZORZI

Periodo: I anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Il corso richiede conoscenze preliminari sull'apprendimento automatico e sulla teoria della probabilità. La familiarità con concetti base di psicologia cognitiva e neuroscienze può facilitare la comprensione dei temi trattati.

Conoscenze e abilità da acquisire:

Il corso fornisce conoscenze sui principali approcci computazionali utilizzati per modellizzare l'apprendimento e la cognizione umana, dalle reti neurali artificiali ai modelli probabilistici strutturati. Queste conoscenze sono rilevanti sia per la comprensione del funzionamento della mente che per il disegno di moderni sistemi di intelligenza artificiale. La discussione teorica dei diversi approcci verrà affiancata da esempi concreti di applicazione a problemi di modellizzazione cognitiva.

Attività di apprendimento previste e metodologie di insegnamento:

L'insegnamento è basato su lezioni frontali in cui vengono trattati gli argomenti teorici. Verranno utilizzate tecniche di apprendimento interattivo, come l'apprendimento cooperativo e le discussioni interattive su domande aperte. Questo promuoverà l'apprendimento e l'abilità di riflettere in modo critico sui concetti discussi.

Contenuti:

1. Introduzione: modellizzazione computazionale e matematica nelle scienze cognitive e nelle neuroscienze cognitive. Rassegna degli approcci simbolici, emergentisti e probabilistici alla simulazione della cognizione umana. 2. Modelli probabilistici della cognizione: concetti base su inferenza Bayesiana e modelli grafici probabilistici; apprendimento induttivo; programmazione probabilistica. 3. Modelli connessionisti della cognizione: concetti base sulla computazione neurale; apprendimento nelle reti neurali; architetture per deep learning. 4. Codifica dell'informazione nelle architetture cognitive: codifica efficiente, codifica probabilistica, codifica predittiva. 5. Casi di studio: modelli della percezione umana e dell'acquisizione di concetti; acquisizione del linguaggio e comprensione del linguaggio naturale; ragionamento causale e decision making.

Modalità di esame:

L'esame consisterà in una prova scritta con domande aperte e domande a scelta multipla. Ogni studente dovrà inoltre preparare inoltre un elaborato scritto individuale che approfondisce un argomento assegnato durante il corso e che dovrà essere consegnato il giorno dell'esame scritto.

Criteri di valutazione:

La valutazione sarà basata sulla comprensione degli argomenti trattati nel corso e sull'acquisizione dei concetti e delle metodologie proposte.

Testi di riferimento:

Russell, Stuart; Norvig, Peter, Artificial Intelligence. Harlow: Pearson Education UK, 2013 Goodfellow, Ian; Bengio, Yoshua; Courville, Aaron, Deep learning. London, England; Cambridge, Mass: The MIT Press, 2016 Koller, Daphne; Friedman, Nir, Probabilistic Graphical Models. Cambridge: MIT Press, 2009

Eventuali indicazioni sui materiali di studio:

Tutti gli argomenti verranno trattati durante le lezioni. Le slides delle lezioni saranno disponibili sulla piattaforma di e-learning Moodle. Gli appunti degli studenti dovranno essere integrati dai libri di testo e da altro materiale (soprattutto articoli scientifici) forniti dal docente sulla piattaforma di e-learning.

CYBERSECURITY AND CRYPTOGRAPHY: PRINCIPLES AND PRACTICES

Titolare: Prof. ALESSANDRO LANGUASCO

Periodo: I anno, annuale

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 88A+8E; 12,00

Prerequisiti:

Per la prima parte (Prof. Languasco; 6 CFU): Gli argomenti dei corsi di Algebra (congruenze, gruppi e gruppi ciclici, campi finiti), Analisi I (calcolo differenziale ed integrale, serie numeriche) del corso di studi in Matematica. Per la seconda parte (Prof. Conti and Prof. Migliardi; 6 CFU): OS, Programming.

Conoscenze e abilità da acquisire:

Per la prima parte (Prof. Languasco; 6 CFU): Lo scopo della prima parte del corso e' quello di offrire una panoramica delle basi teoriche necessarie per permettere uno studio critico dei protocolli crittografici usati oggi in molte applicazioni (autenticazione, commercio digitale). Nella prima parte verranno esposti gli strumenti matematici di base (essenzialmente dalla teoria elementare ed analitica dei numeri) necessari per comprendere il funzionamento dei moderni metodi a chiave pubblica. Nella seconda parte vedremo come applicare queste conoscenze per studiare in modo critico alcuni protocolli crittografici. For the second part (Prof. Conti; 3 CFU): Students will be able to identify, classify, describe, explain, and correlated the key concepts of cybersecurity attacks and defenses. For the second part (Prof. Migliardi; 3 CFU): Assess the risks to which an IT system is exposed, Explain how an attack works, Describe, explain and generalize software vulnerabilities, Avoid software pitfalls.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni frontali in classe, se possibile. In presenza di una continuata emergenza sanitaria, mediante teleconferenza.

Contenuti:

Per la prima parte (Prof. Languasco; 6 CFU): First Part: Basic theoretical facts: Modular arithmetic. Prime numbers. Little Fermat theorem. Chinese remainder theorem. Finite fields: order of an element and primitive roots. Pseudoprimality tests. Agrawal-Kayal-Saxena's test. RSA method: first description, attacks. Rabin's method and its connection with the integer factorization. Discrete logarithm methods. How to compute the discrete log in a finite field. Elementary factorization methods. Some remarks on Pomerance's quadratic sieve. Protocols and algorithms. Fundamental crypto algorithms. Symmetric methods (historical ones, DES, AES) . Asymmetric methods. Attacks. Digital signature. Pseudorandom generators (remarks). Key exchange, Key exchange in three steps, secret splitting, secret sharing, secret broadcasting, timestamping. Signatures with RSA and discrete log. Per la seconda parte (Prof. Conti and Prof. Migliardi; 6 CFU): Introduction to Cybersecurity, User Authentication, Access Control, Database Security, Malicious Software, Denial-of-Service Attacks, Intrusion Detection, Firewalls and Intrusion Prevention Systems, Operating System Security, Trusted Computing and Multilevel Security. The execution environment of a program and the vulnerabilities resulting from the threat model of the time. Languages and threat models. Control hijacking: attack. Control hijacking: defense. Security of operating systems and principle of least privilege necessary (and examples of privilege escalation). Sandboxing and interaction with legacy code. Flaw search techniques.

Modalità di esame:

Per la prima parte (Prof. Languasco; 6 CFU): Esame scritto svolto in presenza se possibile; se non possibile per questioni sanitarie, esame scritto svolto in teleconferenza. Per la seconda parte (Prof. Conti and Prof. Migliardi; 6 credits): Esame scritto, progetti assegnati da svolgere a casa, esame orale.

Criteri di valutazione:

Per la prima parte (Prof. Languasco; 6 CFU): Durante la prova scritta lo studente dovrà rispondere ad alcune domande relative al programma svolto dimostrando di aver compreso gli argomenti del corso. Il massimo dei voti (30/30) verrà assegnato in presenza di un compito privo di errori. Il docente si riserva di fare alcune domande orali nel caso in cui sia necessario investigare ulteriormente la preparazione del candidato. L'orale sarà in presenza se possibile o in videoconferenza se l'emergenza sanitaria sarà ancora presente. Per la seconda parte (Prof. Conti and Prof. Migliardi; 6 CFU): Evaluation of both theoretical competence and operational ability to apply what has been learned to a real case.

Testi di riferimento:

Pfleeger, Charles P.; Pfleeger, Shari Lawrence, Security in Computing. : Prentice Hall; 5 edition, 2015 Wenliang Du, Computer Security: a hands-on approach. : Create Space Independent Publishing Platform, 1 ed, 2017 Stallings, William; Brown, Lawrie, Computer security principles and practice. Boston [etc.]: Pearson, 2015 Knospe, Heiko, A Course in Cryptography. Providence: American Mathematical Society, 2019 A. Languasco; A. Zaccagnini, Manuale di Crittografia. Milano: Hoepli, 2015

Eventuali indicazioni sui materiali di studio:

Per la prima parte (6 CFU): Utilizzeremo i seguenti testi: 1) A.Languasco, A.Zaccagnini - Manuale di Crittografia - Hoepli Editore, 2015. (italian). 2) N. Koblitz - A Course in Number Theory and Cryptography -Springer, 1994. 3) H. Knospe - A Course in Cryptography - American Mathematical Society, 2019. 4) R. Crandall, C.Pomerance - Prime numbers: A computational perspective - Springer, 2005. 5) B. Schneier - Applied Cryptography - Wiley, 1994.

DEEP LEARNING

Titolare: Prof. ALESSANDRO SPERDUTI

Mutuato da: Laurea magistrale in Computer Science (Ord. 2021)

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

E' opportuno possedere le conoscenze di base relative al Calcolo delle Probabilità, alla Programmazione e agli Algoritmi.

Conoscenze e abilità da acquisire:

L'insegnamento introduce i concetti di base relativi al Deep Learning, cioè all'apprendimento automatico tramite reti neurali. Verranno richiamati i concetti matematici necessari per una piena comprensione della materia. Si tratteranno le reti neurali feedforward deep e le relative tecniche di regolarizzazione e di ottimizzazione dell'apprendimento. Verranno introdotti i concetti di base relativi alle reti convolutive. Per quanto riguarda il trattamento di sequenze, saranno presentate le reti neurali ricorrenti, con particolare enfasi all'utilizzo di unità LSTM e analoghe. Infine si tratteranno autoencoder e modelli generativi deep. Inoltre, per quanto riguarda l'implementazione dei modelli trattati nel corso, si introdurrà la piattaforma TensorFlow.

Attività di apprendimento previste e metodologie di insegnamento:

L'insegnamento prevede lezioni frontali o in remoto nel caso si renda necessario per motivi di sicurezza sanitaria.

Contenuti:

La tematiche dell'insegnamento saranno le seguenti: - Introduzione ai contenuti dell'insegnamento; - Reti Neurali Feedforward profonde (deep); - Regolarizzazione per l'apprendimento deep; - Ottimizzazione per l'apprendimento di modelli deep; - Concetti di base per reti neurali convolutive; - Reti neurali ricorrenti e Transformers per la modellazione di sequenze; - Autoencoder; - Modelli generativi deep; - TensorFlow.

Modalità di esame:

Lo studente deve superare un esame scritto. Inoltre lo studente deve sviluppare un notebook concordato con il docente.

Criteri di valutazione:

La valutazione dello studente si basa su una verifica dell'apprendimento dei concetti di base introdotti durante il corso e sulla capacità di analisi dello studente. La valutazione del progetto considera la capacità, da parte dello studente, di individuare un caso di studio adeguato e di svolgere in modo autonomo un'attività di progettazione e realizzazione qualitativamente appropriata.

Testi di riferimento:

Goodfellow, Ian; Bengio, Yoshua; Courville, Aaron, Deep Learning. Cambridge: MA, MIT Press, 2016

Eventuali indicazioni sui materiali di studio:

Materiale aggiuntivo sarà disponibile sul sito e-learning del corso.

DIGITAL FORENSICS

Titolare: Prof. SIMONE MILANI

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: 1 anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

La frequentazione del corso richiede la conoscenza di elementi di base di calcolo, algebra lineare (operazioni elementari sulle matrici, inversione, diagonalizzazione) e teoria della probabilità (variabili aleatorie, funzioni distribuzione/densità di massa/probabilità e loro proprietà). Viene richiesta una conoscenza minima del software Matlab. Sono inoltre caldamente consigliate alcune conoscenze preliminari sull'elaborazione delle immagini, calcolo di descrittori locali, classificazione supervisionata di dati vettoriali. Tali argomenti sono presentati nei corsi di "Computer Vision" e "Machine Learning". Qualora lo studente non avesse frequentato i suddetti corsi, verranno forniti dei materiali online per compensare le eventuali conoscenze mancanti.

