

Course guide

200256 - CRIPTOG - Cryptography

Last modified: 24/05/2026

Unit in charge: School of Mathematics and Statistics
Teaching unit: 749 - MAT - Department of Mathematics.

Degree: BACHELOR'S DEGREE IN MATHEMATICS (Syllabus 2009). (Optional subject).

Academic year: 2026 **ECTS Credits:** 6.0 **Languages:** English

LECTURER

Coordinating lecturer: ROBERTO GUALDI

Others: Primer quadrimestre:
ROBERTO GUALDI - A

PRIOR SKILLS

Some basic knowledge of algebra (group theory, finite fields), algebraic geometry and complexity theory is desirable, but not strictly required.

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:

GM-CE2. CE-2. Solve problems in Mathematics, through basic calculation skills, taking in account tools availability and the constraints of time and resources.

GM-CE4. CE-4. Have the ability to use computational tools as an aid to mathematical processes.

GM-CE6. Ability to solve problems from academic, technical, financial and social fields through mathematical methods.

Generical:

GM-CB5. To have developed those learning skills necessary to undertake further interdisciplinary studies with a high degree of autonomy in scientific disciplines in which Mathematics have a significant role.

GM-CG1. CG-1. Show knowledge and proficiency in the use of mathematical language.

GM-CB4. CB-4. Have the ability to communicate their conclusions, and the knowledge and rationale underpinning these to specialist and non-specialist audiences clearly and unambiguously.

GM-CG2. CG-2. Construct rigorous proofs of some classical theorems in a variety of fields of Mathematics.

GM-CG3. CG-3. Have the ability to define new mathematical objects in terms of others already know and ability to use these objects in different contexts.

GM-CG4. CG-4. Translate into mathematical terms problems stated in non-mathematical language, and take advantage of this translation to solve them.

GM-CG6. CG-6 Detect deficiencies in their own knowledge and pass them through critical reflection and choice of the best action to extend this knowledge.

Transversal:

04 COE. EFFICIENT ORAL AND WRITTEN COMMUNICATION. Communicating verbally and in writing about learning outcomes, thought-building and decision-making. Taking part in debates about issues related to the own field of specialization.

07 AAT. SELF-DIRECTED LEARNING. Detecting gaps in one's knowledge and overcoming them through critical self-appraisal. Choosing the best path for broadening one's knowledge.

TEACHING METHODOLOGY

LEARNING OBJECTIVES OF THE SUBJECT

STUDY LOAD

Type	Hours	Percentage
Hours small group	30,0	20.00
Hours large group	30,0	20.00
Self study	90,0	60.00

Total learning time: 150 h

GRADING SYSTEM

30% final exam, 40% final report and oral presentation, 30% deliverables

BIBLIOGRAPHY

Basic:

- Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H. An introduction to mathematical cryptography [on line]. New York: Springer, 2014 Available on: <https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/978-0-387-77993-5>. ISBN 9781493917105.
- Koblitz, Neal. A Course in number theory and cryptography. 2nd ed. New York: Springer-Verlag, cop. 1994. ISBN 0387942939.
- Washington, Lawrence C. Elliptic curves : number theory and cryptography . Boca Raton [etc.] : CRC Press, cop. 2003. ISBN 978-1584883654.

Complementary:

- Delfs, Hans; Knebl, Helmut. Introduction to cryptography : principles and applications [on line]. Berlin: Springer, 2015 Available on: <https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=6314866>. ISBN 9783662479735.
- Katz, Jonathan; Lindell, Yehuda. Introduction to modern cryptography [on line]. Boca Raton: Taylor & Francis Group, 2021 [Consultation: 19/06/2025]. Available on: <https://www-taylorfrancis-com.recursos.biblioteca.upc.edu/books/mono/10.1201/9781351133036/introduction-modern-cryptography-yehuda-lindell-jonathan-katz>. ISBN 9781466570269.
- Galbraith, Steven D. Mathematics of public key cryptography [on line]. Cambridge University Press, 2012 [Consultation: 13/07/2022]. Available on: <https://www.cambridge.org/core/books/mathematics-of-public-key-cryptography/DDDFA3874A53C4E6846EB3AB06161E43>. ISBN 9781107013926.