**Università degli Studi di L'Aquila - Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica**

# Catalogo Corsi

*Pagina compilata il 18/08/2019*

## Programma del Corso "Teoria dell'Informazione"

- Codice: F0158
- Tipo di corso: Opzionale (Laurea in Informatica percorso Generale), Opzionale (Laurea Magistrale in Informatica percorso GSEEM), Opzionale (Laurea Magistrale in Informatica percorso Generale)
- Livello del corso: Lauree di Primo Livello, Lauree Magistrali
- Semestre: 2

Numero di crediti ECTS: (Laurea Magistrale in Informatica) 6 (carico 150 ore), (Laurea in Informatica) 6 (carico 150 ore)

Docenti: Filippo Mignosi (Filippo.Mignosi@univaq.it)

| | | |
|---|---|---|
| **1** | **Obiettivi del corso** | Lo scopo del corso è quello di fornire agli studenti le conoscenze di alcuni aspetti classici della teoria dell'informazione. In particolare vengono trattati argomenti relativi alla codifica di sorgente, includendo la teoria classica dei codici a blocco, e di compressione dati ma non saranno trattati argomenti di codifica di canale e rumore che sono insegnati in altri corsi presenti nel DISIM. Nella seconda parte vengono insegnati elementi di crittografia moderna. Alla fine delle lezioni, e il superamento dell'esame, lo studente dovrebbe essere in grado di 1) conoscere i fondamenti della teoria dell'Informazione e comprenderne il linguaggi e le nozioni basilari quali Entropia, Mutua informazione, Entropia relativa. 2) Conoscere i primi risultati di Shannon, come il Teorema dell'AEP e le loro conseguenze come la codifica di Shannon per la compressione dati. Conoscere vari tipi di sorgenti. 3) Conoscere la teoria dei codici a blocco e i principali risultati di questa teoria, come la diseguaglianza di Kraft McMillan. 4) Conoscere la codifica di Huffman, la codifica aritmetica e comprendere i differenti tipi di ottimalità che queste codifiche rappresentano quando sono usate su sorgenti I.I.D. 5) Conoscere i compressori di Lempel e Ziv del 1977 e del 1978 e loro varianti e le codifiche di Elias di sequenze di interi. Per quanto riguarda la crittografia moderna gli studenti devono 6) comprendere le distribuzioni di probabilità discreta e saperle applicare nei concetti e risultati successivi. 7) Devono conoscere le nozioni iniziali e basilari della crittografia moderna quali ad esempio di segretezza perfetta e di funzione one-way in termini di distribuzioni e 8) devono comprendere le prove che riguardano i primi teoremi. 9) Devono inoltre avere la capacità di calcolare l'entropia di sorgenti I.I.D. e di catene di Markov semplici, sapere applicare codici a blocco e i compressori studiati a semplici testi, e in generale essere in grado di usare il linguaggio della teoria dell'Informazione classica in modo logico e coerente anche all'interno di dimostrazioni di teoremi. 10) In crittografia gli studenti devono esser in grado di applicare le nozioni acquisite in esercizi classici. Gli studenti devono 11) sapere capire come applicare i concetti di teoria dell'informazione nel mondo reale e avere compreso che l'informazione si paga sempre. 12) riuscire a descrivere gli argomenti del corso con sufficiente rigore matematico, riuscire a descrivere gli algoritmi descritti nel corso in modo completo. Riuscire a formalizzare e a comunicare problemi, idee e soluzioni. 13) sviluppare le competenze necessarie per intraprendere studi successivi con un alto grado di autonomia. Sapere apprendere con facilità argomenti, connessi al corso, di cui si ha solo una parziale conoscenza. |
| **2** | **Contenuti del corso e risultati formativi (descrittori di Dublino)** | Gli argomenti trattati nel corso comprendono:<br>• Il corso è diviso in due parti, la prima di circa quattro crediti formativi tratta la codifica di sorgente in ogni suo possibile aspetto in teoria dell'informazione classica. I restanti due crediti formativi sono dedicati alla introduzione della crittografia moderna. In particolare nella prima parte si studiano l'Entropia, la Mutua informazione e l'Entropia relativa nel caso di sorgenti I.I.D., la diseguaglianza di Jensen e le sue conseguenze. Successivamente si studia il Teorema dell'AEP e tutte conseguenze ovvero limitazioni (bound) sia superiore che inferiore sulla probabilità dell'insieme tipico, la codifica di Shannon per la compressione dati, la definizione e le proprietà dell'insieme più probabile di cardinalità minima e esercizi su quest'ultimo. Si Studiano le catene di Markov e si studia come calcolare la loro entropia e si accenna alle sorgenti HMM. Si studia la teoria dei codici a blocco e i principali risultati di |

