

**Departamento de Matemática**  
**Disciplina de Programação Avançada**  
**Ano lectivo de 2016/2017**  
**Proposta de tema**

**Título:** Quebrar a Cifra do Rei

**Sumário:**

O *Livro dos conselhos de D. Duarte* inclui uma secção encriptada que até aos dias de hoje não foi quebrada. Pretende-se explorar as cifras clássicas e os métodos criptoanalíticos correspondentes aplicados aos textos em questão.

Em comunicação apresentada no IV Colóquio da Secção Portuguesa da Associação Hispânica de Literatura Medieval, realizado na Universidade Nova de Lisboa, entre 23 e 25 de outubro de 2002, João Dionísio e Susana Pedro expuseram os resultados de seus esforços em decifrar as Cyfras del Rey dom Eduarte. Os pesquisadores concluíram serem as cyfras, naquele momento, indecifráveis.

Propõe-se implementar os métodos criptoanalíticos clássicos tentando dessa forma quebrar a Cifra do Rei.

**Condições de Preferência:** C/C++

**Condições Especiais:** -

**Orientador(es):** Professor Pedro Quaresma

Data: 2 de Fevereiro de 2017

O proponente  
Pedro Quaresma