Tarefa 4

Descrição

A tarefa 4 consiste no desenvolvimento de um software que utiliza algoritmos de criptografia para garantir o requisito de confidencialidade de um arquivo de texto. O software deve implementar as seguintes etapas:

1ª. etapa: o usuário deve digitar o seu nome e solicitar a geração de um par de chaves assimétricas (ex. Luciano.pu e Luciano.pr).

2ª. etapa: o usuário deve selecionar o arquivo texto que ele deseja criptografar (ex. x.txt).

3ª. Etapa: o usuário deve solicitar a criptografia do arquivo do texto claro. O software deve gerar de forma pseudoaleatória uma chave simétrica (ex. K.txt), a qual deve ser usada na criptografia do arquivo, criando o texto cifrado (ex. Y.txt). Se for necessário, o software também deve gerar o vetor de inicialização de forma pseudoaleatória. Deve ser implementado apenas o algoritmo AES, usando o modo CBC e chave de 128 bits.

4ª. Etapa: Posteriormente, o usuário deve selecionar os arquivos com a chave simétrica e o vetor de inicialização (pode ser uma de cada vez) e criptografa-los usando a chave pública.

Acima está descrito o processo de criptografia de dados. A equipe também deve implementar o processo de decifragem da chave simétrica e do vetor de inicialização usando a chave privada e, posteriormente, a decifragem do arquivo criptografado com o algoritmo AES.

Importante: o software deve permitir a execução independente do processo de cifragem e decifragem de uma informação. Ou seja, deve permitir que um usuário realize a criptografia do arquivo, envie o arquivo criptografado pela rede e um segundo usuário realize a decriptografia, fazendo uso do mesmo software.

Entregáveis

A equipe necessita entregar os códigos-fonte do software, juntamente com a versão compilada.

Mérito

- Atendimento completo dos requisitos.