| | | |
|---|---|---|
| | | questa teoria, come la diseguaglianza di Kraft McMillan e sue conseguenze. Viene descritto l'algoritmo di Huffman e se ne dimostra l'ottimalità all'interno di tutti i codici prefissi. Si descrive la codifica aritmetica e si prova l'ottimalità per sorgenti I.I.D. nel senso che si prova la convergenza all'entropia. Vengono descritti i compressori di Lempel e Ziv del 1977 e del 1978 e loro varianti e le codifiche di Elias di sequenze di interi al fine di completare la descrizione dell'algoritmo LZ77. Per quanto riguarda la crittografia moderna vengono date le nozioni iniziali e basilari della crittografia moderna quali ad esempio di segretezza perfetta e di funzione one-way in termini di distribuzioni e vengono date le prove che riguardano i primi teoremi che connettono queste nozioni con le classi P ed NP.<br>• <br>• <br><br>Alla fine del corso, lo studente dovrebbe:<br>• Lo scopo del corso è quello di fornire agli studenti le conoscenze di alcuni aspetti classici della teoria dell'informazione. In particolare vengono trattati argomenti relativi alla codifica di sorgente, includendo la teoria classica dei codici a blocco, e di compressione dati ma non saranno trattati argomenti di codifica di canale e rumore che sono insegnati in altri corsi presenti nel DISIM. Nella seconda parte vengono insegnati elementi di crittografia moderna. Alla fine delle lezioni, e il superamento dell'esame, lo studente dovrebbe essere in grado di<br><br>1. conoscere i fondamenti della teoria dell'Informazione e comprenderne il linguaggi e le nozioni basilari quali Entropia, Mutua informazione, Entropia relativa.<br>2. Conoscere i primi risultati di Shannon, come il Teorema dell'AEP e le loro conseguenze come la codifica di Shannon per la compressione dati. Conoscere vari tipi di sorgenti. 3) Conoscere la teoria dei codici a blocco e i principali risultati di questa teoria, come la diseguaglianza di Kraft McMillan. 4) Conoscere la codifica di Huffman, la codifica aritmetica e comprendere i differenti tipi di ottimalità che queste codifiche rappresentano quando sono usate su sorgenti I.I.D. 5) Conoscere i compressori di Lempel e Ziv del 1977 e del 1978 e loro varianti e le codifiche di Elias di sequenze di interi. Per quanto riguarda la crittografia moderna gli studenti devono 6) comprendere le distribuzioni di probabilità discreta e saperle applicare nei concetti e risultati successivi. 7) Devono conoscere le nozioni iniziali e basilari della crittografia moderna quali ad esempio di segretezza perfetta e di funzione one-way in termini di distribuzioni e 8) devono comprendere le prove che riguardano i primi teoremi.<br>3. Devono inoltre avere la capacità di calcolare l'entropia di sorgenti I.I.D. e di catene di Markov semplici, sapere applicare codici a blocco e i compressori studiati a semplici testi, e in generale essere in grado di usare il linguaggio della teoria dell'Informazione classica in modo logico e coerente anche all'interno di dimostrazioni di teoremi.<br>4. In crittografia gli studenti devono esser in grado di applicare le nozioni acquisite in esercizi classici. Gli studenti devono 11) sapere capire come applicare i concetti di teoria dell'informazione nel mondo reale e avere compreso che l'informazione si paga sempre.<br>5. riuscire a descrivere gli argomenti del corso con sufficiente rigore matematico, riuscire a descrivere gli algoritmi descritti nel corso in modo completo. Riuscire a formalizzare e a comunicare problemi, idee e soluzioni.<br>6. sviluppare le competenze necessarie per intraprendere studi successivi con un alto grado di autonomia. Sapere apprendere con facilità argomenti, connessi al corso, di cui si ha solo una parziale conoscenza. |
| **3** | **Prerequisiti** | Indispensabili: avere conoscenze di base di teoria della probabilità e di matematica discreta. |
| **4** | **Modalita' e lingua di insegnamento** | Le lezioni sono di norma frontali e si fanno poche prove in itinere di autovalutazione che sono comunque completate da spiegazioni frontali e vengono fatti gli esercizi strettamente necessari alla capacità di applicare la conoscenza acquisita Si cerca di rendere la didattica centrata sugli studenti anche con domande iniziali sulle attese da parte dei frequentanti relativamente allo svolgimento corso, ai contenuti e alle modalità di |

