Podstawy ochrony danych - Ćwiczenie 6 -

Implementacja wybranego generatora kluczy strumieniowych oraz zastosowanie go w szyfratorze strumieniowym.

Michał Klempka – grupa I3/1 – 17.11.2015

Generator samodecymujący Rueppela

Algorytm:

Algorytm wykonuje operacje XOR na wszystkich bitach z miejsc odczepów (taps). Wynik operacji XOR jest wstawiany na początek rejestru, a ostatni bit jest ucinany. W zależności od wartości wyjściowej algorytm wykonuje różną liczbę taktów (powtórzeń) – jeśli jest równe 0 to 'd' taktów, jeśli jeden to 'k' taktów. Klucz otrzymujemy po wykonaniu zadanej ilości powtórzeń, powyższej operacji.

Prosty przykład:

8bitowy rejestr, miejsca odczepu: 8 i 3, liczba 'd'=3, liczba 'k'=2. Długość klucza=3. Seed=10001010.

Krok:				Reje	estr:				Wyjście:	Komentarz:
1.	1	0	0	0	1	0	1	0	1	wyjście = 1, k –taktów.
2.	1	1	0	0	0	1	0	1	0	takt 1
3.	0	1	1	0	0	0	1	0	0	wyjście = 0, d –taktów.
4.	0	0	1	1	0	0	0	1	0	takt 1
5.	0	0	0	1	1	0	0	0	0	takt 2
6.	0	0	0	0	1	1	0	0	1	koniec generowania.

Szyfrowanie:

Zadaniem szyfratora strumieniowego jest zaszyfrowanie wiadomości zadanej przez użytkownika za pomocą klucza generowanego przez algorytm LFSR. Wykonuje on operacje XOR odpowiedniego bitu z klucza, oraz z tekstu przeznaczonego do zaszyfrowania.

Założenia:

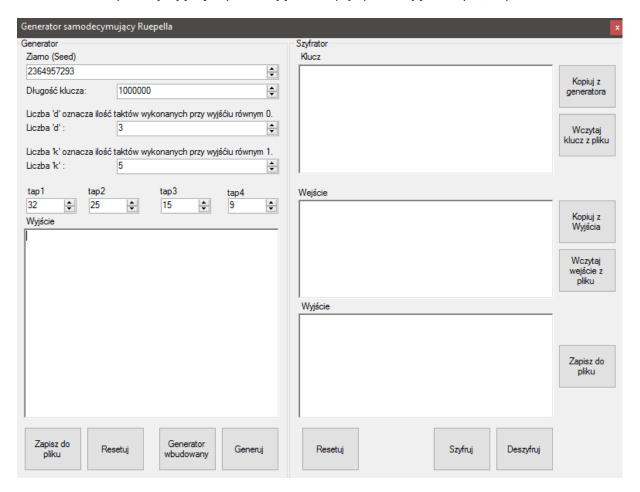
- Rejestr 32 bitowy.
- 4 miejsca odczepu, które można dowolnie ustawić.
- Liczby 'd', oraz 'k' można zmieniać w zakresie od 1 do 100.
- Długość klucza od 1 do 5000000 bitów.
- Wyjście w formie tekstowej, wyprowadzane na ekran, oraz do pliku.
- Ziarno (seed) podawane w systemie dziesiętnym liczby od 1 do 4294967295, lepiej unikać skrajnych wartości.

Środowisko programistyczne i wykonawcze:

- Visual studio 2013
- .NET
- System Windows

Interfejs:

Interfejs dzieli się na 2 części – po lewej Generator, oraz po prawej Szyfrator. U góry w części Generator znajdują się opcje pozwalające dostosować algorytm generowania klucza. Przy każdym okienku tekstowym znajdują się odpowiadające mu opcje pozwalające wczytać/zapisać zawartość.



Testy:

1. Test dla klucza długości 1 000 000 znaków, wygenerowanego z parametrami widocznymi na zdjęciu wyżej:

2 gwiazdki.

