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

Course catalogue

Page compiled on 24/07/2019

Programme of Course "Combinatorics and Cryptography"

- Code: DT0051
- Type of course unit: Elective (Master Degree in Mathematics curriculum Generale), Elective (Master Degree in Mathematical Engineering curriculum Comune)
- Level of course unit: Postgraduate Degrees
- Semester: 2

Number of ects credits: (Master Degree in Mathematics) 6 (workload 150 hours), (Master Degree in Mathematical Engineering) 6 (workload 150 hours)

Teachers: Norberto Gavioli (gavioli@univaq.it)

1	**Course objectives**	The student will be requested to have a good preparation on the presented topics, and to be able to implement some of the algorithms in a programming language
2	**Course content and learning outcomes (dublin descriptors)**	Topics of the module include: • 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	**Course prerequisites**	
4	**Teaching methodsand language**	Lectures to be attended in class **Language**: English **Reference textbooks** • Wade Trappe, Lawrence C. Washington, ***ntroduction to cryptography: with coding theory 2nd ed.***. Pearson Prentice Hall. 2006.
5	**Assessment methods**	oral examination