Cryptography

Academic Year: (2020 / 2021) **Review date: 10-07-2020**

Department assigned to the subject: Computer Science and Engineering Department

Coordinating teacher: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Type: Compulsory ECTS Credits : 6.0

Year : 2 Semester : 1

OBJECTIVES

CB1.Students have demonstrated knowledge and understanding in a field of study that builds upon their general secondary education, and is typically at a level that, whilst supported by advanced textbooks, includes some aspects that will be informed by knowledge of the forefront of their field of study
CB2.Students can apply their knowledge and understanding in a manner that indicates a professional approach to their work or vocation, and have competences typically demonstrated through devising and sustaining arguments and solving problems within their field of study
CB3.Students have the ability to gather and interpret relevant data (usually within their field of study) to inform judgments that include reflection on relevant social, scientific or ethical issues
CB4.Students can communicate information, ideas, problems and solutions to both specialist and non-specialist audiences
CB5.Students have developed those learning skills that are necessary for them to continue to undertake further study with a high degree of autonomy
CG1.Students are able to demonstrate knowledge and understanding of concepts in mathematics, statistics and computation and to apply them to solve problems in science and engineering with an ability for analysis and synthesis.
CG3.Students can solve computationally with the help of the most advanced computing tools mathematical models coming from applications in science, engineering, economy and other social sciences.
CG4.Students are able to show that they can analyze and interpret, with help of computer science, the solutions obtained from problems associated to real world mathematical models, discriminating the most relevant behaviours for each application.
CG6.Students can search and use bibliographic resources, in physical or digital support, as they are needed to state and solve mathematically and computationally applied problems arising in new or unknown environments or with insufficient information.
CE10.Students have shown that they know and understand the algorithmic procedures to design and build programs that solve mathematical problems paying special attention to performance.
CE15.Students have shown that they know the mathematical foundations of cryptography and that they understand the advantages and limitations of different cryptographic algorithms.
RA1.To have acquired sufficient knowledge and proved a sufficiently deep comprehension of the basic principles, both theoretical and practical, and methodology of the more important fields in science and technology as to be able to work successfully in them;
RA3.To be able to search for, collect and interpret relevant information and data to back up their conclusions including, whenever needed, the consideration of any social, scientific and ethical aspects relevant in their field of study;
RA4.To be able to successfully manage themselves in the complex situations that might arise in their academic or professional fields of study and that might require the development of novel approaches or solutions;
RA5.To be able to communicate, in a precise and clear manner, knowledge, methodologies, ideas, problems and solutions in their field or specialty to any kind of audience (specialist or not);
RA6.To be aware of their own shortcomings and formative needs in their field of specialty, and to be able to plan and organize their own training with a high degree of independence.

DESCRIPTION OF CONTENTS: PROGRAMME

1.- Introduction to information technology security.
2.- Mathematical foundations of cryptography.
3.- Introduction to cryptography.
4.- Classic cryptography and cryptanalysis.
5.- Symmetric encryption.

6.- Summary functions and MAC.
7.- Asymmetric encryption.
8.- Keys generation and distribution.
9.- Digital encryption cypher.
10.- Public key infrastructure.
11.- User authentication

LEARNING ACTIVITIES AND METHODOLOGY

AF1.THEORETICAL-PRACTICAL CLASSES. Knowledge and concepts students must acquire. Student receive course notes and will have basic reference texts to facilitatefollowing the classes and carrying out follow up work.Students partake in exercises to resolve practical problems and participatein workshops and an evaluation tests, all geared towards acquiring the necessary capabilities.Subjects with 6 ECTS are44 hours as a general rule/ 100% classroom instruction
AF2.TUTORING SESSIONS. Individualized attendance (individual tutoring) or in-group (group tutoring) for students with a teacher.Subjects with 6 credits have 4 hours of tutoring/ 100% on- site attendance.
AF3.STUDENT INDIVIDUAL WORK OR GROUP WORK.Subjects with 6 credits have 98 hours/0% on-site.
AF8.WORKSHOPS AND LABORATORY SESSIONS. Subjects with 3 credits have 4 hours with 100% on-site instruction. Subjects with 6 credits have 8 hours/100% on-site instruction.
MD1.THEORY CLASS. Classroom presentations by the teacher with IT and audiovisual support in which the subject`s main concepts are developed, while providing material and bibliography to complement student learning.
MD2.PRACTICAL CLASS. Resolution of practical cases and problem, posed by the teacher, and carried out individually or in a group.
MD3.TUTORING SESSIONS. Individualized attendance (individual tutoring sessions) or in-group (group tutoring sessions) for students with teacher as tutor. Subjects with 6 credits have 4 hours of tutoring/100% on-site.
MD6.LABORATORY PRACTICAL SESSIONS. Applied/experimental learning/teaching in workshops and laboratories under the tutor's supervision.

ASSESSMENT SYSTEM

SE1.FINAL EXAM. Global assessment of knowledge, skills and capacities acquired throughout the course.The percentage of the evaluation varies for each subject between 60% and 0%.
SE2.CONTINUOUS EVALUATION. Assesses papers, projects, class presentations, debates, exercises, internships and workshops throughout the course.The percentage of the evaluation varies for each subject between 40% and 100% of the final grade.
A minimum grade might be required at the final exam.

% end-of-term-examination:	20
% of continuous assessment (assigments, laboratory, practicals…):	80

BASIC BIBLIOGRAPHY

- Jean-Philippe Aumasson Serious Cryptography: A Practical Introduction to Modern Encryption , Random House LCC US .
- W. STALLINGS CRYPTOGRAPHY AND NETWORK SECURITY. (5ª EDICIÓN), PRENTICE HALL.