SU	LTS	FOR	THE	UNIF	ORMI	TY O	F P-	VALU	ES A	ND THE PRO	PORTION OF	PASSING SEQUENCES
											PROPORTION	STATISTICAL TEST
0	1	0	0	0	0	0	0	0	0	-1.#IND00		frequency
0	0	0	0	0	1	0	0	0	0	-1.#IND00		block-frequency
0	1	0	0	0	0	0	0	0	0	-1.#IND00		cumulative-sums
0 1	1	0	0	0	0	0	0	0	0	-1.#IND00		cumulative-sums runs
1	0	0	0	0	0	0	0	0	0	-1.#IND00		longest-run
0	0	0	0	0	0	0	0	0	1	-1.#IND00		rank
0	0	1	0	0	0	0	0	0	0	-1.#IND00		fft
0	0	0	0	0	0	0	0	1	0	-1.#IND00	1.0000	nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	1	0	0	0 1	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates
0	0	0	0	1	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	1	0	0	0	0	0	0	0	-1.#IND00		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
1	0	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	1	0	0	-1.#IND00		nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0 1	0	0	1	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	1	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
0	0	1	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
С	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		nonperiodic-templates
)	0	0	0	0	0	1	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	1	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	1	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	1	0	0	0 1	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
))	0	1	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
)	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
)	0	0	1	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
)	0	0	0	1	0	0	0	0	0	-1.#IND00		nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	1	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	1	0	0	0	-1.#IND00		nonperiodic-templates
L	1	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
)	0	0	0	0	1	0	0	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
)	1	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	1	0	0	0	0	0	-1.#IND00		nonperiodic-templates
)	0	0	0	0	0	0	1	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates
0	1	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
) 1	1	0	0	0	0	0	0	0	0	-1.#IND00 -1.#IND00		nonperiodic-templates 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	0	1	-1.#IND00	1.0000	nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00	1.0000	nonperiodic-templates
1	0	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	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
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	0	0	0	0	0	0	1	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	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	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
_	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	0	0	0	0	0	0	1	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	1	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	1	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	1	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
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	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	0	1	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	0	0	0	0	0	0	0	1	-1.#IND00	1.0000	
_									1			nonperiodic-templates
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
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
1	0	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	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	1	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	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	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	0	0	0	0	1	-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
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	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	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	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	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	0	0	0	0	1	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	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	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	1	0	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

```
-1.#IND00
                                                  1.0000
                                                             nonperiodic-templates
0
                                                   1.0000
    0
        0
            0
                0
                    0
                        0
                            0
                                0
                                    1
                                       -1.#TND00
                                                              nonperiodic-templates
                                    0 -1.#IND00
                                                   1.0000
0
    0
        0
            0
                0
                    0
                        1
                            0
                                0
                                                              nonperiodic-templates
0
    0
        0
            0
                    0
                       Ω
                            0
                                0
                                    0 -1.#IND00
                                                   1.0000
                                                              nonperiodic-templates
                1
            0
                                                   1.0000
0
    0
        0
                0
                    0
                        0
                            0
                                1
                                    0
                                       -1.#IND00
                                                              nonperiodic-templates
            0
                    0
                            0
                                0
                                      -1.#IND00
                                                   1.0000
                                                             nonperiodic-templates
0
    1
Ω
    Ω
        Ω
            Ω
                Ω
                    Ω
                        0
                                0
                                    0 - 1. #TND00
                                                   1.0000
                                                              nonperiodic-templates
                            1
Ω
    Ω
        Ω
            1
                Ω
                    Ω
                        0
                            Ω
                                0
                                    0 -1.#IND00
                                                   1.0000
                                                              nonperiodic-templates
                       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
                                                   1.0000
                                                             nonperiodic-templates
   0
        0
            0
                Ω
                   0
                       0
                                0
                                    0 -1.#IND00
0
                            1
   Ω
       Ω
            Ω
                            Ω
                                    0 -1.#IND00
                                                   1.0000
0
                Ω
                   0
                        1
                                0
                                                              nonperiodic-templates
