Criptografia

Cibersegurança e Defesa Cibernética

São Paulo
2025

INTEGRANTES DO PROJETO e RA'S

Daniel Baptista Acioli Vanderlei	23025608
Fábio Oliveira Spíndola	22086131
Fabrício Cândido do Nascimento	23025273
Leonardo de Souza Mouzinho	23025627

Sumário

1. Introdução

No projeto, foi adotado o algoritmo de criptografia RSA (Rivest-Shamir-Adleman) para proteger informações sensíveis dos usuários, como nome e email, antes de armazená-las no banco de dados. Essa medida visa garantir maior segurança e privacidade dos dados, evitando o acesso indevido a informações pessoais como Nome e E-mail.

O RSA é um algoritmo de criptografia assimétrica, amplamente utilizado para garantir a confidencialidade e autenticidade das informações. Diferentemente da criptografia simétrica, que usa a mesma chave para cifrar e decifrar, o RSA utiliza um par de chaves:

- **Chave Pública:** Usada para criptografar os dados. Pode ser compartilhada livremente.
- **Chave Privada:** Usada para descriptografar os dados. Deve ser mantida em segredo.

2. Como foi utilizado o RSA no projeto

2.1. Geração das Chaves

As chaves pública e privada são geradas previamente e armazenadas em arquivos public_key.pem e private_key.pem.

A chave pública é carregada pela aplicação para criptografar os dados antes do armazenamento.

2.2. Criptografia dos Dados

Ao receber os dados do usuário (nome e email) via requisição HTTP, a aplicação utiliza a chave pública para criptografar essas informações.

A criptografia é feita com o esquema OAEP (Optimal Asymmetric Encryption Padding) usando SHA-256, garantindo segurança contra-ataques de texto simples.

2.3. Armazenamento Seguro

Os dados criptografados (em formato base64 para facilitar o armazenamento) são salvos no banco de dados.

Dessa forma, mesmo que o banco seja acessado indevidamente, os dados sensíveis estarão protegidos, pois somente quem possuir a chave privada poderá descriptografá-los.

2.4. Descriptografia (Opcional)

Para acessar os dados originais, a aplicação deve usar a chave privada para descriptografar as informações.

Isso pode ser feito em um ambiente seguro e controlado, garantindo a confidencialidade.

3. Considerações Finais

Os benefícios da criptografia RSA incluem:

Segurança: Dados protegidos contra interceptação e acesso não autorizado.

Privacidade: Proteção da identidade e informações pessoais dos usuários.

Conformidade: Auxilia na conformidade com leis e regulamentações sobre proteção de dados.

A implementação do RSA no projeto representa uma camada importante de segurança para dados sensíveis, tornando a aplicação mais confiável e segura para os usuários.