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

Trabalho

Construa um programa que implemente a criptografia e descriptografia através do algoritmo AES. O programa deve atender aos seguintes requisitos:

a) Permitir que o usuário selecione a operação que deseja realizar (cifrar ou decifrar).

b) Permitir que o usuário informe o arquivo a ser cifrado ou decifrado. O programa deverá suportar qualquer arquivo (texto ou binário) e de qualquer tamanho;

c) Permitir que o usuário possa informar o nome do arquivo de destino a ser gerado;

d) Permitir que o usuário forneça a chave de cifragem/decifragem. Deve ser um campo texto em que possa ser fornecido os valores dos bytes da chave em formato decimal, separando-os por vírgula. Por exemplo: este é um texto que deve ser possível fornecer para indicar os bytes da chave: "20,1,94,33,199,0,48,9,31,94,112,40,59,30,100,248";

e) Implementar o modo de operação ECB e tamanho de chave de 128 bits;

f) Implementar o modo de preenchimento PKCS#7;

g) A solução não pode ser cópia de outros autores e deve utilizar a abordagem vista em sala de aula, isto é, com as etapas de expansão de chave e criptografia. Não deve ser reutilizada uma biblioteca de cifragem.

Pode ser utilizada qualquer linguagem de programação. Para testar seu programa, você pode reusar uma biblioteca para cifragem e comparar com a sua saída do seu programa.

O trabalho poderá ser feito em equipe de até 3 pessoas. Informe no formulário abaixo os integrantes da sua equipe.
https://forms.office.com/r/55GzavrECq

O trabalho deve ser publicado até o dia 10/11/2024.