



**Bollettino Notiziario - A.A. 2024/2025**

**LAUREA MAGISTRALE IN CYBERSECURITY (ORD. 2020)**

**Curriculum: Corsi comuni**

**ADVANCED TOPICS IN COMPUTER AND NETWORK SECURITY**

**Titolare:** Prof. MAURO CONTI

**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 non prevede propedeuticità. Tuttavia, sono consigliate conoscenze di base di reti, crittografia, e sistemi distribuiti (tipicamente acquisite nei corsi di Laurea in Informatica).

**Conoscenze e abilità da acquisire:**

Approfondire i concetti di sicurezza di base, analizzando le più recenti proposte di ricerca nell'ambito. Al termine del corso gli studenti saranno in grado non solo di analizzare con spirito critico un sistema software nel suo complesso, ma anche di aggiornare autonomamente le proprie competenze nel settore, anche tramite risultati recenti della ricerca nell'area.

**Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni frontali; discussione di articoli scientifici.

**Contenuti:**

Teoria: sicurezza RFID, captcha, sistemi di archiviazione non sicuri, sicurezza sugli smartphone, attacchi su smartPhone, protezione di password, attacchi Denial-of-Service distribuiti, deep learning, biometria, sicurezza VoIP, secure content delivery, comunicazioni anonime, rilevamento keylogger, anonimato in WSN, rilevamento di botnet, HW affidabile, sicurezza dei passaporti RFID, attacco di tipo node replication in WSN, aggregazione sicura dei dati in WSN, problemi di privacy nei social media, sicurezza smartphone Android Google, sistemi di votazione elettronica, rilevazione botnet P2P, meccanismi di taint analysis, sicurezza dei browser, privacy di servizi di localizzazione, Named Data Networking security, Named Data Networking privacy, sicurezza dei sistemi cloud, anonimato nella rete wireless, profilazione di utenti su smartphone, problemi di sicurezza SSL in Android, circumvent censorship, secure messaging, sicurezza tecnologica operativa, sicurezza dei sistemi cyber-fisici. Laboratorio: strumenti di sicurezza avanzati, inclusi: analisi del traffico con strumenti di apprendimento automatico, inferenza di dati, strumenti di sicurezza in Android, meccanismi di attacco e difesa per buffer overflow; analisi avanzata di sistema Malware e Advanced Persistent Threat; sicurezza web; strumenti di analisi di reti sociali, trusted platform modules.

**Modalità di esame:**

Progetto con relazione + esame orale.

**Criteri di valutazione:**

Conoscenza dei concetti studiati nel corso.

**Testi di riferimento:**

W. Stallings, L. Brown, Computer Security: Principles and Practice 2/E. : Prentice Hall, M. Bishop, Introduction to Computer Security. : Addison-Wesley Professional,

**Eventuali indicazioni sui materiali di studio:**

Libro (testo principale Computer Security: Principles and Practice 2/E) e articoli scientifici. Il corso sarà tenuto in Inglese. Il sito web del corso offrirà tutte le informazioni e materiale ulteriore: <http://www.math.unipd.it/~conti/teaching.html>

## ADVERSARIAL MACHINE LEARNING

**Titolare:** Prof. STEFANO TOMASIN

**Periodo:** Il anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Il corso richiede una conoscenza di base dell'apprendimento automatico, della statistica, dell'algebra lineare e una certa conoscenza preliminare dell'ottimizzazione (in particolare dell'ottimizzazione convessa).

**Conoscenze e abilità da acquisire:**

Conoscenze da acquisire: 1. conoscenza delle principali minacce alla sicurezza dei sistemi di apprendimento automatico; 2. la tassonomia degli attacchi contro gli apprendenti, in un quadro teorico di gioco 3. attacchi casuali, esplorativi e di evasione 4. attacchi e difese contro i filtri di rilevamento dello spam, 5. Rilevatore PCA di anomalie del traffico Capacità da acquisire: 1. Progettare e comprendere gli attacchi avversari di base alla privacy e i metodi di difesa che preservano la privacy. 4. Distinguere gli attacchi avversari di machine learning tra i diversi attacchi alla sicurezza. 5. Implementare attacchi e difese avversarie contro modelli convenzionali di apprendimento automatico e modelli di apprendimento profondo. 6. Implementare attacchi avversari contro i sistemi di rilevamento delle anomalie per il rilevamento delle intrusioni di rete, i classificatori di malware e i metodi di filtraggio anti-spam.

**Attività di apprendimento previste e metodologie di insegnamento:**

Il corso prevede lezioni e laboratori con l'utilizzo del linguaggio python.

**Contenuti:**

Il corso fornisce una panoramica delle principali minacce alla sicurezza dei sistemi di apprendimento automatico; verranno esaminati i sistemi di apprendimento del mondo reale, verranno valutate le loro vulnerabilità e verranno proposte delle difese per mitigare l'efficacia degli attacchi. Il corso prevede innanzitutto la revisione di alcuni concetti di base dell'apprendimento automatico. In seguito, si introdurrà un quadro di riferimento per valutare le proprietà di sicurezza degli agenti di apprendimento e si presenterà la tassonomia degli attacchi contro gli apprendenti, in un quadro teorico di gioco con due giocatori, l'attaccante e il difensore. Verranno poi analizzati tre tipi di attacchi: causativi, esplorativi e di evasione. Gli attacchi causativi tentano di fornire all'algoritmo dati di addestramento errati e non rappresentativi, in modo che non apprenda la funzione prevista. Gli attacchi esplorativi si verificano dopo che l'algoritmo è stato addestrato e cercano di scoprire informazioni sul suo funzionamento interno, al fine di identificare i punti deboli dell'algoritmo. Anche gli attacchi di evasione vengono sferrati ad algoritmi addestrati e consistono nel fornire all'algoritmo dati di ingresso (di prova) che daranno luogo a un risultato errato. Durante il corso verranno presentati diversi casi di studio di attacchi e strategie di difesa, tra cui gli attacchi contro i filtri di rilevamento dello spam, il rilevatore PCA di anomalie del traffico, la fuga di dati di AOL e l'attacco al premio Netflix. Schema - Concetti di base dell'apprendimento automatico - Struttura dell'apprendimento sicuro \* Attacchi esplorativi \* Attacchi casuali \* attacchi di evasione - Attacco a un discente ipersferico \* Attacchi casuali ai rilevatori di ipersfere \* attacchi ottimali non vincolati \* attacchi vincolati - Caso di studio dell'attacco alla disponibilità: SpamBayes \* Attacchi casuali \* Difesa RONI (Reject on Negative Impact) - Attacco all'integrità Caso di studio: Rilevatore PCA \* Rivelatori resilienti alla corruzione - Meccanismi di conservazione della privacy per l'apprendimento di SVM \* Strategie di difesa basate sulla privacy differenziale \* Limiti sulla privacy differenziale ottimale - Evasione quasi ottimale dei classificatori \* Costo avversario \* Tecniche di evasione

**Modalità di esame:**

Un esame orale che comprenderà l'esposizione degli argomenti presentati nelle lezioni e semplici esercizi sulle tecniche di apprendimento automatico avversariale.

