

## Roteiro para rodar os exemplos:

1. Pra facilitar a execução dos exemplos, copie a pasta Nist descompactada no diretório raiz C:\

2. Os exemplos abaixo são comandos de linha e devem ser executados a partir de uma janela de comandos no DOS do Windows. Para abrir a janela de comandos DOS no Windows, digite na barra de pesquisar: **CMD**  
Em seguida, clique na opção abrir.

3. Entre na pasta Nist digitando no prompt de comando:  
C:\Users\latiq>**cd C:\Nist**

C:\Nist>

4. Para visualizar as opções de execução do programa, digite no prompt de comando:

C:\Nist>**nist**

Uma lista de opções de como executar os testes aparecerá.

5. Para os exemplos, deixei 2 arquivos de extensão **.dat** na subpasta data, são eles **chave01.dat** e **chave02.dat** (a extensão tem que ser **.dat**). O resultado dos testes são 3 arquivos de texto criados na subpasta **\experiments\AlgorithmTesting**. Abra-os no Bloco de notas do windows para visualizar o formato dos resultados.

**ATENÇÃO! A cada teste realizado esses 3 arquivos serão reescritos. Sendo assim, não se esqueça de copiá-los para outra pasta antes de realizar outro teste.**

---

Arquivo **chave01.dat** possui 1 milhão de bytes, para executar os 15 testes de NIST sobre ele digite o comando abaixo **em uma única linha** direto no prompt:

C:\Nist>**nist -fast -file data\chave01.dat -streams 1 -tests 11111111111111 -defaultpar -onlymem -ascii 1000000**

Onde os parâmetros significam:

**-fast** especifica que a versão mais rápida dos testes será usada

**-streams 1** indica que apenas uma sequência será testada, 1 linha

**-tests 11111111111111** o número **1** indica que o teste deve ser executado e **0** que não deve. A ordem dos testes é da esquerda para direita, sendo eles: 1. Frequency, 2. BlockFrequency, 3. CumulativeSums, 4. Runs, 5. LongestRun, 6. Rank, 7. FFT, 8. NonOverlappingTemplate, 9. OverlappingTemplate, 10. Universal, 11. ApproximateEntropy, 12. RandomExcursions, 13. RandomExcursionsVariant, 14. Serial, 15. LinearComplexity

**-defaultpar** indica que os parâmetros padronizados para cada teste deve ser adotado

**-onlymem** indica que a forma simplificada de resultados deve ser adotada.

**-ascii** indica que o formato do arquivo é ascii

**1000000** indica o número de bytes no **streams** (na linha)

---

Arquivo **chave02.dat** possui 2 milhões de bytes, 2 linhas (streams) de 1 milhão de bytes cada. Para executar os 15 testes de NIST sobre as 2 linhas dele, digite o comando abaixo **em uma única linha** direto no prompt:

C:\Nist>**nist -fast -file data\chave02.dat -streams 2 -tests 11111111111111 -defaultpar -onlymem -ascii 1000000**

Observe como ficou a disposição dos resultados dos testes abrindo no Bloco de notas o arquivo na subpasta **experiments\AlgorithmTesting**.

---

Para finalizar, você também pode submeter seus dados aos testes de NIST no site (apenas 14 testes):  
**<https://mzsoltmolnar.github.io/random-bitstream-tester/>**

Na página clique na opção **“Manual bitstream input”**, cole sua sequência na caixa de dados(máximo 1 milhão de bytes). Em seguida, clique no botão **“Insert Input Stream”**. Finalmente, clique no botão **“Start Test”**.

**Bons testes!**