Pontifícia Universidade Católica de Minas Gerais

Instituto de Ciências Exatas e Informática

AED III - Trabalho Prático
Fase IV do TP

Objetivo

Aplicar **compressão** aos **arquivos de dados** do sistema e criptografar **ao menos um campo** dos registros (escolha justificada pelos alunos). Preservar o funcionamento e a integridade das etapas anteriores (CRUD, índices, etc.).

Requisitos

1. Compressão — **obrigatória sobre todos os arquivos de dados.**
    a. O resultado deve ser **um arquivo único compactado**.
    b. A compactação é **exclusivamente a nível de arquivo**, funcionando como um **backup completo**.
    c. O sistema deve gerar **um único arquivo compactado**, contendo os arquivos utilizados pelo aplicativo.
    d. O algoritmo de compressão deve ser **Huffman e LZW**.
2. Criptografia de, pelo menos, um campo de uma tabela
    a. Uso obrigatório de **RSA**.
    b. Proibido usar **Cifra de César, Vigenère, ROT13, XOR simples** ou quaisquer cifras clássicas fracas.
    c. O campo criptografado deve ser armazenado no arquivo já criptografado **antes** de ser gravado no .db.

Formulário

1. Qual foi a taxa de compressão obtida com o algoritmo de Huffman?
    a. Tamanho do arquivo original
    b. Tamanho do arquivo comprimido
    c. Cálculo da taxa
    d. Interpretação do resultado
2. Qual foi a taxa de compressão obtida com o algoritmo de LZW?
    a. Tamanho do arquivo original
    b. Tamanho do arquivo comprimido
    c. Cálculo da taxa
    d. Interpretação do resultado
3. Quais dificuldades surgiram ao implementar Huffman e LZW e como você resolveu?
4. Justifique a escolha da estrutura de dados usada para armazenar as tabelas, dicionários e árvores utilizados pelos algoritmos.

5. Qual campo foi escolhido para criptografia? Por quê?
6. Descreva como o RSA foi implementado no projeto.
    a. Estrutura das chaves pública e privada
    b. Como e onde foram armazenadas
    c. Como foram carregadas pelo sistema
    d. Tamanho das chaves escolhidas e justificativa
    e. Em qual momento a criptografia do(s) campo(s) ocorre (no CRUD).
    f. Em qual momento ocorre a descriptografia.
    g. Conversões realizadas (ex.: string → bytes → blocos).

Entrega

A entrega deve ser feita exclusivamente via Canvas, em um único arquivo PDF contendo:

1. Link para o GitHub
2. Atualização do README no GitHub, com instruções claras de compilação e execução.
3. Formulário técnico (acima) no relatório

Critérios de Avaliação (5 pontos)

Critério	Pontos
Compressão com Huffman	1.0
Compressão com LZW	1.0
Criptografia RSA	1.5
Documentação e Formulário	1.0
Organização e Execução no GitHub	0.5