DOCUMENTAÇÃO – CRIPTOGRAFIA DAS SENHAS

CONTEXTUALIZAÇÃO

A ModalGR possui um cofre eletrônico e precisa ser protegido por 3 senhas, na qual vão estar criptografadas por métodos diferentes, mas com a mesma chave de acesso.

PROBLEMÁTICA

Desenvolver um sistema que após a entrada de três senhas o programa realize a criptografia dessas senhas.

SOLUÇÃO

Escolha dos métodos de criptografia:

- Cifra de Cesar;
- Xxx;
- Xxx.

Linguagem de programação: Linguagem C

Ambiente de desenvolvimento: CodeBlocks.

Chave secreta: #modalGr#GPTW#top#maiorEmpresaTecnologia#baixadaSantista

O sistema deve receber as senhas do usuário, onde o sistema tem como objetivo criptografar essas três senhas.

ESCOPO DO SISTEMA

Chave secreta: #modalGr#GPTW#top#maiorEmpresaTecnologia#baixadaSantista

Título: ModalGR cofre eletrônico

- Digite a primeira senha;
- Digite a segunda senha;

- Digite a terceira senha;

Cada senha foi criptografada e armazenada em um arquivo txt.

O usuário precisa digitar a chave de acesso para acessar as senhas criptografadas; após isso o sistema lê um arquivo onde todas as senhas estão armazenadas e mostra na tela;

PRIMEIRA SENHA - Método de criptografia: Cifra de Cesar.

A escolha do método de criptografia Cifra de Cesar foi por ter regras de desenvolvimento na qual não exige de muito tempo, logo, seu desenvolvimento é mais acelerado. Além disso, pode ser considerado um método de criptografia simétrica, que consiste em usar a mesma chave para criptografar e descriptografar.

Esse método consiste em percorrer o alfabeto de acordo com um número fixo de deslocamento a partir do texto original.

SEGUNDA SENHA - Método de criptografia: Substituição simples.

A Cifra de Substituição Simples é um método clássico de criptografia que envolve a substituição de cada letra do alfabeto por outra letra, de acordo com uma tabela de substituição pré-definida. Este processo é bastante simples, mas pode proporcionar algum grau de segurança contra métodos de quebra mais simples.

TERCEIRA SENHA - Método de criptografia: Cifra de bloco invertido

A Cifra de Bloco Invertido é um método simétrico, o que significa que a mesma chave é usada para criptografar e descriptografar, logo, isso pode simplificar e acelerar implementação e reduzir a complexidade.

- O tempo de desenvolvimento é menor.

Esse método opera invertendo os blocos de caracteres em uma string.