Departamento de Matemática
Disciplina de Programação Avançada
Ano lectivo de 2025/2026

Proposta de tema

Título: Criptoanálise da Cifra de Chave Pública RSA

Sumário: Os sistemas de criptografia e de criptoanálise são omnipresentes nas actuais comunicações digitais. Os sistemas de chave pública, pela forma como permitem um tratamento fácil das chaves de encriptação são uma parte importante de um qualquer sistema.
Partindo de uma implementação da cifra RSA pretende-se implementar alguns ataques criptoanalíticos.

- Implementação dos ataques à cifra RSA: método das divisões, método de Euclides, fórmula de Fermat, crivo quadrático.
- Utilização da biblioteca de funções *GNU Multi-Precision Library* (GMP) como forma de implementar números inteiros de grande dimensão.

Condições de Preferência: C++

Condições Especiais: C/C++

Orientador(es): Professor Pedro Quaresma

Data: 10 de fevereiro de 2026