

Relatório - Criptografia com Cifra de César

Breno Arthur Rotte Fernandes Oliveira - 20.1.8124

Jhonatan Figueiredo Almeida - 20.1.8164

1. Introdução

Nesse trabalho, a gente desenvolveu um programa em Haskell que usa a Cifra de César para criptografar e descriptografar mensagens. Basicamente, ele pega cada letra da mensagem e desloca um certo número de posições no alfabeto. Também fizemos um menu no terminal para facilitar o uso.

2. Como fizemos o programa

Para deixar o programa mais organizado e funcionando direito, tomamos algumas decisões:

Criamos funções separadas: Uma para criptografar, outra para descriptografar e mais algumas para tratar o texto.

Mantivemos maiúsculas e minúsculas: Se uma letra era maiúscula, continua maiúscula depois de ser cifrada.

Os espaços e caracteres especiais continuam iguais: O programa só mexe nas letras, não altera números, espaços e sinais de pontuação.

Criamos um menu simples: Assim, a pessoa escolhe se quer criptografar ou descriptografar uma mensagem.

Validamos a chave de cifragem: Para evitar erros, o programa confere se a pessoa digitou um número antes de continuar.

3. Dificuldades que encontramos

Tivemos que resolver alguns problemas ao longo do programa:

Deslocamento das letras: No começo, algumas letras saíam do alfabeto e ficavam erradas. Resolvemos isso ajustando os cálculos com ord e chr para que elas voltassem ao começo do alfabeto quando passavam do "Z" ou do "z".

Caracteres especiais não deviam ser alterados: No início, o programa tentava cifrar tudo, até espaços e pontuação. Ajustamos isso para modificar só as letras.

Problema na exibição das mensagens: Algumas vezes o terminal pedia a entrada antes de mostrar as mensagens, então usamos hFlush stdout para corrigir isso.

4. Melhorias que poderiam ser feitas

Nosso programa funcionou direito, mas dá para melhorar algumas coisas:

Criar uma interface mais visual: Em vez de usar o terminal, poderíamos fazer um programa com botões.

Salvar e carregar mensagens: Seria legal ter a opção de salvar as mensagens criptografadas em um arquivo e depois descriptografá-las automaticamente.

Adicionar suporte a acentos: Por enquanto, o programa só funciona com letras do alfabeto sem acentos. A gente poderia adaptar para incluir á, é, ç, etc.

5. Conclusão

No fim, conseguimos fazer um programa que criptografa e descriptografa mensagens usando a Cifra de César de um jeito simples. O menu deixa tudo mais fácil de usar e o programa respeita maiúsculas, minúsculas e caracteres especiais. No geral, conseguimos atender todos os requisitos do trabalho e ainda aprendemos bastante sobre Haskell no processo.