Instruções

- Atividade em dupla. Ambos devem entregar.
- **Entrega Esperada:** 1 arquivo `.zip` com o código fonte.
  - Arquivos em outros formatos serão descartados.
  - Cópias serão descartadas.
  - Entregas atrasadas serão descartadas.

Descrição

Implemente um programa para criptografia e descriptografia de mensagens utilizando o algoritmo RSA.
Você pode utilizar materiais de aula para auxílio, incluindo o Capítulo 10 do livro "Criptografia e Segurança de Redes: Princípios e Práticas"de William Stallings 2006.

Requisitos

Entrada:

- Uma mensagem de texto em formato string (texto claro).

Processamento:

1. Converter mensagem para seu valor inteiro correspondente na tabela ASCII.
2. Gerar as chaves pública e privada.
3. Criptografar a mensagem usando a chave pública.
4. Descriptografar a mensagem utilizando a chave privada.
5. Converter os inteiros descriptografados de volta para caracteres ASCII.

Saída:

- Exibir a mensagem original (texto claro).
- Exibir a mensagem criptografada (valores inteiros).
- Exibir a chave pública (n, e).
- Exibir a chave privada (n, d).
- Exibir a mensagem descriptografada (texto claro).

Exemplo:

- Mensagem de entrada: abc
- Mensagem convertida para ASCII: 97 98 99
- Mensagem criptografada: (resultado dos cálculos RSA)
- Chave Pública: (n, e)
- Chave Privada: (n, d)
- Mensagem descriptografada (ASCII): 97 98 99
- Mensagem final (texto claro): abc

Observações Importantes

- Utilize uma biblioteca para manipulação de inteiros grandes (*big integers*) para garantir a precisão dos cálculos durante a geração de chaves e o processo de criptografia/descriptografia.
- Recomenda-se realizar testes com palavras curtas (exemplo: "teste", "abc", etc.), para facilitar a validação dos resultados.
- A conversão ASCII deve ser feita imediatamente após a entrada da mensagem, antes da criptografia.
- Após a descriptografia, deve-se realizar o processo inverso, convertendo os inteiros de volta para os caracteres ASCII.

Linguagens de Programação Permitidas

- *C*;
- *C++*;
- *Java*;
- *C#*.
-

Referências

STALLINGS, William; BROWN, Lawrie. **Computer security: principles and practice**. 1. ed. São Paulo: Pearson Prentice Hall, 2015. p. 492. ISBN 9788576051190.