Con formato: Arriba: 2,5 cm, Abajo: 2,5 cm, Inicio de sección: Página impar, Ancho: 21 cm, Alto: 29,7 cm, Distancia del encabezado desde el borde: 1,25 cm, Distancia del pie de página desde el borde: 1,25 cm, Primera página diferente

Syllabus of Communication Systems

Course guide
Program of activities

Academic year: 2011 / 2012 **Term:** First
Subject's name: Communication systems
Subject's code: 21978 i 21464
Degree: Bachelor's degree in Telematics Engineering and Bachelor's degree in Computer Sciences
Number of ECTS credits: 4 ECTS
Time commitment: 100 hours
Timing:

Year: Second year
Type: one term subject
Period: First term

Teaching staff: Vanesa Daza and Mathieu De Craene

Group: T1

Course guide

1. Descriptive information on the subject

- **Academic year:** 2011 / 2012

Eliminado: 0

Eliminado: 1

- **Subject's name:** Communication Systems **Code:** 21978 i 21464
- **Type of subject:** Compulsory in Bachelor's degree in Telematics Engineering and Optional in Bachelor's degree in Computer Sciences
- **Degree:** Bachelor's degree in Telematics Engineering and Bachelor's degree in Computer Sciences
- **Number of ECTS credits:** 4
- **Time commitment:** 100 h
- **Timing:**
  - Year: Second year
  - Type: one term subject
  - Period: First term
- **Coordination:** Vanesa Daza and Mathieu De Craene
- **Department:** Department of Information and Communication Technologies
- **Teaching staff:** Vanesa Daza and Mathieu De Craene

Eliminado: , Jorge Hernández

- **Group:** T1 and T2
- **Languages:** Catalan, Spanish and English
- **Building where the subject is taught:** Building 52
- **Timetable:**
  - Mondays 16:30 – 18:30
  - Wednesdays 14:30 – 16:30
  - Fridays 18:30 – 20:30

2. Presentation of the subject

The subject Communication Systems (21978) is a compulsory subject offered in bachelor’s degree of Telematics Engineering at the Universitat Pompeu Fabra. It consists of 4 ECTS credits and is taught in the first term of the second academic year.

This document describes in detail the syllabus of the subject.

On the one hand, during the first half of the trimester, the fundamentals and main applications of cryptology are presented. Cryptology is the science of secret communication. It has two main subfields: cryptography, which is the science of creating secret figures, and cryptanalysis, which is the science of breaking these figures. These cryptographic tools will become essential later in other subjects that look into the security of communications, one important key in developing the information society. Historically, cryptography has always had a special role in diplomatic and military communications and, in recent years, it has become essential in developing the information society.

On the other hand, the second half of the trimester will be dedicated to the introduction of basic concepts for defining a communications system: modulation, channel and noise, filters and demodulation. Then, the focus will be set on source quantification and encoding. May of these topics will be studied more in depth in other subjects, in close relationship with Communication Systems. Although this subject is mainly introductory, his aim is not to be a basic mathematics course for engineers. It requires a good mathematical basis in order to acquire knowledge of signals, Fourier transforms and the main axioms of probability.

Eliminado: This subject is divided into two different parts with regard to their content. T

Eliminado: of the first part

Eliminado: the

Eliminado: that corresponds with the first five weeks of the term.

Eliminado: another part of the subject's main objective is

Eliminado: the

Eliminado: of

Eliminado: . The current basic concepts in any transmission system will be explained

Eliminado: e

Eliminado: subject

Eliminado: the subject will focus

Eliminado: the stages of

Eliminado: It is important to consider that many of the knowledge will be taught in

Eliminado: with a

Eliminado:

Eliminado: However, it is not

Eliminado: because i

Eliminado: t

Eliminado: the

3. Competences to be obtained in the subject

Transferable skills	Specific competences
Instrumental 1. Problems solving. 2. Skill to search and manage information. 3. Capacity of analysis and synthesis. **Interpersonal** 4. Capacity of criticism and self-criticism. 5. Capacity to work in team. **Systemic** 6. Capacity to put the concepts into practice.	7. Using a program for numerical matrices and vector computations (Octave) to represent signals and simulate stages and elements of a communications system. 8. Be able to explain and visualize in Octave the effect of simple elements of a communication system (modulation and quantification) in time and frequency. 9. Know the basic concepts of source coding and its applications in particular examples. 10. Determine the relation between the signal and noise of a transmission system. 11. Know the main steps to quantify and encode sequences of bits. 12. Understand the theoretical fundamentals of classical cryptography. 13. Understand the theoretical fundamentals of modern cryptography, both public and secret key. 14. Apply the necessary knowledge to implement secret and public cryptosystems. 15. Define the main components and applications of cryptography to ensure confidentiality, integrity, authentication and non-repudiation.

Eliminado: of mathematical vector

Eliminado: processing

Eliminado: shared

Eliminado: figures

Eliminado: of shared and private key.

