Ficha de Unidade Curricular A3ES
Criptografia e Teoria de Códigos
Mestrado em Matemática Aplicada para a Indústria
2024-25

1. Caracterização da Unidade Curricular

1.1 Designação
[4250] Criptografia e Teoria de Códigos / Cryptography and Code Theory

1.2 Sigla da área científica em que se insere
MAT

1.3 Duração
Unidade Curricular Semestral

1.4 Horas de trabalho
162h 00m

1.5 Horas de contacto
Total: 67h 30m das quais TP: 67h 30m

1.6 ECTS
6

1.7 Observações
Unidade Curricular Obrigatória, Unidade Curricular Opcional

2. Docente responsável [1488] Teresa Maria de Araújo de Melo Quinteiro

3. Docentes e respetivas cargas letivas na unidade curricular
[1488] Teresa Maria de Araújo de Melo Quinteiro | Horas Previstas: 67.5 horas
[1836] Luís Manuel Ferreira da Silva | Horas Previstas: 45 horas
[1917] Lucía Fernández Suárez | Horas Previstas: 67.5 horas

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

Os estudantes que terminam com sucesso esta unidade curricular deverão ser capazes de:

1. Discutir e interpretar os aspetos da Teoria dos Números sobre os quais assentam as técnicas criptográficas modernas;
2. Compreender as técnicas fundamentais da criptografia;
3. Identificar e analisar ameaças genéricas e vulnerabilidades de um sistema;
4. Conhecer exemplos clássicos de códigos corretores de erros clássicos;
5. Reconhecer a importância dos sistemas criptográficos com códigos;
6. Descrever e analisar problemas concretos usando os conceitos estudados.

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

Students who successfully complete this curricular unit should be able to:

1. Interpret and discuss the aspects of Number Theory, of which modern cryptographic techniques are based;
2. Understand the fundamental skills and techniques of cryptography;
3. Identify and analyze generic threats and vulnerabilities of a system;
4. Be familiar with well-known code errors and corrections;
5. Recognize the importance of cryptographic systems with code;
6. Describe and analyze concrete problems using the concepts studied.

5. Conteúdos programáticos

1. Bases matemáticas: Teoria dos Números, corpos finitos e curvas elípticas.
2. Criptografia simétrica:
    1. Cifras clássicas: Cifra de César; Cifra Afim; Cifra de Vigenère; Cifra de Vernam e OTP
    2. Cifras stream e cifras por blocos.
3. Criptografia assimétrica:
    1. Sistemas de cifra baseados em problemas de fatorização de inteiros (RSA, Rabin)
    2. Sistemas de cifra baseados no problema do logaritmo discreto (ElGamal);
    3. Criptografia com Curvas Elípticas (ECDH);
    4. Aplicações dos métodos assimétricos: assinaturas e certificados digitais.
    5. Segurança e ataques a estes sistemas: testes de primalidade, fatorização e o problema do logaritmo discreto.
4. Teoria dos Códigos:
    1. Introdução à teoria de códigos;
    2. Códigos lineares;
    3. Códigos perfeitos: códigos de Hamming e códigos de Gollay;
    4. Códigos cíclicos;
5. Sistema criptográfico de McEliece: versões e ataques.

5. Syllabus

1. Mathematical Foundations: Number Theory, Abstract Algebra and Elliptical Curves.
2. Symmetric Cryptography:
    1. Classical systems: Caesar's Cipher, Affine?s Cipher, Vigenère's Cipher; Vernam's Cipher and OTP;
    2. Stream ciphers and blocks ciphers.
3. Asymmetric Encryption:
    1. Systems based on factorizations problems (RSA, Rabin);
    2. Systems based on discrete logarithm problem (ElGamal)
    3. Elliptic Curve cryptography;
    4. Applications: digital signatures and digital certificates;
    5. Security and attacks on these systems: primality tests, factorization and the discrete logarithm problem.
4. Code Theory:
    1. Introduction to Code Theory
    2. Linear Codes;
    3. Perfect Codes: Hamming's codes and Gollay's codes;
    4. Cyclic Codes.
5. McEliece cryptographic system: versions and attacks.

6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular

A formação matemática em Teoria dos Números em que assentam as técnicas criptográficas modernas (objetivo 1) está contemplada nos pontos 1, 2 e 3 dos conteúdos programáticos. A apresentação de diferentes métodos criptográficos e dos seus ataques nos pontos 2 e 3 possibilita que o aluno atinja os objetivos de aprendizagem 2 e 3. O objetivo 4 é alcançado no conteúdo programático 4. No ponto 5 os alunos estudam um sistema criptográfico com códigos, sistemas mais promissores numa era pós-quântica, e cumprem o objetivo programático 5. O objetivo 6 é completado usando todos os pontos dos conteúdos programáticos.

