Sprawozdanie

Generator BBS

Generator BBS został zaimplementowany w pliku `bbs.py` oraz zostały wygenerowane 4 pliki:

Nazwa pliku	Długość
20k-1.txt	20000b
20k-2.txt	20000b
20k-3.txt	20000b
1kk-1.txt	1000000b

Testy FIPS

Test pojedynczych bitów

Nazwa pliku	Wartość	Wynik
20k-1.txt	9997	PASS
20k-2.txt	9973	PASS
20k-3.txt	10090	PASS

Test serii

Dla bitu 0

Plik	20k-1.txt	20k-2.txt	20k-3.txt
1	2484	2515	2478
2	1221	1239	1307
3	643	621	609
4	311	315	331
5	158	152	136
6 i więcej	164	162	146

Plik	20k-1.txt	20k-2.txt	20k-3.txt
Wynik	PASS	PASS	PASS

Dla bitu 1

Plik	20k-1.txt	20k-2.txt	20k-3.txt
1	2475	2531	2485
2	1290	1245	1271
3	566	602	623
4	322	310	316
5	166	162	146
6 i więcej	161	154	167
Wynik	PASS	PASS	PASS

Test długiej serii

Nazwa pliku	Wartość	Wynik
20k-1.txt	17	PASS
20k-2.txt	17	PASS
20k-3.txt	18	PASS

Test pokerowy

Plik	20k-1.txt	20k-2.txt	20k-3.txt
0	312	304	289
1	308	350	291
2	308	316	333
3	322	303	276
4	333	333	322
5	281	300	292
6	327	295	345

Plik	20k-1.txt	20k-2.txt	20k-3.txt
7	310	304	361
8	333	300	319
9	298	298	320
10	307	326	321
11	301	338	295
12	301	308	281
13	310	310	312
14	316	302	321
15	333	313	322
X	9.996799999999894	12.390400000000227	26.617600000000493
Wynik	PASS	PASS	PASS

Test NIST

Test NIST został przeprowadzony dla pliku `1kk-1.txt` .

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------

------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
  0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    frequency
  0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    block-frequency
  0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    cumulative-sums
  0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    cumulative-sums
  0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    runs
  0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    longest-run
  0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    rank
  1   0   0   0   0   0   0   0   0   0  -1.#IND00   0.0000 *  fft
  0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
  0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
  0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
  0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
  0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
  0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
  0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
```

```
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   0   1  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   0   1  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   0   1  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   0   1  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   0   1  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   0   1  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   0   1  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
```

```
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
```

```
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   0   1  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   1   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   1   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    nonperiodic-templates
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    overlapping-templates
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    universal
0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    random-excursions
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    random-excursions
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    random-excursions
0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    random-excursions
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions
0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    random-excursions
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions
1   0   0   0   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions
0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
```

```
  0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   0   0   0   0   0   1   0  -1.#IND00   1.0000    random-excursions-var
  0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   0   0   0   1   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   1   0   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   1   0   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   0   1   0   0   0   0   0  -1.#IND00   1.0000    random-excursions-var
  0   0   0   0   0   1   0   0   0   0  -1.#IND00   1.0000    linear-complexity


- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the random
excursion (variant) test is approximately = 0.691504 for a sample size = 1
binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately
0.691504 for a sample size = 1 binary sequences.

For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Szyfrator strumieniowy

Szyfrator strumieniowy został zaimplementowany w pliku `stream_crypt.py` . Do przetestowania został wykorzystany plik pantadeusz.txt:

```
python3 stream_crypt.py -i pantadeusz.txt -o pantadeusz.encrypted 2> pantadeusz.seed
```

Dodatkowo informacja o ziarnie została zapisana w pantadeusz.seed. Następnie odszyfrowano kryptogram:

```
python3 stream_crypt.py -i pantadeusz.encrypted -o pantadeusz.decrypted -s pantadeus
```

W celu sprawdzenia poprawności deszyfracji wykorzystano sumy kontrolne:

```
$ md5sum pantadeusz.txt pantadeusz.decrypted
c2c8f685ddde7d6b51b6b07f53d65fe0  pantadeusz.txt
c2c8f685ddde7d6b51b6b07f53d65fe0  pantadeusz.decrypted
```

W celu ponownego wykoniania testów FIPS zamieniono szyfrogram na plik tekstowy zawierający "0" oraz "1":

```
xxd -b pantadeusz.encrypted | cut -d" " -f 2-7 | tr -d "\n " > pantadeusz.encrypted.
```

Wszystkie testy FIPS również przeszły pozytywnie:

```
Testfile pantadeusz.encrypted.binary:
[OK] single bit test 10000
[OK] series test [{1: 2493, 2: 1231, 3: 628, 4: 318, 5: 164, 6: 156}, {1: 2480, 2: 1
[OK] long_series test 13
[OK] poker test {'quantities': [303, 312, 301, 351, 302, 320, 316, 303, 332, 321, 30
```