    0
        0
            0
                0
                    0
                        Ω
                            0
                                0
                                    1
                                       -1.#IND00
                                                   1.0000
                                                              nonperiodic-templates
0
                                    0 -1.#IND00
0
            0
                    0
                       0
                            0
                                1
                                                   1.0000
                                                             nonperiodic-templates
   0
        0
            0
                0
                        0
                                0
                                                   1.0000
0
                    0
                            1
                                    0 -1.#IND00
                                                             nonperiodic-templates
                                    0 -1.#IND00
0
    0
        0
            0
                1
                    0
                        0
                            0
                                0
                                                   1.0000
                                                             nonperiodic-templates
0
   0
        1
            0
                0
                    0
                       Ω
                            0
                                0
                                    0 -1.#IND00
                                                   1.0000
                                                              nonperiodic-templates
            0
                        0
                            0
                                0
                                                   1.0000
0
   1
        0
                0
                    0
                                    0 -1.#IND00
                                                              nonperiodic-templates
Ω
        Ω
            0
                Ω
                    Ω
                       Ω
                            0
                                0
                                    0 -1.#IND00
                                                   1.0000
                                                             nonperiodic-templates
   0
        0
                0
                       0
                            0
                                0
                                                   1.0000
0
            1
                    0
                                    0 -1.#IND00
                                                             nonperiodic-templates
0
   Ω
        Ω
            Ω
                Ω
                    Ω
                        1
                            Ω
                                0
                                    0 -1.#IND00
                                                   1.0000
                                                             overlapping-templates
                                                   1.0000
    0
            0
                0
                    0
                       0
                            0
                                0
                                    0 -1.#IND00
                                                             universal
   0
        0
            0
                0
                    0
                        0
                            0
                                0
                                    0 -1.#IND00
                                                   1.0000
1
                                                             apen
                                    0 -1.#IND00
                                                              random-excursions
0
   0
        0
            0
                       0
                            0
                                0
                                                   -1.#TND
                0
                    0
Ω
   Ω
        Ω
            Ω
                Ω
                    Ω
                       Ω
                            Ω
                                Ω
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions
0
   0
        0
            0
                0
                    0
                        0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions
                                    0 -1.#IND00
            0
                0
                    0
                      0
                            0
                                0
                                                   -1.#IND
                                                              random-excursions
0
   0
       0
            0
                0
                    0
                        0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions
                                                   -1.#IND
0
   Ω
        Ω
            Ω
                0
                    Ω
                       0
                            0
                                Ω
                                    0 -1.#IND00
                                                              random-excursions
Ω
   Ω
        Ω
            Ω
                Λ
                    Ω
                       Ω
                            Ω
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions
0
    0
        0
            0
                Ω
                    0
                        Ω
                            0
                                0
                                    Ω
                                      -1.#IND00
                                                   -1.#IND
                                                              random-excursions
0
   0
        0
            0
                    0
                      0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
0
   0
       0
            0
                0
                   0
                       0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
0
   0
        0
            0
                0
                    0
                        Ω
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
            0
                       0
                            0
                                    0 -1.#IND00
                                                   -1.#IND
0
    0
        0
                0
                    0
                                0
                                                              random-excursions-variant
0
   0
        0
            0
                0
                    0
                        0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
                                    0 -1.#IND00
                       0
   0
        0
            0
                                0
                                                   -1.#TND
0
                0
                   0
                            0
                                                              random-excursions-variant
0
   0
        0
            0
                0
                   0
                        0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
0
   0
        0
            0
                0
                    0
                        0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
