CENTRO UNIVERSITÁRIO FEI

CC8130 - Atividade 02: Testes aleatórios

CC8130 – Segurança na Informação

Andy Silva Barbosa
RA: 22.218.025-9
Vitor Acosta da Rosa
RA: 22.218.006-9

São Bernardo do Campo
2022

1 Objetivo

Através dos testes de aleatoriedade apresentados na FIPS 140-1, o objetivo é classificar 26 chaves de 20.000 bits como aleatórias ou não aleatórias. Para a execução da tarefa, foi escolhida a linguagem **Python** para a programação.

2 Resultados

Através das 26 chaves de 20.000 bits, o resultado para cada chave foi:

- 13 chaves não aleatórias, e portanto apresentaram um ou mais testes aleatórios falho.
- As demais, 13 chaves, aleatórias que passaram em todos os quatro testes aleatórios.

Abaixo, o resultado completo, incluindo se a chave passou ou não em cada um dos testes aleatórios, bem como:

- Quantidade de monobits
- Valor calculado no pokerTest e quantidade de cada nible
- Quantidade de cada sequência do Run test (tanto para zeros como para uns)

```
====================================
Chave 1 - Aprovado: True
Monobit: True
  >Count: 10052

Poker: True
  >Valor (X): 34.253
  >Count: {0: 277.0, 1: 315.0, 2: 341.0, 3: 345.0, 4: 301.0, 5: 305.0,
               6: 341.0, 7: 331.0, 8: 319.0, 9: 310.0, 10: 340.0, 11: 274.0,
               12: 271.0, 13: 300.0, 14: 283.0, 15: 347.0}

The Run Test: True
  >Bits 1 count:{'1': 2531, '2': 1219, '3': 627, '4': 342, '5': 144, '6+': 155}
  >Bits 0 count:{'1': 2511, '2': 1246, '3': 665, '4': 323, '5': 136, '6+': 137}

Long Run Test: True
====================================
Chave 2 - Aprovado: False
Monobit: False
  >Count: 10580

Poker: False
```

```
  >Valor (X): 187.476
  >Count: {0: 161.0, 1: 168.0, 2: 301.0, 3: 377.0, 4: 330.0, 5: 344.0,
              6: 330.0, 7: 320.0, 8: 324.0, 9: 385.0, 10: 316.0, 11: 344.0,
              12: 293.0, 13: 337.0, 14: 313.0, 15: 356.0}

The Run Test: False
  >Bits 1 count:{'1': 2635, '2': 1319, '3': 599, '4': 362, '5': 167, '6+': 172}
  >Bits 0 count:{'1': 2750, '2': 1382, '3': 719, '4': 292, '5': 88, '6+': 23}

Long Run Test: True
====================================
Chave 3 - Aprovado: True
Monobit: True
  >Count: 9944

Poker: True
  >Valor (X): 13.139
  >Count: {0: 327.0, 1: 292.0, 2: 324.0, 3: 332.0, 4: 310.0, 5: 301.0,
              6: 315.0, 7: 288.0, 8: 317.0, 9: 323.0, 10: 328.0, 11: 288.0,
              12: 326.0, 13: 296.0, 14: 297.0, 15: 336.0}

The Run Test: True
  >Bits 1 count:{'1': 2493, '2': 1222, '3': 632, '4': 321, '5': 146, '6+': 155}
  >Bits 0 count:{'1': 2427, '2': 1274, '3': 613, '4': 322, '5': 168, '6+': 164}

Long Run Test: True
====================================
Chave 4 - Aprovado: False
Monobit: False
  >Count: 10665

Poker: False
  >Valor (X): 342.829
  >Count: {0: 0.0, 1: 323.0, 2: 340.0, 3: 349.0, 4: 341.0, 5: 337.0,
              6: 339.0, 7: 342.0, 8: 316.0, 9: 329.0, 10: 319.0, 11: 321.0,
              12: 364.0, 13: 307.0, 14: 331.0, 15: 342.0}

The Run Test: False
  >Bits 1 count:{'1': 2555, '2': 1325, '3': 690, '4': 335, '5': 161, '6+': 178}
