LICENCIATURA: Engenharia Multimédia	**ÁREA CIENTÍFICA:** Engenharia Informática
UNIDADE CURRICULAR/CURRICULAR UNIT: Criptografia / Cryptography	**ECTS: 6**
DURAÇÃO: Semestral	**HORAS DE CONTACTO TEÓRICO PRÁTICAS:** 60 (48 TP+12 OT)

OBJETIVOS DE APRENDIZAGEM/ / LEARNING OUTCOMES OF THE CURRICULAR UNIT

No final desta UC os estudantes que a completarem deverão ser capazes de:

1. Desenvolver competências teóricas e práticas na área da criptografia e segurança informática.
2. Conhecer alguns dos principais métodos criptográficos, e saber aplicá-los.
3. Conhecer algumas das principais ferramentas de segurança informática, e saber aplicá-las.

(English)
At the end of this course, students should be able to:

1. Develop theoretical and practical skills in the area of cryptography and computer security.
2. Know some of the main cryptographic methods and know how to apply them.
3. Know some of the main computer security tools and know how to apply them.

CONTEÚDOS PROGRAMÁTICOS/SYLLABUS

1. INTRODUÇÃO À CRIPTOGRAFIA E À SEGURANÇA DA INFORMAÇÃO
   a) Vulnerabilidades
   b) Ameaças
   c) Medidas de proteção

2. ALGORITMOS DE CIFRA
   a) Introdução
   b) Algoritmos de chave privada
   c) Data Encryption Standard (DES)
   d) Advanced Encryption Standard (AES)
   e) Criptografia de Chave Pública
   f) O Cripto sistema RSA
   g) Cripto sistemas de curvas elípticas
   h) Funções de Hash

3. INFRAESTRUTURAS DE CHAVE PÚBLICA E ASSINATURA DIGITAL

4. AUTENTICAÇÃO
   a) Sistemas pré-informáticos
   b) Sistemas informáticos (RC4, DES, AES)

5. CRIPTOGRAFIA DE CHAVE PÚBLICA

a) Generalidades

b) Autenticação de pessoas

c) Vulnerabilidades na autenticação

6. APLICAÇÕES

(English)

1) INTRODUCTION TO CRYPTOGRAPHY AND INFORMATION SECURITY

a) Vulnerabilities

b) Threats

c) Protection measures

2) CRYPTOGRAPHIC ALGORITHMS

a) Introduction

b) Private Key Algorithms

b) Data Encryption Standard (DES)

c) Advanced Encryption Standard (AES)

d) Public Key Encryption

e) The RSA system crypt

f) Elliptical crypto curve systems

g) Hash Functions

3. PUBLIC KEY INFRASTRUCTURES AND DIGITAL SIGNATURE

4. AUTHENTICATION

a) a) Pre-computer systems

b) b) Computer systems (RC4, DES, AES)

5. PUBLIC KEY ENCRYPTION

a) Generalities

b) Authentication of people

c) Authentication vulnerabilities

6. APPLICATIONS

DEMONSTRAÇÃO DA COERÊNCIA DOS CONTEÚDOS PROGRAMÁTICOS COM OS OBJETIVOS DA UNIDADE CURRICULAR/ DEMONSTRATION OF THE SYLLABUS COHERENCE WITH THE CURRICULAR UNIT'S OBJECTIVES

Correspondência dos objetivos com os conteúdos programáticos:

Todos os conteúdos programáticos (1 a 6) contribuem para a concretização do objetivo (1).

Os conteúdos programáticos (2, 3, 4, 5) endereçam o objetivo (2), conhecer alguns dos principais métodos criptográficos, e saber aplicá-los. Nas aulas práticas são realizadas implementações práticas dos vários algoritmos e ferramentas de segurança informática estudadas que permitem atingir o objetivo (3).

(English)

Correspondence of objectives with syllabus contents:

All syllabus contents (1 to 6) contribute to the achievement of objective (1).

Several topics of the syllabus (2 to 5) address the objective (2) .

IIn practical classes, syllabus content (6), practical implementations, of the various computer security algorithms and tools studied are carried out, which allow achieving the objective (3).

METODOLOGIAS DE ENSINO E AVALIAÇÃO / TEACHING METHODOLOGIES INCLUDING EVALUATION

De acordo com o Regulamento de Funcionamento do ISTEC Porto a avaliação é efetuada através de um exame final obrigatório. Na classificação final, poderão ser considerados elementos de avaliação contínua, tais como testes, trabalhos individuais ou em grupo, assim como a participação nas aulas presenciais e com recursos de aprendizagem proporcionados por sistemas de e-learning. O estudante que realize os trabalhos práticos propostos nas aulas e nas condições aprovadas, poderá prescindir da realização da Prova Prática final.

