Course guide
270131 - C - Cryptography

Last modified: 13/07/2023

Unit in charge: Barcelona School of Informatics
Teaching unit: 749 - MAT - Department of Mathematics.

Degree: BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Optional subject).

Academic year: 2023 **ECTS Credits:** 6.0 **Languages:** Spanish

LECTURER

Coordinating lecturer: FERNANDO MARTÍNEZ SÁEZ

Others: Primer quadrimestre:
FERNANDO MARTÍNEZ SÁEZ - 11, 12
JOSÉ LUIS RUIZ MUÑOZ - 11, 12

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CEC4.2. To demonstrate comprehension, to apply and manage the guarantee and security of computer systems.
CT1.2A. To interpret, select and value concepts, theories, uses and technological developments related to computer science and its application derived from the needed fundamentals of mathematics, statistics and physics. Capacity to solve the mathematical problems presented in engineering. Talent to apply the knowledge about: algebra, differential and integral calculus and numeric methods; statistics and optimization.
CT1.2C. To use properly theories, procedures and tools in the professional development of the informatics engineering in all its fields (specification, design, implementation, deployment and products evaluation) demonstrating the comprehension of the adopted compromises in the design decisions.
CTI2.3. To demonstrate comprehension, apply and manage the reliability and security of the computer systems (CEI C6).
CTI3.1. To conceive systems, applications and services based on network technologies, taking into account Internet, web, electronic commerce, multimedia, interactive services and ubiquitous computation.

Generical:
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.

TEACHING METHODOLOGY

Lectures in which the contents of the subject will be exposed. Lab classes where students solve real situations that can be found in practice.

LEARNING OBJECTIVES OF THE SUBJECT

1.Distinguish between cryptosystems that can be safe and those that are snake oil.
2.Distinguish between public-key and secret-key cryptosystems
3.To understand the main ideas of secret-key cryptosystems.
4.To understand the main ideas of public-key cryptosystems
5.
To understand the idea of digital signature and their role nowadays in internet.

STUDY LOAD

Type	Hours	Percentage
Guided activities	6,0	3.85
Hours large group	30,0	19.23
Hours small group	30,0	19.23
Self study	90,0	57.69

Total learning time: 156 h

CONTENTS

Basic concepts

Description:
Cryptology, Cryptography, and Cryptanalysis.
Classic cryptography and modern cryptography.
Basic techniques: encryption-decryption and signature.
Private key cryptography and public key cryptography.
The mathematical bases of cryptography.

Modern secret key techniques

Description:
Block encryption, Stream ciphers.
Data Encryption Standard: Description, History, Standardisation, Cryptanalysis.
Advanced Encryption Standard: Description, Standardisation.
Operation modes for block-encrypted systems.

Public key encryption

Description:
Multi-precision arithmetic operations. Euclidean algorithms.
Congruences, multiplication group, modular arithmetic, modular exponential, Chinese Remainder Theorem.
Calculation of square roots.
Prime numbers, probabilistic criteria of primeness, random generation of prime numbers.
Factorising integers, current state of the problem.
The discrete algorithm problem: variants over Finite Fields and elliptic curves.
RSA cryptosystem (Rivest, Shamir, Adleman).
ElGamal cryptosystem.
Diffie-Hellman key exchange.

Digital signatures

Description:
Cryptographic hash functions. Secure Hash Standard.
Digital signatures: RSA, DSA and ECDSA
PKI: digital certificates X509, CRL and OCSP.

Cryptographic protocols and standars

Description:
Encryption and decryption transformations. Mixed private key - public key techniques.
Identification schemes and protocols.
SSL.
Micro-payments.
Shared secrets.
Electronic voting.
Watermarks.
SMIME.
PKCS...

New trens in Cryptography

Description:
Lattice-Based Public-Key Cryptography. Hyperelliptic curve cryptography. Quantum Cryptography

ACTIVITIES

Introduction

Specific objectives:
1, 2

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 6h
Theory classes: 2h
Laboratory classes: 2h
Self study: 2h

secrect-key cryptography

Specific objectives:
1, 2, 3

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 22h
Theory classes: 6h
Laboratory classes: 4h
Self study: 12h

Secrect-cryptography test

Specific objectives:
1, 2, 3

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 1h
Guided activities: 1h

public-key cryptography

Specific objectives:
1, 2, 4

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 50h
Theory classes: 12h
Laboratory classes: 8h
Self study: 30h

Digital signature

Specific objectives:
5

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 8h
Theory classes: 4h
Self study: 4h