6. Evidence of the syllabus coherence with the curricular unit´s intended learning outcomes

The mathematical formation of Number Theory on the basis of modern cryptographic techniques (objective 1) is completed by points 1, 2, and 3 of the syllabus. The presentation of different cryptographic methods and their attacks in points 2 and 3 allows the students to meet learning objectives 2 and 3. Objective 4 is completed through the contents of 4 . For point 5 the students study a cryptographic system with codes, more promissory systems in a post-quantitative era, and complete objective 5. Objective 6 is completed through every point of the syllabus.

7. Metodologias de ensino (avaliação incluída)

- Aulas teórico-práticas onde são apresentados os temas, fornecidos exemplos de aplicação e resolvidos exercícios.

- Horas de atendimento aos alunos onde são esclarecidas dúvidas.

- Se reunidas as condições necessárias, esta UC poderá ser parcialmente lecionada à distância de forma síncrona (1/3 das horas de contacto semanais).

A avaliação é distribuída com exame final, com 2 partes, uma teórica e outra prática. A teórica é constituída por 3 testes pedagogicamente fundamentais, cada um com nota mínima de 8,00 valores e média de 9,50, ou um exame com nota mínima de 9,50 valores. A prática é constituída por um trabalho computacional pedagogicamente fundamental com nota mínima de 8,00 valores. Caso o aluno não tenha obtido a classificação mínima exigida num dos testes, pode recuperar por exame parcial em época de recurso. A nota final, NF, é obtida pela fórmula NF=0,8NT+0,2NP, onde NT é o máximo entre a média das notas dos 3 testes e a nota do exame e NP a nota do trabalho computacional.

7. Teaching methodologies (including assessment)

- Theoretical/practical classes where themes are presented along with application examples and completed exercises.

- Office Hours for students to discuss and clarify doubts and work through issues.

- If the necessary conditions are met, this CU can be partially taught remotely in a synchronous manner (1/3 of weekly contact hours)

Assessment is distributed with a final exam, with 2 parts, one theoretical and one practical. The theory consists of 3 pedagogically fundamental tests, each with a minimum grade of 8,00 and an average of 9,50, or an exam with a minimum grade of 9,50. The practice consists of a pedagogically fundamental computational work. If the student has not obtained the minimum classification required in one of the tests, the student can recover through a partial exam during the appeal period. The final grade, FG, is obtained by the formula FG=0,8TG+0,2PG, where TG is the maximum between the grades of the 3 tests and the final exam grade and PG is the grade for the computational work.

8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular

Nas aulas teórico-práticas são expostos os conteúdos programáticos e resolvidos problemas práticos onde se aplicam os conceitos estudados a que correspondem os objetivos de aprendizagem de 1 a 6. As horas de atendimento aos alunos complementam o estudo individual clarificando os temas onde surgem dúvidas.

De modo análogo, na avaliação escrita e na discussão do trabalho final são tidos em consideração todos os objetivos de aprendizagem, colocando na avaliação do trabalho final especial ênfase no objetivo de aprendizagem 6.

8. Evidence of the teaching methodologies coherence with the curricular unit´s intended learning outcomes

In theoretic-practical classes, syllabus content is expounded and practical problems are solved by applying the concepts studied. This corresponds to learning outcomes 1 and 6. Office hours complement individual study with clarification of doubts. In addition to these, the written exam and the final project include all the learning objectives with particular emphasis on learning objective 6, in the evaluation of the final project.

9. Bibliografia de consulta/existência obrigatória

Almeida P., Napp D., "Criptografia e Segurança", Publindustria, 2017.

Stinson D.R., "Cryptography - Theory and Practice", 4th Edition, CRC Press, 2018.

Hoffstein J., Pipher J. & Silverman J.H., "An Introduction to Mathematical Cryptography", 2 nd Edition, Springer, 2014.

Koblitz N., "A Course In Number Theory and Cryptography", 2 nd Edition, Springer, 1994.

Smith R.E., "Internet Cryptography", Addison-Wesley, 1997.

Blaum M., "A Course on Error-Correcting Codes", IBM Corp., 1997.

Lindt J.H. van, "Introduction to Coding Theory ", 3rd Edition, Springer, 1999.

Hill R., "A First Course in Coding Theory", Clarendon Press, 1986.

10. Data de aprovação em CTC 2024-07-17

11. Data de aprovação em CP 2024-06-26