  >Bits 0 count:{'1': 2758, '2': 1403, '3': 702, '4': 268, '5': 85, '6+': 28}

Long Run Test: True
====================================
Chave 5 - Aprovado: True
Monobit: True
  >Count: 9984
```

```
Poker: True
  >Valor (X): 13.139
  >Count: {0: 327.0, 1: 292.0, 2: 324.0, 3: 332.0, 4: 310.0, 5: 323.0,
              6: 315.0, 7: 328.0, 8: 317.0, 9: 288.0, 10: 301.0, 11: 288.0,
              12: 326.0, 13: 296.0, 14: 297.0, 15: 336.0}

The Run Test: True
  >Bits 1 count:{'1': 2462, '2': 1208, '3': 634, '4': 335, '5': 159, '6+': 150}
  >Bits 0 count:{'1': 2461, '2': 1209, '3': 605, '4': 336, '5': 170, '6+': 166}

Long Run Test: True
====================================
Chave 6 - Aprovado: False
Monobit: False
  >Count: 10642

Poker: False
  >Valor (X): 342.829
  >Count: {0: 0.0, 1: 323.0, 2: 340.0, 3: 349.0, 4: 341.0, 5: 329.0,
              6: 339.0, 7: 319.0, 8: 316.0, 9: 342.0, 10: 337.0, 11: 321.0,
              12: 364.0, 13: 307.0, 14: 331.0, 15: 342.0}

The Run Test: False
  >Bits 1 count:{'1': 2528, '2': 1314, '3': 684, '4': 336, '5': 171, '6+': 176}
  >Bits 0 count:{'1': 2679, '2': 1440, '3': 702, '4': 275, '5': 85, '6+': 28}

Long Run Test: True
====================================
Chave 7 - Aprovado: True
Monobit: True
  >Count: 9883

Poker: True
  >Valor (X): 15.282
  >Count: {0: 320.0, 1: 350.0, 2: 285.0, 3: 311.0, 4: 343.0, 5: 314.0,
              6: 297.0, 7: 302.0, 8: 315.0, 9: 317.0, 10: 317.0, 11: 281.0,
              12: 329.0, 13: 311.0, 14: 292.0, 15: 315.0}

The Run Test: True
  >Bits 1 count:{'1': 2574, '2': 1202, '3': 645, '4': 268, '5': 155, '6+': 157}
  >Bits 0 count:{'1': 2465, '2': 1223, '3': 686, '4': 324, '5': 136, '6+': 167}

Long Run Test: True
====================================
Chave 8 - Aprovado: False
```

```
Monobit: False
  >Count: 10368

Poker: False
  >Valor (X): 252.826
  >Count: {0: 54.0, 1: 380.0, 2: 341.0, 3: 324.0, 4: 362.0, 5: 340.0,
              6: 324.0, 7: 338.0, 8: 349.0, 9: 316.0, 10: 313.0, 11: 324.0,
              12: 313.0, 13: 280.0, 14: 318.0, 15: 324.0}

The Run Test: False
  >Bits 1 count:{'1': 2655, '2': 1279, '3': 642, '4': 318, '5': 155, '6+': 163}
  >Bits 0 count:{'1': 2670, '2': 1362, '3': 726, '4': 294, '5': 109, '6+': 50}

Long Run Test: True
====================================
Chave 9 - Aprovado: True
Monobit: True
  >Count: 9853

Poker: True
  >Valor (X): 24.429
  >Count: {0: 306.0, 1: 322.0, 2: 317.0, 3: 295.0, 4: 339.0, 5: 340.0,
              6: 308.0, 7: 274.0, 8: 364.0, 9: 308.0, 10: 304.0, 11: 304.0,
              12: 293.0, 13: 290.0, 14: 333.0, 15: 303.0}

The Run Test: True
  >Bits 1 count:{'1': 2609, '2': 1224, '3': 620, '4': 278, '5': 156, '6+': 147}
  >Bits 0 count:{'1': 2490, '2': 1241, '3': 670, '4': 331, '5': 145, '6+': 157}

Long Run Test: True
====================================
Chave 10 - Aprovado: False
Monobit: False
  >Count: 10346

Poker: False
  >Valor (X): 114.429
  >Count: {0: 189.0, 1: 214.0, 2: 364.0, 3: 355.0, 4: 319.0, 5: 360.0,
              6: 327.0, 7: 321.0, 8: 333.0, 9: 342.0, 10: 276.0, 11: 317.0,