            0
                    0
                       0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
   0
        0
            0
                Ω
                        Ω
                            0
                                0
                                    0 -1.#IND00
0
                    0
                                                   -1.#IND
                                                              random-excursions-variant
                                    0 -1.#IND00
   Ω
        Ω
            Ω
                            Ω
                                Ω
                                                   -1.#TND
0
                0
                   Ω
                       Ω
                                                              random-excursions-variant
                       0
Ω
   Ω
        Ω
            Ω
                Ω
                   Ω
                            Ω
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
    0
        0
            0
                0
                    0
                        0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
0
                                                              random-excursions-variant
                       0
                            0
                                    0 -1.#IND00
                                                   -1.#IND
0
   0
        0
            0
                0
                    0
                                0
                                                              random-excursions-variant
                                    0 -1.#IND00
                                                   -1.#IND
0
   0
       0
            0
                0
                    0
                       0
                            0
                                0
                                                              random-excursions-variant
Ω
   Ω
        0
            0
                0
                    Ω
                        Ω
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
   0
        0
            0
                    0
                      0
                            0
                                0
                                    0 -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
0
                0
    0
            0
                0
                        0
                            0
                                0
                                    0
                                      -1.#IND00
                                                   -1.#IND
                                                              random-excursions-variant
                        0
                                    0 -1.#IND00
                                                   0.0000 *
    0
        0
            0
                0
                   0
                            0
                                0
                                                             serial
1
                   0
                                                   0.0000 * serial
1
    Ω
       Ω
            0
                Ω
                        0 0
                                Ω
                                    0 -1.#IND00
0
    0
       Ω
            0
                0
                   0
                        1
                            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 -1.#INF00 for a sample size = 0 binary sequences.

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

. -------

2. Test dla klucza wygenerowanego przy pomocy wbudowanej funkcji Random(): **3 gwiazdki.**

												PASSING SEQUENCES
	 C2										PROPORTION	STATISTICAL TEST
1	0	0	0	0	0	0	0	0	0	-1.#IND00		frequency
0	0	0	0	0	0	0	1	0	0	-1.#IND00		block-frequency
0	1	0	0	0	0	0	0	0	0	-1.#IND00		cumulative-sums
1 0	0	0	0	0	0	0	0	0	0	-1.#IND00		cumulative-sums runs
0	0	0	0	0	0	0	0	0	1	-1.#IND00		longest-run
0	0	0	0	0	0	0	1	0	0	-1.#IND00	1.0000	rank
0	0	0	0	0	0	0	1	0	0	-1.#IND00		fft
0	0	0	0	0 1	0	0	1	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	1	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates
1 0	0	0	0	0	0 1	0	0	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates
0	0	0	0	0	1	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	1	0	0	0	0	0	0	0 1	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	1	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	1	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0 1	0	1	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	1	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	1	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	1	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	1	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	1	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	1	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	1	0	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00		
0	0	1	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	1	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates
0	0	0	1	0	0	0	1	0	0	-1.#IND00		nonperiodic-templates 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		nonperiodic-templates
0	1	0	0	0	0	0	0	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	1	0	0	0	0	0	0	0	-1.#IND00		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	1	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0 1	0	0	0	0	1	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	0	0	1	0	0	0	-1.#IND00		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		nonperiodic-templates
0	0 1	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	0	0	0	0	0	1	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00		nonperiodic-templates
0	0	0	0	0	0	0 1	0	0	1	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	0	0	0	0	1	0	0	0	0	-1.#IND00		nonperiodic-templates nonperiodic-templates
0	1	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	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	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	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
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
-			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	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	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	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	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	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	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	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	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	0	0	0	0	1	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	0	1	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	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	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	0	1	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		1.0000	
_										-1.#IND00		nonperiodic-templates
1	0	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	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	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	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	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	1	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	1	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	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	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
