UNIVERSITÀ DEGLI STUDI DI PALERMO

DEPARTMENT	Matematica e Informatica
ACADEMIC YEAR	2020/2021
MASTER'S DEGREE (MSC)	COMPUTER SCIENCE
SUBJECT	THEORY OF CODES AND CRYPTOGRAPHY
TYPE OF EDUCATIONAL ACTIVITY	C
AMBIT	20903-Attività formative affini o integrative
CODE	17972
SCIENTIFIC SECTOR(S)	MAT/03
HEAD PROFESSOR(S)	FALCONE GIOVANNI Professore Associato Univ. di PALERMO
OTHER PROFESSOR(S)	
CREDITS	6
INDIVIDUAL STUDY (Hrs)	102
COURSE ACTIVITY (Hrs)	48
PROPAEDEUTICAL SUBJECTS	
MUTUALIZATION	
YEAR	1
TERM (SEMESTER)	1° semester
ATTENDANCE	Not mandatory
EVALUATION	Out of 30
TEACHER OFFICE HOURS	**FALCONE GIOVANNI** Tuesday 14:00 17:00 Dipartimento di Matematica e InformaticaVia Archirafi 34, PalermoStanza 107

DOCENTE: Prof. GIOVANNI FALCONE

PREREQUISITES	Modular arithmetic. Elements of linear algebra: vector spaces, bases, matrix calculus. GCD Euclidean algorithm . Elements of geometry: loci of the plane.
LEARNING OUTCOMES	Knowledge and understanding: At the end of the course the student will acquire the scientific method of investigation that covers the use of mathematical tool, particularly of Discrete Mathematics, supporting information technology and its applications, with obvious reference to telecommunications. Applying knowledge and understanding: The student will be able to use methods and conceptual tools of abstract algebra to solve problems such as: the implementation of a linear code that can determine, and possibly correct, a given number of errors; the implementation of a public key encryption scheme and the analysis of the computational costs of encryption and decryption to authorized/non-authorized users. Making judgements: Through guided exercises, the student will be able to evaluate the difficulty of a coding problem, encryption and decryption, and to choose the most simple strategies to face and solve the corresponding algebraic problems, thus recognizing the usefulness of the studied algorithms. Communication: The student, through the creation of study groups, will acquire, according to her/his individual skill, the ability to communicate and express issues concerning the arguments of the course. She/he must be able to write a solution to a problem in a rigorous and correct form. Lifelong learning skills: The student will face with abstract algebra applications with very concrete models which will give a strong motivation towards the epistemological process of synthesis and analysis. At the end of the course she/he will have acquired the tools for a synthesis of seemingly distant subjects.
ASSESSMENT METHODS	The final grading is based on a written exam and the oral discussion of a topic. The evaluation takes into account the way the candidate explains his/her results or errors in the written part which is therefore just a fulcrum for the following oral discussion. It will be made on the basis of following conditions: 1) Basic knowledge of the proposed topics and limited capacity to apply them independently; sufficient capacity to carry out a rigorous reasoning and sufficient command of the language (18-21 rating); 2) Fairly good knowledge of the proposed topics and sufficient capacity to apply them independently; fairly good ability to complete a rigorous reasoning and good appropriate language (22-25 rating); 3) Good knowledge of the proposed topics and fairly good capacity to apply them independently; good ability to complete a rigorous reasoning; good command of the appropriate language (26-28 rating); 4) Very good and extensive knowledge of the proposed topics; ability to apply them with mathematical rigour and independently; possession of very good communication skills (29-30L rating).
EDUCATIONAL OBJECTIVES	To get the understanding of mathematical concepts supporting the IT disciplines related to telecommunications, such as: linear codes, Reed-Solomon codes, Goppa codes. public key cryptography on Galois fields and on elliptic and hyperelliptic curves: RSA, ElGamal. Digital signature. Cryptanalytic algorithms such as Baby step - Giant step, Pollard rho algorithm, quadratic sieve.
TEACHING METHODS	The course consists of a series of class lectures. Each result will be illustrated by giving examples and introducing exercises. Lecture notes will be distributed containing all the discussed topics. Further suggested reading on Coding theory are chapters "Basic Binary Codes", "The Factorization of Polynomials Over Finite Fields". "The Enumeration of Information Symbols in BCH Codes" [1], while on Criptography chapters 2, 3, 8 e 11 in [2] are recommended.
SUGGESTED BIBLIOGRAPHY	1) Elwyn R. Berlekamp, Algebraic Coding Theory, Aegean Park Press 1984 Per eventuali approfondimenti, si suggerisce la lettura dei capitoli "Basic Binary Codes", "The Factorization of Polynomials Over Finite Fields". "The Enumeration of Information Symbols in BCH Codes"./ Further suggested reading are chapters "Basic Binary Codes", "The Factorization of Polynomials Over Finite Fields". "The Enumeration of Information Symbols in BCH Codes", 2) Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone; Handbook of Applied Cryptography, CRC Press 1996 Per eventuali approfondimenti, si suggerisce la lettura dei capitoli 2, 3, 8 e 11 / Further suggested reading are chapters 2, 3, 8 e 11. 3) Dispensa del corso / Lecture notes La dispensa contiene tutti gli argomenti trattati in aula./Lecture notes contain all

	the discussed topics.

SYLLABUS

Hrs	Frontal teaching
4	Elements of Field theory
6	Linear codes: Hamming codes, Hadamard codes
6	Perfect codes. Cyclic codes.
6	Reed-Solomon codes, BCH codes.
4	Symmetric key criptography: background (substitution ciphers, Vigenere code, criptanalysis, Kasiski method). Vernam cipher (one-time pad).
6	Public key criptography: RSA, ElGamal. Digital signature. Hashing.
6	Baby step-Giant step, Pollard rho algorithm, quadratic sieve.
5	Elements of Projective geometry: elliptic and hyperelliptic curves.
5	Criptography algorithm on elliptic curves: Lenstra algorithm, ElGamal algorithm on elliptic and hyperelliptic curve. Goppa code.