Departamento de Matemática

Disciplina de Programação Avançada

Ano lectivo de 2010/2011

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 na linguagem de programação "C".
Condições Especiais ter experiência prévia com sistemas de criptografia e/ou criptoanálise.
Orientador(es): Pedro Quaresma

Data: 8 de Junho de 2010

O proponente