Escola Superior de Tecnologia e Gestão
Descritor de Unidade Curricular

Nível de ciclo de estudos:
Mestrado
Curso:
Engenharia de Segurança Informática

Unidade Curricular: **1989104 – Criptografia e Criptanálise Aplicadas**

Ano 1 **Semestre 1** **Área CNAEF: 523** **ECTS: 8**

Tipo de Unidade Curricular: Obrigatória **Modo de Ensino:** Presencial **Língua de Trabalho:** Português

DOCENTE RESPONSÁVEL: Rui Miguel Soares Silva

TEMPO DE TRABALHO DO ESTUDANTE EM HORAS

HORAS TOTAIS	**Horas de Contacto**								**Horas de Trabalho Autónomo**
	Ensino teórico (T)	Ensino teórico-prático (TP)	Ensino prático e laboratorial (PL)	Trabalho de campo (TC)	Seminário (S)	Estágio (E)	Orientação tutorial (OT)	Outra (O)	
200		**30**	**15**						**155**

Pré-requisitos (se aplicável):

OBJETIVOS EDUCACIONAIS / RESULTADOS DE APRENDIZAGEM

Faculta os conhecimentos elementares sobre criptografia e criptanálise do ponto de vista matemático, que permitem aos aluno desenvolver algoritmos criptográficos e efectuar ataques criptanalíticos recorrendo a programas de computador. As competências a desenvolver são:

1. Compreender a evolução da criptografia e da criptanálise;

2. Compreender as várias técnicas criptográficas e a sua aplicação;

3. Desenvolver algoritmos criptográficos e criptanalíticos e programa-los de forma eficiente.

CONTEÚDOS PROGRAMÁTICOS

1. Introdução à criptografia e à criptanálise

1.1 Serviços de segurança

1.2 Conceitos essenciais

1.3 Força bruta e criptanálise

2. Criptografia clássica

2.1 Técnicas de substituição

2.2 Técnicas de transposição

2.3 Criptanálise

3. Abordagem à criptografia na segunda grande guerra

4. Criptografia moderna

4.1 Teoria matemática das comunicações

5.Cifras por blocos

5.1 Modos de operação

5.2 Arqitectura de Feistel

5.3 DES e AES e outras cifras

5.4 Criptanálise

6.Cifras por fluxo de chaves

6.1 LFSRs, RC4 e cifras caóticas

6.2 Criptanálise

7. Funções de mistura, códigos de autenticação de mensagens e assinatura digital

7.1 Aplicações e requisitos de segurança

7.2 SHA e outros algoritmos

7.3 Algoritmos MAC

7.4 Assinatura digital

7.5 Criptanálise

8. Abordagem à teoria dos números

9. Criptografia de chaves públicas

9.1 RSA

9.3Diffie-Hellman

9.2 Curvas elípticas

9.3 Criptanálise

10. Gestão e distribuição de chaves

11. Programação com números grandes

11.1 GNU Multiple precision arithmetic library

DEMONSTRAÇÃO DA COERÊNCIA DOS CONTEÚDOS PROGRAMÁTICOS COM OS OBJETIVOS DE APRENDIZAGEM

Os objectivos da unidade curricular dividem-se em duas áreas: os conhecimentos elementares sobre criptografia e criptanálise do ponto de vista matemático; desenvolver algoritmos criptográficos e efectuar ataques criptanalíticos recorrendo a programas de computador. Os conteúdos programáticos reflectem ambos objectivos, pois é abordado um conjunto significativo de tópicos criptográficos desde a sua origem até à actualidade, sendo para cada um deles apresentada a perspectiva criptanalítica. São ainda abordados diversos aspectos puramente matemáticos, considerados essenciais à compreensão de alguns dos tópicos criptográficos. A componente de programação assume que os alunos possuem conhecimentos de programação e é utilizada a biblioteca de código aberto GMP - GNU Multiple precision arithmetic library como suporte à programação com números grandes.

MÉTODOS DE ENSINO E APRENDIZAGEM

1.Aulas teórico-práticas, que incluem a exposição da matéria e o seu debate com os alunos, a análise de casos de estudo do mundo real, demonstrações pelo professor e a realização de exercícios práticos.

2. Aulas laboratoriais, que incluem a experimentação de exemplos e a realização de fichas de trabalho laboratorial.

DEMONSTRAÇÃO DA COERÊNCIA DAS METODOLOGIAS DE ENSINO COM OS OBJETIVOS DAS APRENDIZAGENS*

Os objectivos da unidade curricular dividem-se em duas áreas: conhecimentos elementares sobre criptografia e criptanálise do ponto de vista matemático; o desenvolvimento de algoritmos criptográficos e de ataques criptanalíticos recorrendo a programas de computador. A metodologia de ensino adoptada divide-se em dois tipos de aulas: aulas teorico-práticas focadas na concretização do objectivo relativo aos conhecimentos elementares sobre criptografia e criptanálise do ponto de vista matemático; aulas laboratoriais focadas na concretização do objectivo relativo ao desenvolvimento de algoritmos criptográficos e de ataques criptanalíticos recorrendo a programas de computador. O número de aulas total divide-se igualmente por aulas teorico-práticas e laboratoriais, reflectindo a importância atribuída à componente prática e profissional do Mestrado.

A avaliação divide-se em duas partes com igual peso na nota final, sendo uma de cariz laboratorial e outra de cariz teórico, focando desta forma os dois objectivos da UC.

MÉTODOS DE AVALIAÇÃO

A avaliação inclui uma frequência com um peso de 50% na nota final e um trabalho de grupo de pesquisa e desenvolvimento com um peso de 50% na nota final.

BIBLIOGRAFIA PRINCIPAL

[1] William Stallings, “Cryptography and Network Security: Principles and Practice”, 7th Edition, ISBN: 978-0134444284, Pearson Education, 2016.

[2] Mark Stamp, Richard M. Low, "Applied Cryptanalysis: Breaking Ciphers in the Real World", 1st Edition, ISBN: 978-0470114865, Wiley-In terscience, 2007.

[3] Bruce Schneier, "Applied Cryptography", 2nd Edition, ISBN: 0471117099, Wiley, 1996.
[4] Bruce Schneier, Niels Ferguson, "Practical Cryptography", 1st Edition, ISBN: 978-0471223573, John Wiley & Sons, 2003.

Ano letivo de entrada em vigor: 2018/2019 | Data de aprovação em Conselho Técnico-Científico: