Trabalho de Programação – Processador RAMSES

1. Descrição Geral

Conforme consta na Wikipedia (https://pt.wikipedia.org/wiki/Cifra_de_substituição): "Em criptografia, uma cifra de substituição é um método de criptografia que opera de acordo com um sistema pré-definido de substituição. Para criptografar uma mensagem, unidades do texto - que podem ser letras isoladas, pares ou outros grupos de letras - são substituídas para formar a cifra. As cifras de substituição são decifradas pela substituição inversa".

Existem diversos tipos de cifras de substituição. Se a cifra opera com letras isoladas, é denominada cifra de substituição simples. Uma cifra monoalfabética usa uma só substituição fixa na mensagem inteira.

Nesse trabalho você deverá desenvolver um programa para o processador RAMSES que seja capaz de cifrar e decifrar um string, usando a substituição simples, monoalfabética fixa.

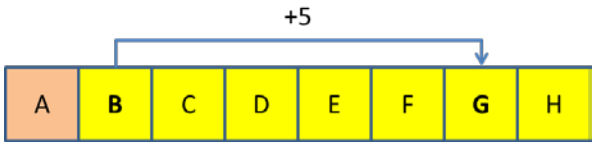
O string a ser cifrado chama-se "*mensagem oral*". O string cifrado chama-se de "*mensagem cifrada*".

Strings: sequencia de bytes que representam as letras maiúsculas entre "A" e "Z" e que termina com "\0" (valor 0).

Cifrar: para cifrar uma letra, basta somar o valor da letra ao passo de cifragem. Caso o resultado ultrapasse o valor ASCII da letra "Z" (90), deve-se continuar a partir da letra "A", de forma circular (diminuir 26).

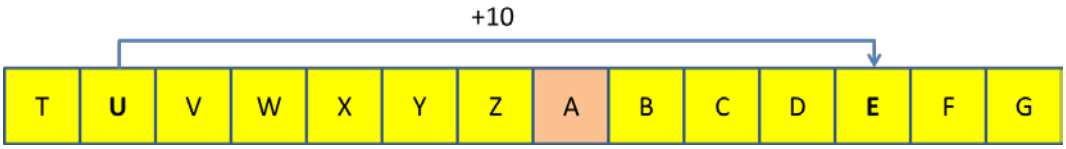
Exemplo 1: Cifrar a letra "B" com passo=5.

- ASCII("B")+5 = 66+5 = 70 = ASCII("G").
- Portanto, a cifragem de "B" com passo 5 é a letra "G"



Exemplo 2: Cifrar a letra "U" com passo=10.

- ASCII("U")+10 = 85+10 = 95
- Como 95 é maior do que 90, temos de retornar e continuar a partir da letra "A".

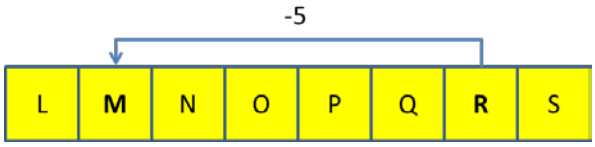


- Portanto, a cifragem de "U" com passo 10 é a legra "E"
- Observar que, neste caso, o valor obtido pela soma com o passo deverá ser diminuído do valor 26. (95 – 26 = 69, que é o ASCII da letra "E")

Decifrar: para decifrar uma letra, basta aplicar a função inversa da função usada na cifragem. Ou seja, basta diminuir o passo e, caso o resultado seja um valor menor do que o ASCII da letra "A" (65), deve-se continuar a partir da letra "Z", de forma circular (somar 26).

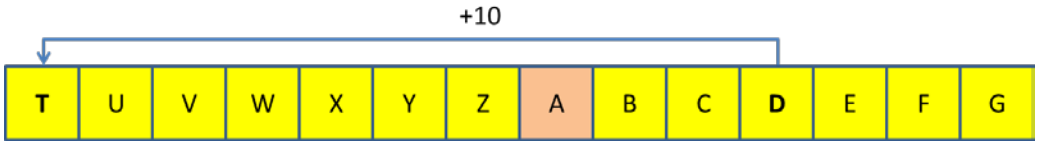
Exemplo 3: Decifrar a letra "R" com passo=5.

- ASCII("R")-5 = 82-5 = 77 = ASCII("M").
- Portanto, a decifragem de "R" com passo 5 é a letra "M"



Exemplo 4: Decifrar a letra “D” com passo=10.

- ASCII(“D”)-10 = 68-10 = 58
- Como 58 é menor do que 65, temos de retornar e continuar a partir da letra “Z”.



