Universidade Federal de Alagoas
Laboratório de Computação Científica e Visualização

Projeto: Módulo RSA

Thyago André Nunes Ribeiro

Abril
2019

Universidade Federal de Alagoas
Laboratório de Computação Científica e Visualização

Projeto: Módulo RSA

Relatório de desenvolvimento de um módulo de criptografia RSA, apresentado como parte do processo seletivo e treinamento do Laboratório de Computação Científica e Visualização.

Thyago André Nunes Ribeiro

Abril
2019

Sumário

1 Apresentação

Como parte do processo de treinamento foi solicitado o desenvolvimento de um módulo de criptografia RSA, utilizando a linguagem de programação Python.

O projeto consiste, basicamente, de um módulo RSA que gera, aleatoriamente, ou recebe do usuário um conjunto de chaves públicas e privadas e executa as operações de criptografia e descriptografia de mensagens. Esse módulo deve ser controlado por uma classe Cliente que, antes de garantir o acesso do usuário ao módulo, faz o gerenciamento de cadastro e autenticação de usuários.

Ao fim da execução do programa, a classe Cliente ainda é responsável por criptografar e armazenar os dados dos usuários cadastrados em um arquivo externo, utilizado, em uma nova execução, para pré-carregar os usuários no sistema.

2 Metodologia de implementação

A implementação do projeto dividiu-se em duas etapas. Na primeira, foram implementadas as classes e funções referentes ao módulo de criptografia RSA. Nessa fase, foram aplicados os conceitos apresentados em [1] referentes ao método de aplicação da criptografia RSA e as devidas funções e conhecimentos necessários.

Com isso, ao final do processo de implementação, foram obtidas as classes: RSA, responsável pela criação e gerenciamento das chaves públicas e privadas do módulo, bem como a garantia da validade de tais chaves, assim como o gerenciamento das chamadas dos métodos de codificação e decodificação da mensagem. A classe Encrypter, responsável pela pré-codificação da mensagem e a aplicação do algoritmo de criptografia RSA. E, por fim, a classe Decrypter, responsável pela aplicação do algoritmo de decodificação da criptografia RSA. Também foi criada uma biblioteca de funções lógicas e matemáticas, com métodos comuns aos processos de codificação e decodificação.

A segunda parte da implementação consistiu no desenvolvimento de uma classe Cliente, cuja principal funcionalidade é o gerenciamento de usuários do sistema. Essa classe é capaz de realizar operações de adição e remoção de usuários do sistema, assim como a verificação da existência de usuários cadastrados e sua devida autenticação no sistema. Além disso, a classe Cliente é responsável pelos processos de pré-carregamento da lista de usuários cadastrados na inicialização do sistema, bem como a exportação de tal lista para um arquivo externo antes de encerrar o programa.

Ao longo de todo o processo de implementação, foram realizados os devidos tratamentos de erros, segundo às especificações fornecidas para o projeto, bem como a documentação de todas as classes, módulos e métodos. Comentários adicionais foram adicionados ao longo do código a fim de esclarecer a compreensão de trechos de sua execução.

3 Conclusão

Analisadas e implementadas as especificações do projeto, obtivemos um sistema funcional, capaz de gerenciar usuários e seu devido acesso ao módulo de criptografia RSA, bem como realizar os devidos procedimentos de codificação e decodificação de mensagens.

Referências

[1] J. Evaristo and E. Perdigão. *Introdução à Álgebra Abstrata.* UFAL, 2013.