Conoscenze e abilità da acquisire:

Il corso è strutturato in modo da fornire agli studenti una buona conoscenza sia tecnica sia teorica delle problematiche legali e delle tecniche di analisi sui dati digitali. In dettaglio, il corso porterà gli studenti ad acquisire e sviluppare le seguenti conoscenze. 1. Conoscenza delle principali tecniche di indagine digitale forense. 2. Conoscenza dei principali modelli matematici che regolano i fenomeni alla base delle tecniche di indagine forense su dati digitali. 3. Conoscenza dei principali scenari applicativi. 4. Conoscenza degli aspetti procedurali rilevanti da un punto di vista legale. 5. Conoscenza della terminologia tecnico-legale associata. Gli studenti svilupperanno le seguenti abilità. 1. Capacità di utilizzo delle tecniche di analisi presentate nel corso. 2. Capacità di implementazione dei principali algoritmi presentati nel corso. 3. Capacità di identificare la metodologia di indagine corretta dato uno specifico caso reale. 4. Capacità di svolgere un'indagine digitale in maniera corretta dal punto di vista degli aspetti procedurali. 5. Capacità di presentare un'indagine digitale utilizzando una terminologia tecnico-legale corretta. Gli studenti avranno inoltre l'opportunità di sviluppare e testare tecniche e algoritmi di analisi forense in alcune esperienze di laboratorio.

Attività di apprendimento previste e metodologie di insegnamento:

Le conoscenze da acquisire possono essere divise in due parti: a) Tecniche di analisi del dato digitale b) La rilevanza legale del dato digitale: utilizzo, presentazione e preservazione. La prima parte è costituita da quattro moduli: a.1 Analisi forense dei supporti digitali; a.2 Tecniche di analisi del traffico dati a.3 Analisi forense di dati multimediali a.4 Tecniche di indagine su social networks. La seconda parte è divisa in due moduli: b.1 Reati informatici. b.2 Indagini penali. Nell'ambito del corso, le attività e le metodologie di insegnamento prevedono: Parte a). Tecniche di analisi del dato digitale 12 lezioni frontali in aula dove su supporto informatico (powerpoint) e alla lavagna vengono presentati i contenuti del corso. Tali contenuti verranno inoltre chiariti con esempi pratici di elaborazione in MATLAB. Le lezioni frontali saranno intervallate da 4 lezioni in laboratorio in cui ogni studente potrà applicare alcune tecniche di indagine. Parte b) La rilevanza legale del dato digitale: Lezioni frontali in aula dove su supporto informatico (powerpoint) e alla lavagna vengono presentati i contenuti del corso.

Contenuti:

Introduzione alla digital forensics. L'elaborazione dei dati digitali in contesti legali. a.1) Disk forensics. a.1.1. Introduzione, identificazione di file come elementi di prova, acquisizione dei dati, autenticazione, elaborazione e analisi, documentazione dei risultati. Mantenimento della "Chain of Evidence". a.1.2. Tecniche di cifratura su disco, tecniche di violazione degli algoritmi di cifratura, utilizzo illegale della cifratura (ransomware). a.2) Network forensics. a.2.1. I protocolli di trasmissione dei dati e i server web. a.2.2. Tecniche di intercettazione: sniffing, analisi dei dati da router, analisi dei file di log su server, acquisizione ed elaborazione del traffico su reti wireless, intercettazioni da malware. a.2.3. Rilevamento di intrusioni su rete. a.2.4. Furto di identità e phishing. a.2.5. Strategie antiforensics: cifratura e mascheramento. Il protocollo TOR. a.3) Multimedia forensics. a.3.1. L'acquisizione del dato multimediale. I modelli della camera digitale e del microfono. a.3.2. Autenticazione della sorgente per immagini/video da stima del rumore (PRNU) o identificazione da firmware (interpolazione CFA, tecniche di compressione). a.3.3. Embedding di dati multimediali: steganografia e steganalisi, watermarking. a.3.4. Tecniche di alterazione di immagini/video. Strategie per il rilevamento di alterazioni: basate sui pixel, formato, dispositivo, ambiente fisico, geometria. a.3.5. Alcuni casi reali. a.3.6. Autenticazione dell'origine del dato audio. Le alterazioni sui file audio e il loro rilevamento. a.3.7. Caratteristiche biometriche. Riconoscimento dei volti, identificazione della voce, analisi e confronto di impronte digitali. Tecniche di miglioramento della qualità di dati

audio/immagine/video nell'indagine forense. a.4) Social network forensics. a.4.1. Condivisione e distribuzione dei dati su social network. a.4.2. Tipologie di informazioni calcolabili dai dati su social network: impronta sociale, pattern di comunicazione, immagini e video, attività di un utente, applicazioni. a.4.3. Tecniche di identificazione, localizzazione (nel tempo e nello spazio) e profilatura di un utente. b.1) Reati informatici b.1.1. Fondamenti di diritto penale: principi costituzionali; definizione di reato; elementi costitutivi del reato. b.1.2. Fonti internazionali e sovranazionali in materia di prevenzione e repressione della criminalità informatica. Il carattere transnazionale dei crimini informatici. b.1.3. Nozione di crimine informatico; distinzione tra reati informatici in senso stretto (computer crimes) e reati informatici in senso lato (computer-related crimes). b.1.4. Analisi di alcuni reati informatici: accesso abusivo ad un sistema informatico o telematico; detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; danneggiamenti informatici; phishing; frode informatica; furto e indebito utilizzo di identità digitale; violazioni informatiche della privacy; reati informatici contro il diritto d'autore; cryptolocker ransomware; cyberbullismo; cyberterrorismo. b.1.5. I reati commessi a mezzo di social media. b.1.6. Profili problematici in tema di responsabilità penale dell'ISP. b.2) Indagini penali b.2.1. Le caratteristiche delle indagini digitali. Immaterialità, transnazionalità e cooperazione. b.2.2. I tipi di indagine digitale. Le indagini preventive, repressive e proattive. b.2.3. I mezzi di ricerca della prova. Ispezioni, perquisizioni, sequestri e intercettazioni. b.2.4. La copia clone. La beat stream image. b.2.5. Il ruolo dell'esperto di digital forensics e il diritto di difesa.

Modalità di esame:

La verifica delle conoscenze e delle abilità attese verrà effettuata tramite una prova scritta e lo sviluppo di un progetto finale (da documentare tramite report). I report andranno consegnati almeno un giorno prima dell'esame finale. La valutazione finale sarà costituita dalla media pesata della valutazione della prova scritta (60%) e dei report (40%). Gli argomenti di valutazione della prova scritta verranno chiaramente indicati nel materiale fornito e durante la lezione. Qualora non fosse possibile effettuare una valutazione scritta in presenza a causa dell'emergenza sanitaria Covid-19, la prova scritta potrà essere sostituita da una prova orale a distanza.

Criteri di valutazione:

La valutazione finale sarà determinata in base al livello di conoscenza dello studente degli argomenti del corso e alla capacità di applicare alcune tecniche di analisi. Gli argomenti di valutazione verranno chiaramente indicati nel materiale fornito e durante la lezione. In dettaglio, i criteri di valutazione sono: 1. Completezza delle conoscenze acquisite nell'analisi del dato digitale. 2. Completezza delle conoscenze relative agli aspetti normativi e procedurali relativi al ruolo dell'esperto forense. 3. Capacità di implementare e utilizzare diversi algoritmi di digital forensics. 4. Proprietà di linguaggio tecnico-legale. 5. Conformità ed efficacia nell'identificazione delle tecniche di indagine più opportune rispetto allo scenario applicativo considerato. 6. Abilità di programmazione. 7. Qualità nell'esposizione orale. Il giudizio finale terrà conto sia dei risultati raggiunti sia dell'impegno e dell'interesse dello studente nella materia trattata.

Testi di riferimento:

Klette, Reinhard, Concise Computer Vision. Springer London: , 2014 Bishop, Christopher M., Pattern recognition and machine learning. New York: Springer, 0 Watt, Jeremy; Borhani, Reza, Machine learning refinedrisorsa elettronicafoundations, algorithms, and applicationsJeremy Watt, Reza Borhani, Angelos Katsaggelos. New York: Cambridge University Press, 2016

Eventuali indicazioni sui materiali di studio:

Il materiale di studio è costituito da lucidi e appunti sulle lezioni forniti dal docente prima di ogni lezione. Gli appunti sono generati da diversi articoli scientifici e testi sull'argomento. L'attività didattica frontale utilizzerà lucidi, appunti alla lavagna, ed esempi di programma che potranno essere verificati a casa. Tutto il materiale presentato a lezione sarà disponibile sulla piattaforma <http://elearning.dei.unipd.it>. Gli studenti potranno usufruire della licenza MATLAB fornita dall'Università di Padova per lo svolgimento delle esercitazioni e per la programmazione.

ENGLISH LANGUAGE B2 (PRODUCTIVE SKILLS)

Titolare: Prof. MAURO MIGLIARDI

Periodo: I anno, annuale

Indirizzo formativo: Corsi comuni

Tipologie didattiche: ; 3,00

ENGLISH LANGUAGE B2 (PRODUCTIVE SKILLS)

Titolare: Prof. MAURO MIGLIARDI

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: ; 3,00

ETHICAL HACKING

Titolare: Prof.ssa ELEONORA LOSIOUK

Periodo: Il anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Nessun prerequisito.

Conoscenze e abilità da acquisire:

Esame dei concetti e dell'ambito dell'hacking etico. In particolare, il corso parte dallo studio sistematico delle metodologie e degli strumenti utilizzati dagli hacker per effettuare i vari attacchi nel cyberspazio. Successivamente, il corso Ethical Hacking illustra come il professionista dell'ethical hacking possa svolgere una serie di attività utili sottoponendo i sistemi informatici a test di vulnerabilità. Al termine del corso gli studenti saranno in grado di pianificare attività

di hacking etico. Con questo corso gli studenti impareranno a conoscere la ricognizione, i protocolli e saranno in grado di seguire un codice di condotta etica e fornire garanzie di buone intenzioni nello svolgimento delle attività di test di penetrazione dei sistemi.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni, dimostrazioni e discussione di casi pratici.

Contenuti:

Il corso spiega in dettaglio le attività degli hacker, come avvengono, come gli hacker riescono a entrare illegalmente in un sistema informatico protetto da misure di sicurezza e come difendersi da loro. Gli studenti studieranno le tecniche di Ethical Hacking. Vale a dire, Casing the Establishment: le tecniche di hacking utilizzate per enumerare completamente gli obiettivi. Endpoint and Server Hacking: gli obiettivi finali di qualsiasi hacker, comprese le minacce persistenti avanzate. Infrastructure hacking: il modo in cui gli hacker attaccano le apparecchiature a cui si connettono. Application and Data Hacking: attacchi al mondo web/database e tecniche di hacking mobile. Le contromisure che possono essere utilizzate per ostacolare le attività degli hacker sui sottosistemi considerati. Standard di esecuzione dei test di penetrazione.

Modalità di esame:

Esame alla fine del corso, che coprirà tutto il materiale fornito durante le lezioni.

Criteri di valutazione:

Conoscenza dei concetti studiati durante il corso.

Testi di riferimento:

CONTENUTO NON PRESENTE

FORMAL METHODS FOR CYBER-PHYSICAL SYSTEMS

Titolare: Prof. DAVIDE BRESOLIN

Mutuato da: Laurea magistrale in Computer Science (Ord. 2021)

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Il corso richiede familiarità con alcuni concetti matematici e informatici di base, quali teoria degli automi e della computabilità, analisi matematica. Non ci sono corsi propedeutici.