4. Learning objectives

Eliminado: aims

The learning objectives through which this subject contributes, on top of previously acquired competences are:

Eliminado: aims

Eliminado: the

Eliminado: to acquire the

- Apply the mathematic knowledge to the engineering (O1).
- Use the encryption and data protection (O2).
- Recognize the classical encryption algorithms using secret key cryptography (O3).
- Recognise the current encryption algorithms using secret key cryptography (O4).
- Recognise the current encryption algorithms and digital signature with public key cryptography (O5).
- Apply the tools of cryptography to transmit data confidentially with integrity, authenticity and non-repudation (O6).
- Describe the general operation of a digital communication system, identify its components and explain briefly its purpose (O7).
- Identify the advantages of a digital communications system with regard to an analog one (08).
- Transform digital input information through the source coding (O9).
- Calculate the relation between signal to noise in single channel models (O10).
- Use Octave as a program to analyze simple communication systems and study the impact of several parameters on the efficiency of the system (O11).

Eliminado: current

Eliminado: public

5. Contents

- Unit 1. Introduction and basic concepts
  - Steganography concepts. Limits and risks.
  - Concepts of cryptology, cryptography and cryptanalysis.
  - Concepts of confidentiality, authentication, integrity and non-repudiation.
  - Types of attackers: passive and active ones.
  - Concepts of unconditional security and computational security.
- Unit 2. Classical secret key cryptography
  - Cryptosystems of simple substitution and transposition.
  - Cryptosystems of polyalphabetic replacement (Vigenère, Vernam and Rotors machines).

Eliminado: shared-

Eliminado: Figures

Eliminado: Figures

- Unit 3. Modern shared-key cryptography
  - Block cipher (DES and AES)
  - Flow figures (RC4)
  - Authentication protocols of challenge-response based on shared-key figures.
  - Attack against the man in the middle in secret key cryptosystems.

Eliminado: halfway

Eliminado: against shared-key figures.

- Unit 4. Public-key cryptography
  - Operation of the public key cryptosystem.
  - Fundamentals of modular arithmetic.
  - The problem of integer factorization.
  - RSA cryptosystem.
  - The discrete logarithm problem.
  - ElGamal cryptosystem.
  - Digital envelope.
  - Digital signature in RSA and ElGamal
  - Authentication protocols of challenge-response based on public-key cryptosystems.
  - Attack against the man in the middle in public key cryptosystems.

Eliminado: figure

Eliminado: figure

Eliminado: figure

Eliminado: figures

Eliminado: Attack against the man halfway against public-key figures.

- Unit 5. Introduction to communication systems:
  - Digital and analogical communications.
  - Elements of a communication system..
  - Channels.
  - Noise:
    - Random process and signs.
    - Additive white Gaussian noise (AWGN).
    - Probability of error.

- Unit 6. Analogical communications:
  - Definition of modulation.
  - Modulation amplitude.
    - Modulation and demodulation schemes.
    - Power calculation
    - Overmodulation and aliasing
  - Modulation frequency.

- Unit 7. Quantification:
  - Scalar and vector quantization.
  - Quantification error.
  - A-law and μ-law.
  - DPCM:
    - Differential pulse code modulation.
    - Prediction error.
    - Calculation of the relation between signal and noise.
    - ADPCM.
  - DM:
    - Delta modulation.
    - ADM.
  - LPC (Linear Predictive Code) of voice signals.

- Unit 8. Encoding source:
  - Measured information.
  - The source encoding theorem
  - Huffman encoding.

- Lempel-Ziv encoding.

6. Methodology

This subject is given through in-class and virtual sessions. The in-class sessions will be lectures, seminar sessions and sessions in the laboratory. The lectures and sessions in the laboratory will last two hours and the seminar sessions, one hour.

Eliminado: done

Eliminado: face-to-face

Eliminado: face-to-face

In the seminar sessions, one or more activities will be issued to the students to be solved by them in class. Previously, students will have material to prepare the session. They will have to deliver, at the end of the session, the work done to ensure the use of the session seminar. During the resolution of these activities, they will be able to ask any question to the teacher or classmates. In the following days, they will have to write and deliver a document detailing their solution.

Eliminado: T

Eliminado: will be raised

Eliminado: that

Eliminado: necessary

Eliminado: before the beginning

In laboratory sessions students will perform activities in small groups implementing in Octave simple examples of communication systems. Students will have to discuss the results comparing the simple theoretical arguments. A statement will be distributed in each session and students will have to deliver their report in Moodle.

Eliminado: do little

Eliminado: with the computer

The virtual sessions will be devoted to activities in the computer. These activities will consist in the implementation of small programs or the use of cryptographic tools that are freeware. In each of these sessions, students will have to present a document showing the work done.

Eliminado: distributed

All materials of the subject (slides and statements) will be available in Aula Global (the virtual classroom) in the subject's Moodle. Students non-attending the classe could take advantage . This will facilitate tracking of the subject by students who cannot attend class.

When a block is finished, students will have to complete an on-line questionnaire in Moodle about the ended block. The aim is to use multiple choice questionnaires of Moodle as an asynchronous teaching tool that allows supervise the students at the end of each block, with the main purpose to improve student learning. In this way, learning difficulties can have identified, and there is the opportunity to take measures, providing additional support.

