
Laboratório #2 - lab2.c

RC4

Prof. Valério Rosset

1 DEFINIÇÃO DO PROBLEMA

Desenvolva o RC4.

TAREFA A

Desenvolva um algoritmo em linguagem C/Java que reproduza as operações de cifração executadas pelo RC4.

O programa deverá imprimir uma saída com uma sequência de bytes do fluxo de entrada em formato hexadecimal resultante da operação de cifração.

ENTRADA

A entrada contém um único conjunto de teste, que deve ser lido do dispositivo de entrada padrão (normalmente o teclado). O conjunto de teste é composto por 2 linhas.

1. A entrada contém na primeira linha um conjunto de caracteres P de entrada, de tamanho máximo de 256 bytes. Na segunda linha o valor da chave K , um conjunto de caracteres de tamanho máximo de 256 bytes.

SAÍDA

Ao final da execução, seu programa deverá imprimir a sequência correta de bytes resultante da operação de cifragem, em formato hexadecimal, separado por ":". Para as operações de saída, considere a sintaxe em C:

```
for ( ...  
printf("%x:", cifrado[i]);  
...
```

Considerando que "cifrado" é um vetor de caracteres.

EXEMPLOS:

Entrada	Saída
batata teste	39:ce:e9:e3:56:36:
valedoparaiba 1234	73:28:1d:ca:97:83:77:6c:7d:7a:69:32:84:

OBSERVAÇÕES

- É fundamental que o programa imprima apenas o valor de saída.
- Os exercícios devem ser postados no site do Judge: <http://kp.unifesp.br:9001>
- Cada aluno deverá postar apenas um exercício dentro da data limite.
- Os plágios serão penalizados. Como não será possível saber quem copiou, todos os casos envolvidos receberão punições iguais, portanto, não divulgue seu código.