FCT – FACULDADE DE CIÊNCIAS E TECNOLOGIA

DMC – DEPARTAMENTO DE MATEMÁTICA E COMPUTAÇÃO

BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

JUAN CARDOSO DA SILVA - 171257138

**MATÉRIA SEGURANÇA DA INFORMAÇÃO**

ATIVIDADE 4



**Presidente Prudente, 25/08/2022**

# **INTRODUÇÃO**

# **OBJETIVO**

O objetivo desse trabalho é ajudar o programador-aluno a entender como os mecanismos de criptografias assimétricas tais como o RSA, podem funcionar em conjunto de outros mecanismos distribuidores de chaves, neste caso, escolhido o Diffie-Hellmam.

Considerando o RSA, não existe compartilhamento de chaves, sejam públicas ou privadas, no meio de comunicação entre usuários, logo a utilização de um método seguro foi implementada para fazer o trabalho funcionar.

# **DISCUSSÃO**

O problema inicial no desenvolvimento foi a construção do RSA e pensar em um meio de fazer com que ambos lados dos usuários, A e B, possam desencriptar com sucesso as chaves, no mecanismo, a escolha do co-primo para execução do programa pode ser feita de maneiras diferentes, uma delas seria utilizar Diffie-Hellmam para compartilhar uma chave do qual é parte dos números primos geradores de e , considerando que seja um número primo quadrado de , entretanto essa geração não permite a aleatoriedade na geração de um co-primo.

Uma solução foi utilizar a chave final no calculo do Diffie-Hellman como um index para escolher números co-primos aleatórios de 2 até a Φ calculado pelo programa, assim dando um fator de segurança a mais ao projeto. Desta maneira foi possível encontrar um meio de compartilhar as chaves do Diffie-Hellmam e utiliza-las no RSA para poder realizar as criptografias entre usuários.

Na construção do projeto foi utilizado o protocolo UDP para realizar a comunicação entre as pessoas A e B, por ser um protocolo não voltado a conexão, utilizar mecanismos de criptografia desenvolvido nesse projeto é importante para adicionar uma camada de segurança, caso as pessoas A e B utilizem esse protocolo para se comunicarem, todo dado enviado está criptografado e qualquer terceira parte obtendo essas informações não seria capaz de compreender o que está sendo compartilhado entre elas.

Para gerar as encriptações, foi utilizado uma tabela de tuplas em Python, onde o caractere representa a chave (k) e o valor numérico correspondido a essa chave, sendo um valor (v), com essas tuplas é possível realizar o algoritmo de criptografia do RSA do qual:

O valor numérico é pego da seguinte maneira: comparando o char da string com o valor da chave, convertemos esse valor para inteiro e realizamos a conta, no calculo da volta, a mesma coisa é feita, mas começamos com o valor numérico direto e fazemos o cálculo do reverso, comparando o resultado com o valor da chave e acrescentando a chave a um construtor de string, assim, encriptando e desencriptando as trocas de mensagem.

**CONCLUSÃO**

Com isso concluímos que o RSA, como um poderoso mecanismo de criptografia, necessita de um método para definir os co-primos entre usuários, já que a natureza assimétrica do algoritmo, impede de compartilhamento de chaves, sendo assim, a necessidade de utilizar algo como o Diffie-Hellmam para conseguir com que ambos os lados, possam encriptar e desencriptar as mensagens trocadas.

# **CÓDIGO FONTE?**