

Pesquisa e Ordenação - 2003

Trabalho Prático nº 1 Cifragem por substituição

Introdução

Este trabalho deverá ser realizado por grupos de até três alunos. O trabalho deve ser entregue impreterivelmente até o dia **26 de junho**, e corresponde a metade da nota do 2º. bimestre (média aritmética simples com a nota da prova).

Enunciado

Pretende-se que neste trabalho os alunos estudem o comportamento dos métodos de cifragem por substituição, como passo introdutório à criptografia.

Um esquema de codificação de textos usado há mais de 2000 anos é a chamada Cifra de César. Esse esquema de codificação era utilizado pelo imperador romano para se comunicar com seus generais. Para implementá-lo, siga os seguintes passos:

Numa primeira etapa, substitua as ocorrências de brancos e sinais de pontuação por uma seqüência de caracteres seguindo a seguinte tabela:

Tabela 1

Caracter	Substituição
(branco)	WBRW
,	WVRW
.	WPTW
;	WPVW
:	WDPW
!	WEXW
?	WINW
-	WHFW

Depois de feita essa substituição o texto terá apenas letras do alfabeto. Então, dado um natural k , substitua cada letra i pela $(i+k)$ -ésima letra do alfabeto, aplicando rotação (ou seja, após a última letra segue-se a primeira novamente). Observe o exemplo a seguir:

Texto original:

ESSE EXERCICIO-PROGRAMA VAI SER MUITO FACIL.

Após substituir-se os brancos e sinais de pontuação:

ESSEWBRWEXERCICIOWHFWPROGRAMAWBRWVAIWBRWSEWBRWUITOWBRWFACILWPTW

Então, usando-se $k = 2$, obtemos o seguinte texto codificado:

```
GUUGYDITYGZGTEKEKQYJHYRTQITCOCYDITYXCKYDITYUGTYDITYOWKVQYDITYHCEKNYRVY
```

O que você deve fazer

Você irá programar um sistema completo de criptografia, ou seja, você deverá fazer um programa que:

1. leia um string s (vetor de caracteres) contendo um texto;
2. leia um natural k ;
3. leia uma opção: 1 para cifrar ou 2 para decifrar;
4. se a opção for 1, então seu programa deverá cifrar o texto contido no string s e em seguida imprimi-lo;
5. se a opção for 2, então seu programa deverá decifrar o texto contido no string s e em seguida imprimi-lo (com espaços em branco e sinais de pontuação).

Como você deve fazer este exercício

Para fazer seu programa, você deverá implementar as seguintes funções – os exemplos estão em C, mas você pode utilizar a linguagem que achar mais conveniente:

1. `void troca_sinal (char frase_sai[], char frase_ent[], char sinal, char pal[]);`

Percorre a frase guardada em *frase_ent*, trocando toda ocorrência do sinal de pontuação guardado em *sinal* pela palavra guardada em *pal*. A frase obtida é armazenada em *frase_sai*.

Por exemplo, a chamada

```
troca_sinal (frase, "AH! AH! AH!", '!', "WEXW");
```

coloca no vetor *frase* o string "AHWEXW AHWEXW AHWEXW".

2. `void troca_todos_sinais (char frase_sai[], char frase_ent[]);`

Troca todos os sinais da Tabela 1 que ocorrem na frase guardada em *frase_ent* pelos respectivos strings e coloca a frase obtida em *frase_sai*.

Por exemplo, a chamada

```
troca_todos_sinais (frase, "FACIL? - SIMPLES!");
```

coloca no vetor *frase* o string "FACILWINWWBRWWHFWWBRWSIMPLESWEXW".

OBS.: Esta função deve **obrigatoriamente** usar a função do item 1.

3. `void troca_letras (char frase_sai[], char frase_ent[], int k);`

Esta função troca cada letra *i* da frase guardada em *frase_ent* pela (i+k)-ésima letra do alfabeto (após a última letra, segue-se a primeira novamente). A nova frase obtida é armazenada em *frase_sai*.

Por exemplo, a chamada

```
troca_letras (frase, "ESSEWBRWEXERCICIOWBRWEWBRWLEGALWPTW", 2);
```

coloca no vetor *frase* o string "GUUGYDITYGZGTEKEKQYDITYGYDITYNGICNYGZY".

4. `int procura_pal (char frase[], int i, char pal[]);`

Esta função procura no vetor *frase*, a partir da posição *i*, a palavra guardada em *pal*. Esta função retorna -1, se a palavra *pal* não está no vetor *frase* a partir da posição *i*, ou o índice da primeira ocorrência da palavra.

Exemplos:

```
c = procura_pal ("FACILWINWWBRWWHFWWBRWSIMPLESWEXW", 0, "WINW");  
c recebe o valor 5.
```

```
c = procura_pal ("FACILWINWWBRWWHFWWBRWSIMPLESWEXW", 9, "WINW");  
c recebe o valor -1.
```

```
c = procura_pal ("FACILWINWWBRWWHFWWBRWSIMPLESWEXW", 13, "WBRW");  
c recebe o valor 17.
```

5. `void troca_string (char frase_sai[], char frase_ent[], char pal[], char sinal);`

Percorre a frase guardada em *frase_ent*, trocando toda ocorrência do string guardado em *pal* pelo sinal de pontuação guardado em *sinal*. A frase obtida é armazenada em *frase_sai*.

Por exemplo, a chamada

```
troca_string (frase, "AH!WBRWAH!WBRWAH!", "WBRW", ' ');
```

coloca no vetor *frase* o string "AH! AH! AH!".

OBS.: Esta função deve **obrigatoriamente** usar a função do item 4.

6. `void troca_todos_strings (char frase_sai[], char frase_ent[]);`

Troca todos os strings da Tabela 1 que ocorrem na frase guardada em *frase_ent* pelos respectivos sinais e coloca a frase obtida em *frase_sai*.

Por exemplo, a chamada

```
troca_todos_strings (frase, "FACILWINWWBRWWHFWWBRWSIMPLESWEXW");
```

coloca no vetor *frase* o string "FACIL? - SIMPLES!".

OBS.: Esta função deve **obrigatoriamente** usar a função do item 5.

O seu programa

A chamada de execução de seu programa deve utilizar **obrigatoriamente** as funções dos itens 2, 3 e 6.

Desafio

Você seria capaz de decifrar o texto abaixo?

```
VJNSINZJKNSINVZENSINKVOKNSINZENSINUVLKJTYNGKNNSINVJNSINNRVIVNSINQLNSINVZEWRTYNMIN  
NSINNVEENSINUVINSINKVOKNSINZENSINGFIK LXZVJZJTYNSINXVJTYIZVSVENSINNFIUVENSINNRVIVN  
GKNNSINZTYNSINNVZJJNGKNNSINZTYNSINNVZJJNMINNSINVJNSINZJKNSINEZTYKNSINWRZINGKNNSIN  
YVIQCZTYVENSINXCLVTBNLVEJTYVENSINQLDNSINXVNZE EVINNONNVONNVON
```

Referência

Este exercício foi proposto pelo Prof. Ronaldo Fumio Hashimoto, do Instituto de Geociências da USP. Disponível em <<http://www.ime.usp.br/~ronaldo/mac115/ig98/eps/ep3/ep3.html>>. Acesso em 26 de jun. de 2003.