Matheus Rafalski

TIAGO MALLMANN ROHDE

Segurança de Dados

17 de Março de 2025

Criptografia

INTRODUÇÃO

O trabalho foi realizado em Python em específico a versão 3.9, a escolha do python foi principalmente devido a sua função acadêmica que permite a abstração de diversos fatores para focar na parte principal da comunicação encriptada de mensagens além de eu ṕossuir um conhecimento prévio com a linguagem. Para realização do trabalho foi utilizado quatro bibliotecas principais:

- cryptography

  Para fazer a criptografia das mensagens, a escolha dela foi pelo fato de ela conseguir abstrair a complexidade de forma eficiente, tornando a implementação extremamente intuitiva, possui todas a funcionalidades necessárias e além disso eu tinha um conhecimento prévio de outras utilizações

- socket

  Para realização da comunicação entre os servidores, é uma biblioteca padrão do python que cumpre o objetivo de forma eficiente.

- base64 e json

Ambas bibliotecas padrões do python que cumprem o mesmo objetivo a transformação dos dados para serem possíveis serem enviados através da biblioteca socket, ambas já existem no python por padrão então optei por utiliza-las também.

EXECUÇÃO

A execução segue um fluxo base onde se inicia o servidor, o cliente conecta-se ao servidor por outra porta, o cliente se registra no servidor mandando a chave pública serializada, o servidor recebe a chave pública serializada então desserializar a chave pública criptografa uma mensagem e manda de volta para o cliente, o cliente recebe a mensagem criptografada então descriptografa com sua chave secreta e exibe a mensagem criptografada.

POSSÍVEIS CENÁRIOS

Entre os cenários mais comuns de uso do RSA está a transmissão segura de dados, como ocorre quando um cliente precisa enviar informações confidenciais a um servidor. Nesse caso, o cliente utiliza a chave pública do servidor para criptografar os dados, que só poderão ser descriptografados com a chave privada do servidor, garantindo que apenas o destinatário consiga acessar as informações.

Outro uso importante é na assinatura digital, utilizada para garantir a autenticidade e integridade de documentos e softwares. O emissor gera uma assinatura criptografando o hash do conteúdo com sua chave privada, e o receptor pode verificar a autenticidade usando a chave pública do emissor. Essa técnica é essencial, por exemplo, na distribuição de software confiável.