Con formato: Fuente: Century Gothic, 11 pt, Diseño: Claro (Blanco)

Eliminado: can not

Con formato: Fuente: Century Gothic, 11 pt, Diseño: Claro (Blanco)

Eliminado: In this way, the support of subject will be facilitated for students who can not attend the class. ¶

Con formato: Diseño: Claro (Blanco)

Eliminado: unit

Eliminado: unit

Eliminado: following

Eliminado: the students

Eliminado: in

Eliminado: ending of each section of the subject's unit

7. Evaluation

The evaluation of the subject is based mainly on the evaluation for competences.

Two different itineraries have been designed to the evaluation of students. On the one hand, an itinerary proposes a continuous evaluation with those learning activities proposed in the subject. On the other hand, there is another itinerary where a large percentage of the evaluation relies on a final exam. Both itineraries are described below.

Eliminado: continuing

Eliminado: assessment

Eliminado: assessment

For those students who follow the continuing assessment, the subject's final mark depends on three factors:

- Delivery of activities in seminar sessions (20%)
- Delivery of practical activities in the laboratory sessions (20%)
- On-line questionnaire at the end of each unit (25%)
- On-line questionnaire at the end of each part (cryptography and communication) of the subject (35%)

Eliminado: raised

Eliminado: raised

In order to be evaluated with the continuing evaluation, and to ensure the acquirement of the competence of the second part of the subject, the student must pass with more than 40% of all questionnaires and in-class and virtual practical activities. In addition, the final mark of the questionnaire has to be more than 40%.

Eliminado: a student can

Eliminado: assessment

Eliminado: ing

Eliminado: face-to-face

In the in-class and virtual activities, the subject's general competences are evaluated. In those cases where the evaluation of these competences is not passed, students must resit them to pass successfully the subject.

Eliminado: face-to-face

Eliminado: practical

Students who choose the second itinerary should follow the continuing assessment doing a global exam at the end of the subject. In this case, the final mark depends on two factors:

- Delivery of the practical activities of the subject, both the face-to-face (although student do not attend class) and virtual ones. It is compulsory to pass the practical activity with more than 40% of the maximum mark to pass the subject (20%).
- A global exam at the end of the subject (80%).

For those who do not pass this first competition, there is a second examination in September. If student pass one of the two parts (cryptography and communication), the student must stand only for the failed part.

Eliminado: sitting

Eliminado: sitting

Eliminado: resit

8. Bibliography and didactic resources

- Basic bibliography
  - Cryptography: theory and practice, Douglas Stinson, Chapman & Hall, CRC, 2006.
  - B. Schneier, Applied cryptography. Wiley. 1996.
  - Digital Commnications: Fundamentals and Applications, Sklar, Bernard.
  - Sistemas de Comunicación, Haykin, Simon S., Limusa Wiley, edición 2002

- Complementary bibliography
  - W. Stallings, Cryptography and network security. Prentice-Hall, 2nd edition. 1999.
  - A. Menezes, P.Oorschot, S.Vanstone, Handbook of applied cryptography. CRC Press. 1997.

  - Communication Systems, Carlson, A. B. Et al., McGraw-Hill, edición 2002.
  - Comunicaciones Digitales, Artés, A. V. et. al., Pearson - Prentice Hall 2007

Con formato: Español (España - alfab. internacional)

Con formato: Español (España - alfab. internacional)

- Didactic resources and teaching material
  - In the subject's Moodle, there will be available for students the teaching material about lectures.
  - In the subject's Moodle, there will be available for students a collection of problems of the seminar sessions.

Program of Activities

Week	*Activity in the classroom* *Group / type of activity*	*Activity outside the classroom* *Group / type of activity*
Week 1	Session 2 : Theory (ST1)	
Week 2	Session 1 : Theory (ST2) Session 2 : Seminar (SS1) Session 3 : Seminar (SS1)	
Week 3	Session 1 : Lab1 Session 2 : Theory (ST3) Session 3 : Seminar (SS2)	Online practical activity 1
Week 4	Session 1 : Seminar (SS2) Session 2 : Theory (ST4) Session 3 : Seminar (SS3)	Online practical activity 2
Week 5	Session 1 : Seminar (SS3) Session 2 : Theory (ST5) Session 3 : Seminar (SS4)	
Week 6	Session 1 : Seminar (SS4) Session 2 : Theory (ST6) Session 3 : Theory (ST7)	
Week 7	Session 1 : Holiday Session 2 : Lab2 Session 3 : Seminar (SS5)	
Week 8	Session 1 : Theory (ST8) Session 2 : - Session 3 : Seminar (SS6)	
Week 9	Session 1 : Theory (ST9) Session 2 : Lab3 Session 3 : Seminar (SS7)	
Week 10	Session 1 : Theory (ST10) Session 2 : - Session 3 : Seminar (SS8)	Online practical activity 3
Week 11	Session 1 : Theory (ST11) Session 2 : - Session 3: -	