**Criteri di valutazione:**

I criteri di valutazione delle conoscenze e delle abilità acquisite saranno: 1. Completezza delle conoscenze acquisite 2. Capacità di descrivere accuratamente gli attacchi e le difese avversarie di base dell'apprendimento automatico. 3. Capacità di progettare attacchi e difese di base per l'apprendimento automatico avversario. 4. Appropriattezza nell'uso del linguaggio tecnico.

**Testi di riferimento:**

Vorobeychik, Yevgeniy; Kantarcioglu, Murat; Vorobeychik, Yevgeniy, Adversarial machine learning. S.I: Springer, 2022 Joseph, Anthony D.; Nelson, Blaine; Rubinstein, Benjamin I. P.; Tygar, J. D., Adversarial Machine Learning. Cambridge: Cambridge University Press, 2019

**Eventuali indicazioni sui materiali di studio:**

Le slide delle lezioni saranno rese disponibili attraverso la piattaforma <https://stem.elearning.unipd.it/> e sarà fornito anche un riferimento al libro di testo del materiale presentato.

## 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: buone competenze relative al progetto e all'analisi di algoritmi e strutture dati, conoscenza delle nozioni fondamentali di calcolo delle probabilità e statistica, buone capacità di programmazione in Java o Python, e la capacità di usare Linux via command line.

**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. Distributed frameworks: MapReduce, Apache Spark. Clustering for data analysis and summarization. Analysis of data streams. Similarity Search.

**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, 3rd Edition. : Cambridge University Press, 2020

**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: buone competenze relative al progetto e all'analisi di algoritmi e strutture dati; conoscenza delle nozioni fondamentali di calcolo delle probabilità e statistica; buon livello di programmazione in Java o Python; capacità di utilizzo dell'ambiente Linux e della linea di comando.

**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. \* Frameworks: - Distributed (MapReduce, Apache Spark) - Streaming \* Techniques with applications: - Partitioning (data distribution) - Coresets (unsupervised learning) - Sketches (estimation of moments, set membership) - Locality sensitive hashing (similarity search).

**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:**

Leskovec, Jure; Rajaraman, Anand; Ullman, Jeffrey D.; Leskovec, Jure, Mining of massive datasets. Cambridge: Cambridge University Press, 2020

**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.

**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 di base sull'apprendimento automatico e sulla teoria della probabilità. Sono inoltre richieste capacità di programmazione in Python per svolgere il mini-progetto individuale richiesto per l'esame. La familiarità con concetti base delle scienze cognitive può facilitare la comprensione dei temi trattati.

**Conoscenze e abilità da acquisire:**

Il corso fornisce conoscenze sui principali approcci computazionali utilizzati per modellizzare le funzioni cognitive, dalle reti neurali artificiali ai modelli probabilistici. Queste conoscenze sono rilevanti sia per la comprensione del funzionamento della mente che per lo sviluppo e la valutazione dei moderni sistemi di intelligenza artificiale. La discussione teorica dei diversi approcci verrà affiancata da esempi concreti di applicazione (es. visione, linguaggio, ragionamento).

**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 le discussioni interattive su domande aperte, per promuovere la riflessione critica sui concetti discussi. Il corso include alcune esercitazioni (in aula informatica) con simulazioni al computer.

**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. Casi di studio: visione e acquisizione di concetti; elaborazione del linguaggio; ragionamento.

**Modalità di esame:**

L'esame consisterà in una prova scritta con circa 20 domande a scelta multipla (durata massima 30 minuti). Ogni studente dovrà inoltre consegnare entro il giorno precedente l'esame scritto un Python notebook del progetto assegnato durante il corso.

**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:**

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 Russell, Stuart; Norvig, Peter, Artificial Intelligence. Harlow: Pearson Education UK, 2013

**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 (articoli scientifici) forniti dal docente sulla piattaforma di e-learning.

<b>CYBER PHYSICAL SYSTEMS AND IOT SECURITY</b>
--

**Titolare:** Dott. ALESSANDRO BRIGHENTE

**Mutuato da:** Laurea magistrale in International Cybersecurity and Cyberintelligence (Ord. 2023)

**Periodo:** Il anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Conoscenze base di architettura degli elaboratori e principali protocolli di rete (TCP, UDP, IP). Capacità di analizzare codice, capire il suo funzionamento, e modificarlo in base alle necessità.

**Conoscenze e abilità da acquisire:**

Alla fine del corso, lo studente sarà in grado di - Analizzare un flusso di controllo e capirne le operazioni fondamentali, con particolare riferimento al protocollo CAN. Capacità di implementare attacchi a livello controllo e a livello rete. Capacità di analizzare il traffico CAN bus e inferire informazioni sul suo funzionamento. - Implementare semplici controllori e testarne la sicurezza. - Analizzare un programma ladder logic per PLC e capirne il funzionamento. Implementare attacchi in grado di alterarne il funzionamento e progettare programmi sicuri. - Comprendere il funzionamento dei principali protocolli industriali, implementare attacchi ad integrity ed availability, e sviluppare contromisure. - Comprendere il funzionamento dei protocolli di posizionamento di droni e procedure di fail safe. Implementare attacchi di GPS spoofing per deviare le traiettorie. - Implementare protocolli di remote attestation per dispositivi IoT ed analizzarne le performance.

**Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni frontali comprendenti sia teoria che laboratori. In particolare, l'attività di laboratorio ha l'obiettivo di fornire allo studente le conoscenze basilari sugli attacchi e tecniche di prevenzione.

**Contenuti:**

Fundamentals - What is a Cyber-Physical System - Security Requirements in CPS Automotive Security - The CAN bus protocol - Error handling in CAN bus and bus-off attack - Network attacks on CAN bus - Keyless cars security and attacks to distance bounding protocols Autonomous Driving - Introduction to controllers - Levels of automation and modes of operation - Attacks on controllers and countermeasures Industrial Control Systems - Industrial Control Network Protocols - PLC and their functioning - Attacks and countermeasures to industrial control systems Drones - Drone components and basic functioning - Protocols for drone location and fail-safe procedures - Drone detection systems Internet of Things - Network protocols for the internet of things - Remote attestation - Intrusion and anomaly detection

**Modalità di esame:**

La totalità dei punti dell'esame, è suddivisa secondo i seguenti criteri: 40%: report di metà corso su un lavoro di implementazione di attacchi e contromisure su un topic a scelta della prima parte del corso 40%: report di fine corso su un lavoro di implementazione di attacchi e contromisure su un topic a scelta della seconda parte del corso 20%: esame teorico finale (10 domande a scelta multipla)

**Criteri di valutazione:**

I criteri di valutazione riflettono la padronanza delle conoscenze e abilità acquisite dallo studente secondo la sezione "Conoscenze e abilità d'acquisire". L'esame finale valuta la conoscenza dei concetti base introdotti durante il corso.

**Testi di riferimento:**

Walid M., et al., Cyber-Physical Systems: A Model-Based Approach. : Springer, 2021 E.D. Knapp, Industrial Network Security. : Elsevier, 2011

**Eventuali indicazioni sui materiali di studio:**

Durante le lezioni verranno forniti articoli scientifici a supporto della didattica. Additional Material Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain: Cyber Security for Cyber Physical Systems. Springer International Publishing (2018) Edward J. M. Colbert, Alexander Kott: Cyber-security of SCADA and Other Industrial Control Systems. Springer International Publishing (2016)

<b>CYBERSECURITY AND CRYPTOGRAPHY: PRINCIPLES AND PRACTICES</b>
---

**Titolare:** Prof. CARLO MARICONDA

**Periodo:** I anno, annuale

**Indirizzo formativo:** Corsi comuni

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

**Prerequisiti:**

Per la prima parte ( CRYPTOGRAPHY, Prof. Mariconda; primo semestre, 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 nel I semestre e Prof. Migliardi nel II semestre; 6 CFU): OS, Programming.

