RELATÓRIO REDES

Relatório sobre a aplicação RSA

João da Silva Muniz Neto

Mateus Monteiro Santos

27.05.2021

INTRODUÇÃO

O modo como nos comunicamos hoje está alterado graças a Internet a qual faz o uso de vários tipos de serviços como movimentações bancárias, compras, jogos, etc. Todas estas atividades, além de muitas vezes serem mais produtivas e ágeis via Web e principalmente menos burocráticas ou melhor dizendo, burocráticas na medida certa para termos a segurança necessária, ainda nos possibilitam uma interação maior, seja com pessoas ou estabelecimentos comerciais, ainda mais na fase pandêmica que estamos enfrentando. Assim facilitando muitas vidas. E assim, como no dia-a-dia, são necessários vários cuidados com a nossa segurança e de nossos bens para que não sejam interceptados por qualquer um nessa rede. Visando este aspecto, a criptografia RSA é um dos primeiros sistemas de criptografia de chave pública e é amplamente utilizado para transmissão segura de dados. Assim temos essa solução para uma comunicação segura.

FUNCIONALIDADES

Esse trabalho busca trazer um servidor e cliente onde o usuário possa criptografar sua mensagem. Sendo assim, o servidor conterá a criptografia para a transformação da mensagem “humana” em uma mensagem criptografada. Quando o usuário digitar uma mensagem em uma linguagem usada por nós, será enviada a um servidor que terá um algoritmo de transformação em uma mensagem criptografada. Em seguida, a mensagem já criptografada retorna ao usuário para usos afins.

DIFICULDADES APRESENTADAS

Devido ao baixo conhecimento da equipe a respeito da linguagem python, houve dificuldade na manipulação das funções para obtê-las com êxito. Ademais, utilizamos a criptografia na sua pureza somente pelo cmd, já que no seu uso por arquivo vimos dificuldade na manipulação.

FUTURAS IMPLEMENTAÇÕES

- Uma interface para o usuário.
- Automatizar o uso da criptografia para não uso humano no servidor.
- Envio de arquivos para criptografia utilizando o protocolo UDP.
- Outros tipos de criptografia, além da RSA.

INSTRUÇÕES PARA UTILIZAÇÃO DA APLICAÇÃO

Primeiro, para o uso da aplicação, precisamos instalar alguns programas e pacotes:

- Instale Python3.9 (https://www.python.org/downloads/), ao acessar o link clique no botão amarelo “Download Python 3.9.5” (Na instalação lembre de marcar a opção “Add Python 3.9 to PATH” e siga em “Install Now”);
- Após a instalação do programa acima, será necessário o passo a passo da instalação do pip no PATH, para melhor esclarecimento, acesse o link: https://dicasdepython.com.br/resolvido-pip-nao-e-reconhecido-como-um-comando-interno/
- Após instalado o pip, faremos o uso do promt de command (cmd) para instalação de alguns pacotes, abra o cmd e instale com os seguintes comandos:
    - pip install python-socketio
    - pip install pickle4
    - pip install keyboard
    - pip install random2
    - pip install pycryptodome
- Após a instalação dos pacotes reinicie o cmd e baixe os arquivos no seguinte link do github (https://github.com/YodaDevs/Criptografia-RSA-com-Thread.git)
- Após baixado os dois arquivos, inicie o arquivo “server_thread.py” para abrir o servidor e inicie o arquivo “client_thread.py” para iniciar o cliente e ser possível a criptografia da mensagem. (lembrando que o servidor está em localhost)
- Aqui podemos ver que o servidor fará a criptografia perguntando quais números primos utilizaremos para gerar a criptografia, sendo assim podemos seguir passo a passo como solicitado no programa e ele retornará nossa mensagem.

CONCLUSÃO

Com o aperfeiçoamento sobre o assunto de redes e sobre a criptografia RSA, foi executada uma implementação que nos rendeu conhecimentos, como ditos antes, extras sobre esses assuntos. E em um futuro próximo poderemos aperfeiçoar ainda mais nossos estudos a respeito de ambas as matérias e ir implementando novas funcionalidades ao nosso projeto.

REFERÊNCIAS

Coutinho, Severino Colier. *Números inteiros e criptografia RSA*. IMPA, 1997.