1	0	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	0.0000 *	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	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	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	0	1	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	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	1	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	0	0	0	1	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	0	1	-1.#IND00	1.0000	nonperiodic-templates	
0	0	1	0	0	0	0	0	0	0		1.0000		
		0		0	0	0	0	0	0	-1.#IND00		nonperiodic-templates	
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	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	1	0	0	0	0	-1.#IND00	1.0000	nonperiodic-templates	
1	0	0	0	0	0	0	0	0	0	-1.#IND00	0.0000 *	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	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	0	0	0	0	0	0	1	-1.#IND00	1.0000	nonperiodic-templates	
0	0	0	0	1	0	0	0	0	0	-1.#IND00	1.0000	overlapping-templates	
0	0	0	0	0	0	0	0	1	0	-1.#IND00	1.0000	universal	
1	0	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	apen	
0	0	0	0	0	1	0	0	0	0	-1.#IND00	1.0000	random-excursions	
0	0	0	0	0	0	0	0	0	1	-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	0	1	-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	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	1	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-variant	
0	0	1	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	1	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	1	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	0	0	0	1	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	0	0	0	0	0	0	1	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	1	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	0	1	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	0	0	0	0	0	0	1	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	0	1	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	0	1	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	0	1	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	1	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	1	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
0	1	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant	
	0	1	0	0	0	0	0	0	0			random-excursions-variant	
0	0	1	0	0	0	0	0	0	0	-1.#IND00 -1.#IND00	1.0000	random-excursions-variant random-excursions-variant	
0	0	1	0	0	0	0	0	0	0	-1.#IND00	1.0000	random-excursions-variant random-excursions-variant	
1		0		0	0	0	0	0					
	0		0	0			0	0	0	-1.#IND00 -1.#IND00	1.0000	serial	
1	0	0	0		0	0					1.0000	serial	
0													
excur	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.												

3. Test dla zaszyfrowanego tekstu o długości 125 000 znaków (po 8 bitów każdy) przy pomocy klucza z testu nr 1:

1 gwiazdka.

				IINITE	ODMIT						ODODETON OF	PASSING SEQUENCES
			Ine	ONIF								
												STATISTICAL TEST
										P-VALUE	PROPORTION	STATISTICAL TEST
1	0	0	0	0	0	0	0	0	0	-1.#IND0	0 1.0000	frequency
0	0	0	0	0	0	0	0	0	1	-1.#IND0	0 1.0000	block-frequency

1	0	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	cumulative-sums
1	0	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	cumulative-sums
0	0	1	0	0	0	0	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	0	1	0 1	0	0	0	0	-1.#IND00	1.0000	rank
0	0	0	0	0	0	0	0	1	0	-1.#IND00 -1.#IND00	1.0000	fft
0	0	0	0	0	0	0	1	0	0	-1.#IND00	1.0000	nonperiodic-templates 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	1	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	0	1	0	-1.#IND00	1.0000	nonperiodic-templates
0	0	0	0	0	0	1	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	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	1	0	0	0	-1.#IND00	1.0000	nonperiodic-templates
0	0	0	0	0	0	0	0	1	0	-1.#IND00 -1.#IND00	1.0000 1.0000	nonperiodic-templates
0	0	0	0	1	0	0	0	0	0	-1.#IND00	1.0000	nonperiodic-templates 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	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	0	0	1	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
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	-1.#IND00 -1.#IND00	1.0000 1.0000	nonperiodic-templates
0	0	0	1	0	0	0	0	0	0	-1.#IND00	1.0000	nonperiodic-templates 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	1	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	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	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	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	-1.#IND00	1.0000	nonperiodic-templates nonperiodic-templates
0	0	0	1	0	0	0	0	0	0	-1.#IND00 -1.#IND00	1.0000 1.0000	nonperiodic-templates nonperiodic-templates
1	0	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	1	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	1	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	1	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
1 0	0	1	0	0	0	0	0	0	0	-1.#IND00 -1.#IND00	1.0000 1.0000	nonperiodic-templates 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	0.0000 *	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	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	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	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	1	0	0	0	0	0	0	0	-1.#IND00	1.0000	nonperiodic-templates
0	0	0	0	0	1	0	1	0	0	-1.#IND00 -1.#IND00	1.0000 1.0000	nonperiodic-templates nonperiodic-templates
1	0	0	0	0	0	0	0	0	0	-1.#IND00 -1.#IND00	1.0000	nonperiodic-templates 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	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	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	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	0	0	0	0	0	0	0	1	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	1	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	0	1	-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	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	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	1	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	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	0	0	1	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	1	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	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	0	0	0	1	0	0	0	0	-1.#IND00	1.0000	nonperiodic-templates
		0	1			0	0	0				1 1
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	1	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		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	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	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
1	0	0	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	0	0	1	-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	1	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
_												
1	0	0	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	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	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	0	0	0	1	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
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	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	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	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	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
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	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	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	1	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
												- +