              12: 306.0, 13: 336.0, 14: 299.0, 15: 341.0}

The Run Test: False
  >Bits 1 count:{'1': 2649, '2': 1321, '3': 605, '4': 308, '5': 163, '6+': 161}
  >Bits 0 count:{'1': 2623, '2': 1394, '3': 762, '4': 269, '5': 108, '6+': 50}

Long Run Test: True
```

```
====================================
Chave 11 - Aprovado: False
Monobit: False
  >Count: 10761

Poker: False
  >Valor (X): 193.146
  >Count: {0: 146.0, 1: 194.0, 2: 283.0, 3: 335.0, 4: 321.0, 5: 345.0,
              6: 335.0, 7: 367.0, 8: 300.0, 9: 356.0, 10: 308.0, 11: 356.0,
              12: 306.0, 13: 374.0, 14: 291.0, 15: 382.0}

The Run Test: False
  >Bits 1 count:{'1': 2529, '2': 1295, '3': 655, '4': 354, '5': 200, '6+': 183}
  >Bits 0 count:{'1': 2757, '2': 1376, '3': 733, '4': 238, '5': 94, '6+': 18}

Long Run Test: True
====================================
Chave 12 - Aprovado: True
Monobit: True
  >Count: 9926

Poker: True
  >Valor (X): 11.646
  >Count: {0: 337.0, 1: 314.0, 2: 318.0, 3: 317.0, 4: 331.0, 5: 310.0,
              6: 289.0, 7: 317.0, 8: 313.0, 9: 291.0, 10: 310.0, 11: 323.0,
              12: 306.0, 13: 275.0, 14: 335.0, 15: 313.0}

The Run Test: True
  >Bits 1 count:{'1': 2478, '2': 1249, '3': 615, '4': 302, '5': 143, '6+': 166}
  >Bits 0 count:{'1': 2462, '2': 1221, '3': 600, '4': 329, '5': 163, '6+': 178}

Long Run Test: True
====================================
Chave 13 - Aprovado: False
Monobit: False
  >Count: 10677

Poker: False
  >Valor (X): 170.003
  >Count: {0: 174.0, 1: 191.0, 2: 297.0, 3: 331.0, 4: 312.0, 5: 384.0,
              6: 291.0, 7: 377.0, 8: 290.0, 9: 319.0, 10: 338.0, 11: 370.0,
              12: 304.0, 13: 372.0, 14: 303.0, 15: 346.0}

The Run Test: False
  >Bits 1 count:{'1': 2628, '2': 1314, '3': 676, '4': 352, '5': 181, '6+': 150}
  >Bits 0 count:{'1': 2862, '2': 1346, '3': 721, '4': 272, '5': 77, '6+': 22}
```

```
Long Run Test: True
====================================
Chave 14 - Aprovado: False
Monobit: False
  >Count: 10578

Poker: False
  >Valor (X): 345.92
  >Count: {0: 0.0, 1: 325.0, 2: 351.0, 3: 357.0, 4: 354.0, 5: 350.0,
              6: 317.0, 7: 304.0, 8: 348.0, 9: 337.0, 10: 316.0, 11: 345.0,
              12: 323.0, 13: 318.0, 14: 321.0, 15: 334.0}

The Run Test: False
  >Bits 1 count:{'1': 2636, '2': 1322, '3': 612, '4': 344, '5': 161, '6+': 179}
  >Bits 0 count:{'1': 2733, '2': 1410, '3': 724, '4': 263, '5': 99, '6+': 25}

Long Run Test: True
====================================
Chave 15 - Aprovado: True
Monobit: True
  >Count: 10167

Poker: True
  >Valor (X): 15.378
  >Count: {0: 309.0, 1: 277.0, 2: 277.0, 3: 298.0, 4: 320.0, 5: 310.0,
              6: 344.0, 7: 326.0, 8: 310.0, 9: 304.0, 10: 300.0, 11: 326.0,
              12: 318.0, 13: 328.0, 14: 315.0, 15: 337.0}

The Run Test: True
  >Bits 1 count:{'1': 2410, '2': 1298, '3': 624, '4': 340, '5': 156, '6+': 165}
  >Bits 0 count:{'1': 2564, '2': 1215, '3': 602, '4': 312, '5': 152, '6+': 148}

Long Run Test: True
====================================
Chave 16 - Aprovado: False
Monobit: True
  >Count: 10052