Nas aulas práticas, os alunos têm de desenvolver projetos onde utilizam as técnicas de Criptografia aprendidas, onde são incentivados a estudar aplicações específicas da Criptografia atual e olhar para técnicas e tecnologias emergentes neste domínio.

(English)

In accordance with ISTEC Porto's Operating Regulations, assessment is carried out through a mandatory final exam. In the final classification, elements of continuous assessment may be considered, such as tests, individual or group work, as well as participation in face-to-face classes and with learning resources provided by e-learning systems.

The student who carries out the practical work proposed in the classes and under the approved conditions, may waive the final practical test.

In practical classes, students have to develop projects where they use the learned Cryptography techniques, where they are encouraged to study specific applications of current Cryptography and look at emerging techniques and technologies in this domain.

DEMONSTRAÇÃO DA COERÊNCIA DAS METODOLOGIAS DE ENSINO COM OS OBJETIVOS DA UNIDADE CURRICULAR / DEMONSTRATION OF THE COHERENCE BETWEEN THE TEACHING METHODOLOGIES AND THE LEARNING OUTCOMES

Correspondência das metodologias de ensino com os objetivos da Unidade Curricular:

1 - Desenvolver competências teóricas e práticas na área da criptografia e segurança informática.

- Os trabalhos de grupo / individuais focam os temas principais dos conteúdos programáticos, que por sua vez estão alinhados com os objetivos da Unidade Curricular. Não é possível realizar os trabalhos nos temas propostos sem competências teóricas e práticas na área da criptografia e segurança informática. A prova teórica final, avalia as referidas competências pelo que o objetivo 1 é também cumprido.

2. Conhecer alguns dos principais métodos criptográficos, e saber aplicá-los.

- Os trabalhos de grupo / individuais, requerem o conhecimento dos principais métodos criptográficos, e saber aplicá-los, estando alinhado com os objetivos da Unidade Curricular. Não é possível realizar os trabalhos práticos nos temas propostos sem conhecer os principais métodos criptográficos e conseguir aplicá-los. A prova teórica final, avalia as referidas o conhecimento dos principais métodos criptográficos e sua aplicação, pelo que o objetivo 2 é também cumprido.

3 - Conhecer algumas das principais ferramentas de segurança informática, e saber aplicá-las.

- Os trabalhos de grupo / individuais, requerem o conhecimento das principais ferramentas de segurança informática, e saber aplicá-las, estando alinhado com os objetivos da Unidade Curricular. Não é possível realizar os trabalhos práticos nos temas propostos sem o conhecimento dessas ferramentas. A prova teórica final, avalia os referidos conhecimentos das ferramentas e sua aplicação, pelo que o objetivo 3 é também cumprido.

(English)

Correspondence of teaching methodologies with the objectives of the Curricular Unit:

1 - Develop theoretical and practical skills in the field of cryptography and computer security.

- Group / individual projects focuses on the main themes of the syllabus, which in turn are aligned with the objectives of the Curricular Unit. It is not possible to carry out work on the proposed topics without theoretical and practical skills in the area of cryptography and computer security. The final theoretical test evaluates these skills, so that objective 1 is also met.

2. Know some of the main cryptographic methods and know how to apply them.

- Group/individual assignments require knowledge of the main cryptographic methods, and know how to apply them, in line with the objectives of the Curricular Unit. It is not possible to carry out practical work on the proposed topics without knowing the main cryptographic methods and being able to apply them. The final theoretical test assesses the knowledge of the main cryptographic methods and their application, so that objective 2 is also fulfilled.

3 - Know some of the main computer security tools and know how to apply them.

- Group/individual work requires knowledge of the main computer security tools, and know how to apply them, in line with the objectives of the Curricular Unit. It is not possible to carry out practical work on the proposed topics without knowing these tools. The final theoretical test assesses the aforementioned knowledge of the tools and their application, so that objective 3 is also fulfilled.

BIBLIOGRAFIA / BIBLIOGRAPHY

FUNDAMENTAL/ ESSENTIAL:

ZÚQUETE, André (2018). Segurança em Redes Informáticas. FCA.

PAAR, Christof, PELZI, Jan, & FOREWORD Preneel Bart (2014). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.

COMPLEMENTAR/ COMPLEMENTARY:

STALLINGS, William (2009). *Cryptography and Network Security. Principles and Practice*. Pearson.

INTERNET:

Acesso a publicações da especialidade, gratuitamente, através da rede SPRINGER:

https://link.springer.com/