**Conoscenze e abilità da acquisire:**

Per la prima parte A (Prof. Mariconda; 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. La seconda parte è suddivisa in due moduli: Modulo B: nel primo modulo (Prof. Conti; 3 CFU, I semestre): gli studenti saranno in grado di identificare, classificare, descrivere, spiegare e correlare i concetti chiave degli attacchi e delle difese informatiche. Modulo C: nel secondo modulo della seconda parte (Prof. Migliardi; 3 CFU, II semestre): Valutare i rischi a cui è esposto un sistema IT, Spiegare come funziona un attacco, Descrivere, spiegare e generalizzare le vulnerabilità del software, Evitare le insidie del software.

**Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni frontali in classe. Per la prima parte (CRYPTOGRAPHY) sono previste attività in aula, partecipazione attiva e saranno disponibili i video delle lezioni.

**Contenuti:**

La prima parte (Prof. Mariconda; 6 CFU) costituisce anche l'insegnamento di CRYPTOGRAPHY per i corsi ICT FOR INTERNET AND MULTIMEDIA, COMPUTER ENGINEERING, COMPUTER SCIENCE, MATHEMATICS, International Cybersecurity and Cyberintelligence. Fatti teorici di base: Aritmetica modulare. Numeri primi. Teorema piccolo di Fermat. Teorema del resto cinese. Campi finiti: ordine di un elemento e radici primitive. Test di pseudoprimalità. Test di Agrawal-Kayal-Saxena. Metodo RSA: prima descrizione, attacchi. Metodo di Rabin e la sua connessione con la fattorizzazione degli interi. Metodi di logaritmo discreto. Come calcolare il logaritmo discreto in un campo finito. Metodi elementari di fattorizzazione. Alcune osservazioni sul setaccio quadratico di Pomerance. Protocolli e algoritmi. Algoritmi crittografici fondamentali. Metodi simmetrici (storici, DES, AES). Metodi asimmetrici. Attacchi. Firma digitale. Generatori pseudocasuali (osservazioni). Scambio di chiavi, scambio di chiavi in tre passaggi, divisione del segreto, condivisione del segreto, trasmissione del segreto, marcatura temporale. Firme con RSA e logaritmo discreto. Simboli di Legendre e di Jacobi, legge di reciprocità quadratica e applicazioni alla crittografia. Per la seconda parte (Prof. Conti and Prof. (da determinare); 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:**

gli studenti dell'insegnamento di CRYPTOGRAPHY devono sostenere solo la prima parte A, quelli di CYBERSECURITY AND CRYPTOGRAPHY: PRINCIPLES AND PRACTICES devono sostenere i moduli A, B, C. Per la prima parte A (CRYPTOGRAPHY, Prof. Mariconda; 6 CFU): Esame scritto, prova orale se ritenuta necessaria. In alternativa all'esame finale sono proposte prove intermedie e lavori individuali (esercizi, peer review). Per la seconda parte -modulo B (Prof. Conti, 3 crediti): Esame scritto, progetti assegnati da svolgere a casa, esame orale. - modulo C (Prof. Migliardi, 3 crediti): Esame scritto. Per ogni modulo lo studente può scegliere tra 5 date possibili per sostenere l'esame, senza nessun vincolo di esclusione tra l'una e l'altra, anche se la consegna del compito ad una prova successiva annulla la precedente. - \*\*Modulo A:\*\* 2 prove nella sessione invernale, 1 esame a giugno-luglio, 2 esami ad agosto-settembre. - \*\*Modulo B:\*\* 2 prove nella sessione invernale, 2 esami a giugno-luglio, 1 esame ad agosto-settembre. - \*\*Modulo C:\*\* 2 prove a giugno-luglio, 1 esame a settembre, 2 esami a gennaio-febbraio (dell'anno successivo). Il voto finale per gli studenti del corso CYBERSECURITY and CRYPTOGRAPHY: PRINCIPLES AND PRACTICES è determinato dalla media ponderata dei tre esami parziali—A (Prima parte del corso, 6 crediti, I semestre), B (Primo modulo della seconda parte del corso, 3 crediti, I semestre) e C (Secondo modulo della seconda parte del corso, 3 crediti, II semestre)—in proporzione ai rispettivi crediti. Tutti e tre gli esami parziali devono essere completati all'interno dello stesso anno accademico (in particolare, gli esami dei Moduli A e B devono essere completati entro la fine di settembre, mentre l'esame del Modulo C può essere completato nella sessione invernale dell'anno successivo). Al termine di ogni sessione d'esame, i voti degli studenti che hanno superato tutte e tre le parti vengono automaticamente registrati su Uniweb (non è richiesta alcuna registrazione). Di norma, salvo altre indicazioni della commissione, gli studenti che rifiutano il voto finale dovranno ripetere tutti e tre i moduli.

**Criteri di valutazione:**

Per la prima parte (Prof. Mariconda; 6 CFU): Si prevedono due percorsi possibili: per chi frequenta e studia regolarmente è previsto un bonus costituito dagli esiti di valutazioni in itinere su lavori a casa singoli o di gruppo da utilizzare in un appello nella prima sessione di esami dopo il corso o nei tre esami parziali durante il corso, altrimenti la prova è costituita dal solo appello finale. Durante la prova scritta finale lo studente dovrà rispondere ad alcune

domande relative al programma svolto e risolvere alcuni esercizi dimostrando di aver compreso gli argomenti del corso. Il voto costituisce l'esito finale per l'insegnamento di Cryptography. Per la seconda parte (Prof. Conti and Prof. Migliardi; 3+3 CFU): Valutazione sia della competenza teorica che della capacità operativa di applicare quanto appreso a un caso reale. Il voto per gli studenti che seguono l'intero insegnamento di CYBERSECURITY AND CRYPTOGRAPHY: PRINCIPLES AND PRACTICES è dato dalla media pesata in proporzione ai CFU dei voti della prima parte e della seconda parte.

**Testi di riferimento:**

Hoffstein J., Pipher J. , Silverman J., An introduction to mathematical cryptography (2nd ed.). New York: Springer, 2014 Stallings, William; Brown, Lawrie, Computer security principles and practice. Boston [etc.]: Pearson, 2015 Pflieger, Charles P.; Pflieger, 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

**Eventuali indicazioni sui materiali di studio:**

Per la prima parte (6 CFU) il testo di riferimento è: Hoffstein J., Pipher J. e Silverman J. - An introduction to mathematical cryptography. 2nd ed. Undergraduate Texts in Mathematics. New York, NY: Springer (2014) Per la prima parte sono testi di consultazione e approfondimento: 1) N. Koblitz - A Course in Number Theory and Cryptography -Springer, 1994. 2) H. Knospe - A Course in Cryptography - American Mathematical Society, 2019. 3) R. Crandall, C. Pomerance - Prime numbers: A computational perspective - Springer, 2005. 4) B. Schneier - Applied Cryptography - Wiley, 1994. 5) A. Languasco, A.Zaccagnini - Manuale di Crittografia - Hoepli Editore, 2015. (Italian).