| | | |
|---|---|---|
| | | valutazione. Si stimola la creazione di gruppi di discussione sia con che senza il docente relativamente alla materia di studio e si stimola la discussione incrociata. Si stimolano gli studenti a porre domande e al senso critico. Tra i metodi didattici si usano anche tecniche motivazionali come i riferimenti a fatti recenti di cronaca per suscitare interesse. La verifica formativa viene vista come metodo didattico e su molti argomenti si spiega quali saranno le modalità di verifica su quello specifico argomento e questo genera attenzione.<br>**Lingua**: Italiano<br>**Testi/Bibliografia**<br>• Arora, Barak, ***Computational Complexity: A Modern Approach,*** . Cambridge University press . 2009.<br>• Cover e Thomas, ***Elements of Information Theory***. 2006.<br>• Amir Said, ***Introduction to Arithmetic Coding- Theory and Practice***. *https://www.hpl.hp.com/techreports/2004/HPL-2004-76.pdf* |
| **5** | **Metodi di accertamento** | Viene fatto uno scritto che viene chiamato “interattivo”. Difatti dopo che lo studente ha risposto alle prime domande riguardanti concetti e definizioni e prove basilari e necessarie al superamento dell’esame, la correzione viene fatta insieme allo studente stesso e, di norma, vengono fatte domande in funzione delle risposte date, ovvero dalla precisione, correttezza, capacità espositiva dello studente, dalla capacità logica dimostrata. Questo avviene in più fasi analoghe sino a quando la commissione non raggiunge un giudizio ritenuto valido e affidabile. In generale uno studente deve conoscere le definizioni di base e le tecniche fondamentali per potere superare l’esame e successivamente il voto inoltre crescerà anche in proporzione agli argomenti in cui è stato capace di rispondere e anche, e ci ripetiamo, in funzione delle risposte date, ovvero dalla precisione, correttezza, capacità espositiva dello studente, dalla capacità logica dimostrata. In particolare per valutare la capacità di applicare conoscenza e comprensione e anche le capacità di apprendimento si valuteranno le capacità degli studenti di capire e integrare e completare insieme al docente che compie l’esame dimostrazioni e ragionamenti logici su 1) argomenti connessi a corso ma che non sono stati strettamente trattati come argomenti del corso o discussione sugli argomenti più avanzati in caso di studenti con una valutazione vicino al massimo oppure 2) argomenti in cui gli studenti abbiano manifestato incertezze o imprecisioni per vedere se riescono ad essere più certi o precisi. A volte si chiede anche una autovalutazione da parte dello studente a cui segue una discussione. Dato che la parte del corso che tratta crittografia moderna è molto sofisticata, verrà dato meno peso a imprecisioni e carenze su di essa al fine del voto finale. |