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 L03

Tema: Cifra de Vigenère (*Vigenère Cipher*).

Descrição

A mais conhecida, e uma das mais simples cifras polialfabéticas é a Cifra de Vigenère. Neste esquema, aplica-se um conjunto de regras de substituições monoalfabéticas baseadas na Cifra de César. Apesar de simples, a cifra de Vigenère manteve-se inquebrável por centenas de anos. Agora é hora de praticar a teoria já estudada sobre esta importante técnica de criptografia.

Objetivos

Exercitar o uso da Cifra de Vigenère. 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 alunos de exercitarem o uso de uma linguagem de programação para implementar algoritmos.

Tarefas

Criar um programa para criptografar e decodificar mensagens criptografadas com a Cifra de Vigenère. A chave criptográfica é a palavra **SHAME**.
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 Vigenère, 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 **28/04/2016** e **03/05/2016**.

Valor
Este trabalho vale: **3 pontos**.

- Código fonte: **0.7 pontos**.
- Arquivo de instruções decodificado: **1.05 pontos**.
- Arquivo de resposta criptografado: **1.05 pontos**.
- Resposta correta: **0.2 pontos**.

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