**DEEP LEARNING (MATICOLE DISPARI)**

**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, e il Transformer. Infine si tratteranno autoencoder e modelli generativi deep. Inoltre, gli studenti dovranno consegnare homework pratici che coprono i contenuti dell'insegnamento.

**Attività di apprendimento previste e metodologie di insegnamento:**

L'insegnamento prevede lezioni frontali.

**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;

**Modalità di esame:**

Lo studente deve superare un esame scritto. Per essere ammesso all'esame lo studente deve aver consegnato ed ottenuto valutazione positiva tutti gli homework previsti dall'insegnamento.

**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.

**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.

**DEEP LEARNING (MATICOLE PARI)**

**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, e il Transformer. Infine si tratteranno autoencoder e modelli generativi deep. Inoltre, gli studenti dovranno

consegnare homework pratici che coprono i contenuti dell'insegnamento.

**Attività di apprendimento previste e metodologie di insegnamento:**

L'insegnamento prevede lezioni frontali.

**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.

**Modalità di esame:**

Lo studente deve superare un esame scritto. Per essere ammesso all'esame lo studente deve aver consegnato ed ottenuto valutazione positiva tutti gli homework previsti dall'insegnamento.

**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.

**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 AND BIOMETRICS**

**Titolare:** Prof. SIMONE MILANI

**Periodo:** I anno, 1 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 di base del linguaggio Python e delle tecniche principali di machine learning. Qualora lo studente non possedesse tali competenze, verranno indicati dei materiali per uno studio individuale.

**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 delle principali misure biometriche. 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:**

Nell'ambito del corso, le attività e le metodologie di insegnamento prevedono 20 lezioni frontali in aula dove su supporto informatico (powerpoint) e alla lavagna vengono presentati i contenuti del corso. Saranno presentati dei casi reali e verranno svolte esercitazioni tramite problemi alla lavagna e quiz interattivi. Tali contenuti verranno inoltre chiariti con esempi pratici in 4 lezioni in laboratorio in cui ogni studente dovrà applicare alcune tecniche di indagine. Nelle sessioni di laboratori, verrà utilizzata la programmazione in linguaggio Python e la piattaforma Google Colaboratory (disponibili gratuitamente).

**Contenuti:**

Introduzione alla digital forensics. L'elaborazione dei dati digitali in contesti legali. Parte a: Digital forensics a.1) Acquisizione di prove digitali. 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. 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. a.2.3. Rilevamento di intrusioni su rete. a.2.4. Strategie antiforensic: 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 e loro rilevamento. 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.4) Rilevamento di anomalie a.4.1. Tecniche e algoritmi di anomaly detection a.4.2. Algoritmi di tipo avversario. Adversarial Machine Learning a.4.3. Tecniche avversarie iterative: Generative adversarial Networks Parte 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 progetto finale (da documentare tramite report) o di una relazione scientifica sulla letteratura. 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.

**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 Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, J. D. Tygar, Adversarial Machine Learning. Cambridge: Cambridge University Press, 2019 Hani Farid, Photo Forensics. : MIT Press, 2019 Watt, Jeremy; Borhani, Reza, Machine learning refinedrisorsa elettronicafoundations, algorithms, and applicationsJeremy Watt, Reza Borhani, Aggelos Katsagelos. 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>.

**ENGLISH LANGUAGE B2 (PRODUCTIVE SKILLS)**

**Titolare:** Prof. MAURO MIGLIARDI

**Periodo:** I anno, annuale

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** ; 3,00

**ETHICAL HACKING**

**Titolare:** Dott. ALESSANDRO BRIGHENTE

**Periodo:** Il anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Nessun prerequisito obbligatorio. E' raccomandabile una conoscenza di base su protocolli di rete, applicazioni web, linguaggi C e assembly.

**Conoscenze e abilità da acquisire:**

Introduzione, a livello teorico e pratico, di metodologie e strumenti utilizzati negli attacchi più noti in letteratura in ambito di comunicazioni di reti, sicurezza hardware, sicurezza web, gestione della memoria dei programmi, reverse-engineering.

**Attività di apprendimento previste e metodologie di insegnamento:**

Prima di ogni lezione, il docente pubblica un video in cui illustra gli argomenti della lezione. Gli studenti devono vedere il video prima di partecipare alla lezione. All'inizio della lezione, il docente rilascia un breve questionario per verificare se gli studenti abbiano compreso i concetti principali descritti nella lezione registrata. Il questionario viene somministrato attraverso la piattaforma Moodle. L'insegnante, quindi, risponde a qualsiasi dubbio o domanda. Il docente individua i gruppi di lavoro scegliendo i componenti di ciascun gruppo (i gruppi saranno diversi per ogni nuovo laboratorio) e rilascia il nuovo laboratorio. Anche se tutti i gruppi sono incoraggiati a svolgere il laboratorio, l'insegnante seleziona il gruppo che dovrebbe risolverlo e illustra la soluzione agli altri gruppi, facendo una presentazione una settimana dopo il rilascio del laboratorio. Durante la lezione successiva, il gruppo selezionato presenta la sua soluzione e risponde alle domande del docente o degli altri studenti. Se l'insegnante è soddisfatto della prestazione del gruppo, ogni membro del gruppo riceve un bonus che verrà sommato al voto ottenuto durante l'esame finale.

**Contenuti:**

Il corso riguarderà i seguenti argomenti: - Sicurezza di rete: analisi e monitoraggio del traffico di rete; sicurezza dei protocolli di rete; sniffing e spoofing di pacchetti di rete; firewall - Sicurezza hardware: attacco meltdown; attacco spectre - Sicurezza web: cross-site scripting attack; HTTP request smuggling; SQL injection attacks; cross-site requests forgery attack - Pwn: shellcode; buffer overflow; return-to-libc; format string attack - Reverse-engineering: reversing in x86; gdb; debuggers

**Modalità di esame:**

L'esame finale consisterà in una serie di domande a risposta multipla su tutti gli argomenti del corso. Il bonus accumulato con la partecipazione durante il semestre verrà sommato al voto ottenuto all'esame. Poiché la partecipazione non è obbligatoria, uno studente può ottenere il voto massimo (es. 30L) anche senza frequentare il corso.

**Criteri di valutazione:**

Conoscenza dei concetti presentati durante il corso.

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**FINAL EXAM**

**Titolare:** da definire

**Periodo:** Il anno, 2 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** ; 30,00

## FORMAL METHODS FOR CYBER-PHYSICAL SYSTEMS

**Titolare:** Prof. DAVIDE BRESOLIN

**Mutuato da:** Laurea magistrale in International Cybersecurity and Cyberintelligence (Ord. 2023)

**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, logica. 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, e di comprenderne e analizzarne i risultati. 4. Capacità di utilizzare algoritmi e strumenti per la sintesi automatica di controllori, e di comprenderne e analizzarne i risultati.

