
Laboratório #1 - lab1

S-DES

Prof. Valério Rosset

1 DEFINIÇÃO DO PROBLEMA

Desenvolva o S-DES.

TAREFA A

Desenvolva um algoritmo em linguagem C/Java que reproduza as operações de cifragem e decifragem executadas pelo S-DES.

O programa deverá imprimir uma saída com uma sequência de bits do bloco de entrada resultante da operação de cifragem (ou decifragem), dependendo do tipo de operação que será solicitada.

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 $L + 1$ linhas, $1 \leq L \leq 100$.

1. A entrada contém na primeira linha um valor inteiro L , $1 \leq L \leq 100$, que representa a quantidade de operações a serem realizadas. A partir da segunda linha são apresentados os dados para cada execução: começando por um caractere O ($O = [C, D]$) que representa a operação a ser realizada (cifrar ou decifrar). Uma sequência de 10 valores inteiros representando a chave K ($K = [0, 1]$) e uma outra sequência de 8 valores inteiros ($B = [0, 1]$) representando a sequência de bits do bloco a ser utilizado na operação.

SAÍDA

Ao final da execução, seu programa deverá imprimir a sequência correta de 8 valores inteiros $R = [0, 1]$ resultante da operação de cifragem/decifragem do bloco de entrada.

EXEMPLO:

Entrada	Saída
2	00101011
C	01010101
1000000000	
01010101	
D	
1000000000	
00101011	

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.