



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	<b>Course objectives</b>	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	<b>Course content and learning outcomes (dublin descriptors)</b>	<p>Topics of the module include:</p> <ul style="list-style-type: none"> <li>• Abstract: Basic cryptography and coding theory will be developed. Some protocols and algorithms will be discussed focusing on security and data integrity.</li> <li>• 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 <math>p^n</math>, Fields with <math>p</math> 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 Cipher, Substitution Cipher, 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.</li> </ul>
3	<b>Course prerequisites</b>	
4	<b>Teaching methods and language</b>	<p>Lectures to be attended in class</p> <p><b>Language:</b> English</p> <p><b>Reference textbooks</b></p> <ul style="list-style-type: none"> <li>• Wade Trappe, Lawrence C. Washington, <i>Introduction to cryptography: with coding theory 2nd ed.</i>. Pearson Prentice Hall. 2006.</li> </ul>
5	<b>Assessment methods</b>	oral examination