**Attività di apprendimento previste e metodologie di insegnamento:**

Il corso comprende lezioni frontali, attività di laboratorio e assignment da svolgere fuori dalle ore di lezione. Le lezioni frontali introducono le conoscenze di base e gli argomenti teorici. Le attività di laboratorio permettono di provare le metodologie e gli strumenti appresi su semplici casi di studio. Gli assignment richiedono l'implementazione di soluzioni originali e la loro applicazione a casi di studio di media complessità.

**Contenuti:**

Sistemi ciberfisici: definizione e caratteristiche chiave. Modelli formali per sistemi ciberfisici: modelli sincroni e asincroni. Verifica dei sistemi ciberfisici: proprietà di sicurezza e liveness, model checking, algoritmi enumerativi e tecniche simboliche. Sintesi di controllori per sistemi ad eventi discreti.

**Modalità di esame:**

Esame scritto per la parte di teoria. Per la parte pratica, due assignment da svolgere e consegnare durante il semestre di lezione, o in alternativa, un 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 5. Capacità di utilizzare strumenti per la sintesi automatica di controllori

**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 STEM. 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 dei Docenti.

## FOUNDATIONS OF DATABASES

**Titolare:** Dott. STEFANO MARCHESIN

**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:**

- Basic knowledge of the Java programming language

**Conoscenze e abilità da acquisire:**

The goal is to learn to design and develop a distributed application for the management of and access to structured data over time. The achievement of this goal consists of: - acquisition of strong competences concerning databases, their data models and properties, formal languages for querying a database, and suitable methodologies for designing a database; - acquisition of the capability of carrying out an actual project for the design and development of a database application using a relational database management system (RDBMS)

**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

#### **Modalità di esame:**

+ Individual oral exam with questions and exercises on the topics covered during the lectures. If a large number of students will be attending the exam, it will be turned into a Moodle quiz. + Project to document, design, develop, implement, and code an actual database application, carried out in student groups via homeworks during the semester: -- git repository containing the project source code and all the related material; -- report on the contents and state of the project as well as the usage of the developed system.

#### **Criteri di valutazione:**

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

#### **Testi di riferimento:**

Ramez Elmasri, Shamkant B. Navathe, Fundamentals of Database Systems. : 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 will be available on the Moodle platform (<https://elearning.dei.unipd.it/>) for the course. Examples of teaching material and videos from the course are available at: <https://iiaa.dei.unipd.it/education/foundations-of-databases/> 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:** Prof. LEONARDO BADIA

**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. Possibile utilizzo di video registrati.

#### **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, completezza, e completezza dell'equilibrio Aste, bargaining Aste di primo e secondo prezzo, criterio VCG (cenni) Giochi cooperativi, il nucleo, il valore di Shapley (cenni) Allocazione delle risorse Utilità, scelte e paradossi Giochi potenziali, coordinazione Algoritmi bio-inspired Giochi evolutivi Reti cognitive Selfish routing Age of information 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 piu' domande, tipicamente tre. Il punteggio massimo che si puo' conseguire allo scritto e' 27. Per frequentanti, l'esame puo' coinvolgere lo sviluppo di un progetto in gruppi di 1-3 persone, su argomenti del corso applicati alle ICT. L'adesione a questa modalita' va dichiarata anticipatamente e l'argomento del progetto sono concordati con il docente durante il corso. Il progetto va consegnato entro circa un mese dalla fine delle lezioni. Se il test scritto e' sufficiente, si puo' registrare il voto, a seconda dei casi esso sara': - senza progetto: punteggio conseguito allo scritto + 3 punti - con progetto: punteggio conseguito allo scritto + valutazione del progetto che va da 0 a 8 punti

#### **Criteri di valutazione:**

Ogni domanda nei test scritti viene valutata fino a un massimo di 3 punti. Il punteggio finale dello scritto e' la somma numerica dei punteggi individuali delle domande. Studenti che non svolgono il progetto ricevono ulteriori 3 punti per arrivare fino a un massimo di 30. Il progetto viene invece valutato da 0 a 8 punti, sommati al punteggio dello scritto. Un punteggio di 30 e lode e' assegnato agli studenti il cui punteggio totale 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 capacita' di problem solving - la capacita' di discussione e verifica ex-post della soluzione trovata Nella valutazione del progetto (se presente) vengono tenuti in considerazione: - l'originalita' della proposta e la pertinenza sia con le tematiche del corso che con le metodologie ingegneristiche tipiche dell'ICT - la capacita' di lavoro di gruppo e la presenza di singoli

contributi attribuibili ai partecipanti al progetto - la capacità di trarre conclusioni significative dal punto di vista scientifico grazie alle metodologie apprese nel corso

**Testi di riferimento:**

S. Tadelis, Game Theory: An Introduction. : Princeton, 2013 A. MacKenzie, L. DaSilva, Game Theory for Wireless Engineers. : Morgan & Claypool, 2006 N. Nisan, T. Roughgarden, E. Tardos, V. V. Vazirani, Algorithmic game theory. : Cambridge Univ. Press, 2007 L. Badia, T. Marchioro, Game theory. A handbook of problems and exercises. Bologna: Esculapio, 2022 R. Lucchetti, A Primer in Game Theory. Bologna: Esculapio,

**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. Per gli esercizi, si consiglia il Badia-Marchioro. Il libro di MacKenzie-DaSilva è un buon esempio per le applicazioni, 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, 2 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:**

L'esame sarà scritto, della durata di 90 minuti, con eventuale integrazione orale. Ci saranno indicativamente 6-12 domande chiuse (che prevedono risposte puntuali e specifiche) e 1-3 aperte (che richiedono riflessione ed elaborazione), a seconda della complessità delle medesime. Modalità alternative potranno essere previste per i frequentanti.

**Criteri di valutazione:**

In generale, ai fini di una valutazione positiva, è necessario che lo studente sappia argomentare in modo corretto e pertinente, durante l'esame, le tematiche trattate a lezione.

**Testi di riferimento:**

Rogers, Yvonne; Sharp, Helen; Preece, Jennifer; Rogers, Yvonne, Interaction design beyond human-computer interaction. Hoboken, NJ: Wiley, 2023

**Eventuali indicazioni sui materiali di studio:**

FREQUENTANTI INTERACTION DESIGN (6th 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 (6th 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, 2 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 5. crittografia

**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.

**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, Maura B. Paterson, Cryptography: Theory and Practice. Boca Raton: 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. MARCO GIORDANI

**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:**

Si assumono le conoscenze di base dei principi delle reti di telecomunicazioni, in particolare dello stack protocollare di Internet. Si assume che gli studenti abbiano familiarità con concetti di base delle telecomunicazioni a livello fisico (principalmente propagazione radio e modulazione digitale), a livello MAC (principalmente controllo dell'accesso al mezzo) e a livello di rete.

**Conoscenze e abilità da acquisire:**

Il corso mira a fornire le seguenti conoscenze e abilità: 1. Conoscenza e comprensione dei concetti di base di Internet of Things. 2. Capacità di applicare i paradigmi di Internet of Things a problemi reali di telecomunicazioni. 3. Conoscenza e comprensione dei concetti di base delle Smart Cities. 4. Capacità di applicare i paradigmi delle Smart Cities a problemi reali di gestione delle città, con particolare riferimento agli aspetti dell'ICT.

**Attività di apprendimento previste e metodologie di insegnamento:**

Il modulo prevede lezioni frontali.

