UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"

LUIZ HENRIQUE SERAFIM DA SILVA

ALGORITMO RSA

Presidente Prudente
2023

Explicação do programa:

1- Importamos as bibliotecas necessárias - “random” para gerar números aleatórios e “gcd” (máximo divisor comum) da biblioteca “math”.

2- Definimos uma função interna “gerar_candidato_primo(comprimento)” para gerar um número primo candidato com um certo número de bits (“comprimento”). Para garantir que o número gerado seja ímpar, definimos o bit mais significativo e o menos significativo como 1.

3- Definimos uma função interna “e_primo(num, iteracoes=50)” para verificar se um número é primo usando o teste de Miller-Rabin. Essa função é usada para verificar se os números gerados são realmente primos.

4- Definimos uma função interna “gerar_primo(comprimento=1024)” para encontrar um número primo de aproximadamente “comprimento” bits. Essa função usa um loop para gerar candidatos até encontrar um número que passe no teste de primalidade.

5- Geramos dois números primos grandes, “p” e “q”.

6- Calculamos o módulo “n” para ambas as chaves, que é o produto de “p” e “q”.

7- Calculamos o totiente de Euler “phi(n)”, que é o produto de “(p - 1)” e “(q - 1)”.

8- Encontramos um número inteiro “e” que seja co-primo a “phi(n)”, ou seja, o maior divisor comum entre “e” e “phi(n)” é 1. Esse valor será o expoente da chave pública.

9- Usamos o algoritmo estendido de Euclides para encontrar o inverso multiplicativo de “e” modulo “phi(n)”. Esse valor será o expoente da chave privada.

10- Retornamos a chave pública “(n, e)” e a chave privada “(n, d)”.

11- Chamamos a função “gerar_par_chaves()” para obter as chaves pública e privada.

Para a distribuição da chave pública, a ideia central é que ela pode ser amplamente divulgada e compartilhada com qualquer pessoa que queira se comunicar com o proprietário da chave privada correspondente, afinal o algoritmo RSA é seguro mesmo quando a chave pública é de conhecimento público. A chave pública é usada para criptografar mensagens que serão enviadas ao proprietário da chave privada. Apenas a chave privada correspondente pode descriptografar as mensagens criptografadas. Algumas formas que pensei da divulgação são:

1- Assinaturas digitais: A chave pública pode ser enviada junto com assinaturas digitais em documentos ou e-mails, permitindo que outras pessoas verifiquem a autenticidade do remetente.

2- Servidores de chaves públicas: Existem servidores dedicados que armazenam e compartilham chaves públicas, como o PGP (Pretty Good Privacy) Global Directory.