

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 samodecydujący 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:

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

Krok:	Rejestr:								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.

Generator samodecymujący Ruepella

Generator

Ziano (Seed)
2364957293

Długość klucza: 1000000

Liczba 'd' oznacza ilość taktów wykonanych przy wyjściu równym 0.
Liczba 'd': 3

Liczba 'k' oznacza ilość taktów wykonanych przy wyjściu równym 1.
Liczba 'k': 5

tap1: 32 tap2: 25 tap3: 15 tap4: 9

Wyjście

Szyfrator

Klucz

Wyjście

Wyjście

Zapisz do pliku Resetuj Generator wbudowany Generuj

Resetuj Szyfruj Deszyfruj

Kopiuj z generatora
Wczytaj klucz z pliku
Kopiuj z Wyjścia
Wczytaj wejście z pliku
Zapisz do pliku

Testy:

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

[illegible]

[illegible]

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

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	
1	0	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	frequency	
0	0	0	0	0	0	0	1	0	0	-1.#IND00	1.0000	block-frequency	
0	1	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	0	0	0	0	0	0	0	1	-1.#IND00	1.0000	runs	
0	0	0	0	0	0	0	0	0	1	-1.#IND00	1.0000	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	1.0000	fft	
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	
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	
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	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	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	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	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	
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	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	
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	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	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	
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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							

[illegible]

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.#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	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	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	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
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	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	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	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
1	0	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	serial
1	0	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	serial
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.

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

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

1	0	0	0	0	0	0	0	0	0	-1.#IND00	1.0000	frequency
0	0	0	0	0	0	0	0	0	1	-1.#IND00	1.0000	block-frequency

[illegible]

