

Criptografia 2022-2023

Apresentação

António Santos

ISTEC

Tópicos

1 Disciplina

Classroom

2 Programa da Disciplina

1.Introdução à Criptografia e à Segurança da Informação

2.Algoritmo de Cifra

3.Infraestruturas de Chave Pública e Assinatura Digital

4. Autenticação

5. Aplicações

3 Bibliografia

Bibliografia

4 Critérios de Avaliação

Avaliação

Cenário Létivo

Classroom - Manhã

Criptografia LEI - A
Código da turma
njxcjqj

Classroom - Tarde

Criptografia LEI - B

Código da turma

qxcinuw

Classroom - Noite

Criptografia LEI - PL A

Código da turma

tspb6lf

1.Introdução à Criptografia e à Segurança da Informação

Introdução

- Vulnerabilidades
- Ameaças
- Medidas de proteção

Algoritmo de Cifra

- Introdução
- Algoritmos de chave privada
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Criptografia de chave pública
- O cripto sistema RSA
- Cripto sistemas de curvas elípticas
- Funções de Hash

3. Infraestruturas de Chave Pública e Assinatura Digital

Introdução

- Infraestruturas de Chave Pública
- Assinatura Digital

4. Autenticação

Autenticação

- Generalidades
- Autenticação de pessoas
- Vulnerabilidades na autenticação

5. Aplicações

Aplicações

- Aplicações

Bibliografia Recomendada

- Apontamentos da Disciplina
- Apresentações das aulas

Bibliografia Recomendada

- ZÚQUETE, André (2014); Segurança em Redes Informáticas; FCA.
- SCHNEIER, Bruce (2015); Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, USA.

Bibliografia 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.

Tipos de Avaliação

O aluno pode optar por um dos dois tipos de avaliação

- Avaliação Contínua
- Avaliação não Contínua

Avaliação Contínua

- Projeto (40%)
- Exame Final (60%) (Obrigatório)

Avaliação não Continua

- Exame Final (100%)

Presencial

De acordo com o Regulamento do ISTEC

- Ensino tradicional
- Aulas presenciais (4 horas semanais)
- Avaliações presenciais

Ferriados 1 e 8 Dezembro - Reposição LEI-A

Opção 1: Quarta-Feira: 9/11/2022: 9:00-13:00 e 14:00-18:00

Feriados 1 e 8 Dezembro - Reposição LEI-B

Opção 1: Sexta-Feira: 11/11/2022: 9:00-13:00 e 14:00-18:00

Feriados 1 e 8 Dezembro - Reposição LEI- PL A

Opção 1: Sexta-Feira: 4 semanas das 22:00-24:00 de
03/11/2022 a 24/11/2022