Conoscenze e abilità da acquisire:

Un sistema cyber-fisico consiste in una collezione di dispositivi informatici in grado di interagire in modo continuo con il mondo fisico tramite sensori e attuatori. Tali sistemi sono sempre più diffusi nelle società moderne, dagli edifici intelligenti ai dispositivi medici alle automobili. Questo corso offre un'introduzione ai principi di progettazione, specifica, modellazione e analisi dei sistemi ciberfisici, fornendo le seguenti conoscenze e competenze: 1. Capacità di modellare un sistema ciberfisico. 2. Capacità di formulare le proprietà che il sistema dovrebbe rispettare in modo matematicamente rigoroso. 3. Capacità di progettare e implementare un algoritmo di verifica per i sistemi ciberfisici. 4. Capacità di eseguire l'implementazione su un test case e di comprenderne e analizzarne i risultati.

Attività di apprendimento previste e metodologie di insegnamento:

Il corso è suddiviso in blocchi tematici, ognuno dei quali affronta un problema reale e lo risolve seguendo l'approccio del pensiero algoritmico. Ogni blocco inizia con una serie di lezioni frontali in aula durante le quali vengono affrontati i contenuti del corso. Terminata l'attività frontale, il blocco prosegue con una o più lezioni di laboratorio dove gli studenti divisi a gruppi implementeranno e testeranno la soluzione del problema reale su un dataset di media dimensione, e si conclude con una fase di confronto e discussione delle varie soluzioni realizzate.

Contenuti:

Sistemi ciberfisici: definizione e caratteristiche chiave. Modelli formali per sistemi ciberfisici: modelli sincroni e asincroni, modelli temporizzati e ibridi. Analisi dei sistemi ciberfisici: proprietà di sicurezza e vivacità, sistemi dinamici e proprietà di controllo.

Modalità di esame:

Esame orale e/o progetto.

Criteri di valutazione:

I criteri di valutazione sono i seguenti: 1. Completezza delle conoscenze acquisite; 2. Proprietà della terminologia tecnica utilizzata; 3. Capacità di modellare un sistema ciberfisico e le proprietà desiderate 3. Capacità di utilizzare strumenti di verifica formale per i sistemi ciberfisici 4. Capacità di progettare e implementare algoritmi di verifica per sistemi ciberfisici

Testi di riferimento:

Alur, Rajeev, Principles of cyber-physical systems. Cambridge: MS, MIT, 2015

Eventuali indicazioni sui materiali di studio:

Il corso ha una sezione dedicata sul Moodle del Dipartimento di Matematica. Il Moodle raccoglierà le dispense del corso, le specifiche dettagliate delle attività di laboratorio, gli esercizi e le loro soluzioni. Verrà usato anche per comunicazioni e aggiornamenti da parte del Docente.

FOUNDATIONS OF DATABASES

Titolare: Prof. NICOLA FERRO

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Attività di apprendimento previste e metodologie di insegnamento:

+ Lectures + Labs --- use of an open source database management system (PostgreSQL); --- programmatic access to databases (JDBC) --- use of indexes in PostgreSQL + Seminars of visiting colleagues on research topics and/or seminar by companies on the use and perspectives for innovative products based on databases, role of the engineer in a company, stage opportunities, simulation of job interviews. + Homeworks: there are 3 homeworks (gathering and analysis of the requirements; conceptual design and logical design; physical design and implementation), to be carried out in group, in order to design and develop a "real" database application. Homework deadlines are aligned with the contents of the lectures so that students can immediately apply the learned concepts to a case study of their own interests. + Interactive lessons and exercises in classroom: students are divided into group (different from the homework ones) and try to apply the learned concepts (gathering and analysis of the requirements; conceptual design; logical design; physical design and implementation) to a case study proposed by the teacher. Then, each group, presents its works to the class and discusses it with the teacher and the other students.

Contenuti:

+ Overview of database management systems + Gathering, analysis and design of user requirements + The Entity-Relationship (ER) model --- conceptual design + The Relational model and the relational database management systems --- logical design --- relational algebra --- mapping from conceptual to relational model + The SQL language --- data definition language --- data manipulation language --- advanced concepts (indexes, views, stored procedures, foreign data wrappers) + Programmatic access to databases --- the JDBC APIs for the Java programming language

Testi di riferimento:

Ramez Elmasri, Shamkant B. Navathe, Fundamentals of Database Systems, 7th Edition. : Pearson, 2016

Eventuali indicazioni sui materiali di studio:

The teaching material consists of: - reference book - instructor's slides - suggested readings - examples of homeworks + output of the interactive classroom exercises produced by student groups All the teaching material is available on the Moodle platform (elaarning.dei.unipd.it). Suggested readings: + Batini, C., Ceri, S., and Navathe, S. B. (1992). Conceptual Database Design. An Entity-Relationship Approach. The Benjamin/Cummings Publishing Company, Inc., Redwood City (CA), USA. + Celko, J. (2011). Joe Celko's SQL for Smarties: Advanced SQL Programming. Morgan Kaufmann Publishers, San Francisco (CA), USA.

GAME THEORY

Titolare: ELVINA GINDULLINA

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Un corso anche basilare di teoria della probabilità.

Conoscenze e abilità da acquisire:

L'insegnamento prevede l'acquisizione delle seguenti conoscenze e abilità, suddivise in due insiemi. 1: parte base. Apprendere e padroneggiare concetti teorici di base e avanzati della teoria dei giochi e saper risolvere problemi generali multi-obiettivo multi-agente con tecniche della teoria dei giochi. 2: parte applicativa. Sapere applicare i concetti della teoria dei giochi a scenari pratici, specialmente di tipo ICT; in questo contesto, e' di particolare interesse l'abilità di contestualizzare la teoria dei giochi come strumento di valutazione per l'efficacia della risoluzione tramite procedure multi-agente distributed.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni convenzionali con il supporto di slide. Prevista interazione su piattaforma moodle. Caricamento video via Kaltura.

Contenuti:

Concetti base di teoria dei giochi Utilità, mercato, fattore di sconto Giochi statici in forma normale Dominanza, Equilibri di Nash Efficienza, prezzo dell'anarchia Giochi a somma zero, giochi minimax Strategie miste, equilibri misti Teorema di Nash, il teorema minimax The tragedy of the commons Giochi dinamici Strategie e sottogiochi Backward utility Equilibri di Stackelberg Giochi ripetuti, collaborazione Duopoli dinamici, collusione Cooperazione, pricing Informazione incompleta/imperfetta Giochi bayesiani, signaling, beliefs Principio di rivelazione Teoria dei giochi assiomatica Fictitious play Best response dynamics Ottimizzazione distribuita Game theory algoritmica Calcolo, complessità, e completezza dell'equilibrio Aste, bargaining Aste di primo e secondo prezzo Criterio VCG Giochi cooperativi, il nucleo, il valore di Shapley Allocazione delle risorse Utilità, scelte e paradossi Giochi potenziali, coordinazione Algoritmi bio-inspired Giochi evolutivi Reti cognitive Selfish routing Sistemi multi-input con teoria dei giochi

Modalità di esame:

In qualunque caso l'esame comprende un test scritto obbligatorio a libro aperto, dove vengono sottoposti diversi problemi di game theory allo studente su argomenti toccati durante il corso. Per ogni esercizio, vengono poste più domande, tipicamente tre. Per frequentanti, l'esame può coinvolgere lo sviluppo di un progetto in gruppi di 1-3 persone, su argomenti del corso applicati alle ICT. L'adesione a questa modalità e l'argomento del progetto sono concordati con il docente durante il corso. Se il test scritto e' sufficiente, si può registrare il voto conseguito come voto finale dell'esame. Si può ulteriormente discutere il progetto sviluppato durante il corso con un esame orale, da svolgersi dopo l'esame scritto. Questi esami orali si svolgono nella stessa giornata di un esame scritto, ma non necessariamente bisogna presentarsi nella stessa giornata per l'esame scritto e la discussione orale del progetto. La discussione orale integra il voto dello scritto.

Criteri di valutazione:

Ogni domanda nei test scritti viene valutata fino a un massimo di 3 punti. La discussione del progetto viene valutata fino a 10 punti. Il voto finale e' la somma numerica dei punteggi individuali delle domande e della discussione del progetto (se presente), limitata a 30. Un punteggio di 30 e lode e' assegnato agli studenti il cui punteggio numerico e' superiore a 31. Nella valutazione di ogni domanda scritta vengono tenuti in considerazione: - la pertinenza, la correttezza, e la completezza della risposta; - l'utilizzo appropriato delle terminologie, metodologie, e rappresentazioni formali tipiche della teoria dei giochi - l'acquisita capacità di problem solving - la capacità di discussione e verifica ex-post della soluzione trovata Nella valutazione del progetto (se presente) vengono tenuti in considerazione: - l'originalità della proposta e la pertinenza sia con le tematiche del corso che con le metodologie ingegneristiche tipiche dell'ICT - la qualità dell'esposizione orale - la capacità di lavoro di gruppo e la presenza di singoli contributi attribuibili ai

partecipanti al progetto - la capacita' di trarre conclusioni significative dal punto di vista scientifico grazie alle metodologie apprese nel corso

Testi di riferimento:

CONTENUTO NON PRESENTE

Eventuali indicazioni sui materiali di studio:

Diversi libri forniscono una trattazione generale di teoria dei giochi. A mero titolo di suggerimento, si può usare il libro di Tadelis come riferimento in senso generale. Questa parte comunque dovrebbe essere integrata con materiale per le applicazioni. Il libro di MacKenzie e DaSilva è un buon esempio, anche se non è obbligatorio usare un libro per questo scopo (si può fare riferimento anche a materiale trovato in rete). In ogni caso, il docente fornirà agli studenti tutte le dispense delle lezioni e appunti aggiuntivi.

HUMAN COMPUTER INTERACTION

Titolare: Prof. LUCIANO GAMBERINI

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: I anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 42A; 6,00

Prerequisiti:

Non sono richiesti particolari prerequisiti. Per gli studenti che parlano italiano, si suggerisce di frequentare contemporaneamente il laboratorio di INTERACTION DESIGN progettato per mettere ulteriormente in pratica quanto appreso in questo corso.

Conoscenze e abilità da acquisire:

Il corso offre la possibilità di acquisire conoscenze teoriche, metodi di ricerca e tecniche innovative per lo studio, la progettazione e la valutazione dell'interazione tra le persone e le tecnologie. Tali conoscenze sono utili per rendere l'interazione persona-macchina efficace ed efficiente e l'esperienza d'uso semplice, piacevole e complessivamente soddisfacente per l'utente. Le competenze che si acquisiranno interesseranno quindi i domini di conoscenza dell'interazione persona-computer (HCI) e dell'ergonomia cognitiva; in dettaglio si acquisiranno competenze negli ambiti: - del design centrato sull'utente - dei principi di base dell'ergonomia cognitiva - della valutazione dell'esperienza dell'utente e dell'usabilità dei prodotti - della comunicazione visiva e della visualizzazione dei dati - dell'accessibilità e del design universale (es: design for older adults) - del social computing e dell'ergonomia sociale

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni tradizionali e interattive (presentazioni studenti, multimedia, risorse on-line) sugli aspetti teorici della disciplina saranno intervallati da laboratori didattici in cui si sperimenteranno i metodi e le tecniche appresi durante il corso. Lavori individuali e di gruppo tramite il design e lo sviluppo di prototipi di interfacce e sistemi interattivi permetteranno allo studente di acquisire competenze specifiche e pratiche. Sono benvenute, ma non sono obbligatorie particolari precedenti competenze tecniche o informatiche.

Contenuti:

Seguendo il libro si analizzeranno i seguenti argomenti: 1 What is Interaction Design? 2 The Process of Interaction Design 3 Conceptualizing Interaction 4 Cognitive Aspects 5 Social Interaction 6 Emotional Interaction 7 Interfaces 8 Data Gathering 9 Data Analysis, Interpretation, and Presentation 10 Data at Scale 11 Discovering Requirements 12 Design, Prototyping, and Construction 13 Interaction Design in Practice 14 Introducing Evaluation 15 Evaluation Studies: From Controlled to Natural Settings 16 Evaluation: Inspections, Analytics, and Models Durante le lezioni verranno discussi e sperimentati praticamente metodi di ricerca e tecniche per la progettazione e la valutazione di sistemi interattivi.

