

## NÚMEROS ALEATÓRIOS

### Sequência de números pseudoaleatórios - construção

#### 1) Funções da biblioteca stdlib.h:

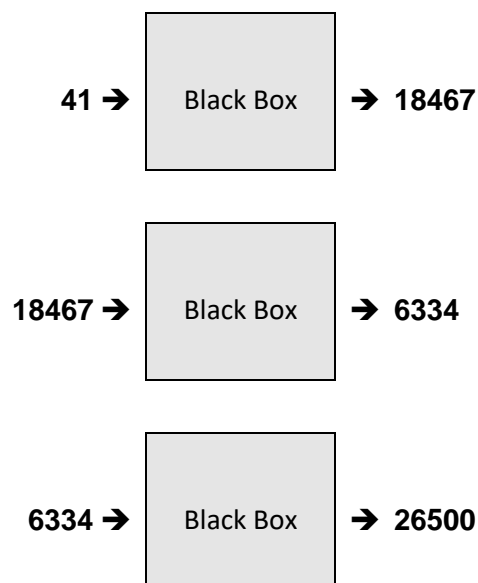
- `int rand();` // devolve um número pertencente à faixa [0, RAND\_MAX]
- `void srand(int);` // define a semente utilizada pela função rand para inicializar o processo

A constante `RAND_MAX`<sup>1</sup> tem valor igual a 32767. A cada chamada consecutiva a função `rand` devolve um número diferente do anterior e após 32768 chamadas repete o primeiro número. Isto porque há um algoritmo implementado pela função `rand`, ou seja, o processo é determinístico, fazendo com a que sequência de números não seja verdadeiramente aleatória, mas possa parecer aleatória.

A função `rand` utiliza como semente inicializadora no algoritmo que gera o número seguinte o valor 1, mas pode ter essa semente escolhida pelo usuário por meio da função `srand`.

```
Primeiras 10 chamadas de rand com semente 1:  
41 18467 6334 26500 19169 15724 11478 29358 26962 24464
```

A primeira chamada de `rand` fornece o número 41. Esse número é usado pelo algoritmo para calcular o segundo número, 18467, que é usado para calcular o terceiro, 6334, e assim por diante.



Para gerar uma sequência diferente dessa é preciso mudar a semente utilizada no algoritmo para a inicialização. Se fizermos a chamada `srand(2)`, teremos esta outra sequência:

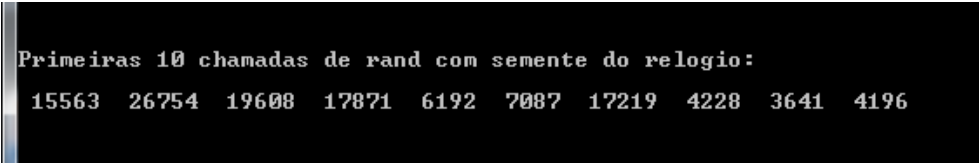
```
Primeiras 10 chamadas de rand com semente 2:  
45 29216 24198 17795 29484 19650 14590 26431 10705 18316
```

<sup>1</sup> Em uma workstation Unix `RAND_MAX` vale 2147483647. [E.S.Roberts – The Art and Science of C]

## NÚMEROS ALEATÓRIOS

Para obter uma sequência diferente cada vez que executamos o programa podemos usar o relógio do sistema para definir a semente:

```
srand((int) time(NULL));
```



```
Primeiras 10 chamadas de rand com semente do relógio:  
15563 26754 19608 17871 6192 7087 17219 4228 3641 4196
```

### 2) Algoritmo de D.H. Lehmer<sup>2</sup> - gerador congruente linear

Os números pseudoaleatórios podem ser gerados pela sequência definida por:

$$y_{k+1} = (a \times y_k + c) \text{ MOD } m, \quad k = 1, 2, 3, \dots$$

$$y_1 = s, \quad c = 12$$

$$0 \leq a, s < m, \quad m = \text{número primo}$$

Valores sugeridos para as constantes a, c, m, respectivamente, 16807, 0, 2147483647

### Sequência de números pseudoaleatórios pertencentes a uma faixa determinada

Para gerar uma sequência de números pseudoaleatórios pertencentes a uma faixa de valores pré-definida basta fazer uma transformação, levando cada valor gerado pela função geradora da sequência aleatória para um valor no intervalo desejado.

Por exemplo, a função rand devolve um número inteiro pertencente à faixa [0..RAND\_MAX] e desejamos obter números na faixa [a,b].

Podemos fazer:

- A divisão desse número por RAND\_MAX+1 obtendo um número d tal que  $0 \leq d < 1$ .
- A multiplicação de (b-a+1) por d (d é número real maior ou igual a 0 e menor do que 1) produz como resultado um número cuja parte inteira pertence à faixa de números inteiros 0,1,2,3...b-a.
- A soma desse número inteiro (parte inteira do resultado anterior) com o número a resulta um número pertencente à faixa de inteiros de a até b.

$$k = d \times (b - a + 1) \quad \text{e} \quad 0 \leq d < 1 \Rightarrow k \in \{0, 1, 2, \dots, b - a\}$$

$$g = a + k \Rightarrow g \in [a, b]$$

<https://www.ime.usp.br/~pf/algoritmos/aulas/random.html>

---

<sup>2</sup> Derrick Henry Lehmer, 1905-1991.