```
-1.#IND00
                                                  1.0000
                                                            overlapping-templates
  0
     0
                                    0
             0
                 0
                     0
                        0
                            0
                                       -1,#TND00
                                                  1.0000
                                                            universal
                                    0 -1.#IND00
  0
     0
         0
             0
                     0
                        0
                                0
                                                  1.0000
                                                            apen
  0
     0
             0
                 0
                     0
                        0
                            0
                                0
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions
             0
                        0
                                       -1.#IND00
                                                  -1.#IND
                                                            random-excursions
     0
             0
                     0
                                0
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions
  Ω
     Ω
         Ω
             Ω
                 Ω
                     Ω
                        Ω
                            0
                                Ω
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions
  0
     0
             0
                 Ω
                     0
                        Ω
                                0
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions
                       0
             0
                                0
                                    0 -1.#IND00
                                                  -1.#IND random-excursions
  0
                     0
     0
             0
                        0
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions
                       0
  0
     0
             0
                                0
                                    0 -1.#IND00
                                                  -1.#IND
                    0
                                                            random-excursions
     Ω
             Ω
                       0
                                Ω
  0
         0
                 0
                    Ω
                            Ω
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions-variant
  0
     0
             0
                 0
                     0
                        0
                                0
                                    0 -1.#IND00
                                                  -1.#IND
                                                             random-excursions-variant
                                   0 -1.#IND00
                                                  -1.#IND
             0
                                                            random-excursions-variant
                       0
  0
     0
             0
         0
                 0
                     0
                            0
                                0
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions-variant
                               0
     0
  0
         0
             0
                 0
                     0
                            0
                                    0 -1.#IND00
                                                  -1.#IND
                                                             random-excursions-variant
                               0
  0
     0
         0
             0
                 0
                    0
                       0
                            Ω
                                   0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions-variant
             0
                                0
  0
                        0
                                    0 -1.#IND00
                                                  -1.#IND
                                                             random-excursions-variant
                       0
  0
     0
             0
                     0
                               0
                                   0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions-variant
                       0
  0
     0
         0
             0
                            0
                                0
                 0
                     0
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions-variant
                               0
                                   0 -1.#IND00
  Ω
     0
         0
             0
                 Ω
                     0
                            Ω
                                                  -1.#IND
                                                            random-excursions-variant
                                    0 -1.#IND00
                                                  -1.#IND random-excursions-variant
                     0 0
                       0
  0
     0
             0
                 0
                     0
                            0
                                0
                                   0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions-variant
                               0
                                   0 -1.#IND00
  0
     0
             0
                            0
                                                  -1.#TND
                    0
                                                            random-excursions-variant
                                  0 -1.#IND00
                       0 0 0 0
  Ω
     0
         0
             0
                 Ω
                    Ω
                                                  -1.#IND
                                                            random-excursions-variant
  0
     0
         0
             0
                 0
                     0
                                    0 -1.#IND00
                                                  -1.#IND
                                                             random-excursions-variant
                    0 0 0 0
                                  0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions-variant
                       0
0
  0
     0
             0
                 0
                    0
                            0
                                0
                                    0 -1.#IND00
                                                  -1.#IND
                                                            random-excursions-variant
                               0
                                                  -1.#IND
  0
     Ω
             Ω
                 0
                    Ω
                            Ω
                                    0 -1.#IND00
                                                            random-excursions-variant
                       0
                                   0 -1.#IND00
  Ω
     0
         0
             1
                 Ω
                    Ω
                            0 0
                                                  1.0000
                                                            serial
  0
             0
                 0
                     0
                        0
                            0
                                0
                                    0
                                      -1.#IND00
                                                  1.0000
                                                            serial
                                    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
-1.#INF00 for a sample size = 0 binary sequences.
```

Wnioski:

Z przeprowadzonych testów wynika, że można osiągnąć dość dobre wyniki – porównywalne, a nawet lepsze od generowanych przez wbudowany generator Random(), korzystając z tego typu algorytmu, jednak dużo zależy od parametrów podanych na wejście – ziarna, miejsc odczepu, zła ich kombinacja może dać dużo gorsze wyniki. Zaszyfrowana wiadomość przy pomocy szyfratora powinna osiągnąć lepsze wyniki w testach niż klucz wygenerowany przy pomocy generatora i tak też było.

For further guidelines construct a probability table using the MAPLE program

provided in the addendum section of the documentation.