UDESC UNIVERSIDADE DO ESTADO DE SANTA CATARINA | JOINVILLE CENTRO DE CIÊNCIAS TECNOLÓGICAS

Trabalho:

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

Linguagens permitidas: *C*, *C++*, *Java*, *Rust* ou *Haskell*.

É obrigatória a implementação das seguintes funções:

- Geração das chaves pública e privadas, principalmente a verificação de primalidade de um número (que deve executar em tempo polinomial);
- Algoritmo de Euclides Estendido;
- Função para criptografar e descriptografar dados de um arquivo (usar a potência modular);
- Algoritmo de força bruta para a fatoração da chave pública nos números primos que a geraram.

Fazer um vídeo explicando os resultados e o código, o vídeo deve conter:

- Um exemplo de execução do programa, usando uma chave de 256 bits ou maior;
- A explicação da implementação da geração das chaves pública e privada, incluindo como foi feito o teste de primalidade;
- A explicação da implementação da criptografia e descriptografia da mensagem;
- A complexidade do teste de primalidade e da quebra da chave;
- Devem ser apresentados gráficos com os tempos de execução da geração das chaves, da fatoração, do processo de criptografia e descriptografia da mensagem. O gráfico do processo de criptografia deve incluir exemplos até 1024, os tempos devem ser medidos com intervalos de chaves de 64 bits.