Poker: True
  >Valor (X): 13.357
  >Count: {0: 297.0, 1: 318.0, 2: 307.0, 3: 324.0, 4: 298.0, 5: 291.0,
              6: 329.0, 7: 299.0, 8: 325.0, 9: 334.0, 10: 304.0, 11: 333.0,
              12: 317.0, 13: 299.0, 14: 287.0, 15: 338.0}

The Run Test: True
```

```
  >Bits 1 count:{'1': 2474, '2': 1257, '3': 604, '4': 303, '5': 183, '6+': 154}
  >Bits 0 count:{'1': 2479, '2': 1261, '3': 605, '4': 296, '5': 182, '6+': 151}

Long Run Test: False
====================================
Chave 17 - Aprovado: True
Monobit: True
  >Count: 9971

Poker: True
  >Valor (X): 11.488
  >Count: {0: 295.0, 1: 329.0, 2: 321.0, 3: 323.0, 4: 326.0, 5: 293.0,
               6: 315.0, 7: 328.0, 8: 308.0, 9: 339.0, 10: 297.0, 11: 328.0,
               12: 302.0, 13: 308.0, 14: 295.0, 15: 293.0}

The Run Test: True
  >Bits 1 count:{'1': 2449, '2': 1294, '3': 664, '4': 322, '5': 138, '6+': 140}
  >Bits 0 count:{'1': 2461, '2': 1306, '3': 630, '4': 302, '5': 158, '6+': 150}

Long Run Test: True
====================================
Chave 18 - Aprovado: False
Monobit: False
  >Count: 10799

Poker: False
  >Valor (X): 231.056
  >Count: {0: 132.0, 1: 164.0, 2: 332.0, 3: 362.0, 4: 288.0, 5: 334.0,
               6: 321.0, 7: 353.0, 8: 296.0, 9: 365.0, 10: 298.0, 11: 370.0,
               12: 326.0, 13: 368.0, 14: 329.0, 15: 361.0}

The Run Test: False
  >Bits 1 count:{'1': 2522, '2': 1330, '3': 651, '4': 370, '5': 180, '6+': 181}
  >Bits 0 count:{'1': 2776, '2': 1417, '3': 697, '4': 237, '5': 85, '6+': 21}

Long Run Test: True
====================================
Chave 19 - Aprovado: False
Monobit: False
  >Count: 10685

Poker: False
  >Valor (X): 343.238
  >Count: {0: 0.0, 1: 309.0, 2: 333.0, 3: 323.0, 4: 321.0, 5: 327.0,
               6: 362.0, 7: 325.0, 8: 345.0, 9: 336.0, 10: 347.0, 11: 321.0,
               12: 334.0, 13: 326.0, 14: 361.0, 15: 330.0}
```

```
The Run Test: False
  >Bits 1 count:{'1': 2553, '2': 1317, '3': 694, '4': 361, '5': 184, '6+': 151}
  >Bits 0 count:{'1': 2771, '2': 1415, '3': 693, '4': 283, '5': 79, '6+': 18}

Long Run Test: True
====================================
Chave 20 - Aprovado: True
Monobit: True
  >Count: 10047

Poker: True
  >Valor (X): 19.539
  >Count: {0: 257.0, 1: 308.0, 2: 328.0, 3: 305.0, 4: 317.0, 5: 319.0,
               6: 334.0, 7: 307.0, 8: 326.0, 9: 319.0, 10: 309.0, 11: 306.0,
               12: 347.0, 13: 288.0, 14: 321.0, 15: 309.0}

The Run Test: True
  >Bits 1 count:{'1': 2504, '2': 1246, '3': 635, '4': 308, '5': 163, '6+': 156}
  >Bits 0 count:{'1': 2477, '2': 1285, '3': 629, '4': 328, '5': 160, '6+': 133}

Long Run Test: True
====================================
Chave 21 - Aprovado: True
Monobit: True
  >Count: 10065

Poker: True
  >Valor (X): 19.123
  >Count: {0: 282.0, 1: 314.0, 2: 307.0, 3: 311.0, 4: 309.0, 5: 353.0,
               6: 314.0, 7: 311.0, 8: 296.0, 9: 321.0, 10: 329.0, 11: 330.0,
               12: 294.0, 13: 346.0, 14: 298.0, 15: 285.0}

The Run Test: True
  >Bits 1 count:{'1': 2557, '2': 1324, '3': 636, '4': 323, '5': 133, '6+': 141}
