UNIVERSITA' DEGLI STUDI MEDITERRANEA DI REGGIO CALABRIA

Subject Code	**16529**
Subject Name	**Theory of cryptography**
Professor	**Vittoria Bonanzinga**
Department:	**DIIES**
Degree course:	**Computer Engineering and Systems for Telecommunications**
Class:	**LM27**
Type of educational activity:	
Disciplinary Area:	**Geometry**
Scientific-Disciplinary Sector:	**MAT/03**
Compulsory preliminary exams:	**NO**
Course Year:	**II**
Semester:	**II**
ECTS:	**6**
Hours:	**48**

Synthetic description:

Introduction to the basic concepts and results in number theory and cryptography: divisibility, Euclidean algorithm, congruences, factorization, finite fields and quadratic residues, cryptosystem, public and private key, RSA, discrete logarithm, primality and factorization, elliptic curves.

Acquisition of knowledge on:

Knowledge of the basics of Algebra, Number Theory and the Geometry of which are essential in the development of cryptographic protocols. Knowledge of the tools and techniques of Algebra, number theory and geometry for the study of cryptographic protocols. Ability to understand and use appropriate mathematical tools to solve problems of cryptography. Ability to communicate the knowledge gained through an appropriate scientific-technical language.

Evaluation method:

Written and oral tests

Student's independent work

For each credit 18 hours of individual study must be undertaken

Detailed course program

- Integers and finite fields, modular arithmetic, Euler function, Chinese remainder theorem. Structu.re of Z/pZ. Gauss' theorem: the existence of primitive roots.

- Primality and factorization: Consequences of Fermat's little theorem, pseudoprimes numbers, some primality test (Fermat, Miller-Rabin), method (p-1) for the factorization of Pollard. Complexity of the algorithms.

- Symmetric cryptographic systems and public key cryptography: RSA. Diffie and Hellman cryptosystem. The discrete logarithm problem.

- Elliptic curves: Weierstrass equation, the group of points of an elliptic curve, elliptic curves over finite fields. Cryptosystems based on elliptic curves: exchange of key Diffie-Hellman, ElGamal protocol.

- -Factoring with elliptic curves, primality test with elliptic curves.

Resources and main references

1.N. Koblitz. A Course in Number Theory and Cryptography, Second Edition, Springer, 1994.
2. A. Languasco, A. Zaccagnini. Introduzione alla Crittografia, Ulrico Hoepli Editore, Milano, 2004.