Universidade de São Paulo
Instituto de Ciências Matemáticas e de Computação
Departamento de Ciências de Computação
SCC0222 – Laboratório de Introdução à Ciência da Computação I

Trabalho 1

Prof. Rodrigo Fernandes de Mello – `mello@icmc.usp.br`
Monitores: Victor Forbes – `victor.forbes@usp.br`,
Yule Vaz – `yule.vaz@usp.br`

1 Descrição

Atenção! Para este trabalho deverá ser utilizado o alfabeto de 26 letras.

Parte 1: Cifra de César

A cifra de César é um algoritmo de criptografia de substituição no qual, dado um número k, as letras de uma mensagem são trocadas pela próxima k-ésima letra. Antigamente, essa cifra era efetuada com um objeto que consistia em um círculo externo (que chamaremos de referência) e outro interno (que chamaremos de cifra), ambos contendo as letras de um alfabeto em sequência.

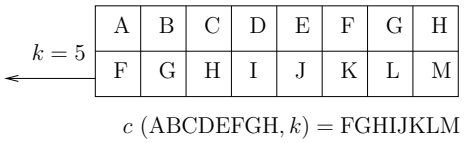

Figura 1: Criptografia com a cifra de césar.

Para criptografar uma mensagem m, seu remetente girava a cifra no sentido anti-horário deslocando o alfabeto k elementos a frente de sua posição original como mostra a Figura 1. Assim, para cada letra em sua mensagem, o indivíduo verifica sua posição no círculo externo e a letra correspondente do círculo interno, que será a substituta, gerando uma mensagem cifrada $c(m, k)$. Para decriptografar a mensagem, o destinatário, que também possui o mesmo artefato de cifragem e conhece o valor de k, rotaciona a cifra em k elementos no sentido horário e substitui as letras da mensagem criptografada da forma citada anteriormente gerando a mensagem decriptografada $d(m, k)$. Esse processo é apresentado na Figura 2.

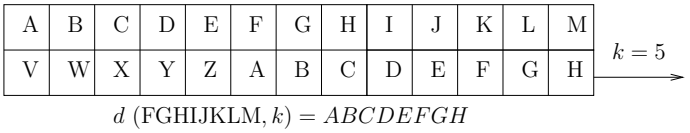

Figura 2: Decriptografia com a cifra de césar.

Então, se um indivíduo criptografa a mensagem "CESAR", com $k = 2$ por exemplo, o resultado seria a mensagem cifrada "EGUCT".

Implemente uma função que efetue a criptografia de César. Espaços, numerais e símbolos devem ser mantidos como na mensagem original.

Dica: Para aplicar rotação sobre uma sequência verifique a operação "mod", que retorna o resto de uma divisão.

Parte 2: Cifra de Vigenère

Outro algoritmo de criptografia é a Cifra de Vigenère, que utiliza uma chave de tamanho c compartilhada pelo remetente e pelo destinatário da mensagem. Nesse algoritmo o remetente seleciona duas letras de forma sequencial, uma na mensagem e outra na chave. Assim, seja k a posição da letra selecionada na chave no alfabeto, o remetente criptografa a letra da mensagem com uma cifra de César utilizando um deslocamento k.

A posição das letras no alfabeto vão de 0 a 25 (totalizando 26), uma para cada letra. A letra "C", por exemplo, está na posição 2 do alfabeto.

Por exemplo, se um indivíduo criptografa uma mensagem M = "AVE CESAR" com uma chave C = "JULIO", tem-se que as posições da chave no alfabeto são $\{9, 20, 11, 8, 14\}$. Além disso, como o tamanho da mensagem é maior que o da chave, podemos ampliar a chave para C' = "JUL IOJUL". Assim, o deslocamento de cada letra será $\{0+9, 21+20, 4+11, 2+8, 4+14, 18+9, 0+20, 17+11\} = \{9, 41, 15, 10, 18, 27, 20, 28\}$. Note que algumas posições extrapolam o tamanho do alfabeto, assim retorna-se o resto da divisão do valor pelo tamanho do alfabeto (26 no caso). Então, os deslocamentos produzidos para cada letra são $\{9, 15, 15, 10, 18, 1, 20, 2\}$ e, portanto, a criptografia da mensagem é "JPP KSBUC".

Implemente uma função que efetue a criptografia de Vigenère. Espaços, numerais e símbolos devem ser mantidos como na mensagem original.

2 Entrada

A primeira linha da entrada possui apenas um inteiro n, a quantidade de caracteres na mensagem. A segunda linha possui a mensagem m, constituida por letras **maiúsculas**, espaços e símbolos. Na terceira linha haverá um inteiro *op* indicando qual o tipo de criptografia a ser utilizado (1 para a criptografia de César e 2 para a criptografia de Vigenère).

Caso a criptografia a ser efetuada seja a de César, haverá na quarta linha um inteiro k representando o "deslocamento" da mensagem.

Caso a criptografia a ser efetuada seja a de Vigenère, haverá um inteiro s, a quantidade de caracteres na chave, na quarta linha e a chave c com s caracteres na quinta linha. A chave será constituída por uma palavra com letras **maiúsculas** apenas.

3 Saída

Imprima a mensagem criptografada. Algo como:

```
printf(''%s\n'', str);
```

4 Instruções Complementares

É obrigatório o uso da memória Heap para armazenar tanto a mensagem m, quanto a chave c. A quantidade de caracteres de cada uma das strings é fornecida na entrada para facilitar a alocação de memória.

É obrigatória a implementação de, pelo menos, duas funções. Uma para a criptografia de César e outra para a criptografia de Vigenère.

Comente seu código.