INSTITUTO FEDERAL
Triângulo Mineiro
Campus Uberlândia Centro

Tecnologia em Sistemas para Internet
1º Semestre 2016

Professor	Disciplina
Saulo da Mata	Segurança em Sistemas para Internet

Laboratório L02

Tema: Cifra de César (*Caesar Cipher*).

Descrição

A cifra de César é a mais antiga e talvez a mais conhecida técnica de criptografia por substituição. Apesar de simples, esta cifra é a base para diversas outras cifras de substituição.

Objetivos

Exercitar o uso da Cifra de César. Neste laboratório o aluno terá a oportunidade de testar seus conhecimentos sobre esta cifra clássica, bem como testar a capacidade de resolução de problemas através de algoritmos. Outro objetivo indireto deste laboratório é dar a oportunidade aos de alunos de exercitar o uso de uma linguagem de programação para implementar algoritmos.

Tarefas

Criar um programa para encriptação e decodificação de mensagens criptografadas com a Cifra de César padrão (k = 3).
Para avaliar se o programa está correto, cada grupo deverá decodificar uma mensagem criptografada e enviada pelo professor. A mensagem contém instruções que devem ser seguidas pelos alunos. Cada grupo tem sua própria mensagem.

Alguns detalhes de implementação:

- O aluno tem liberdade para escolher a linguagem de programação e a estratégia do algoritmo.
- Nesta versão da cifra de César, não iremos criptografar caracteres especiais, apenas as 26 letras do alfabeto. Dessa forma, a mensagem "ATENÇÃO!" seria criptografada como "DWHQÇÃR!".
- O programa deverá ler um arquivo .txt que contém a mensagem criptografada e escrever o texto decodificado em um outro arquivo .txt.

Para acessar o arquivo criptografado, cada grupo deve acessar **esta planilha**, escolher e se inscrever (colocando o nome dos integrantes) em alguns dos grupos designados na planilha.

Prazo
A atividade deverá ser realizada durante as aulas dos dias **14/04/2016** e **19/04/2016**. Caso o aluno não consiga concluir a atividade ou tenha faltado a aula, ela deverá ser entregue até o dia **21/04/2016**.

Valor
Este trabalho vale: **2 pontos**.

Observações: O trabalho poderá ser realizado em grupos de até dois integrantes.