**Contenuti:**

PARTE 1: Internet of Things 1. Definizione di Internet of Things e delle relative applicazioni e trend scientifici e di mercato. 2. Internet of Things per comunicazioni a lungo e a corto raggio. 3. Principali problematiche di ricerca legate ad Internet of Things, nello specifico relative al livello fisico, all'indirizzamento ed al routing, e alla sicurezza. 4. Gli enti di standardizzazione ed i consorzi di Internet of Things: ETSI, IETF, 3GPP, IEEE. 5. I principali standard Internet of Things: ZigBee, 6LoWPAN, WiFi (802.11ah), Bluetooth Low Energy, SigFox, Lo-Ra. 6. Le principali piattaforme per Internet of Things: Microsoft, Amazon, Google. PARTE 2: Smart Cities 1. Definizione di Smart Cities e delle relative applicazioni e trend scientifici e di mercato. 2. Principali architetture di comunicazione per le Smart Cities. 3. Principali problematiche legate alla regolamentazione ed open data per le Smart Cities. 4. Principali esempi di applicazioni Smart Cities. 5. Principali problematiche di ricerca legate alle Smart Cities, nello specifico relative alla privacy e alla sicurezza.

**Modalità di esame:**

L'esame consisterà in una PROVA SCRITTA sugli argomenti teorici del corso, che potrà essere integrata da un progetto di fine corso al fine di ottenere dei punti aggiuntivi nella valutazione finale. Agli studenti saranno offerti quattro tentativi per superare l'esame: due alla fine del semestre in cui è offerto il corso (gennaio e febbraio), uno nella sessione successiva (giugno), e uno nella sessione di recupero (settembre). Gli studenti che ottengono un punteggio almeno pari a 18/30 nella prova scritta hanno la facoltà di richiedere una PROVA ORALE, che verterà sull'intero programma del corso.

**Criteria di valutazione:**

1. Completezza delle conoscenze acquisite. 2. Livello di comprensione degli argomenti del corso. 3. Livello di partecipazione alle discussioni di classe. 4. Capacità di discutere i pro e i contro delle diverse opzioni di progettazione. 5. Conoscenza della terminologia tecnica. 6. Capacità di applicare le conoscenze acquisite nel corso a casi di studio ed applicazioni pratiche.

**Testi di riferimento:**

McClellan, Stan; Jimenez, Jesus A.; Koutitas, George; McClellan, Stan, Smart cities applications, technologies, standards, and driving factors. Cham: Springer, 2018 Anton-Haro, Carles; Dohler, Mischa; Anton-Haro, Carles, Machine-to-machine (M2M) communications architecture, performance and applications. Cambridge, UK: Woodhead Publishing, 2015 Kellmerein, Daniel; Obodovski, Daniel; Kellmerein, Daniel, Silent intelligence the Internet of Things. San Francisco: DnD Ventures, 2013 Milenkovic, Milan., Internet of Things: Concepts and System Design. Cham: Springer International Publishing, 2020 Vasseur, Jean Pierre; Dunkels, Adam; Vasseur, Jean Pierre, Interconnecting smart objects with IP the next Internet. Burlington, MA: Morgan Kaufmann Publishers, 2010 Shelby, Zach; Bormann, Carsten; Shelby, Zach, 6LoWPAN: the wireless embedded internet. Chichester, UK: Wiley, 2009 Parker, Geoffrey G.; Choudary, Sangeet Paul; Alstyn, Marshall W. : van; Parker, Geoffrey G., Platform revolution how networked markets are transforming the economy and how to make them work for you. New York London: Norton, 2016 Greengard, Samuel, Internet of Things. Cambridge (MA): The MIT Press, 2015 Farahani, Shahin, ZigBee wireless networks and transceivers. Burlington, MA: Newnes, 2008

**Eventuali indicazioni sui materiali di studio:**

Si suggeriscono diversi libri di testo. Durante il corso verranno inoltre fornite note, slide, articoli e altro materiale di studio. Tutto il materiale sarà reso disponibile sul sito STEM del corso.

**LAW AND DATA**

**Titolare:** Dott.ssa FIORELLA DAL MONTE

**Mutuato da:** Laurea magistrale in Data Science (Ord. 2023)

**Periodo:** I 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

**Criteria 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, Luxemburg (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 (CANALE A)**

**Titolare:** Prof. FABIO VANDIN

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

**Periodo:** I 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 calcolatore. 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 calcolatore (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 calcolatore (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:**

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 C. M. Bishop, Pattern Recognition and Machine Learning.. : Springer, 2006

**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>

**MACHINE LEARNING (CANALE B)**

**Titolare:** Dott.ssa BARBARA DI CAMILLO

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

**Periodo:** I 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 calcolatore. 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 calcolatore (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 ( <https://stem.elearning.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 calcolatore (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:**

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

#### **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 <https://stem.elearning.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 base di ricerca operativa, programmazione lineare, 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. Richiami, approfondimenti e applicazioni di Programmazione Lineare e dualità : metodo del simplesso 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 SECURITY

**Titolare:** Prof.ssa ELEONORA LOSIOUK

**Periodo:** Il anno, 1 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. 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:**

Prima di ogni lezione, il docente pubblica un video in cui illustra gli argomenti della lezione. Gli studenti devono vedere il video prima di partecipare alla lezione. All'inizio della lezione, il docente rilascia un breve questionario per verificare se gli studenti abbiano compreso i concetti principali descritti nella lezione registrata. Il questionario viene somministrato attraverso la piattaforma Moodle. L'insegnante, quindi, risponde a qualsiasi dubbio o domanda. Il docente individua i gruppi di lavoro scegliendo i componenti di ciascun gruppo (i gruppi saranno diversi per ogni nuovo laboratorio) e rilascia il nuovo laboratorio. Anche se tutti i gruppi sono incoraggiati a svolgere il laboratorio, l'insegnante seleziona il gruppo che dovrebbe risolverlo e illustra la soluzione agli altri gruppi, facendo una presentazione una settimana dopo il rilascio del laboratorio. Durante la lezione successiva, il gruppo selezionato presenta la sua soluzione e risponde alle domande del docente o degli altri studenti. Se l'insegnante è soddisfatto della prestazione del gruppo, ogni membro del gruppo riceve un bonus che verrà sommato al voto ottenuto durante l'esame finale.

**Contenuti:**

Gli argomenti sono i seguenti: - Architettura interna del sistema operativo Android. - Componenti di un'app mobile (Activity, Service, Content Provider, Broadcast Receiver). - Tecniche di analisi delle app. - Tecniche di reverse engineering per app. - Valutazione della vulnerabilità delle app. - Tecniche di analisi statica e dinamica per app. - Sfruttamento della vulnerabilità delle app.

**Modalità di esame:**

L'esame finale consisterà in una serie di domande a risposta multipla su tutti gli argomenti del corso. Il bonus accumulato con la partecipazione durante il semestre verrà sommato al voto ottenuto all'esame. Poiché la partecipazione non è obbligatoria, uno studente può ottenere il voto massimo (es. 30L) anche senza frequentare il corso.

**Criteri di valutazione:**

Conoscenza dei concetti presentati durante il corso.