Protocols and cryptographic standars

Specific objectives:
1

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 19h
Theory classes: 3h
Self study: 16h

public-key test

Specific objectives:
1, 2, 4, 5

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 1h
Guided activities: 1h

New trends in cryptography

Specific objectives:
1, 2

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 5h
Theory classes: 1h
Self study: 4h

eDNI

Specific objectives:
2, 5

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 2h
Laboratory classes: 1h
Self study: 1h

secure email

Specific objectives:
1, 2, 3, 4, 5

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 3h
Laboratory classes: 2h
Self study: 1h

Cryptographic hash functions

Specific objectives:
5

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 3h
Laboratory classes: 1h
Self study: 2h

AES

Specific objectives:
1, 2, 3

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 11h
Laboratory classes: 5h
Self study: 6h

Key distribution and digital signatures

Specific objectives:
2, 3, 4, 5

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 10h
Laboratory classes: 4h
Self study: 6h

Cryptographic system

Specific objectives:
2, 3, 4, 5

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 1h
Laboratory classes: 1h

Openssl/TLS

Specific objectives:
3, 4, 5

Related competencies :
G9. PROPER THINKING HABITS: capacity of critical, logical and mathematical reasoning. Capacity to solve problems in her study area. Abstraction capacity: capacity to create and use models that reflect real situations. Capacity to design and perform simple experiments and analyse and interpret its results. Analysis, synthesis and evaluation capacity.
G3. THIRD LANGUAGE: to know the English language in a correct oral and written level, and accordingly to the needs of the graduates in Informatics Engineering. Capacity to work in a multidisciplinary group and in a multi-language environment and to communicate, orally and in a written way, knowledge, procedures, results and ideas related to the technical informatics engineer profession.

Full-or-part-time: 8h
Laboratory classes: 2h
Self study: 6h

GRADING SYSTEM

There will be two tests in which the total content corresponding to Secret Key Cryptography has a weight of 20% of the final grade and the total content corresponding to Public Key Cryptography has a weight of 40% of the final grade. These two tests may be replaced by a final examination.

The other 40% of the grade will correspond to the laboratory.

BIBLIOGRAPHY

Basic:

- Paar, C.; Pelzl, J. Understanding cryptography: a textbook for students and practitioners. Springer, 2010. ISBN 9783642041006.
- Hoffstein, J.; Pipher, J. C.; Silverman, J. H. An Introduction to mathematical cryptography. 2nd ed. Springer, 2014. ISBN 9781493917105.
- Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. Handbook of applied cryptography. CRC Press, 1997. ISBN 0849385237.
- van Oorschot, Paul C. Computer Security and the Internet : tools and jewels. Cham: Springer, 2020. ISBN 9783030336486.
- Mollin, R.A. RSA and public-key cryptography. Chapman & Hall/CRC, 2003. ISBN 1584883383.
- Stallings, W. Cryptography and network security: principles and practice. 7th ed. Prentice Hall, 2017. ISBN 9781292158587.

Complementary:

- Anderson, R.J. Security engineering : a guide to building dependable distributed systems. 3rd ed. Indianapolis, Indiana: John Wiley & Sons, Inc., 2020. ISBN 9781119642831.
- Stinson, D.R.; Paterson, M.B. Cryptography: theory and practice. 4th ed. Chapman & Hall/CRC, 2018. ISBN 9781138197015.
- Salomaa, A. Public-key cryptography. Springer-Verlag, 1996. ISBN 9783642082542.
- Koblitz, N. A course in number theory and cryptography. 2nd e. Springer-Verlag, 1994. ISBN 0387942939.
- Blake, I. F; Seroussi, G.; Smart, N. Elliptic curves in cryptography. Cambridge University Press, 1999. ISBN 0521653746.
- Delfs, H.; Knebl, H. Introduction to cryptography: principles and applications. 2nd ed. Springer, 2007. ISBN 3540492437.
- Schneier, B. Applied cryptography: protocols, algorithms, and source code in C. 2nd ed. John Wiley & Sons, 1996. ISBN 0471117099.
- Yan, S.Y. Computational number theory and modern cryptography. Hoboken: John Wiley & Sons, 2013. ISBN 9781118188583.
- Daemen, J.; Rijmen, V. The design of Rijndael: AES the advanced encryption standard. Springer, 2001. ISBN 3540425802.
- Hankerson, D.; Menezes, A.; Vanstone, S. Guide to elliptic curve cryptography. Springer, 2004. ISBN 038795273X.
- Pastor Franco, J.; Sarasa López, M.Á.; Salazar Riaño, J.L. Criptografía digital : fundamentos y aplicaciones. 2a ed. Zaragoza: Prensas Universitarias de Zaragoza, 2001. ISBN 9788477335580.