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. Responda as perguntas de cada questão.

Questão 1

Crie um programa que gere um par de chaves privada e pública relacionadas.

Exiba o valor do módulo e dos expoentes de cada chave gerada.

Salve cada uma das chaves num arquivo separado, pois as chaves precisarão ser recuperadas nas questões seguintes.

Qual é o expoente e o módulo do par de chaves gerados?

Questão 2

Crie um programa que criptografe um arquivo submetido pelo usuário utilizando o algoritmo AES.

Criptografe a chave simétrica utilizada (do algoritmo AES) utilizando a chave pública gerada na questão 1.

Qual é o texto simples e o texto cifrado pelo algoritmo RSA?

Questão 3

Crie um programa que decriptografe a chave de um algoritmo AES, utilizando a chave simétrica gerada na questão 2. Será preciso recorrer a chave privada, gerada na questão 1, para poder decifrar a chave.

Decriptografe o arquivo utilizando a chave obtida.