Modalità di esame:

NON FREQUENTANTI: L'esame sarà orale con 3 domande sul libro, una delle quali proposta come esercizio (vedere il libro per trovare esempi). In caso di permanenza della situazione di emergenza l'orale sarà svolto on-line FREQUENTANTI: L'esame sarà basato su un lavoro personale di ricerca da svolgere durante il corso come lavoro per casa e su una breve prova orale di presentazione e discussione del medesimo. Un report sintetizzerà il lavoro svolto in modo simile a un paper scientifico o a un report professionale. La ricerca da sviluppare verrà riassunta in un report che includerà i seguenti punti: 1 - introduzione, contestualizzazione teorica, benchmarking 2 - processo di design/co-design 3 - sviluppo/modifica prototipo (per chi ha meno esperienza tecnica ci sono soluzioni) 4 - valutazione - analisi dei dati (es: UX, usability, presence, acceptance) 5 - risultati - discussione finale Qualsiasi tecnologia potrà essere sviluppata/adottata per la ricerca purché sia interattiva (es: web, robot, realtà virtuale/aumentata, dispositivi smart home, strumenti di lavoro, tools di Arduino, veicoli, strumenti musicali, apps. su cellulare/Tablet).

Criteri di valutazione:

NON PARTECIPANTI: Ogni domanda ha lo stesso valore, in altri termini ogni domanda ha un peso di 10 su 30. Il punteggio finale sarà la somma del punteggio di ogni domanda. PARTECIPARE La valutazione si baserà in gran parte sulla qualità del report e delle sue parti con un punteggio di 5 punti per ciascuna di esse, per un punteggio massimo di 25. I restanti 5 punti saranno basati sulla presentazione orale della ricerca.

Testi di riferimento:

Helen Sharp, Jenny Preece, Yvonne Rogers, Interaction Design: Beyond Human-computer Interaction. : Wiley, 2019

Eventuali indicazioni sui materiali di studio:

FREQUENTANTI INTERACTION DESIGN (5th ed.)- di Helen Sharp, Jenny Preece e Yvonne Rogers è il libro di testo. Materiali didattici saranno a disposizione a lezione e su moodle per tutti gli studenti frequentanti e sostituiranno parti del libro. NON FREQUENTANTI INTERACTION DESIGN (5th ed.)- di Helen Sharp, Jenny Preece e Yvonne Rogers è l'unico materiale da utilizzare per questo corso se non lo si frequenta.

INFORMATION SECURITY

Titolare: Prof. NICOLA LAURENTI

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: I anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 40A+8L; 6,00

Prerequisiti:

Il corso richiede conoscenze di base su: 1. reti di telecomunicazioni o di calcolatori. 2. trasmissione digitale 3. algoritmi e complessità computazionale 4. statistica, probabilità e teoria dell'informazione

Conoscenze e abilità da acquisire:

L'insegnamento mira a guidare lo studente tra i concetti fondamentali e gli strumenti più significativi nella sicurezza dell'informazione, con particolare attenzione alle soluzioni, agli attacchi e alle contromisure che possono essere messe in opera ai vari livelli di una moderna rete di comunicazioni. Esso prevede che lo studente acquisisca le seguenti conoscenze: 1. Prendere consapevolezza dell'importanza di proteggere informazioni critiche in contesti con possibilità di attacco. 2. Avere una chiara visione dei diversi obiettivi e servizi di sicurezza dell'informazione, nonché delle modalità in cui possono essere forniti da diversi meccanismi di protezione. 3. Conoscere meccanismi di sicurezza computazionale e incondizionata per vari servizi ai diversi livelli dell'architettura di rete. Inoltre si prevede che lo studente acquisisca le seguenti abilità: 1. Riconoscere le minacce possibili in una specifica rete di telecomunicazioni. 2. Saper identificare in uno specifico contesto gli obiettivi e servizi di sicurezza dell'informazione richiesti, nonché le modalità in cui possono essere forniti da diversi meccanismi di protezione. 3. Saper valutare anche quantitativamente il grado di sicurezza offerto da un meccanismo o da un protocollo. 4. Saper dimensionare i parametri di un meccanismo di sicurezza (ad es., lunghezza della chiave o numero di round) secondo il livello di sicurezza richiesto.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni frontali e sessioni di laboratorio. Discussioni in piccoli gruppi e lezioni interattive. IL corso ospiterà anche alcune lezioni on line e laboratori virtuali tenuti dal Prof. A. Soceanu (Hochschule München) sul tema "Gestione sicura di reti" nell'ambito del progetto "Shaping a world-class university - Seed funding for Digitalization & Innovation" 2021, tipologia "Short term Visiting Professors"

Contenuti:

1. Concetti fondamentali di sicurezza dell'informazione. 2. Modelli quantitativi e determinazione del grado di sicurezza. 3. Meccanismi di sicurezza crittografici e non. 4. Protocolli di sicurezza ai vari strati dei modelli di rete. 5. Ulteriori problematiche di sicurezza specifiche per reti wireless, ad hoc e mobili.

Modalità di esame:

L'esame consta di due prove: 1. Una prova scritta con domande analitiche e problemi numerici. 2. Una prova orale tradizionale sugli argomenti del corso. Il superamento della prova scritta è condizione necessaria per l'ammissione alla prova orale, al termine della quale si determina il risultato dell'esame.

Criteri di valutazione:

L'esame mira ad accertare che lo studente abbia acquisito le seguenti competenze: 1. una profonda comprensione dei concetti fondamentali della sicurezza 2. l'abilità di applicare modelli generali ad esempi particolari di algoritmi e protocolli di sicurezza 3. la capacità di valutare criticamente e confrontare tra loro diversi meccanismi di sicurezza.

Testi di riferimento:

Douglas R. Stinson, Cryptography: Theory and Practice.. : Chapman&Hall/CRC, 2014

Eventuali indicazioni sui materiali di studio:

Materiale aggiuntivo e riferimenti bibliografici saranno disponibili sulla pagina Moodle del corso.

INTERNET OF THINGS AND SMART CITIES

Titolare: Prof. LORENZO VANGELISTA

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: Il anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Conoscenze impartite nel corso di Telecomunicazioni; conoscenze dei principi di base delle reti di telecomunicazioni, in particolare dei protocolli internet

Conoscenze e abilità da acquisire:

Conoscenza del concetto di Internet delle cose nelle sue articolazioni e capacità di applicare il paradigma dell'Internet delle cose a problemi concreti di telecomunicazioni. Conoscenza del concetto di Smart City nelle sue articolazioni e capacità di applicare il paradigma della Smart City a problemi concreti gestione delle città, con particolare riferimento agli aspetti di ICT

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni frontali e discussione di casi concreti

Contenuti:

Introduzione - Definizione di Internet delle cose, sue applicazioni, trend scientifici e di mercato. - Internet delle cose e domotica - Internet delle cose e applicazioni industriali - Definizione di Smart City, trend scientifici e di mercato Internet delle cose - Diversi approcci: Long range cellular (M2M), long range su frequenze libere, short range, RFID - Principali problematiche a livello scientifico: livello fisico, addressing e routing, security - Enti di standardizzazione e consorzi: ETSI M2M, IETF, IEEE, OMA Lightweight M2M, Thread, OIC, Allseen Alliance etc. - Alcuni standard principali: ZigBee, 6LoWPAN, WiFi (802.11ah), Bluetooth Low Energy, SigFox, Lo-Ra, - Piattaforme per l'Internet delle cose: Xively, ThingWorx, OpenHAB - Analytics SmartCity - Definizione di Smart city readiness per una città - Architetture di comunicazione e applicative - Problemi normativi e open data - Applicazioni: metering, parking, monitoring - Analytics per Smart City - Privacy e security

Modalità di esame:

Esame scritto o progetto integrato da esame orale. In caso di progetto integrato da esame orale, il progetto sarà focalizzato su un argomento e l'orale servirà ad assicurare che lo studente abbia conoscenze sufficienti degli argomenti dell'intero corso.

Criteri di valutazione:

Verifica della conoscenza degli argomenti esposti nel corso. Capacità di applicare i concetti esposti a casi pratici. Nel caso di project work: innovatività, capacità di lavorare in autonomia, capacità di stendere una relazione ben organizzata e informativa sul project work.

Testi di riferimento:

J. Vasseur and A. Dunkels, Interconnecting Smart Objects with IP - The Next Internet. Burlington, MA 01803, USA: Morgan Kaufmann, 2010 Z. Shelby and C. Bormann, 6LoWPAN: The Wireless Embedded Internet. Chichester, West Sussex, UK: John Wiley & Sons Ltd, 2009 Geoffrey G. Parker, Marshall W. Van Alstyne, Sangeet Paul Choudary, Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You. USA: W.W. Norton & c, 2016 Samuel Greengard, The Internet of Things. USA: MIT press, 2015 Carles Anton-Haro, Mischa Dohler (Editors), Machine-to-machine (M2M) Communications: Architecture, Performance and Applications. UK: Woodhead Publishing, 2015 D. Kellmerit and D. Odovoski, The Silent Intelligence - The Internet of Things. USA: DnD Ventures, 2013 Milan Milenkovic, Internet of Things: Concepts and System Design. : Springer International Publishing, 2020 Shahin Farahani, ZigBee Wireless Networks and Transceivers. UK: Newnes, 2008 Stan McClellan, Jesus A. Jimenez, George Koutitas (Editors), Smart Cities: Applications, Technologies, Standards, and Driving Factors. : Springer, 2018

Eventuali indicazioni sui materiali di studio:

Appunti dalle lezioni; come libro di riferimento si consiglia il testo "Internet of Things: Concepts and System Design", Milan Milenkovic, Springer International Publishing, 2020

LAW AND DATA

Titolare: da definire

Mutuato da: Laurea magistrale in Data Science (Ord. 2017)

Periodo: l'anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

No prerequisites

Conoscenze e abilità da acquisire:

The course aims to introduce non-law students to a proper understanding of the main legal issues related to the processing of data, personal and non. The first part of the course aims to enable students to approach EU personal data protection regulation. In the second part, instead, students will reflect on the main problems related to the use of data-intensive technologies (big data and artificial intelligence) and the technical and legal solutions now debated.

Attività di apprendimento previste e metodologie di insegnamento:

Classes Seminars Workshops Preassigned readings.

Contenuti:

All the info about the course are on Moodle - Introduction to Law and Legal Studies - Introduction to the EU Law - Introduction to the EU GDPR - The concept of data; personal, sensitive and economic data; big data - Property of data, choices in the management of data - The right to be forgotten - Civil and criminal aspects of profiling activity - Automatic data processing, human responsibilities - The Data Protection Officer and DP Authorities - Civil and criminal protection of privacy - Sanctioning powers and system - Open Data for the public interest - Big data (collection, analysis, processing) and their influence on fundamental rights - Digital Surveillance - Facial Recognition: Open Issues - Disinformation - Artificial Intelligence in the EU law

Modalità di esame:

Written Exam

Criteri di valutazione:

The grading scale used to assess the students is the Italian one, with the highest score of 30/30 and a minimum score of 18/30 (sufficient) (info: here). The students will be graded according to their level of theoretical and practical knowledge of the fields covered throughout the course and their capacity to critically reflect on the most contentious legal issues on data-intensive technologies.

