English version at the end of this document

Ano Letivo	2022-23
Unidade Curricular	CRIPTOGRAFIA MODERNA
Cursos	CIBERSEGURANÇA
Unidade Orgânica	Faculdade de Ciências e Tecnologia
Código da Unidade Curricular	19381001
Área Científica	
Sigla	
Código CNAEF (3 dígitos)	481
Contributo para os Objetivos de Desenvolvimento Sustentável - ODS (Indicar até 3 objetivos)	4,8,10
Línguas de Aprendizagem	Inglês

Modalidade de ensino

B-Learning

Docente Responsável Daniel da Silva Graça

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
Daniel da Silva Graça	T; TP	T1; TP1	14T; 14TP

* Para turmas lecionadas conjuntamente, apenas é contabilizada a carga horária de uma delas.

ANO	PERÍODO DE FUNCIONAMENTO*	HORAS DE CONTACTO	HORAS TOTAIS DE TRABALHO	ECTS
1º	S1	14T; 14TP	75	3

* A-Anual;S-Semestral;Q-Quadrimestral;T-Trimestral

Precedências

Sem precedências

Conhecimentos Prévios recomendados

Não aplicável

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

A unidade curricular (UC) de Criptografia Moderna pretende dotar os alunos de conhecimentos sobre os sistemas criptográficos mais utilizados, incluindo cifras sequenciais, por blocos, simétricas e assimétricas. É ainda objetivo desta UC que os alunos sejam capazes de utilizar sistemas criptográficos, e que reconheçam as suas limitações e as atuais ameaças da criptografia quântica. Pretende ainda dotar os alunos de conhecimentos sobre as metodologias de distribuição de chaves. Outro objetivo é dotar os alunos do conhecimento necessário para compreenderem como a criptografia é utilizada em diversas aplicações práticas.

Conteúdos programáticos

- Princípios e conceitos fundamentais em criptografia;
- Tipos de cifras;
- Criptografia de chave privada;
- Criptografia de chave pública;
- Funções de dispersão;
- Metodologias na utilização de sistemas criptográficos, suas limitações e ameaças;
- Distribuição de chaves;
- Assinaturas digitais e outras aplicações.

Metodologias de ensino (avaliação incluída)

A presente unidade curricular combina diversos métodos de ensino:

- Exposição dos conteúdos programáticos, através das aulas teóricas;

- Práticas laboratoriais onde são utilizadas metodologias de criptografia e criptanálise;

- Discussão alargada em sala de aula sobre os temas apresentados, envolvendo o docente e alunos.

A avaliação é contínua, com exame final, e inclui:

- Teste individual para avaliação de conhecimentos (50%);

- Trabalho/projeto (50%).

Os alunos que obtiverem uma classificação final igual ou superior a 9,5 valores, estão dispensados do exame final. No caso do aluno se apresentar a exame final, a classificação final da disciplina será obtida ponderando a nota do exame (50%) com a nota do trabalho/projeto (50%), sendo aprovados os alunos que obtiverem uma classificação final igual ou superior a 9,5 valores. Qualquer aluno poderá ser sujeito a uma prova complementar para confirmação da nota do teste, exame, ou trabalho/projeto.

Bibliografia principal

- Fernando Boavida e Mário Bernardes (2019), Introdução à Criptografia, FCA, ISBN-13: 9789727229024
- Keith Martin (2017), Everyday Cryptography: Fundamental Principles and Applications, 2nd Edition, Oxford University Press, ISBN-13: 9780198788003
- Jean-Philippe Aumasson (2017), Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, ISBN-13: 97815932782671

Academic Year	2022-23
Course unit	
Courses	
Faculty / School	FACULTY OF SCIENCES AND TECHNOLOGY
Main Scientific Area	
Acronym	
CNAEF code (3 digits)	481
Contribution to Sustainable Development Goals - SGD (Designate up to 3 objectives)	4,8,10
Language of instruction	English
Teaching/Learning modality	B-learning

Coordinating teacher Daniel da Silva Graça

Teaching staff	Type	Classes	Hours (*)
Daniel da Silva Graça	T; TP	T1; TP1	14T; 14TP

* For classes taught jointly, it is only accounted the workload of one.

Contact hours

T	TP	PL	TC	S	E	OT	O	Total
14	14	0	0	0	0	0	0	75

T - Theoretical; TP - Theoretical and practical ; PL - Practical and laboratorial; TC - Field Work; S - Seminar; E - Training; OT - Tutorial; O - Other

Pre-requisites

no pre-requisites

Prior knowledge and skills

Not aplicable

The students intended learning outcomes (knowledge, skills and competences)

The curricular unit (CU) of Modern Cryptography intends to provide students with knowledge about the most commonly used cryptography systems, including stream ciphers, block ciphers, and also symmetric and asymmetric ciphers. Another goal of this CU is that students are able to use cryptographic systems, and are able to recognize their limitations and identify the threat posed by quantum computers. This CU also intends to provide knowledge about key distribution. It is also intended that students gain enough knowledge to understand how cryptography is used in practical applications.

Syllabus

- Fundamental concepts and principles in cryptography;
- Cipher types;
- Private-key cryptography;
- Public-key cryptography;
- Hash functions;
- Methods used in cryptography systems, threats and limitations;
- Key distribution;
- Digital signatures and other applications.

Teaching methodologies (including evaluation)

This curricular unit combines various teaching methods:
- Theoretical lectures where the main concepts are presented;
- Practical laboratorial sessions where cryptography and cryptanalysis methods are applied;
- Open classroom discussion about the topics discussed in this course, involving both students and teachers.

Evaluation is continuous, with a final exam, and includes:
- Individual evaluation test (50%);
- Project (50%).
Students that achieve a final grade of 9.5 or higher, are exempt of the final exam. In the case of a student atending the final exam, the final course grade will be given by the weighted arithmetic mean of the grades of the final exam (50%) and of the project (50%), and students with a final grade of 9.5 or higher will be approved. Students may be subject to a complimentary test to confirm the grades obtained in the test, project or exams.

Main Bibliography

- Fernando Boavida e Mário Bernardes (2019), Introdução à Criptografia, FCA, ISBN-13: 9789727229024 (in Portuguese)
- Keith Martin (2017), Everyday Cryptography: Fundamental Principles and Applications, 2nd Edition, Oxford University Press, ISBN-13: 9780198788003
- Jean-Philippe Aumasson (2017), Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, ISBN-13: 97815932782671