Universidade do Estado de Santa Catarina
Departamento de Ciência da Computação

Implementar um programa para criptografia e descriptografia de um arquivo usando o algoritmo RSA, e um algoritmo de força bruta para quebra da chave criptográfica.

Linguagens permitidas: C, C++, Java, Python ou Haskell.

É obrigatória a implementação das seguintes funções:

- Geração das chaves pública e privadas, principalmente a verificação de primalidade de um número;
- Algoritmo de Euclides Estendido;
- Função para criptografar e descriptografar dados de um arquivo;
- Algoritmo de força bruta para a fatoração da chave pública nos números primos que a geraram.

Escrever um relatório técnico de até sete páginas no formato de artigo da SBC, o artigo deve conter:

- Uma introdução sobre o funcionamento de criptografia de chave pública;
- Uma descrição da complexidade das funções implementadas;
- Gráficos com os tempos de execução da geração das chaves e fatoração para inteiros com n-bits.