4. Criptografia

Disciplina: LAED - Laboratório de Algoritmos e Estruturas de Dados I
Prazo de Entrega: 05/09/2019 23:55:55 Fechado
Em grego, cryptos significa secreto, oculto. A criptografia estuda os métodos para codificar uma mensagem de modo que somente seu destinatário legítimo consiga interpretá-la. É a arte dos “códigos secretos” (Coutinho, 2015).

Uma das técnicas de criptografia mais simples e conhecida consite em substituir cada letra da mensagem por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes. Conta a história que Júlio César (100-44 a.C.) utilizava este código nas mensagens enviadas a seus generais.

A transformação pode ser representada alinhando-se dois alfabetos: o alfabeto cifrado e o alfabeto normal rotacionado à direita ou esquerda por um número de posições. Por exemplo, a seguir está uma cifra de César usando uma rotação à esquerda de três posições:

```
Normal:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC
```

Embora cifra de César seja facilmente decifrada e na prática não ofereça essencialmente nenhuma segurança na comunicação, é frequentemente incorporada como parte de esquemas mais complexos de criptografia (Wikipedia, 2019).

Este exercício consiste em ler uma mensagem criptografada de um arquivo texto e imprimir a mensagem descriptografada na saída padrão. A técnica de criptografia será a de códigos em bloco, que consiste em subdividir a mensagem em blocos de várias letras e embaralhar esses blocos. Antes, porém, será utilizada a cifra de César.

Por exemplo, considere a mensagem AMO LIVROS. Para codificá-la seguiremos os seguintes passos:

```
• Substituir os espaços pelo símbolo # e completar a mensagem com este mesmo símbolo no fin
al, caso tenha uma quantidade ímpar de letras;

• Substituir cada letra por outra, utilizando a cifra de César com uma rotação à esquerda d
e três posições;

• Subdividir a mensagem em blocos de n letras (neste caso n=2);

• Refletir cada bloco;

• Permutar os blocos trocando o primeiro com o último, o terceiro com a antepenúltimo, e as
sim por diante, mas deixando os outros como estão.
```

Aplicando isto, passo a passo, à mensagem acima, obtemos primeiro:

AMO#LIVROS

Depois usamos a cifra de César:

DPR#OLYURV

Separamos em blocos de 2 letras:

DP-R#-OL-YU-RV

em seguida

PD-#R-LO-UY-VR

E, finalmente,

VR-#R-LO-UY-PD

que nos dá como mensagem codificada:

VR#RLOUYPD.

Use o método explicado para poder decodificar a mensagem contida em um arquivo texto cujo nome será lido da entrada padrão. Para simplificar, foram eliminados acentos e pontuação. As letras maiúsculas e minúsculas do texto deverão ser mantidas.

A saída do programa deverá seguir o padrão abaixo, mas lembre-se que o seu programa será testado com arquivos distintos:

```
Digite o nome do arquivo: mensagem.txt

--------------------
Mensagem codificada:
--------------------
rglfil#drwF#w#udvdgrsdhvkqdi#hpohxhwrpfhp#dudgilvhg#t#qhv#lfhw#u#d#hqhs#r#vhahhgf#uidu#D

----------------------
Mensagem decodificada:
----------------------
A cifra de Cesar pode ser facilmente decifrada mesmo que se tenha apenas o texto cifrado
```

Referências:

Coutinho, S. C. Criptografia. 2015. Disponível em: http://www.obmep.org.br/docs/apostila7.pdf.

Wikipedia. Cifra de César. 2019. Disponível em: https://pt.wikipedia.org/wiki/Cifra*de*C%C3%A9sar.