

CURSO	Licenciatura em Engenharia Multimédia		
UNIDADE CURRICULAR	Criptografia	Obrigatória	X
		Opcional	
ÁREA CIENTÍFICA	Engenharia Informática		

Ano: 3º	Semestre: 1º	ECTS: 6	Horas de Contacto teórico práticas: 60
---------	--------------	---------	--

OBJETIVOS DA APRENDIZAGEM

Para concluir com sucesso esta unidade curricular, os alunos deverão demonstrar possuir os seguintes conhecimentos e capacidades:

1. Entender os conceitos de criptografia, criptoanálise, algoritmos de chave simétrica, algoritmos de chave assimétrica e assinatura digital de documentos;
2. Cifrar e decifrar utilizando diferentes algoritmos;
3. Fazer cálculos em espaços modulares;
4. Entender os conceitos de confidencialidade, integridade e não-repudição;
5. Compreender os princípios fundamentais das infraestruturas de chave pública e assinatura digital.

PROGRAMA

1. INTRODUÇÃO À CRIPTOGRAFIA E À SEGURANÇA DA INFORMAÇÃO
 - 1.1. Vulnerabilidades
 - 1.2. Ameaças
 - 1.3. Medidas de proteção
2. ALGORITMOS DE CIFRA
 - 2.1. Introdução
 - 2.2. Algoritmos de chave privada
 - 2.3. Data Encryption Standard (DES)
 - 2.4. Advanced Encryption Standard (AES)
 - 2.5. Criptografia de chave pública
 - 2.6. O cripto sistema RSA
 - 2.7. Cripto sistemas de curvas elípticas
 - 2.8. Funções de Hash
3. INFRAESTRUTURAS DE CHAVE PÚBLICA E ASSINATURA DIGITAL
4. AUTENTICAÇÃO
 - 4.1. Generalidades
 - 4.2. Autenticação de pessoas
 - 4.3. Vulnerabilidades na autenticação
5. APLICAÇÕES

DEMONSTRAÇÃO DE COERÊNCIA ENTRE CONTEÚDOS PROGRAMÁTICOS E RESULTADOS DA APRENDIZAGEM

Os conteúdos programáticos foram definidos em função dos objetivos (1 a 5) e competências a serem adquiridos pelos estudantes. Os conteúdos programáticos incluem os principais algoritmos de cifra usados atualmente (1 e 2), os conceitos de confidencialidade, integridade e não-repudição (4) e os princípios fundamentais das infraestruturas de chave pública e assinatura digital (5) que são absolutamente cruciais em qualquer aplicação moderna, seja no espaço das aplicações móveis, seja no da web.

METODOLOGIA DE ENSINO E AVALIAÇÃO

Esta unidade curricular tem uma natureza teórico-prática. Estão previstas 60 horas de contato. O tempo total de trabalho do aluno corresponde a 162 horas. A criptografia assumiu um papel ubíquo, estando presente na generalidade das aplicações das tecnologias de informação e comunicação da atualidade. É, portanto, fundamental dotar os alunos de uma base sólida que lhe permita entender e implementar, nas futuras áreas de atividade profissional, mecanismos de cifra e de segurança, à altura dos desafios colocados pelo contexto atual. A presente unidade curricular de Criptografia dará resposta a esta necessidade, introduzindo os conceitos matemáticos necessários, os algoritmos (quer os de chave simétrica, quer os de chave assimétrica) e respetivas implementações, assim como aplicações práticas, nomeadamente nas áreas de segurança de informação e de segurança de redes, das modernas técnicas de criptografia e criptoanálise. São também apresentados conceitos emergentes na área da criptografia e da segurança, de modo a preparar os alunos quer para os desafios que encontrarão nas futuras áreas profissionais, quer para eventuais opções de aprofundamento em ambiente académico ou empresarial.

De acordo com o Regulamento de Funcionamento do ISTECS a avaliação é efetuada através de um exame escrito individual e 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 em recursos de aprendizagem proporcionados por sistemas de e-learning.

DEMONSTRAÇÃO DE COERÊNCIA ENTRE METODOLOGIAS DE ENSINO E RESULTADOS DE APRENDIZAGEM

Embora a unidade tenha uma importante componente teórica, procurar-se-á utilizar exemplos práticos dos conceitos abordados que permitam aos estudantes atingir os objetivos da aprendizagem propostos para a unidade curricular.

As competências cognitivas são desenvolvidas através da exposição participativa e da resolução de exercícios. As competências práticas são dos trabalhos em grupo supervisionados. As competências de comunicação são adquiridas através de dinâmicas de grupo e das apresentações orais.

Esta unidade curricular funcionará em articulação com Direito de Informática numa parte comum de ambos os programas. Nesta unidade curricular abordar-se-ão questões de proteção de dados pessoais informatizados e criminalidade informática sendo que em criptografia se abordarão as tecnologias que ajudem a minimizar essa criminalidade e abusos.

BIBLIOGRAFIA

Fundamental:

ZÚQUETE, André (2014); Segurança em Redes Informáticas; FCA.

SCHNEIER, Bruce (2015); Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, USA.

Complementar:

JOHNSON, Bud (2013); Break the Code: Cryptography for Beginners, EA, USA.

PIPER, Fred (2002); Cryptography: A Very Short Introduction, OXFORD, UK.

KATZ, Jonathan (2014); Introduction to Modern Cryptography, Second Edition, CRC Papers, USA.

STALINGS, William (2016); Cryptography and Network Security: Principles and Practice (7th Edition), EA, USA.

HOLDEN, Joshua (2017); The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption, EA, USA.

SMITH, Laurence (1955); Cryptography: The Science of Secret Writing, EA, USA.

INTERNET:

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

<https://link.springer.com/>

Utilização obrigatória de uma das redes internas do ISTECS.