Testi di riferimento:

CONTENUTO NON PRESENTE

Eventuali indicazioni sui materiali di studio:

The course has no official textbooks. Students can study on their notes and the additional material provided by the instructor. Nevertheless, here are some helpful handbooks to approach some modules. These books are not mandatory, and students have sole discretion to refer them. ? Mireille Hildebrandt (2020). Law for Computer Scientists and Other Folk, OUP (open access: here) – especially chapters 2-3-4-5-9-10 ? Paul Voigt, Axel von dem Bussche (2017). The EU General Data Protection Regulation (GDPR). A practical guide, Springer (unipd access: here) ? European Fundamental Rights Agency (2018). Handbook on European data protection law, Luxembourg (open access: here) ? Karen Yeung, Martin Lodge (2019). Algorithmic Regulation, OUP (Public Law Dept. Library) – especially chapters 2-3-4-6-7-11

MACHINE LEARNING

Titolare: Prof. FABIO VANDIN

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: l'anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Conoscenze di Base di Analisi Matematica, Probabilità, Statistica, Algebra Lineare, Algoritmi, e elementi di base di Programmazione.

Conoscenze e abilità da acquisire:

Lo scopo del corso è di fornire i principi fondamentali del problema di apprendimento e di introdurre i principali algoritmi per la regressione e la classificazione. Il corso includerà esercitazioni al computer. Alla fine del corso lo studente avrà le seguenti conoscenze ed abilità: 1. Conoscerà i principi fondamentali e le principali metodologie dell'apprendimento automatico. 2. Sarà in grado di affrontare problemi di apprendimento supervisionato e non supervisionato. 3. Saprà applicare queste metodologie a diversi scenari e problemi. 4. Sarà in grado di selezionare la metodologia più adatta alla soluzione di uno specifico problema di apprendimento sulla base delle caratteristiche del problema e dei dati a disposizione. 5. Avrà le competenze per utilizzare e adattare sistemi software in grado di risolvere i problemi considerati. 6. Se possibile saranno fornite anche competenze relative ad argomenti più avanzati come sparsità, boosting e deep learning.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni teoriche con utilizzo sia di lucidi che della lavagna. Esercitazioni in aula con coinvolgimento degli studenti. Esercitazioni al computer (in laboratorio), anche con l'utilizzo di casi di studio. Tutto il materiale didattico presentato durante le ore di lezione frontale sarà reso disponibile sulla piattaforma elearning (<http://elearning.dei.unipd.it>).

Contenuti:

Motivazioni, componenti del problema di apprendimento e applicazioni dell'apprendimento automatico. Apprendimento supervisionato e non supervisionato. Parte I: Apprendimento supervisionato. 1. Introduzione: Dati, classi di modelli, funzioni di costo. 2. Modelli probabilistici e ipotesi sui dati. Funzione di regressione. Regressione e Classificazione. 3. Bontà di un modello, complessità, compromesso tra distorsione e varianza (dimensione di Vapnik-Chervonenkis, errore di generalizzazione). 4. Modelli per la regressione: regressione lineare (scalare e multivariata), selezione di variabili, modelli lineari nei parametri, regolarizzazione. 5. Classi di modelli non lineari: Sigmoidi, Reti Neurali. 6. Metodi "Kernel": Support Vectors Machines. 7. Metodi per la classificazione: Regressione Logistica, Reti Neurali, Perceptron, Classificatore di Bayes, SVM, Deep Learning. 8. Validazione e selezione dei modelli: errore di generalizzazione, compromesso tra distorsione e varianza, cross validation. Determinazione della complessità del modello. Parte II: Apprendimento non supervisionato 1. Analisi di clusters: K-means, misture di Gaussiane e stima EM. 2. Riduzione della dimensionalità: analisi delle componenti principali (PCA).

Modalità di esame:

La valutazione delle conoscenze e delle abilità acquisite viene effettuata mediante due contributi: 1. Una prova scritta a libro chiuso in cui lo studente deve risolvere dei problemi, al fine di verificare l'acquisizione dei principali ingredienti e strumenti del problema di apprendimento, la capacità analitica nel loro utilizzo e la capacità di interpretare i risultati tipici in un problema pratico di apprendimento. 2. Esercitazioni al computer (facoltative) rivolte all'acquisizione delle competenze, anche pratiche, per l'utilizzo degli strumenti di machine learning. Queste esercitazioni, da svolgere a casa, consentono di verificare la capacità di mettere in pratica i concetti teorici acquisiti. Lo studente deve produrre una breve relazione che descriva le metodologie utilizzate per risolvere il progetto assegnato assieme ai risultati ottenuti. Il voto finale sarà basato sulla prova scritta con un bonus fino ad un massimo di 3 punti per gli studenti che svolgeranno le esercitazioni di laboratorio

Criteri di valutazione:

La valutazione con cui verrà effettuata la verifica delle conoscenze e delle abilità acquisite considera: 1. La completezza delle conoscenze acquisite per quanto riguarda gli strumenti per la predizione (regressione e classificazione). 2. La capacità di risolvere un problema di apprendimento attraverso le tecniche proposte 3. La proprietà nella terminologia tecnica usata, sia scritta che orale 4. L'originalità e indipendenza nella identificazione delle metodologie più adatte a risolvere uno specifico problema di apprendimento. 5. La capacità di interpretare i risultati in un problema pratico di apprendimento 6. Abilità nell'utilizzo degli strumenti informatici per l'apprendimento automatico 7. L'abilità analitica e pratica nell'uso di questi strumenti per la soluzione di semplici problemi.

Testi di riferimento:

C. M. Bishop, Pattern Recognition and Machine Learning.. : Springer, 2006
Murphy, Kevin P., Machine Learning: a probabilistic perspective.. : Mit press, 2012
Shalev-Shwartz, Shai; Ben-David, Shai, Understanding machine learning: from theory to algorithms.. : Cambridge University Press, 2014
T. Hastie, R. Tibshirani, J. Friedman, The Elements of Statistical Learning.. : Springer, 2008

Eventuali indicazioni sui materiali di studio:

Il corso sarà basato sui libri di testo: "Understanding Machine Learning: from Theory to Algorithms", "Machine Learning, a probabilistic perspective", "Pattern Recognition and Machine Learning", e "The Elements of Statistical Learning" (vedi Sezione "Testi di Riferimento"). Materiale aggiuntivo e informazioni dettagliate sulle modalità d'esame sono rese disponibili sul sito web del corso, accessibile dalla pagina <http://elearning.dei.unipd.it>

METHODS AND MODELS FOR COMBINATORIAL OPTIMIZATION

Titolare: Prof. LUIGI DE GIOVANNI

Mutuato da: Laurea magistrale in Computer Science (Ord. 2021)

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 32A+4E+12L; 6,00

Prerequisiti:

Elementi di ricerca operativa, elementi di programmazione lineare, elementi di base di programmazione.

Conoscenze e abilità da acquisire:

Uso di metodologie quantitative di supporto alle decisioni per la modellazione e la soluzione di problemi di ottimizzazione combinatoria. Il corso intende fornire strumenti matematici e algoritmici per la soluzione di problemi pratici di ottimizzazione con l'utilizzo dei pacchetti software e delle librerie di ottimizzazione più diffusi.

Attività di apprendimento previste e metodologie di insegnamento:

L'insegnamento prevede lezioni frontali, esercitazioni in laboratorio, discussione di esempi notevoli, realizzazione di progetti individuali o di gruppo con stesura di relazione finale. Le esercitazioni in laboratorio consistono nell'implementazione di algoritmi di ottimizzazione combinatoria sia esatti (con l'uso di librerie di programmazione lineare intera) sia euristici.

Contenuti:

1. Approfondimenti e applicazioni di Programmazione Lineare e dualità : metodo del semplice primale-duale, tecniche di generazione di colonne, applicazioni a problemi di ottimizzazione su grafo. 2. Metodi avanzati di Programmazione Lineare Intera (PLI): Branch & Bound e tecniche di rilassamento, formulazioni alternative di modelli PLI, metodo dei piani di taglio e tecniche di Branch & Cut, applicazioni ad esempi notevoli: commesso viaggiatore, problemi di localizzazione, problemi di network design etc. 3. Meta-euristiche di Ottimizzazione Combinatoria: ricerca di vicini e varianti, algoritmi evolutivi, metodi data-driven (integrazione di tecniche da Machine Learning e Data Science). 4. Applicazione di metodi di modellazione e ottimizzazione su

grafo. 5. Laboratori: utilizzo di software e librerie di ottimizzazione.

Modalità di esame:

Esame orale sui contenuti del corso e su esercizi di applicazione di metodi di ottimizzazione a problemi realistici. Realizzazione facoltativa di un progetto individuale su un caso di studio riguardante la soluzione di un problema, reale o realistico, di ottimizzazione combinatoria (definizione del problema, modellazione, applicazione di un metodo di soluzione esatto e/o euristico).

Criteri di valutazione:

L'esame verifica il livello di apprendimento degli argomenti svolti e la capacità dello studente di applicarli per la soluzione di problemi reali di ottimizzazione combinatoria.

Testi di riferimento:

CONTENUTO NON PRESENTE

Eventuali indicazioni sui materiali di studio:

Dispense fornite dal docente. Articoli scientifici.

MOBILE AND IOT SECURITY

Titolare: Prof.ssa ELEONORA LOSIOUK

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Qualsiasi linguaggio di programmazione orientato agli oggetti.

Conoscenze e abilità da acquisire:

Acquisizione dei concetti fondamentali di sicurezza del sistema operativo Android e dei protocolli Bluetooth/Bluetooth Low-Energy. Alla fine del corso, gli studenti avranno acquisito le conoscenze necessarie per analizzare un dispositivo mobile o un'applicazione mobile e identificarne le possibili vulnerabilità.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni; esercitazioni pratiche.

Contenuti:

Teoria: modello di sicurezza di Android, autorizzazioni, gestione dei pacchetti, gestione degli utenti, provider crittografici, sicurezza della rete, archiviazione delle credenziali, gestione degli account online, sicurezza dei dispositivi, SELinux, aggiornamenti del sistema e accesso root, protocolli di comunicazione Bluetooth/Bluetooth Low-Energy. Esercitazione: sicurezza delle applicazioni, superficie di attacco di Android, debugging e analisi delle vulnerabilità, sfruttamento del software dello spazio utente, attacchi a Bluetooth/Bluetooth Low-Energy.

Modalità di esame:

Gli studenti hanno due opzioni. (Opzione 1) Esame pratico, in cui gli studenti risolvono esercizi sulla sicurezza Android; (Opzione 2) Progetto, in cui gli studenti affrontano un tema di ricerca assegnato dal docente e illustrano i risultati ottenuti in una presentazione orale.

Criteri di valutazione:

Conoscenza dei concetti studiati durante il corso.

Testi di riferimento:

CONTENUTO NON PRESENTE

QUANTUM CRYPTOGRAPHY AND SECURITY

Titolare: Prof. NICOLA LAURENTI

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Il corso richiede conoscenze di base di fisica quantistica, informazione quantistica, teoria dell'informazione, crittografia e sicurezza. Un breve ripasso dei necessari concetti di informazione e tecnologie quantistiche, sicurezza e crittografia sarà svolto all'inizio del corso.