**Testi di riferimento:**

Elenkov, Nikolay, Android security internals : an in-depth guide to Android's security architecture. : No Starch Press, 2015

## PRIVACY PRESERVING INFORMATION ACCESS

**Titolare:** Dott. GUGLIELMO FAGGIOLI

**Periodo:** Il anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

Requested competencies: + Undergraduate level knowledge of statistics + Background on algorithms and linear algebra + Basic knowledge of Databases

**Conoscenze e abilità da acquisire:**

The objective of the course is to learn what are the main challenges to privacy protection in the information access environment and what solutions can be adopted to preserve privacy. At the end of the course, the student is expected to learn: + How to define privacy and classify threats and techniques according to Solove's Taxonomy. Additionally, the student is expected to know basic elements of the European regulation concerning the protection of privacy. + Main statistical techniques adopted to achieve privacy in a computational environment (k-anonymity, l-diversity and t-closeness and differential privacy). + Main challenges linked to privacy protection, possible solutions and protection approaches for information access technologies, such as databases, search engines and recommender systems.

**Attività di apprendimento previste e metodologie di insegnamento:**

+ Lectures + Labs + Seminars of visiting colleagues on research topics and/or seminars by companies on the use and perspectives for innovative products based on Privacy-Preserving information access systems, stage opportunities, simulation of job interviews. + Oral presentation of research papers: to highlight the fact that this line of research is cutting-edge, students will present a paper among a pool of highly recent research papers. The presentation will be followed by a proactive discussion with the rest of the class.

**Contenuti:**

The course focuses on how to face the principal privacy challenges that arise when developing information access solutions. The course will cover the following privacy-preserving information access related topics: The first part of the course details the definition of privacy from both societal and legal

aspects. During the first module, the student learns about Solove's Taxonomy and how to classify the different privacy-related aspects. The course provides basic elements of the European regulation on privacy protection. The second part of the course focuses on the most known computational techniques to grant privacy. The student learns the main computational and statistical approaches used to achieve privacy and/or anonymity, such as k-anonymity, l-diversity and t-closeness, and Differential Privacy. The main part of the course focuses on information access, privacy threats linked to the use of databases, search engines and recommender systems. The student learns how state-of-the-art techniques are used to preserve users' privacy. More in detail, the following aspects will be covered: + Databases: interpretation of the threats in the Solove's hierarchy framework, practical application of computational techniques previously learned, microdata and macrodata protection and geomasking. + Information Retrieval and Search Engines: interpretation of the threats in the Solove's hierarchy framework, practical application of computational techniques previously learned, privacy risks linked to Search Engines and IR systems, development and evaluation of Privacy preserving IR models and Searchable encryption. + Recommender systems: interpretation of the threats in the Solove's hierarchy framework, practical application of computational techniques previously learned, analysis of the risks associated with collaborative filtering and social recommender systems, federated learning for privacy-preserving RS.

**Modalità di esame:**

Individual oral exam with questions and exercises on the topics covered during the lectures. - Projects to document, design, develop, implement, and code privacy-preserving techniques, carried out via homeworks during the semester. - Final presentation of a research paper about privacy-preserving approaches.

**Criteri di valutazione:**

The evaluation will be based on the comprehension and knowledge of the notions and methodologies specific to privacy-preserving information access techniques, on the capability of identifying potential threats and weaknesses of the information access systems and correctly deploying countermeasures and protection strategies. Students will be evaluated on the capability of carrying out comparative analyses of the different solutions required to handle the various information access channels, but also on the capability of recognizing commonalities. Furthermore, the evaluation will also include the active participation of the students in the lectures and in the discussion of cutting-edge research papers.

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

The teaching material consists of: - instructor's slides - suggested readings - additional material shared during lectures All the teaching material is available on the Moodle platform.

<b>QUANTUM CRYPTOGRAPHY AND SECURITY</b>
--

**Titolare:** Prof. NICOLA LAURENTI

**Mutuato da:** Laurea magistrale in International Cybersecurity and Cyberintelligence (Ord. 2023)

**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 i 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 - esperienza 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:**

**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: - homeworks (20%) - 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:**

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

**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:** 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 per pianificare e gestire la sicurezza dei sistemi informativi e conoscere le diverse alternative nell'identificazione dei rischi per la sicurezza. Svilupperanno le competenze per pianificare e gestire la sicurezza dei sistemi informativi e conoscere le diverse alternative

nell'identificazione dei rischi di sicurezza. Inoltre, svilupperanno la conoscenza del contesto lavorativo relativo alla sicurezza dell'informazione, in particolare sulle certificazioni riguardanti le organizzazioni, le tecnologie, le competenze e le persone, con una panoramica dei principali quadri di riferimento.

**Attività di apprendimento previste e metodologie di insegnamento:**

Lezioni frontali e discussione di casi pratici.

**Contenuti:**

Il corso affronta la valutazione dei rischi informatici che possono danneggiare un sistema informativo aziendale, le metodologie per mitigare questi rischi e le contromisure necessarie da applicare con l'obiettivo di rendere sicura l'azienda o l'istituzione pubblica dal punto di vista informatico. Gradualmente gli studenti saranno introdotti ai principi, ai concetti e alle pratiche per governare, gestire e controllare la cybersecurity secondo gli standard internazionali, le best practice professionali generalmente accettate, le certificazioni e i framework di riferimento. Programma del corso: - Concetti di base; - Pianificazione della Cybersecurity; - Operazioni e gestione della cybersecurity; - Valutazione della sicurezza e casi d'uso; - Utilizzo di agenti AI a supporto dei cybersecurity assessment report; - Certificazione e quadri di riferimento per organizzazioni e sistemi di gestione; - Certificazione di prodotti e tecnologie; - Framework che descrivono le competenze; - Certificazione delle persone; - Certificazioni più comuni disponibili sul mercato; - Tecniche di audit ed esempi.

**Modalità di esame:**

Gli studenti sosterranno un esame alla fine del corso. L'esame finale riguarderà tutto il materiale spiegato a lezione.

**Criteri di valutazione:**

Conoscenza dei concetti studiati durante il corso.

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

- Effective Cybersecurity: A Guide to Using Best Practices and Standards, 2019, Stallings, W. <https://www.pearson.com/us/higher-education/program/Stallings-Effective-Cybersecurity-A-Guide-to-Using-Best-Practices-and-Standards/PGM1835803.html?tab=resources> -Materiale aggiuntivo fornito dal docente a lezione [letture aggiuntive opzionali] - CyBok v.1.1 - The Cyber Security Body of Knowledge, 2021 [https://www.cybok.org/media/downloads/CyBOK\\_v1.1.0.pdf](https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf)

