Caracterização da Unidade Curricular / Characterization of the Curricular Unit

Designação da Unidade Curricular (UC) / Title of Curricular Unit (CU): Criptografia Aplicada / Applied Cryptography

Área científica da UC / CU Scientific Area: Ciências Informáticas / Computer Science

Semestre / Semester: 1º

Número de créditos ECTS / Number of ECTS credits: 6

Carga horária por tipologia de horas / Workload by type of hours: TP: 45; OT: 6; O: 9

Carga letiva semanal / Weekly letive charge: 3h

Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Esta unidade curricular tem como objetivo principal a aquisição de conhecimentos teóricos e práticos sobre técnicas e algoritmos de criptografia. Os estudantes deverão ficar aptos a aplicar os mecanismos base de criptografia na segurança de informação, ao nível da utilização, programação e administração de redes e sistemas informáticos. Nesta unidade curricular os estudantes deverão adquirir competências para aplicar técnicas e algoritmos de criptografia, nomeadamente algoritmos de chave simétrica e algoritmos de chave assimétrica, assim como assinatura digital de documentos. Deverão ainda desenvolver capacidades para entender e aplicar os conceitos de autenticação e de confidencialidade e integridade de dados.

Intended learning outcomes (knowledge, skills and competences to be developed by the students):

This curricular unit has as main objective the acquisition of theoretical and practical knowledge about cryptography techniques and algorithms. Students must be able to apply the basic cryptography mechanisms to information security, in terms of the use, programming and administration of networks and computer systems. In this curricular unit, students should acquire skills to apply cryptography techniques and algorithms, namely symmetric and asymmetric key algorithms, as well as digital signature of documents. They should also develop skills to understand and apply the concepts of authentication, confidentiality and data integrity.

Conteúdos programáticos:

1. Introdução a Criptografia e Segurança de Dados

1.1. Perspetiva histórica da criptografia

1.2. Fundamentos de criptografia

1.3. Vulnerabilidade e ameaças à segurança de dados

1.4. Medidas de proteção de dados

2. Algoritmos de Criptografia

2.1. Algoritmos de chave privada

2.2. Data Encryption Standard (DES)

2.3. Advanced Encryption Standard (AES)

2.4. Criptografia de chave pública

2.5. O sistema RSA

3. Infraestruturas de Chave Pública e Assinatura Digital

4. Confidencialidade e Integridade de Dados

4.1. Algoritmos e técnicas de garantia de confidencialidade

4.2. Algoritmos e técnicas de controlo de integridade

5. Autenticação

5.1. Algoritmos e técnicas de autenticação

5.2. Algoritmos e técnicas de não repudiação

6. Casos Práticos de Aplicação de Criptografia

Syllabus:

1. Introduction to Cryptography and Data Security

1.1. Historical perspective of cryptography

1.2. Cryptography Fundamentals

1.3. Vulnerability and data security threats

1.4. Data protection measures

2. Cryptography Algorithms

2.1. Private key algorithms

2.2. Data Encryption Standard (DES)

2.3. Advanced Encryption Standard (AES)

2.4. Public key cryptography

2.5. The RSA system

3. Public Key and Digital Signature Infrastructures

4. Confidentiality and Data Integrity

4.1. Confidentiality guarantee algorithms and techniques

4.2. Integrity control algorithms and techniques

5. Authentication

5.1. Authentication algorithms and techniques

5.2. Non-repudiation algorithms and techniques

6. Cryptography Application Cases