  >Bits 0 count:{'1': 2643, '2': 1265, '3': 614, '4': 301, '5': 155, '6+': 135}

Long Run Test: True
====================================
Chave 22 - Aprovado: True
Monobit: True
  >Count: 10081

Poker: True
  >Valor (X): 23.994
  >Count: {0: 286.0, 1: 311.0, 2: 325.0, 3: 295.0, 4: 308.0, 5: 319.0,
```

```
              6: 334.0, 7: 280.0, 8: 331.0, 9: 303.0, 10: 278.0, 11: 316.0,
              12: 310.0, 13: 366.0, 14: 310.0, 15: 328.0}

The Run Test: True
  >Bits 1 count:{'1': 2435, '2': 1307, '3': 609, '4': 330, '5': 150, '6+': 162}
  >Bits 0 count:{'1': 2489, '2': 1253, '3': 634, '4': 341, '5': 131, '6+': 145}

Long Run Test: True
====================================
Chave 23 - Aprovado: False
Monobit: False
  >Count: 10564

Poker: False
  >Valor (X): 347.936
  >Count: {0: 0.0, 1: 352.0, 2: 331.0, 3: 299.0, 4: 347.0, 5: 328.0,
              6: 355.0, 7: 343.0, 8: 351.0, 9: 339.0, 10: 342.0, 11: 295.0,
              12: 331.0, 13: 324.0, 14: 343.0, 15: 320.0}

The Run Test: False
  >Bits 1 count:{'1': 2634, '2': 1260, '3': 633, '4': 363, '5': 177, '6+': 170}
  >Bits 0 count:{'1': 2726, '2': 1374, '3': 741, '4': 266, '5': 99, '6+': 30}

Long Run Test: True
====================================
Chave 24 - Aprovado: True
Monobit: True
  >Count: 9981

Poker: True
  >Valor (X): 12.019
  >Count: {0: 298.0, 1: 318.0, 2: 334.0, 3: 325.0, 4: 299.0, 5: 291.0,
              6: 330.0, 7: 301.0, 8: 326.0, 9: 334.0, 10: 303.0, 11: 307.0,
              12: 317.0, 13: 300.0, 14: 288.0, 15: 329.0}

The Run Test: True
  >Bits 1 count:{'1': 2507, '2': 1229, '3': 618, '4': 316, '5': 171, '6+': 150}
  >Bits 0 count:{'1': 2453, '2': 1273, '3': 633, '4': 307, '5': 174, '6+': 150}

Long Run Test: True
====================================
Chave 25 - Aprovado: False
Monobit: False
  >Count: 10593

Poker: False
```

```
  >Valor (X): 170.553
  >Count: {0: 157.0, 1: 198.0, 2: 334.0, 3: 356.0, 4: 297.0, 5: 323.0,
              6: 321.0, 7: 381.0, 8: 333.0, 9: 373.0, 10: 289.0, 11: 351.0,
              12: 310.0, 13: 323.0, 14: 292.0, 15: 361.0}

The Run Test: False
  >Bits 1 count:{'1': 2510, '2': 1254, '3': 663, '4': 331, '5': 202, '6+': 182}
  >Bits 0 count:{'1': 2600, '2': 1370, '3': 778, '4': 271, '5': 97, '6+': 25}

Long Run Test: True
====================================
Chave 26 - Aprovado: True
Monobit: True
  >Count: 10034

Poker: True
  >Valor (X): 11.846
  >Count: {0: 297.0, 1: 318.0, 2: 307.0, 3: 325.0, 4: 299.0, 5: 292.0,
              6: 330.0, 7: 300.0, 8: 326.0, 9: 334.0, 10: 305.0, 11: 334.0,
              12: 317.0, 13: 300.0, 14: 288.0, 15: 328.0}

The Run Test: True
  >Bits 1 count:{'1': 2479, '2': 1260, '3': 605, '4': 305, '5': 184, '6+': 153}
  >Bits 0 count:{'1': 2487, '2': 1261, '3': 607, '4': 297, '5': 182, '6+': 151}

Long Run Test: True
```

3 Conclusão

Todos os códigos empregados para a classificação apresentada na Seção 2 estão disponíveis no Github dos autores[1].

[1]Caso o link não funcione, copie e cole no seu navegador a página: https://github.com/VitorAcosta/TestesAleatorios