- Portanto, a decifragem de “D” com passo 10 é a legra “T”
- Observar que, neste caso, o valor obtido pela diferença com o passo deverá ser somado com o valor 26. (58 + 26 = 84, que é o ASCII da letra “T”)

2. Disposição dos dados na memória

Ao iniciar a execução, seu programa vai encontrar na memória as seguintes informações, que deverão ser usadas para gerar o resultado solicitado.

- Endereço 192: contém o endereço de início do string a ser processado pelo seu programa (SRC);
- Endereço 193: contém o endereço de início do string onde colocar o resultado do seu programa (DST);
- Endereço 194: passo de deslocamento para o processamento da mensagem oral (PASSO). Valor entre 1 e 25;
- Endereço 195: processamento a ser realizado (OPERACAO): Valor zero, se for cifragem, ou um valor diferente de zero, se for decifragem.

O string a ser processado e o string de resultado estarão, sempre, contidos na área de memória que inicia no endereço 196 e termina no endereço 255. Os string nunca estarão sobrepostos.

Seu programa deve estar completamente contido entre o endereço 0 (zero) e o endereço 191. Isso inclui todas as variáveis que o seu algoritmo precisa para operar.

3. Exemplo

Cifrar a palavra “ARQUITETURA”, que inicia no endereço 200, usando um “passo” igual a 7. O resultado deve ser escrito a partir do endereço 220.

Isso significa que, ao iniciar a execução de seu programa, ele vai encontrar as seguintes informações na memória:

- Endereço 192 (SRC) contém 200;
- Endereço 193 (DST) contém 220;
- Endereço 194 (PASSO) contém 7;
- Endereço 195 (OPERACAO) contém 0 (zero)

Além disso, o string a ser cifrado encontra-se na memória a partir do endereço 200, conforme representado abaixo (observar o “\0” no final do string):

Endereço	200	201	202	203	204	205	206	207	208	209	210	211
Dado	“A”	“R”	“Q”	“U”	“I”	“T”	“E”	“T”	“U”	“R”	“A”	0

Como o passo escolhido é 7 (conteúdo do endereço 194), cada letra da palavra deverá ser somada com o passo e, caso o resultado seja maior do que 90 (ASCII de "Z"), o valor deverá ser diminuído de 26. Abaixo estão indicados essas operações, para cada uma das letras do string a ser cifrado.

Endereço	200	201	202	203	204	205	206	207	208	209	210	211
Dado	"A"	"R"	"Q"	"U"	"I"	"T"	"E"	"T"	"U"	"R"	"A"	0
ASCII	65	82	81	85	73	84	69	84	85	82	65	0
ASCII+7	72	89	88	92	80	91	76	91	92	89	72	0
ASCII+7 corrigido	72	89	88	66	80	65	76	65	66	89	72	0

No resultado final estão indicados os caracteres que tiveram de ser ajustados, tendo em vista que o resultado da soma foi maior do que 90.

Portanto, o resultado esperado no string de destino será o seguinte:

Endereço	220	221	222	223	224	225	226	227	228	229	230	231
Dado	H	Y	X	B	P	A	L	A	B	Y	H	0

4. Correção dos Trabalhos

Os arquivos fonte do RAMSES entregues serão montados usando o montador DAEDALUS.

Para a correção, serão aplicados 20 (vinte) casos de teste. Há apenas duas opções de correção dos casos de teste: correto ou errado.

Para cada caso de teste em que o programa fornecer a reposta correta, serão atribuídos 5 pontos. Portanto, os programas que fornecerem os resultados corretos para todos os casos de teste receberão 100 pontos.

5. O que deve ser entregue?

Deverá ser entregue somente o arquivo fonte (arquivo .RAD) escrito na linguagem simbólica do RAMSES, com a solução do problema apresentado, no Moodle da disciplina.

O programa fonte deverá conter comentários descritivos da implementação. Por exemplo, nos comentários podem ser usados comandos da linguagem "C".

O trabalho deverá ser entregue até a data especificada no link de entrega no sistema Moodle. **Não serão aceitos trabalhos após o prazo estabelecido**.

6. Observações

Recomenda-se a troca de ideias entre os alunos. Entretanto, a identificação de cópias de trabalhos acarretará na aplicação do Código Disciplinar Discente e a tomada das medidas cabíveis para essa situação. Inicialmente, nesses casos, **ambos os o trabalhos: original e cópias, receberão nota zero**.

O professor da disciplina reserva-se o direito, caso necessário, de solicitar uma demonstração do programa, onde o aluno será arguido sobre o trabalho como um todo. Nesse caso, a nota final do trabalho levará em consideração o resultado da demonstração.