# Teoria da Informação

Programa, Bibliografia e Avaliação

LEI - 2º Ano - 1º Semestre
Edição 2024-25

Rui Pedro Paiva, Paulo de Carvalho

# Docentes

- Teóricas
  - Rui Pedro Paiva
- Teórico-Práticas
  - Rui Pedro Paiva
- Práticas
  - Ismael Jesus
  - Lorena Petrella
  - Rui Pedro Paiva
- Horário de atendimento
  - Consultar inforestudante

# Informações, Materiais, etc.

- Inforestudante
- UCStudent

# Modelo de Aulas

- Aulas Teóricas
  - Todas as semanas (2h)
  - Introdução de conceitos.
  - Resolução de problemas
- Aulas Práticas (TP)
  - Todas as semanas (1h)
  - Aulas teorico-práticas (desafios)
  - Introdução dos TPs
  - Resolução de exercícios
- Aulas Laboratoriais (PL)
  - Todas as semanas (2h)
  - Apoio aos TPs
  - Defesa dos TPs
  - Avaliação Presencial

| **Actividade** | **Horas** | **ECTS** |
|---|---|---|
| Aulas T | 20 | 0.74 |
| Aulas PL | 26 | 0.96 |
| Aulas TP | 10 | 0,37 |
| Trab. autónomo | 47 | 1.74 |
| Estudo | 51 | 1,89 |
| Avaliação | 8 | 0,30 |
| | 162 | 6,00 |

# Objectivos

- Fornecer de uma forma sistemática as noções fundamentais da teoria da informação
  - Fundamentos: informação, entropia, etc.
  - Codificação de fontes
  - Criptografia

# Programa

1. Fundamentos:
–Informação: intuição, conceito e propriedades;
–Entropia Shannon, incerteza e dispersão;
–Entropia conjunta, condicionada e propriedades;
–Divergência Kullback-Leibler; Informação Mútua;
–Regras da Cadeia;
–Princípio da entropia máxima.

2. Entropia e compressão:
–O teorema da codificação da fonte;
–Teorema de Kraft e de McMillan;
–Códigos Óptimos;
–Códigos de Shannon-Fano-Elias; Códigos de Huffman; Códigos Aritméticos; Códigos de dicionário.
–Códigos preditivos
–Transformações e Aplicações

# Programa

3. Criptografia
- Domínios e tipos de algoritmos;
- Algoritmos clássicos (cifra de césar, vignerè, one time pads);
- Encriptação perfeita e imperfeita;
- Alg. de chave assimétrica – o RSA, limites de segurança do RSA, Implementação (Geração de números aleatórios Alg.s de Euclides, peq. Teor. de Fermat);
- Alg. de chave simétricas (DES e AES);
- Funções de Hashing (MDC e MD).
- Distribuição de chaves (diffie-Helman, ElGamal)
- Kerberos e Certificados

# Programa

- Práticas
  1. TP0- Introdução ao Python
     (2 semanas)

  2. Entropia e Informação Mútua
     (5 semanas)

  3. Algoritmos de compressão – implementação de um algoritmo de compressão/descompressão
     (6 semanas)

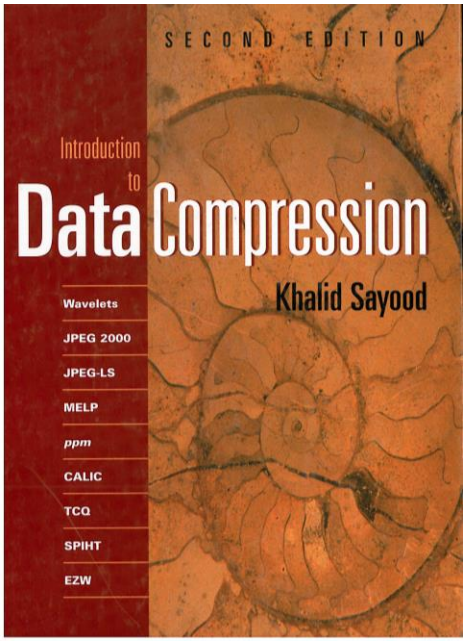
  Ferramentas a usar: **Python** (em particular a biblioteca **numpy**)

