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

Lista de Exercícios 8

Publique as soluções no AVA e salve os resultados num documento no Word, conforme indicado em 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.

Num documento do Word, coloque o expoente da chave pública, da chave privada 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 (do algoritmo AES) utilizando a chave pública gerada na questão 1.

Num documento do Word, coloque o texto simples, bem como o texto cifrado pelo algoritmo RSA.

Questão 3

Crie um programa que decriptografe a chave de um algoritmo AES, utilizando a chave assimétrica privada gerada na questão 1.

Decriptografe o arquivo utilizando a chave obtida.