Atividade de Laboratório **15.1**

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é decriptar mensagens encriptadas com o El Gamal.

Entrada

Inicialmente, o programa deverá ler um número inteiro k. Este número irá indicar quantas *quádruplas* de números inteiros o programa deverá ler na sequência. Isto é, se $k = 6$, o programa deverá ler, em seguida, seis *quádruplas* de números inteiros.

Abaixo, é apresentado um exemplo de possível entrada para o programa.

Saída

Para cada quádrupla lida, o primeiro elemento será o primo p (parâmetro público do El Gamal), o segundo elemento será a chave privada a e o terceiro e o quarto elementos serão a mensagem encriptada (s, t). O programa deverá imprimir a tabela do algoritmo de exponenciação modular (conforme Atividade 6.2) utilizado no primeiro passo da decriptação. Após esta tabela, o programa deve imprimir o valor obtido para o bloco decriptado, seguido de uma linha com apenas três traços: `---`.

Abaixo, é apresentado um exemplo de saída para o programa. Esta é justamente a saída que deve ser produzida caso o programa receba a entrada fornecida no exemplo.

Exemplo

Entrada

```
2
167,10,124,157
199,3,27,190
```

Saída

```
1 124 156 N
1 12 78 N
1 144 39 S
144 28 19 S
24 116 9 S
112 96 4 N
112 31 2 N
112 126 1 S
84 11 0 N
162
---
1 27 195 S
27 132 97 S
181 111 48 N
181 182 24 N
181 90 12 N
181 140 6 N
181 98 3 S
27 52 1 S
11 117 0 N
100
---
```