Electronic security systems

Academic Year: (2019 / 2020) **Review date: 27/03/2017 12:48:01**

Department assigned to the subject: Electronic Technology Department

Coordinating teacher:

Type: Electives ECTS Credits : 3.0

Year : 1 Semester : 2

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

No further requirement, but those needed to be admitted In the Master Course.

OBJECTIVES

CB7. Can apply their knowledge and understanding, and problem solving abilities in new or unfamiliar environments within broader (or multidisciplinary) context related to their field of study.
CB8. Have the ability to integrate knowledge and handle complexity, and formulate judgments with incomplete or limited information, but that include reflecting on social and ethical responsibilities linked to the application of their knowledge and judgments.
CG1. Can write information clearly and concisely in a technical report, including action plans, and resources needed to accomplish the development, integration and implementation of complex and high added value electronic systems.
CG2. Have demonstrated the ability to conceive, design, implement and maintain an electronic system in a specific application.
CG4. Can establish effective working relationships among team members and solving problems and making decisions in multidisciplinary teams.

DESCRIPTION OF CONTENTS: PROGRAMME

Electronic security systems. Security is a growing need in today's society. Electronic systems are contributing greatly to the improvement of safety in the individual mobility, banking, information exchange form. Different people recognition techniques for use in identification systems (compared to a database) or authentication is described. There will be a greater emphasis on technology Smart Card and Biometric Recognition in (fingerprint, iris, voice, face, etc..). Different complementary techniques taking into account requirements of cost, speed and consumption are also described. Existing mechanisms to ensure confidentiality and authentication of the information security will be studied, as well as access to information and services. Finally the evaluation of these solutions will be discussed, as well as potential points of vulnerability and the main strategies to combat fraud.
program:
1 - Introduction to Identification Systems
2 - Identification Cards
3 - Smart Cards
4 - Security in Information Transmission
5 - Biometric Identification

LEARNING ACTIVITIES AND METHODOLOGY

LEARNING ACTIVITIES:
- Theoretical lectures
- Theoretical-Practical lectures
- Office hours
- Work-sharing homework
- Individual homework

METHODOLOGY:
- Professor dissertations using computer and audiovisual means, explaining the main concepts involved and providing those relevant references to allow students to get more in depth in the subject.
- Critical reading of international references recommended by the professor.
- Journal papers, reports and manuals for further discussion in class, to enhance and consolidate the knowledge acquired.
- Solving practical cases, presented by the professor to the students either individually or in groups
- Presentation and discussion in class, under the moderation of the professor, of subjects related to the course.
- Development of individual or group reports.

ASSESSMENT SYSTEM

% end-of-term-examination/test:	60
% of continuous assessment (assigments, laboratory, practicals…):	40

The evaluation of the course will be based on the following criteria:
1.- Individual/Group homework: A couple of proposed works (potentially one Individual and the other in groups). Each of them is weighted 20% of the total grade.
2.- Course Final Exam: At the end of the course, a written exam Is given covering the whole course material,accounting for 60% of the total grade.