Tecnologies de la Informació i Seguretat 2014/2015

Code: 43341
ECTS Credits: 6

Degree	Type	Year	Semester
4314660 Computer Engineering	OB	1	1

Contact

Name: Joaquim Borges Ayats
Email: Joaquim.Borges@uab.cat

Use of languages

Principal working language: anglès (eng)
Some groups entirely in English: No
Some groups entirely in Catalan: Yes
Some groups entirely in Spanish: No

Teachers

Jordi Herrera Joancomarti
Mercè Villanueva Gay

Prerequisites

No needed.

Objectives and Contextualisation

The objective of this module consists of providing an introduction to information processing, emphasizing the mathematical theory of information and its treatment, the encoding for error correction, techniques and cryptographic encoding for the security of the information, applications to communications networks, and the design of applications.

Skills

- Design, develop, manage and evaluate mechanisms for certifying and guaranteeing data security in a local or distributed processing system.
- Direct work on computer systems, complying with current rules and guidelines and safeguarding the quality of the service.
- Display a capacity for general and technical management and management of research, development and innovation projects in companies and technology centres, in the field of computer engineering.
- Display a spirit of enterprise and innovation and a wide-ranging vision in the search for new areas to explore in a specific field of the computer engineering profession.
- Integrate and apply the knowledge acquired and solve problems in new or little-known situations within broader (or multidisciplinary) contexts.
- Integrate knowledge and use it to make judgements in complex situations, with incomplete information, while keeping in mind social and ethical responsibilities.
- Propose, calculate and design products, processes and installations in all areas of computer engineering.
- Responsibly manage information and knowledge when leading multidisciplinary groups and/or projects.
- Understand and apply the workings and organisation of internet, new-generation network technologies and protocols, models of components, intermediary software and services.

- Undertake mathematical modelling, calculation and simulation in technological centres and engineering companies, especially in research, development and innovation tasks in all areas related to computer engineering.
- Use acquired knowledge as a basis for originality in the application of ideas, often in a research context.

Learning outcomes

1. Decide on the most suitable type of coding for the characteristics of the signal and the transmission channel.
2. Direct work on computer systems, complying with current rules and guidelines and safeguarding the quality of the service.
3. Display a capacity for general and technical management and management of research, development and innovation projects in companies and technology centres, in the field of computer engineering.
4. Display a spirit of enterprise and innovation and a wide-ranging vision in the search for new areas to explore in a specific field of the computer engineering profession.
5. Evaluate the security of network protocols on the basis of the cryptographic components used.
6. Integrate and apply the knowledge acquired and solve problems in new or little-known situations within broader (or multidisciplinary) contexts.
7. Integrate knowledge and use it to make judgements in complex situations, with incomplete information, while keeping in mind social and ethical responsibilities.
8. Propose, calculate and design products, processes and installations in all areas of computer engineering.
9. Responsibly manage information and knowledge when leading multidisciplinary groups and/or projects.
10. Undertake mathematical modelling, calculation and simulation in technological centres and engineering companies, especially in research, development and innovation tasks in all areas related to computer engineering.
11. Use acquired knowledge as a basis for originality in the application of ideas, often in a research context.

Content

Channel encoding (10 sessions)
1. Introduction to information theory
2. Introduction to channel encoding
3. Introduction to finite field with characteristic 2
4. Linear codes over finite fields
5. Decoding methods for linear codes
6. Hamming codes
7. Cyclic codes
8. Algebraic codes I
9. Algebraic codes II
10. Algebraic codes decoding

Security and information hiding (5 sessions)
11. Private key cryptosystems
12. Public key cryptosystems
13. Public key infraestructures
14. Cryptographic protocols I
15. Cryptographic protocols II

Methodology

The methodology will combine classroom work with solving exercises by the students and the teacher. Some of the exercises will be done by the teacher, some other ones will be prepared for the next sesssion in class

and some ones will be done by students theyselves.

We ask the delivery and exhibition of some of these exercises.

Activities

Title	Hours	ECTS	Learning outcomes
Type: Directed			
Lectures	30	1.2	5, 1, 4, 9, 7, 6, 2, 3, 10, 8, 11
Solving exercices	10	0.4	5, 2, 3, 8
Type: Supervised			
Solved exercices exposition	30	1.2	1, 4, 9, 7, 3, 10
Type: Autonomous			
Preparation to solve exercices	75	3	5, 2, 3, 8

Evaluation

The final qualification will take into account the delivered works during the course by the students, support and class participation.
1 Attendance and active participation is mandatory. Faults can be compensated with some extra work. Weight: 30% (minimum: 5 out of 10).
2 Solving exercises on the blackboard and delivery of exercises. Weight: 70% (minimum: 5 out of 10).
To pass the module should get a grade equal to or greater than 5 in each of the sections.

Evaluation activities

Title	Weighting	Hours	ECTS	Learning outcomes
Resolution and delivery of exercices	70%	3	0.12	1, 4, 9, 7, 3, 10
Sessions participation	30%	2	0.08	5, 1, 4, 9, 7, 6, 2, 3, 10, 8, 11

Bibliography

- M.A. Sarasa López J.P. Franco. Criptografía Digital: Fundamentos y Aplicaciones. Prensas Universitarias de Zaragoza, 1998.
- Thomas M. Cover and Joy A. Thomas (1991). Elements of Information Theory, John Wiley & Sons, Inc.
- Robert Ash. Information theory. John Wiley and Sons Inc, 1965.
- F.J. MacWilliams and N.J.A. Sloane. The theory of error-correcting codes. North-Holland, 1977.
- Bruce Schneier, Applied Cryptography, (2nd edition), Wiley, 1995.