Conoscenze e abilità da acquisire:

La crittografia quantistica è a volte presentata come una scatola magica capace di fornire una soluzione definitiva ad ogni problema nel campo della sicurezza dell'informazione, altre volte come una visione astratta e idealizzata inadatta ad essere efficace in contesti realistici. Questo corso mira invece a permettere agli studenti di sviluppare la propria visione critica di questa area innovativa ed entusiasmante dell'information security, che rappresenta anche una delle più affascinanti e realistiche applicazioni della fisica quantistica, fornendo loro: - una formulazione solida e coerente dei modelli e delle architetture fondamentali dei meccanismi di crittografia quantistica, comprendendo minacce ed attacchi; - un'illustrazione dettagliata delle opportunità tecnologiche e delle loro limitazioni, la scelta degli osservabili, gli inconvenienti pratici, la chiusura dei loopholes; - una discussione rigorosa delle dimostrazioni di sicurezza e della derivazione di metriche di sicurezza dalla stima dei parametri osservati - esperienze pratiche di laboratorio sia hardware (con dispositivi ottici su banco) che software (per l'elaborazione delle informazioni) Si prevede che gli studenti acquisiscano le seguenti abilità: - saper valutare criticamente la necessità e la fattibilità di soluzioni basate su crittografia quantistica per specifiche esigenze di sicurezza; - saper identificare le soluzioni tecnologiche che meglio si adattano al meccanismo crittografico richiesto in un dato contesto; - valutare i parametri richiesti al sistema per le soluzioni opportune.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni frontali ed esperienze di laboratorio

Contenuti:

Introduzione: ripasso di informazione e tecnologie quantistiche, di servizi, meccanismi e misure di sicurezza. Generatori aleatori quantistici (QRNG): a variabili discrete, a variabili continue, aspetti tecnologici, QRNG certificati dalla disuguaglianza di Bell, semidevice independent QRNG, randomness extractor. Distribuzione di chiavi crittografiche per via quantistica (QKD): protocolli (prepare-and-measure, entanglement-based, continuous-variable), aspetti tecnologici e non ideali, modelli di attacco, algoritmi di post-elaborazione e dimostrazioni di sicurezza, uso di decoy states, QKD device independent, twin-field QKD, reti QKD, memorie e ripetitori quantistici. Altri meccanismi di sicurezza quantistici: comunicazione diretta segreta, information commitment quantistico, secret sharing quantistico, firme digitali quantistiche.

Modalità di esame:

Lo studente dovrà consegnare le proprie relazioni individuali delle esperienze di laboratorio, e successivamente sostenere un esame orale tradizionale con domande analitiche e discussione critica degli argomenti del corso.

Criteri di valutazione:

L'esame orale mira ad accertare il livello a cui lo studente ha acquisito: - una solida comprensione dei concetti fondamentali di crittografia quantistica; - la capacità di applicare modelli generali ad esempi particolari di dispositivi, algoritmi e protocolli; - una visione critica nel valutare problemi e soluzioni in protocolli specifici; - la capacità di identificare chiaramente le corrispondenze tra funzionalità astratte e elementi tecnologici, includendo la modellizzazione degli aspetti non ideali. Le relazioni di laboratorio, che verranno anche discusse all'esame orale, mirano ad accertare il lavoro dello studente e la sua comprensione delle singole esperienze, in collegamento con gli argomenti del corso.

Testi di riferimento:

CONTENUTO NON PRESENTE

Eventuali indicazioni sui materiali di studio:

A causa del carattere innovativo ed avanzato degli argomenti del corso non sono disponibili libri di testo con una trattazione sufficientemente completa e coerente. Lucidi e appunti per le lezioni saranno perciò forniti dai docenti. Tuttavia i seguenti articoli di revisione descrivono aspetti avanzati di QKD e QRNG in maniera ampia ed esauriente: - V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. 81, 1301 (2009). - F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. 92, 025002 (2020). - M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. 89, 015004 (2017). - X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," Npj Quantum Inf. 2, 16021 (2016). Ulteriori riferimenti saranno indicati durante il corso, ad articoli di approfondimento e di completamento sugli argomenti di alcune lezioni.

QUANTUM INFORMATION AND COMPUTING
--

Titolare: Prof. GIUSEPPE VALLONE

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Algebra lineare.

Conoscenze e abilità da acquisire:

Nozione di qubit e misure quantistiche Nozione di entanglement e utilizzo nelle disuguaglianze di Bell Confronto tra informazione classica e quantistica Conoscenze su applicazioni dell'informazione quantistica come il Dense coding, il Teletrasporto quantistico, la Quantum Key distribution, i Generatori di numeri casuali quantistici e la Metrologia Quantistica Confronto tra computazione classica e quantistica Nozione di QFT Conoscenza di algoritmi quantistici, come l'algoritmo di Shor, il Quantum Database Search, simulazioni Quantistiche Analisi dati di esperimenti di ottica quantistica

Attività di apprendimento previste e metodologie di insegnamento:

L'insegnamento avviene mediante lezioni frontali alla lavagna o con slides, in quanto si ritiene che questa modalità di erogazione consenta di mantenere il giusto ritmo e mantenga alta l'attenzione da parte degli studenti, con possibilità di interazione e coinvolgimento. Alcuni risultati vengono illustrati mediante l'ausilio del calcolatore con visualizzazione su grande schermo. Inoltre sono previste esercitazioni in classe, sia svolte dagli studenti in classe in gruppi di 2/3 persone, sia dal docente alla lavagna Sono previsti inoltre homework da svolgere a casa ed esperienze di laboratorio per approfondire e sperimentare alcuni concetti visti a lezione.

Contenuti:

PARTE I: concetti generali - Cos'è il qubit: introduzione alla meccanica quantistica - Spazi di Hilbert, operatori e proiettori - Misura quantistica - Evoluzione temporale, decoerenza - Entanglement: definizione, generazione e rivelazione - Tomografia quantistica - Disuguaglianze di Bell PARTE II: Informazione Quantistica - Confronto tra informazione classica e quantistica - Canali quantistici e teorema del no-cloning - Dense coding - Teletrasporto quantistico - Quantum Key distribution - Generatori di numeri casuali quantistici - Metrologia Quantistica PART III: Computazione quantistica - Confronto tra computazione classica e quantistica - dalla FFT alla QFT - algoritmo di Shor - Quantum Database Search - simulazioni Quantistiche - implementazioni

fisiche

Modalità di esame:

L'esame consiste di tre parti: - due homeworks (20%) - due relazioni sull'attività di laboratorio (20%) - prova orale (60%) Il voto finale sarà la media pesata con le percentuali riportate

Criteri di valutazione:

La valutazione dello studente sarà basata sugli homework, sulle relazioni di laboratorio e sulla prova orale. Gli homework e le relazioni di laboratorio pesano il 40% sul voto finale. Negli homework si valuterà la capacità di risolvere i problemi legati ai concetti studiati. Le relazioni di laboratorio verranno valutate sulla capacità di sintesi e di analisi delle esperienze di laboratorio. Durante l'orale la valutazione si basa sulla comprensione degli argomenti svolti a lezione e sulla capacità di esporli in maniera chiara e esauriente.

Testi di riferimento:

G. Benenti, G. Casati, and G. Strini, Principles of quantum computation and information.. : New Jersey: World Scientific, 2004 Nielsen, Michael A., Chuang, Isaac L., Quantum computation and quantum information.. : Cambridge: Cambridge university press,

Eventuali indicazioni sui materiali di studio:

Tutti gli argomenti del corso vengono illustrati in aula. Gli appunti delle lezioni possono essere integrati dai libri di testo. Sulla piattaforma moodle sarà reso disponibile un elenco degli argomenti trattati lezione per lezione.

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Titolare: Dott. SIMONE SODERI

Periodo: Il anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Nessun prerequisito.

Conoscenze e abilità da acquisire:

Gli studenti svilupperanno le competenze necessarie per valutare le diverse alternative che si pongono durante il processo di identificazione dei rischi per la sicurezza di un Sistema Informativo. Si farà particolare riferimento alla valutazione delle scelte architettoniche e dei rischi che possono comportare tali valutazioni in relazione agli obiettivi di sicurezza imposti al sistema in relazione livello di sensibilità delle informazioni che gestisce.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni frontali; dimostrazione e discussione di casi pratici.

Contenuti:

Il corso affronta la valutazione dei rischi informatici che possono danneggiare un sistema informatico aziendale, le metodologie per mitigare tali rischi e le contromisure necessarie da applicare, con l'obiettivo di rendere sicura l'azienda o ente pubblico dal punto di vista informatico. Gli studenti verranno introdotti a principi, concetti e pratiche per governare, gestire e controllare la sicurezza informatica in conformità con gli standard internazionali (ad esempio, International Organization for Standardization - ISO) e le migliori pratiche professionali generalmente accettate. Materiali di riferimento: ISO / IEC 27000, Sistemi di gestione della sicurezza delle informazioni - Panoramica e vocabolario ISO / IEC 27001, Sistemi di gestione della sicurezza delle informazioni - Requisiti ISO / IEC 27002, Codice di condotta per i controlli di sicurezza delle informazioni ISO / IEC 27005: 2011 Tecnologia dell'informazione - Tecniche di sicurezza - Gestione dei rischi per la sicurezza delle informazioni Valutazione del rischio per la sicurezza delle informazioni "OCTAVE Allegro" - Carnegie Mellon University / Istituto di ingegneria del software Standard e migliori pratiche ISACA Altro riferimento rilevante (ad esempio, pubblicazioni NIST)

Modalità di esame:

Gli studenti dovranno sostenere un esame finale sul materiale fornito a lezione.

Criteri di valutazione:

Conoscenza dei concetti studiati durante il corso.

Testi di riferimento:

CONTENUTO NON PRESENTE

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Titolare: Dott. SIMONE SODERI

Mutuato da: Laurea magistrale in Cybersecurity (Ord. 2020)

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Nessun prerequisito.

Conoscenze e abilità da acquisire:

Gli studenti svilupperanno le competenze necessarie per valutare le diverse alternative che si pongono durante il processo di identificazione dei rischi per la sicurezza di un Sistema Informativo. Si farà particolare riferimento alla valutazione delle scelte architettoniche e dei rischi che possono comportare tali valutazioni in relazione agli obiettivi di sicurezza imposti al sistema in relazione livello di sensibilità delle informazioni che gestisce.

Attività di apprendimento previste e metodologie di insegnamento:

Lezioni frontali; dimostrazione e discussione di casi pratici.

Contenuti:

Il corso affronta la valutazione dei rischi informatici che possono danneggiare un sistema informatico aziendale, le metodologie per mitigare tali rischi e le contromisure necessarie da applicare, con l'obiettivo di rendere sicura l'azienda o ente pubblico dal punto di vista informatico. Gli studenti verranno introdotti a principi, concetti e pratiche per governare, gestire e controllare la sicurezza informatica in conformità con gli standard internazionali (ad esempio, International Organization for Standardization - ISO) e le migliori pratiche professionali generalmente accettate. Materiali di riferimento: ISO / IEC 27000, Sistemi di gestione della sicurezza delle informazioni - Panoramica e vocabolario ISO / IEC 27001, Sistemi di gestione della sicurezza delle informazioni - Requisiti ISO / IEC 27002, Codice di condotta per i controlli di sicurezza delle informazioni ISO / IEC 27005: 2011 Tecnologia dell'informazione - Tecniche di sicurezza - Gestione dei rischi per la sicurezza delle informazioni Valutazione del rischio per la sicurezza delle informazioni "OCTAVE Allegro" - Carnegie Mellon University / Istituto di ingegneria del software Standard e migliori pratiche ISACA Altro riferimento rilevante (ad esempio, pubblicazioni NIST)

Modalità di esame:

Gli studenti dovranno sostenere un esame finale sul materiale fornito a lezione.

Criteri di valutazione:

Conoscenza dei concetti studiati durante il corso.

Testi di riferimento:

CONTENUTO NON PRESENTE

SEMINARS AND OTHER ACTIVITIES

Titolare: da definire

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: ; 3,00

SERVICE MANAGEMENT

Titolare: Prof. MARCO UGO PAIOLA

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: I anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 42A; 6,00

Prerequisiti:

I contenuti del corso richiedono che gli studenti abbiano una conoscenza di base di management, della strategia aziendale e dei fondamenti di marketing, nonché delle strategie innovative per la creazione di valore.

