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

Catalogo Corsi

Pagina compilata il 22/07/2019

Programma del Corso "Combinatorics and Cryptography"

- Codice: DT0051
- Tipo di corso: Opzionale (Laurea Magistrale in Matematica percorso Generale), Opzionale (Laurea Magistrale in Ingegneria Matematica percorso Comune)
- Livello del corso: Lauree Magistrali
- Semestre: 2

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

Docenti: Norberto Gavioli (gavioli@univaq.it)

1	**Obiettivi del corso**	Allo studente sarà richiesta una conoscenza di base degli argomenti presentati e capacità di implementare in un linguaggio di programmazione alcuni degli algoritmi presentati.
2	**Contenuti del corso e risultati formativi (descrittori di Dublino)**	Gli argomenti trattati nel corso comprendono: • Abstract: Basic cryptograpy and coding theory will be developed. Some protocols and algorithms will be discussed focusing an security and data integrity. • Programme: Elementary arithmetics: Integers, divisibility, prime numbers, Euclidean division and g.c.d., Congruence classes, Chinese remainder theorem, cyclic and abelian groups, Lagrange theorem, Euler theorem, the structure of invertible classes mod p^n, Fields with p elements, polynomials, Euclidean division and g.c.d., Congruence classes of polynomials, Finite fields, primitive elements and polynomials, Legendre/Jacoby symbols and quadratic reciprocity. Cryptography: Classical cryptosystems: Shift cyphers, Vigenère Chipher, Substitution Chiper, One time pads, LFSR Data Encryption Standard: Simplified DES and differential cryptanalysis, Attacks, password encryption RSA: the algorithm, Attacks, Primality testing, the public key concept. Discrete logarithms: Bit commitment, Diffie-Helman Key exchange, ELGAMAL Hash function: SHA, birthday attacks Digital signatures: RSA signatures, Hashing and signing, DSA Error correcting codes: Binary block codes, distance and correction of errors, classical bounds, linear codes, cyclic codes, Hamming codes, BCH and Reed-Solomon codes.
3	**Prerequisiti**	
4	**Modalita' e lingua di insegnamento**	Lezioni in classe **Lingua**: Inglese **Testi/Bibliografia** • Wade Trappe, Lawrence C. Washington, ***ntroduction to cryptography: with coding theory 2nd ed.***. Pearson Prentice Hall. 2006.
5	**Metodi di accertamento**	Esame Orale