# Avaliação

- Trabalhos práticos – 10 valores
  - Mínimos de 40.0%
  - Defesa individual (não defesa equivalente a não entrega)
  - Avaliação contínua: 25% + 75% trabalhos práticos (trabalhadores Estudantes: 100% trabalhos))
  - Grupos da MESMA TURMA
- Exame – 10 valores:
  - Mínimos de 40.0%
  - Com **consulta condicionada** (1 página A4 – 1 folha A4 de um lado - escrita a times >=8; espaçamento simples; margens de 2cm; não observância deste template implica a não utilização da folha para efeitos de consulta)

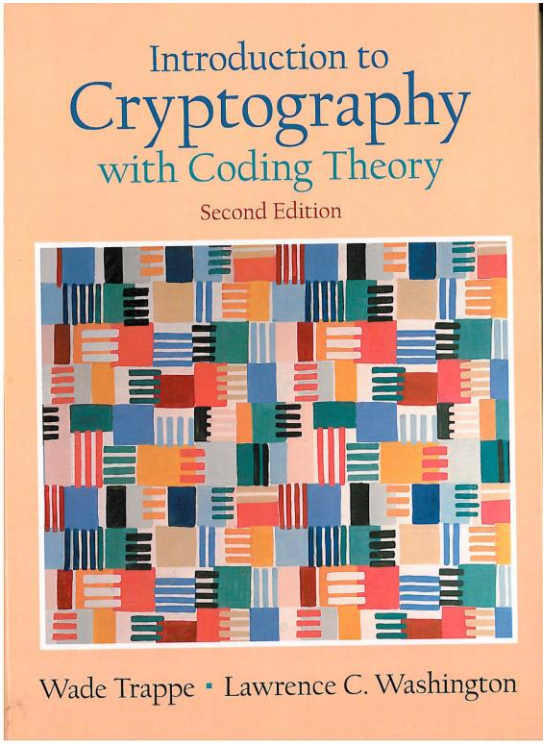
# Bibliografia

- Principal
  - Capítulos I e II
    - K. Sayood, Introduction to data compression: second edition, Morgan Kaufman, 2000.
    - J. C. MacKay, Information Theory, Inference and Learning Algorithms, University of Cambridge, 2003 (http://www.inference.phy.cam.ac.uk/mackay/itila/book.html)
- Complementar
  - T. Cover, J. Thomas, Elements of Information Theory, John Wiley&Sons, 1991.



# Bibliografia

- Principal
  - Capítulo III
    - W. Trappe, L.. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall



# Avaliação

- Notas:
  - Qualquer tentativa de **fraude** implica para todos os intervenientes a **não admissão a exame e comunicação ao Diretor do DEI**
  - É considerado fraude a cópia explicita ou de partes dos trabalhos práticos
  - É considerado fraude a utilização de fragmentos código público ou "emprestado" sem a respectiva referência aos autores
  - **As datas fixadas serão para cumprir sem adiamentos possíveis (entregas efectuadas depois das datas definidas não serão aceites)**

# Avaliação

- Trabalhos práticos (Grupos de três alunos)
  - Cada grupo (3 elementos, 4 se necessário) deve:
    - Devem ser da mesma turma prática
    - Entregar um relatório de cada um dos trabalhos práticos e o respetivo código
    - Avaliação com defesa **individual** nas aulas práticas
    - Mínimos: 40%
  - Cotação: 10 valores

# Avaliação

- Exame
  - Sobre toda a matéria da disciplina
  - Com consulta condicionada
    - 1 página A4 impressa com times 8pt
  - Cotação: 10 valores
  - Mínimos: 40%
  - A componente prática da disciplina é realizada exclusivamente durante a parte letiva.

  - Nota: Não são permitidos meios eletrónicos (computadores, telemóveis, etc.) exceto calculadoras

# Avaliação

- Elementos de Avaliação
  - Todos os elementos de avaliação entregues deverão dispor de:
    - Nome completo dos autores
    - Número de estudante dos autores
    - Data de entrega
  - A entrega de qualquer documentação deverá ser em formato electrónico (a definir)

# Sucesso

- Sucesso na Disciplina
  - 80%-85% dos alunos que participam na disciplina
  - Cerca de 40% dos alunos deixam de participar

  - Ano passado:
    - 180 inscritos
    - 35 alunos não participaram
    - 135 aprovados
    - Taxa de Aprovação global:  75%