Conoscenze e abilità da acquisire:

ABILITÀ COGNITIVE Al termine del corso gli studenti saranno in grado di: C1. Delineare le ragioni fondamentali per cui le aziende ricercano la crescita nei servizi; C2. Mostrare l'allineamento e le connessioni tra la strategia di business relativa ai servizi e gli obiettivi aziendali; C3. Dimostrare come è possibile realizzare l'integrazione tra servizi e struttura organizzativa; C4. Identificare e descrivere come le tecnologie digitali possono favorire modelli di business innovativi orientati ai servizi. ABILITÀ PRATICHE Gli studenti saranno in grado di: P1. Applicare i concetti appresi durante il corso ad un caso di studio reale e illustrare gli effetti pratici delle soluzioni proposte; P2. Descrivere analiticamente e proporre in modo proattivo modelli di business nuovi (o rivisti) orientati ai servizi. COMPETENZE TRASVERSALI Gli studenti svilupperanno: T1. Abilità comunicative e di public-speaking, T2. Pensiero creativo e innovativo, T3. Capacità di problem-solving.

Attività di apprendimento previste e metodologie di insegnamento:

Il corso offrirà: • Lezioni tradizionali, • Discussione di casi studio, • Seminari, • Presentazioni di relatori esterni (manager ed esperti). Gli studenti frequentanti saranno coinvolti in lavori di gruppo e nelle discussioni sui casi. Gli studenti apprenderanno attraverso lo studio individuale, la partecipazione alle discussioni in aula e il lavoro di gruppo.

Contenuti:

Questo corso si propone di fornire agli studenti le competenze teoriche e tecniche di base utili a comprendere la crescita del moderno business dei servizi nelle aziende B2B, con particolare attenzione ai processi di trasformazione digitale. Il corso tratterà i seguenti argomenti: • Perché i servizi? L'imperativo del servizio: i driver di servitizzazione, sfide e categorie dei servizi B2B. • Le aziende manifatturiere sono adatte ai servizi? Risorse, capacità e organizzazione; sfide di prezzo; gestione dei canali di vendita e di distribuzione. • Innovazione e tecnologia nei servizi: utilizzo dei dati e delle tecnologie 4.0 per migliorare la presenza dell'azienda nei servizi e rinnovare i modelli di business. • Allineamento della strategia del servizio: costruzione di una cultura orientata al servizio All'inizio del corso, verrà fornito un programma con una rappresentazione più dettagliata dei contenuti delle lezioni.

Modalità di esame:

Per gli studenti frequentanti, le conoscenze e le abilità saranno valutate attraverso: • Un esame scritto - agli studenti verrà chiesto di rispondere a 2 domande aperte (una relativa a un argomento ampio del corso, una relativa a un argomento specifico trattato nel corso). Verranno valutate le abilità C1, C2, C3, C4. • Lavori di gruppo: ciascun gruppo lavorerà su temi concordati direttamente con aziende locali selezionate e applicherà i concetti trattati durante il corso a un caso reale. Ciascun gruppo dovrà preparare una presentazione e una relazione finale. Verranno valutate le abilità P1, P2, T1, T2, T3. Per gli studenti non-frequentanti, le conoscenze e le abilità saranno valutate attraverso: • Un esame scritto - agli studenti verrà chiesto di rispondere a 3 domande aperte (due relative ad argomenti ampi del corso, una relativa a un argomento specifico trattato nel corso). Verranno valutate le abilità C1, C2, C3, C4.

Criteri di valutazione:

Gli studenti frequentanti saranno valutati come segue: 50% esame scritto - Gli studenti saranno valutati sulla completezza delle conoscenze acquisite e sulle competenze sviluppate nell'applicazione autonoma degli argomenti del corso. 50% lavori di gruppo - Gli studenti saranno valutati sulla loro capacità di

lavorare in gruppo, di immaginare soluzioni innovative e di svolgere analisi relative a casi di studio reali. Gli studenti non frequentanti saranno valutati come segue: 100% esame scritto - Gli studenti saranno valutati sulla completezza delle conoscenze acquisite e sulle competenze sviluppate nell'applicazione autonoma degli argomenti del corso.

Testi di riferimento:

Kowalkowsky C. and Ulaga W., Service strategy in action. : Service Strategy Press, 2017

Eventuali indicazioni sui materiali di studio:

Gli studenti frequentanti sono tenuti a studiare i capitoli 1, 2, 3, 4, 5, 7, 10, 11, 12 del libro di testo " Kowalkowsky and Ulaga, Service strategy in action, 2017" e le letture obbligatorie. Gli studenti non frequentanti sono tenuti a studiare l'intero libro di testo "Kowalkowsky and Ulaga, Service strategy in action, 2017" e le letture obbligatorie. LETTURE OBBLIGATORIE: Capitolo 5: • Oliva, R., & Kallenberg, R. (2003), Managing the transition from products to services, International Journal of Service Industry Management, 14(2), 160-172. Capitoli 8-9: • Allmendinger, G., & Lombreglia, R., 2005, 'Four strategies for the age of smart services', Harvard Business Review, 83(10), 131-145. • Porter, M. E., & Heppelmann, J. E., 2014, 'How Smart, Connected Products Are Transforming Companies', Harvard Business Review, October, pp.96–112. Capitolo 12: • R. Wise and P. Baumgartner, "Go Downstream: The New Profit Imperative in Manufacturing," Harvard Business Review, Vol. 77, No. 5, 1999, pp. 133-141.

SOFTWARE VERIFICATION

Titolare: Prof. FRANCESCO RANZATO

Mutuato da: Laurea magistrale in Computer Science (Ord. 2021)

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Conoscenze di base dei linguaggi di programmazione. L'insegnamento non prevede propedeuticità.

Conoscenze e abilità da acquisire:

Il corso mira ad introdurre metodi e strumenti per la specifica del comportamento run-time dei programmi, l'analisi statica e la verifica automatica dei programmi e, più in generale, dei sistemi software. In particolare, il corso fornisce una introduzione alla semantica formale dei linguaggi di programmazione ed ai metodi formali per la loro analisi statica e verifica.

Attività di apprendimento previste e metodologie di insegnamento:

L'insegnamento prevede lezioni frontali (o in modalità telematica) e la risoluzione in modo indipendente a casa di vari esercizi e/o lo sviluppo di un progetto di verifica del software. Sono previste lezioni invitate di ospiti ricercatori su tematiche avanzate di verifica del software.

Contenuti:

- Semantica dei programmi: Modellazione del comportamento (in particolare il comportamento input/output) dei programmi mediante la teoria dell'ordinamento e dei punti fissi. (cf. [https://en.wikipedia.org/wiki/Semantics_\(computer_science\)](https://en.wikipedia.org/wiki/Semantics_(computer_science))) - Analisi statica e verifica di programmi mediante interpretazione astratta: L'interpretazione astratta è una notoria tecnica basata su una approssimazione della semantica dei programmi che permette di specificare le proprietà dei programmi deducibili mediante analisi statica e di provarne la correttezza. (cf. https://en.wikipedia.org/wiki/Abstract_interpretation) - Analisi statica dataflow di programmi: tecnica per dedurre staticamente informazioni sull'insieme dei possibili valori delle variabili nei vari punti del programma. Un grafo di flusso del controllo è utilizzato per determinare le parti di un programma a cui un particolare valore assegnato ad una variabile potrebbe propagarsi. Le informazioni raccolte sono spesso utilizzate dai compilatori (come gcc e javac) per ottimizzare un programma. (cf. https://en.wikipedia.org/wiki/Data-flow_analysis) - Strumenti di verifica del software: ad esempio, Clousot (Microsoft, USA), Interproc (INRIA, Francia), Jandom (Università di Pescara) (cf. https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis)

Modalità di esame:

Esame orale e/o progetto software, possibilmente suddivisi in parti distinte.

Criteri di valutazione:

L'esame orale verte su vari esercizi che lo studente deve svolgere in modo indipendente a casa. Il progetto di laboratorio verte su qualche tool di verifica del software.

Testi di riferimento:

H. Riis Nielson, F. Nielson, Semantics with Applications: A Formal Introduction. : Wiley, 1992 Antoine Minè, Tutorial on static inference of numeric invariants by abstract interpretation. : Now, The Essence of Knowledge, 2017

Eventuali indicazioni sui materiali di studio:

Le slide utilizzate a lezione verranno distribuite.

STOCHASTIC PROCESSES

Titolare: Prof. MICHELE ZORZI

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Il corso prevede conoscenze preliminari di: Analisi Matematica, Algebra Lineare, Probabilità, variabili aleatorie e processi aleatori. Per gli esempi trattati, e' utile (anche se non necessario) aver seguito un corso di base di reti e protocolli.

Conoscenze e abilità da acquisire:

L'obiettivo formativo del corso prevede l'acquisizione delle seguenti conoscenze e abilità: 1. Comprendere a fondo e saper usare la teoria della probabilità e dei processi casuali per modellare sistemi reali e poterne valutare le prestazioni. 2. Acquisire strumenti analitici avanzati per la valutazione delle prestazioni di sistemi e reti 3. Saper tradurre la descrizione di un problema in un modello matematico che lo rappresenti 4. Sapere quali metriche di prestazioni si possono calcolare (e come) a partire da una rappresentazione matematica/probabilistica 5. Essere in grado di enunciare in maniera precisa e di dimostrare in maniera rigorosa i risultati teorici più importanti relativi agli argomenti principali del corso (catene di Markov, processi di Poisson, processi di rinnovamento)

Attività di apprendimento previste e metodologie di insegnamento:

L'insegnamento avviene mediante lezioni frontali alla lavagna, in quanto si ritiene che questa modalità di erogazione consenta di mantenere il giusto ritmo di presentazione degli argomenti e mantenga alta l'attenzione da parte degli studenti, con possibilità di interazione e coinvolgimento. Per verificare il livello di apprendimento durante il corso, vengono proposti allo studente esercizi o sviluppi da fare a casa, che verranno poi spesso svolti in aula durante una lezione successiva.

Contenuti:

1. richiami di probabilità e processi casuali 2. catene di Markov: definizioni e risultati principali 3. catene di Markov: comportamento asintotico 4. processi di Poisson: definizioni e risultati principali 5. processi di rinnovamento: definizioni e risultati principali, comportamento asintotico 6. processi renewal reward, rigenerativi, e semi-Markov 7. esercizi e esempi di applicazioni Una lista dettagliata degli argomenti trattati durante il corso, con riferimenti specifici a capitoli e pagine dei testi, è disponibile sul sito del corso sulla piattaforma elearning.

Modalità di esame:

La valutazione delle conoscenze e delle abilità acquisite viene effettuata mediante una prova scritta articolata in due parti. La parte A, della durata di 90 minuti e a libro aperto, consiste in undici domande numeriche raggruppate in quattro esercizi. Ogni domanda ha un valore di tre punti. La parte B, della durata di 60 minuti e a libro chiuso, consiste in tre domande teoriche (tipicamente dimostrazioni viste a lezione). Ogni domanda ha un valore di undici punti. Se lo studente totalizza almeno 15 punti nella parte A e la media dei punti fra parte A e parte B è almeno pari a 18, quest'ultima può essere accettata come voto finale. Se il punteggio nella parte A è inferiore a 15 o la media delle due prove è insufficiente, l'esame non è superato. Anche se la prova finale può essere superata sostenendo con successo il solo esame scritto (in due parti), lo studente può sempre richiedere di sostenere in aggiunta una prova orale se vuole migliorare il voto. La prova orale non sostituisce in nessun caso la prova scritta. Esempi di compiti sono disponibili sul sito del corso sulla piattaforma elearning, e vengono ampiamente trattati a lezione.

Criteri di valutazione:

La valutazione con cui verrà effettuata la verifica delle conoscenze e delle abilità acquisite considera: 1. La completezza e il grado di approfondimento delle conoscenze degli argomenti trattati durante il corso. 2. La capacità di modellare un problema usando uno degli strumenti analitici visti a lezione 3. La capacità di ottenere risultati numerici corretti negli esercizi proposti 4. La capacità di sviluppare un ragionamento analitico in maniera rigorosa e completa.

