

Trabalho

Construa um programa que implemente o algoritmo de criptografia AES. O programa deve atender aos seguintes requisitos:

- a) Permitir que o usuário informe um arquivo a ser criptografado. O programa deverá suportar qualquer arquivo (texto ou binário) e de qualquer tamanho;
- b) Permitir que o usuário possa informar o nome do arquivo de destino a ser gerado;
- c) Permitir que o usuário forneça a chave de criptografia. 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";
- d) Implementar o modo de operação ECB e tamanho de chave de 128 bits;
- e) Implementar o modo de preenchimento PKCS#7;
- f) 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.

Não implementaremos neste programa a decifragem. 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/cSSBcXJj4i>

O trabalho deve ser publicado até o dia 03/11/2023.