



Universidade Federal de Alagoas
Instituto de Computação
Matemática Discreta
Professor Bruno Pimentel



Projeto Final - Criptografia RSA

Informações gerais:

- Projeto a ser realizado por equipes com até 5 pessoas. Todos os membros deverão participar ativamente da elaboração e apresentação do projeto;
- Apresentação do projeto para todas as equipes: 19/05 e 24/05/2021 (ordem das equipes definida por sorteio)
- Data de entrega: 18/05/2021

Requisitos do projeto sobre Criptografia RSA: Desenvolver um programa em uma linguagem de programação à escolha da equipe que realize a seguinte tarefa:

- Solicite que o usuário escolha entre 3 opções: 1 - Gerar chave pública, 2 - Encriptar, 3 - Desencriptar.
- Caso escolhida a opção 1 - Gerar chave pública:
 - Solicite que o usuário digite um par de números primos p e q e um expoente e relativamente primo a $(p - 1)(q - 1)$.
 - Salve, no diretório de execução do programa, um arquivo txt com os dois números que formam a chave pública.
- Caso escolhida a opção 2 - Encriptar:
 - Solicite que o usuário digite a mensagem de texto a encriptar.
 - Solicite que o usuário digite a chave pública recebida previamente.
 - Salve, no diretório de execução do programa, um arquivo txt com a mensagem encriptada.
- Caso escolhida a opção 3 - Desencriptar:
 - Solicite que o usuário digite p , q e e .
 - Salve, no diretório de execução do programa, um arquivo txt com a mensagem desencriptada.

Observação: A mensagem deve ser encriptada usando o alfabeto de letras A - Z, codificado com inteiros de 2 a 28, onde 2 = A, 3 = B,..., 27 = Z, 28 = espaço.

Documentos: Cada equipe deve entregar:

1. Código-fonte do programa (.zip ou link);
2. Apresentação do projeto, mostrando: 1 - conceitos matemáticos usados, 2 - demonstração do funcionamento das tarefas;

Critérios de Avaliação:

1. Uso e entendimento correto dos conceitos matemáticos envolvidos (30%);
2. Organização do programa (20%);
3. Eficácia do programa: funcionamento correto (25%);
4. Apresentação: didática e clareza na explicação, demonstração de domínio do assunto (25%).