Testi di riferimento:

S. Ross, Stochastic processes. : Wiley (2nd ed.), 1996 H. Taylor, S. Karlin, An introduction to stochastic modeling. : Academic Press (3rd or 4th edition), 1998 D. Bertsekas, R. Gallager, Data Networks. : Prentice-Hall (2nd ed.), 1992 S. Ross, Applied probability models with optimization applications. : Dover (2nd ed.), 1996 S. Karlin, H. Taylor, A first course in stochastic processes. : Academic Press (2nd ed.), 1975

Eventuali indicazioni sui materiali di studio:

Il corso segue un libro di testo principale, con integrazioni da altri testi, appunti e articoli scientifici. Ad eccezione del libro di testo principale, tutto il resto del materiale didattico è reso disponibile agli studenti sul sito del corso sulla piattaforma elearning, compresi esempi di compiti e esercizi proposti dal testo (con soluzioni).

WEB APPLICATIONS

Titolare: Prof. NICOLA FERRO

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: Il anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Requested competencies: - good and proactive programming skills and, in particular, the object-oriented paradigm and its design principles; - good knowledge of the Java programming language; - foundations of database management systems and, in particular, entity-relationship model, relational model, SQL, JDBC; - computer networks and, in particular, the HTTP protocol

Conoscenze e abilità da acquisire:

The objective of the course is to learn the methodologies for the design and development of Web applications, practicing them through the design and implementation of an actual full-stack Web application. This objective calls for: + a strong computer science competence on Web engineering, design methodologies and architectural alternatives + knowledge of the characteristics of Web 1.0 applications and Web 2.0 application (rich internet application) + capability of developing a full-stack Web application using Java servlets, Javascript, CSS3 and HTML5

Attività di apprendimento previste e metodologie di insegnamento:

+ Lectures + Labs --- use of git and maven --- use of Apache Tomcat and Java servlets --- use of JSP pages --- use of REST Web services --- use of HTML and CSS --- use of Javascript and AJAX --- use of Javascript libraries, e.g. jQuery + Seminars of visiting colleagues on research topics and/or seminar by companies on the use and perspectives for innovative products based on Web applications, role of the engineer in a company, stage opportunities, simulation of job interviews. + Homeworks: there are 2 homeworks (server-side design and development; client-side design and development), to be carried out in group, in order to design, develop, implement, code, and document a "real" full-stack Web application. Homework deadlines are aligned with the schedule and contents of the lectures so that students can immediately apply, during the course, the learned concepts to a case study of their own interests. + Oral presentation with slides and demo of the homework project

Contenuti:

+ Design methodologies for Web applications --- Introduction to Web engineering --- Requirement analysis --- Modelling Web applications (contents, hypertext, presentation) --- Architectures for Web applications + Development of Web 1.0 Applications --- Model-View-Controller (MVC) paradigm --- Web programming (HTML5, CSS3, Javascript) --- Web server and Web browser architecture --- Java servlet and Java Server Pages, Apache Tomcat --- Development tools: git for code management and maven for the build process + Web Services --- REST Web services --- SOAP Web services + Development of Web 2.0 Applications --- Introduction to Rich Internet Applications (RIA) and mash-ups --- Introduction to JSON and XML --- AJAX and

revised MVC paradigm + Notions on Web 3.0 applications: --- semantic representation of the data and RDF --- open linked data

Modalità di esame:

Written Exam at computer: + questions on the topics covered during the lectures (Moodle quiz) Project to design, develop, implement, code and document an actual full-stack Web application, carried out in student groups via homeworks + git repository containing the project source code and all the related material + report documenting the developed full-stack Web application application + oral presentation of the project outcomes + demo of the developed full-stack Web application application

Criteri di valutazione:

The evaluation will be based on the comprehension and knowledge of the notions and methodologies about Web application, on the capability of facing the different phases of the design, development and implementation of a Web application, on the comprehension and knowledge of the models and languages for developing a Web application, on the implementation of a project for the development of a Web application.

Testi di riferimento:

Kappel, G., Pröll, B., Reich, S., and Retschitzegger, W., Web Engineering. The Discipline of Systematic Development of Web Applications. New York, USA: John Wiley & Sons, 2006 Shklar, L. and Rosen, R., Web Application Architecture: Principles, Protocols and Practices. New York, USA: John Wiley & Sons, 2009

Eventuali indicazioni sui materiali di studio:

The teaching material consists of: - reference book - instructor's slides - suggested readings - examples of homeworks Suggested readings: + Casteleyn, S., Daniel, F., Dolog, P., and Matera, M. (2009). Engineering Web Applications. Springer-Verlag Berlin Heidelberg + Johnson, D.C., White, A., and Charland, A. (2007). Enterprise AJAX: Strategies for Building High Performance Web Applications. Prentice Hall. + Møller, A. and Schwartzbach, M. I. (2006). An Introduction to XML and Web Technologies. Addison-Wesley. + Rossi, G., Pastor, O., Schwabe, D., and Olsina, D., editors (2008). Web Engineering: Modelling and Implementing Web Applications. Springer-Verlag, London, UK. + Tanenbaum, A. S., and M. Van Steen (2006). Distributed Systems: Principles and Paradigms (2nd Edition). Prentice Hall.

WEB APPLICATIONS

Titolare: Prof. NICOLA FERRO

Mutuato da: Scuola Galileiana di Studi Superiori - Classe di Scienze Naturali

Periodo: I anno, 2 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 48A; 6,00

Prerequisiti:

Requested competencies: - good and proactive programming skills and, in particular, the object-oriented paradigm and its design principles; - good knowledge of the Java programming language; - foundations of database management systems and, in particular, entity-relationship model, relational model, SQL, JDBC; - computer networks and, in particular, the HTTP protocol

Conoscenze e abilità da acquisire:

The objective of the course is to learn the methodologies for the design and development of Web applications, practicing them through the design and implementation of an actual full-stack Web application. This objective calls for: + a strong computer science competence on Web engineering, design methodologies and architectural alternatives + knowledge of the characteristics of Web 1.0 applications and Web 2.0 application (rich internet application) + capability of developing a full-stack Web application using Java servlets, Javascript, CSS3 and HTML5

Attività di apprendimento previste e metodologie di insegnamento:

+ Lectures + Labs --- use of git and maven --- use of Apache Tomcat and Java servlets --- use of JSP pages --- use of REST Web services --- use of HTML and CSS --- use of Javascript and AJAX --- use of Javascript libraries, e.g. jQuery + Seminars of visiting colleagues on research topics and/or seminar by companies on the use and perspectives for innovative products based on Web applications, role of the engineer in a company, stage opportunities, simulation of job interviews. + Homeworks: there are 2 homeworks (server-side design and development; client-side design and development), to be carried out in group, in order to design, develop, implement, code, and document a "real" full-stack Web application. Homework deadlines are aligned with the schedule and contents of the lectures so that students can immediately apply, during the course, the learned concepts to a case study of their own interests. + Oral presentation with slides and demo of the homework project

Contenuti:

+ Design methodologies for Web applications --- Introduction to Web engineering --- Requirement analysis --- Modelling Web applications (contents, hypertext, presentation) --- Architectures for Web applications + Development of Web 1.0 Applications --- Model-View-Controller (MVC) paradigm --- Web programming (HTML5, CSS3, Javascript) --- Web server and Web browser architecture --- Java servlet and Java Server Pages, Apache Tomcat --- Development tools: git for code management and maven for the build process + Web Services --- REST Web services --- SOAP Web services + Development of Web 2.0 Applications --- Introduction to Rich Internet Applications (RIA) and mash-ups --- Introduction to JSON and XML --- AJAX and revised MVC paradigm + Notions on Web 3.0 applications: --- semantic representation of the data and RDF --- open linked data

Modalità di esame:

Written Exam at computer: + questions on the topics covered during the lectures (Moodle quiz) Project to design, develop, implement, code and document an actual full-stack Web application, carried out in student groups via homeworks + git repository containing the project source code and all the related material + report documenting the developed full-stack Web application application + oral presentation of the project outcomes + demo of the developed full-stack Web application application

Criteri di valutazione:

The evaluation will be based on the comprehension and knowledge of the notions and methodologies about Web application, on the capability of facing the different phases of the design, development and implementation of a Web application, on the comprehension and knowledge of the models and languages for developing a Web application, on the implementation of a project for the development of a Web application.

Testi di riferimento:

Kappel, G., Pröll, B., Reich, S., and Retschitzegger, W., Web Engineering. The Discipline of Systematic Development of Web Applications. New York, USA: John Wiley & Sons, 2006 Shklar, L. and Rosen, R., Web Application Architecture: Principles, Protocols and Practices. New York, USA: John Wiley & Sons, 2009

Eventuali indicazioni sui materiali di studio:

The teaching material consists of: - reference book - instructor's slides - suggested readings - examples of homeworks Suggested readings: + Casteleyn, S., Daniel, F., Dolog, P., and Matera, M. (2009). Engineering Web Applications. Springer-Verlag Berlin Heidelberg + Johnson, D.C., White, A., and Charland, A. (2007). Enterprise AJAX: Strategies for Building High Performance Web Applications. Prentice Hall. + Møller, A. and Schwartzbach, M. I. (2006). An Introduction to XML and Web Technologies. Addison-Wesley. + Rossi, G., Pastor, O., Schwabe, D., and Olsina, D., editors (2008). Web Engineering: Modelling and Implementing Web Applications. Springer-Verlag, London, UK. + Tanenbaum, A. S., and M. Van Steen (2006). Distributed Systems: Principles and Paradigms (2nd Edition). Prentice Hall.

WIRELESS NETWORKS

Titolare: Prof. CLAUDIO ENRICO PALAZZI

Mutuato da: Laurea magistrale in Computer Science (Ord. 2021)

Periodo: Il anno, 1 semestre

Indirizzo formativo: Corsi comuni

Tipologie didattiche: 40A+8L; 6,00

Prerequisiti:

Reti di Calcolatori

Conoscenze e abilità da acquisire:

Questo corso offre una panoramica delle problematiche inerenti sistemi e servizi basati su reti wireless. A questo scopo, sono analizzati i principali problemi e soluzioni protocollari disponibili per ambienti wireless. Inoltre, sono discussi la terminologia, il funzionamento e le possibili alternative allo stato dell'arte nelle comunicazioni wireless. Attraverso l'analisi dei servizi che possono essere offerti su tecnologia wireless, lo studente diventerà consapevole delle possibili evoluzioni ed utilizzi futuri dei sistemi wireless. Infine, il corso si conclude con alcune nozioni utili all'implementazione di un elaborato volto all'analisi e alla progettazione di protocolli/applicazioni wireless.

Attività di apprendimento previste e metodologie di insegnamento:

L'insegnamento prevede lezioni frontali e la realizzazione di un progetto.

Contenuti:

Introduzione alle reti wireless. Problematiche relative alle reti wireless: perdite per errore e collisione, equità e ritardi di trasmissione, handoff Standard MAC: 802.11 a/b/g/n/p/s Protocolli di trasporto in ambiente wireless: TCP Vegas, TCP Westwood, TCP Hybla, CUBIC. Reti ad hoc e protocolli di routing: MANET, VANET, DSDV, AODV, DSR. Applicazioni e servizi su reti mobili.

Modalità di esame:

Gli studenti sono valutati attraverso progetti individuali o di squadra ed attraverso un esame orale sulle tematiche discusse in aula.

Criteri di valutazione:

L'esame orale finale e il progetto realizzato consentono di valutare il livello di apprendimento delle nozioni discusse in classe e l'abilità dello studente nel maneggiare concetti in modo pratico.

Testi di riferimento:

William Stallings, Wireless Communications & Networks (2nd Edition). : Prentice Hall, 2005

Eventuali indicazioni sui materiali di studio:

Vengono rese disponibili le trasparenze utilizzate in aula.