UNIVERSIDADE REGIONAL DE BLUMENAU
CENTRO DE CIÊNCIAS EXATAS E NATURAIS
DEPARTAMENTO DE SISTEMAS E COMPUTAÇÃO
PROFESSOR GILVAN JUSTINO
SEGURANÇA DA INFORMAÇÃO

Lista de Exercícios 9

O objetivo desta lista de exercícios é praticar a utilização de algoritmo de chave assimétrica. Forme dupla com outro aluno para resolver esta lista de exercícios.

Neste exercício, você e outro colega irão trocar mensagens sigilosas, para isso:

1) Cada aluno deve gerar seu par de chaves
    a. Guarde cada chave num arquivo separado.
    b. Crie uma convenção sobre como armazenar a chave
2) Cada aluno deve compartilhar sua chave pública um com o outro

Questão 1

Cada aluno deve cifrar uma frase pequena (até 50 caracteres) para ser enviada para o colega. Salve a mensagem cifrada num arquivo e compartilhe com seu colega.

O outro aluno, deve usar sua chave privada para descriptografar a mensagem.

Questão 2

Tente criptografar o arquivo PDF deste exercício. Qual o comportamento do programa?

Questão 3

Cada aluno deve cifrar uma imagem qualquer usando AES e disponibilizar o arquivo cifrado para seu colega.
Em seguida, cada aluno deve cifrar a chave simétrica usando o RSA e compartilhar a chave cifrada para o colega.
Depois disso, descriptografe a imagem recebida pelo colega, usando a chave AES recebida.

Compartilhe no AVA:

- Os pares de chaves usados
- Os arquivos criptografados e descriptografados da questão 3