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;
- Data de definição das equipes: 18/12/2019 (enviar e-mail para brunopimentel@ic.ufal.br)
- Apresentação do projeto para todas as equipes: 03/02 a 10/02/2020 (ordem das equipes definida por sorteio)
- Data de entrega: 02/02/2020

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 1: 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.

Observação 2: Os programas apresentados serão testados da seguinte forma:

1. Uma primeira equipe fornecerá uma chave pública para uma segunda equipe, que criará uma mensagem e a encriptará com a chave fornecida pela primeira equipe;
2. Em seguida, a segunda equipe entregará a mensagem encriptada para a primeira equipe (via e-mail ou pendrive) que terá que realizar a desencriptação sem quaisquer problemas;
3. Em seguida, o processo inverso será testado (a segunda equipe recebe a mensagem).

Critérios de Avaliação:

1. Uso e entendimento correto dos conceitos matemáticos envolvidos (30%);
2. Organização do programa (20%);
3. Eficácia do programa: funcionamento correto no teste final, descrito na Observação 2 (25%);
4. Apresentação: didática e clareza na explicação, demonstração de domínio do assunto, e etc (25%).