## SECURITY OF ADVANCED NETWORKING AND SERVICES

**Titolare:** Prof. CRISTINA NITA-ROTARU

**Periodo:** I anno, annuale

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 48A; 6,00

**Prerequisiti:**

CONTENUTO NON PRESENTE

**Conoscenze e abilità da acquisire:**

CONTENUTO NON PRESENTE

**Attività di apprendimento previste e metodologie di insegnamento:**

CONTENUTO NON PRESENTE

**Contenuti:**

CONTENUTO NON PRESENTE

**Modalità di esame:**

CONTENUTO NON PRESENTE

**Criteri di valutazione:**

CONTENUTO NON PRESENTE

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

CONTENUTO NON PRESENTE

## SEMINARS AND OTHER ACTIVITIES

**Titolare:** Prof. SIMONE MILANI

**Periodo:** Il anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** ; 3,00

## SERVICE MANAGEMENT

**Titolare:** da definire

**Periodo:** l'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:** • Wise R. & Baumgartner P. (1999), "Go Downstream: The New Profit Imperative in Manufacturing," Harvard Business Review, 77(5): 133-141. • Oliva, R. & Kallenberg, R. (2003), "Managing the transition from products to services", International Journal of Service Industry Management, 14(2): 160-172. • Tukker, A. (2004), "Eight types of product-service system: eight ways to sustainability? Experiences from SusProNet". Business Strategy and the Environment, 13: 246-260. • Porter, M. E. & Heppelmann, J. E. (2015), "How Smart, Connected Products Are Transforming Companies", Harvard Business Review, October: 96-112. • Gebauer H., Paiola M., Sacconi N. & Rapaccini M. (2021), "Digital servitization: Crossing the perspectives of digitization and servitization", Industrial Marketing Management, 93: 382-388

**SOFTWARE VERIFICATION**

**Titolare:** Prof. FRANCESCO RANZATO

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

**Periodo:** l'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](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](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](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 piu' 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, e' 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 studente totalizza almeno 15 punti nella parte A e la media dei punti fra parte A e parte B e' almeno pari a 18, quest'ultima puo' essere accettata come voto finale. Se il punteggio nella parte A e' inferiore a 15 o la media delle due prove e' insufficiente, l'esame non e' superato. Anche se la prova finale puo' essere superata sostenendo con successo il solo esame scritto (in due parti), lo studente puo' 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. Karlin (with H. Taylor for the 3rd ed, with M.A. Pinsky for the 4th ed), 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 S. Ross, Stochastic processes. : Wiley (2nd ed.), 1996

**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).

**VISION AND COGNITIVE SYSTEMS**

**Titolare:** Prof. LAMBERTO BALLAN

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

**Periodo:** Il anno, 1 semestre

**Indirizzo formativo:** Corsi comuni

**Tipologie didattiche:** 32A+16L; 6,00

**Prerequisiti:**

Lo studente deve avere conoscenze di base di programmazione e algoritmi, così come di analisi matematica, probabilità e statistica, algebra lineare. È inoltre consigliabile una familiarità con concetti di base di apprendimento automatico.

**Conoscenze e abilità da acquisire:**

Questo corso insegna i concetti, i metodi e le tecnologie alla base della visione artificiale e dei sistemi cognitivi, incluso i moderni servizi cognitivi, vale a dire API e servizi tipicamente disponibili su cloud, che aiutano gli sviluppatori a creare applicazioni di intelligenza artificiale. Esempi di funzioni intelligenti che possono essere aggiunte ad un'applicazione tramite l'utilizzo di servizi cognitivi sono: il riconoscimento visuale; il rilevamento delle emozioni da video ed il riconoscimento facciale; comprensione linguistica e del parlato. Il corso insegna inoltre le competenze e le abilità specifiche necessarie per applicare tali concetti alla progettazione e all'implementazione di applicazioni di intelligenza artificiale. Gli studenti dovranno affrontare esercizi pratici in laboratorio informatico, in modo da provare l'applicazione delle conoscenze acquisite a piccoli esempi pratici.

**Attività di apprendimento previste e metodologie di insegnamento:**

Il corso consiste in lezioni e esercizi in laboratorio informatico. Gli esercizi in laboratorio informatico consentono agli studenti di sperimentare, in diversi scenari operativi, le tecniche introdotte a lezione. In questo modo gli studenti possono verificare sperimentalmente i concetti appresi in classe, acquisire la capacità di applicare i concetti appresi e di esprimere un giudizio critico.

**Contenuti:**

Il corso comprende gli argomenti elencati di seguito: - Introduzione: Dalla cognizione umana all'intelligenza artificiale e ai sistemi cognitivi; breve introduzione ai paradigmi di intelligenza artificiale e apprendimento automatico; la rivoluzione dell'IA: attuali tendenze e applicazioni, le principali sfide. - Servizi cognitivi: Concetti basilari; servizi linguistici, vocali e di visione; principali provider e API (IBM Watson, AWS, Google Cloud); tecnologie abilitanti. - Apprendimento automatico ed applicazioni: Classificazione; introduzione al deep learning e all'apprendimento di rappresentazioni; fasi di addestramento e test; misure di valutazione; il bias negli algoritmi. - Visione ed elaborazione di immagini: Percezione nelle macchine; formazione dell'immagine, campionamento, filtraggio e operatori lineari; gradiente dell'immagine, edge e corner; progettare descrittori visuali efficaci (SIFT e feature basate sul gradiente); confronto tra immagini. - Riconoscimento visivo e oltre: "Insegnare ai computer a vedere": bag-of-feature, piramidi spaziali e pooling; apprendimento di rappresentazioni per la visione, reti neurali convoluzionali; R-CNN e segmentazione; descrizione di immagini, scenari multi-modalità e uno sguardo oltre al paradigma di apprendimento supervisionato. - Esercizi pratici: Cosa c'è nella scatola? Come costruire una pipeline di riconoscimento visivo; utilizzare i servizi cognitivi per il riconoscimento / comprensione delle immagini; combinare diversi servizi e modalità.

**Modalità di esame:**

Lo studente deve sviluppare, in accordo con il docente, un piccolo progetto applicativo. Inoltre, lo studente deve presentare una relazione scritta sul progetto svolto, in cui si discutono criticamente tutte le questioni trattate durante la sua realizzazione. L'esame consisterà prevalentemente in una breve presentazione e discussione del progetto svolto, in cui il docente potrà anche chiedere dettagli e/o altri contenuti visti a lezione.

**Criteri di valutazione:**

Il lavoro di progetto e l'esame orale saranno valutati sulla base dei seguenti criteri: a) conoscenza da parte dello studente dei concetti, dei metodi e delle tecnologie alla base dei servizi cognitivi (con particolare enfasi sulle tematiche di visione artificiale); b) capacità dello studente di padroneggiare la tecnologia di implementazione; c) capacità di sintesi, chiarezza e astrazione dello studente, come dimostrato dalla relazione scritta e dal progetto.

**Testi di riferimento:**

CONTENUTO NON PRESENTE

**Eventuali indicazioni sui materiali di studio:**

Le presentazioni mostrate durante le lezioni sono rese disponibili su Moodle come materiale di riferimento.

**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:**

Individual oral exam with questions and exercises on the topics covered during the lectures, including coding of a full-stack Web application. If a large number of students will be attending the exam, part of the exam may be turned into a Moodle quiz. Project to design, develop, implement, code and document an actual full-stack Web application, carried out in student groups via homeworks during the semester + 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:**

Shklar, L. and Rosen, R., Web Application Architecture: Principles, Protocols and Practices. New York, USA: John Wiley & Sons, 2009 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

**Eventuali indicazioni sui materiali di studio:**

The teaching material consists of: - reference book - instructor's slides - suggested readings - examples of homeworks Teaching material will be available on the Moodle platform (<https://elearning.dei.unipd.it/>) for the course. Examples of teaching material and videos from the course are available at: <https://iiaa.dei.unipd.it/education/web-applications/> 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. : Prentice Hall,

**Eventuali indicazioni sui materiali di studio:**

Vengono rese disponibili le trasparenze utilizzate in aula.