

Departamento de Matemática
Disciplina de Programação Avançada

Ano lectivo de 2024/2025

Proposta de tema

Título: Criptoanálise

Sumário: Os métodos de criptoanálise para sistemas de substituição ou transposição (mono-alfabéticos ou poli-alfabéticos) têm como ferramenta básica de análise várias medidas de índole estatística sobre língua natural usada no texto original da mensagem.

Pretende-se, com este projecto, construir um programa de criptoanálise para sistemas de substituição ou transposição, de tal forma que, dado um texto cifrado, o programa consiga “adivinhar” o método utilizado, quebrando-o de seguida.

Condições de Preferência: o projecto é para ser desenvolvido nas linguagens de programação “C” e Flex.

Condições Especiais ter experiência prévia com sistemas de criptografia e/ou criptoanálise.

Orientador(es): Pedro Quaresma

Data: 5 de Fevereiro de 2025

O proponente