Ficha de Unidade Curricular – (Versão A3ES 2018-2023)

1. Caracterização da Unidade Curricular.

1.1. Designação da unidade curricular ***(1.000 carateres).***
Criptografia e Teoria dos Códigos /
Criptography and Code Theory

1.2. Sigla da área científica em que se insere ***(100 carateres).***
MAT

1.3. Duração[1] ***(100 carateres).***
Semestral/Semester

1.4. Horas de trabalho[2] ***(100 carateres).***
162

1.5. Horas de contacto[3] ***(100 carateres).***
67,5 - TP

1.6. ECTS ***(100 carateres).***
6

1.7. Observações[4] ***(1.000 carateres).***
Optativa

1.7. Remarks ***(1.000 carateres).***
Optative

2. Docente responsável e respetiva carga letiva na Unidade Curricular ***(preencher o nome completo) (1.000 carateres).***
Teresa Maria de Araújo Melo Quinteiro – 67,5h

3. Outros docentes e respetivas cargas letivas na unidade curricular ***(1.000 carateres).***

4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes). ***(1.000 carateres).***

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

1. Discutir e interpretar os aspectos 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). ***(1.000 characters).***

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

1. Interpret and discuss the aspects of Number Theory, of which modern criptographic techniques are based;
2. Understand the fundamental skills and tecnhinques of criptography;
3. Identify and analyze generic threats and vunerabilities 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 ***(1.000 carateres).***

1. Bases matemáticas: Teoria dos Números, álgebra abstrata e curvas elíticas.
2. Criptografia clássica:
  2.1. Cifra de César;
  2.2. Cifra Afim e criptoanálise da Cifra Afim;
  2.3. Cifra de Vigenère e criptoanálise da Cifra de Vigenère.
3. Criptografia com chave pública:
  3.1. Sistema RSA;
  3.2. Cifra de Rabin;
  3.3. Sistema EL Gamal para corpos finitos e para curvas elíticas;
  3.4. Segurança e ataques a estes sistemas: testes de primalidade, fatorização e o problema do logaritmo discreto.
4. Teoria dos Códigos:
  4.1. Códigos de blocos;
  4.2. Códigos de Hamming;
  4.3. Códigos de Reed-Salomon;
  4.4. Códigos de Goppa.
5. Sistema criptográfico de McEliece: versões e ataques.

5. Syllabus ***(1.000 characters).***

1. Mathematical Foundations: Number Theory, Abstract Algebra and Elliptical Curves.
2. Classical Cryptography:
  2.1. Caesar Cipher;
  2.2. Affine Cipher and cryptanalysis of the Affine Cipher;
  2.3. Vigenère Cipher and cryptanalysis of the Vigenère Cipher.
3. Public Key Encryption:
  3.1. RSA system;
  3.2. Rabin Cipher;
  3.3. ElGamal encryption system for finite fields and elliptic curves;
  3.4. Security and attacks on these systems: primality tests, factorization and the discrete logarithm problem.
4. Code Theory:
  4.1. Block Codes;
  4.2. Hamming Codes;
  4.3. Reed-Salomon Codes;
  4.4. Goppa Codes.
5. McEliece cryptographic system: versions and attacks.

6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular ***(1.000 carateres).***

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 ataque 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 ***(1.000 characters).***

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 met the 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 sytems in an post-quantitative

era, and complete objective 5. Objective 6 is completed through every point of the syllabus.

7. Metodologias de ensino (avaliação incluída) ***(1.000 carateres).***

Metodologia de ensino:
- Aulas teórico-práticas onde são apresentados os temas, fornecidos exemplos de aplicação e resolvidos exercícios.
- Horas de atendimento aos alunos onde são esclarecidas dúvidas.

Avaliação:
A avaliação de conhecimentos é efectuada através de um teste escrito (peso 80%) e um trabalho final (peso 20%). Para obter aprovação à disciplina é necessária uma nota mínima de 9.5 valores no teste escrito e no trabalho final.

7. Teaching methodologies (including assessment) ***(1.000 characters).***

Teaching Methods:
- Theoretical/practical classes where themes are presented along with application examples and completed exercises.
- Office Hours for students to discuss and clarify their doubts and work through any issues.

Evaluation:
A written exam (80%) will be administered as an evaluation of requisite knowledge along with a final project (20%). In order to approval students must recieve a minimum grade value of 9.5 on both the written exam and the final project.

8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular ***(3.000 carateres).***

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 ***(3.000 characters).***

In theoretic-practical classes, syllabus content is expounded and practical problems solved applying the concepts studied. This corresponds to the 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 ***(1.000 carateres).***

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", 2nd Edition, Springer, 2014.
Koblitz N., "A Course In Number Theory and Cryptography", 2nd 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.

---

[1] Anual, semestral, trimestral, …
[2] Número total de horas de trabalho.
[3] Discriminadas por tipo de metodologia adotado (T - Ensino teórico; TP - Ensino teórico-prático; PL - Ensino prático e laboratorial; TC - Trabalho de campo; S - Seminário; E - Estágio; OT - Orientação tutorial; O - Outro).
[4] Assinalar sempre que a unidade curricular seja optativa.