W wynikach skupię się głównie na tym co się „nie udało” (w ramach zwięzłości). Zostawiam również krótką notkę, za co poszczególny test odpowiada (żeby było wiadomo co się udało).

Zarówno dla Mersenne Twistera jak i LCG przeprowadziłem 5 testów (na podanej w poleceniu stronie), każdy z 1 000 000 bitów. Dla SHA-1 test przeprowadziłem jedynie raz, z uwagi na to, że dla jednego nazwiska hash będzie ten sam => nie ma fizycznej możliwości na otrzymanie innego wyniku używając tej samej strony i tego samego nazwiska.

Za co odpowiadają poszczególne testy NIST?(w DUŻYM uproszczeniu)

1. Sprawdza czy ilość 1 i 0 jest ”+/-” = 50%.
2. Sprawdza czy 1 i 0 są ”+/-” równomiernie rozłożone tj. nie ma sytuacji, gdzie wszystkie jedynki są w pierwszej połowie ciągu znaków, a wszystkie zera w drugiej.
3. Sprawdza czy ilość ciągów 0 i 1 różnej długości (np. #0111110 itp.) jest odpowiednia.
4. Sprawdza czy częstość z jaką pojawiają się najdłuższe przewidywane ciągi 1.
5. Sprawdza czy istnieją powtarzające się wzory (”patterns”).
6. Sprawdza czy powyższe powtarzające się wzory są blisko siebie.
7. Sprawdza czy istnieją konkretne (ustalone) ciągi bitów i czy ich liczba jest odpowiednia (ciągi te nie mogą na siebie nachodzić).
8. Sprawdza czy istnieją konkretne (ustalone) ciągi bitów i czy ich liczba jest odpowiednia (ciągi te mogą na siebie nachodzić).
9. Sprawdza odległości między takimi samymi wzorami.
10. Sprawdza długość ” a linear feedback shift register (LFSR)” potrzebnego do wygenerowania danego ciągu bitów.
11. Sprawdza częstość występowania wszystkich możliwych nachodzących na siebie m-bitowych wzorów. Dla każdego takiego wzoru, częstość występowania powinna być taka sama jak innych wzorów tej samej długości. Liczba takich wzorów powinna być odpowiednia.
12. Sprawdza entropie (czyli także ”randomness”). Aproksymuje przez podzielenie # ww. m-bitowych wzorów przez # m+1-bitowych wzorów. Wynik ten porównuje się z oczekiwanym (maksymalnie ~ln2).
13. Sprawdza czy 1 lub 0 występują w dużych ilościach na początkowych i/lub końcowych etapach ciągu lub czy są równomiernie wymieszane w całym ciągu.
14. Sprawdza ile razy w danym cyklu występuje dana ”cumulative sum”.

Dokładniejsze informacje/ew. niedopowiedzenia można znaleźć/rozwiać tutaj: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

LCG

Generator przechodzi większość testów.

Raz nie przeszedł testu 3 (P-value >1 => możliwa wina po stronie strony).

Raz nie przeszedł testu 11, P-value było bardzo niskie. Z definicji LCG jest dość podatny na wpadanie w bardzo krótkie cykle, pętle; stosunkowo łatwo aby występowała duża powtarzalność. Możliwym jest, że coś takiego miało właśnie miejsce i stąd bardzo niska entropia (choć dziwi pomyślne przejście innych testów).

Raz nie przeszedł testu 13 (zabrakło 0,004). Jednak przeszedł test 14. Testy te są w pewien sposób „bliźniacze", 13 bada 8 stanów (stany powyżej najwyższego lub poniżej najniższego są liczone jak najniższy lub najwyższy) a 14 aż 18 stanów. Możliwym jest więc, LCG „lubi wpadać" w stany wyższe i niższe stosunkowo często w porównaniu do tych bliskich zeru.

Wnioski: LCG jest dość dobrym generatorem liczb pseudo losowych, jednak nie tak dobrym jak Mersenne Twister(MT). Rozkład jego „stanów (testy 13 i 14)" nie jest tak dobry jak dla MT (wysoka ilość błędów dla tych testów również nie napawa optymizmem). Natomiast największą jego wadą jest łatwość wpadania w krótkie („mało losowe") cykle.

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.26613815033873445	Passed
2. Frequency Test within a Block	0.538825560133964	Passed
3. Runs Test	0.09079123478508888	Passed
4. Test for the Longest Run of Ones in a Block	0.13072457786463879	Passed
5. Binary Matrix Rank Test	0.609690254926168	Passed
6. Non-overlapping Template Matching Test	0.5135620741805507	Passed
7. Overlapping Template Matching Test	0.2595160232832814	Passed
8. Maurer's "Universal Statistical" Test	0.8541273105696405	Passed
9. Linear Complexity Test	0.5198673939424223	Passed
10. Serial Test	P-value 1: 0.12964646929109103 P-value 2: 0.09141122440010724	Passed
11. Approximate Entropy Test	0.08391381031961366	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.16761776274043227 P-value Reverse: 0.3076989681109852	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.9617162426084771	Passed
2. Frequency Test within a Block	0.09447021019028307	Passed
3. Runs Test	1.8793789192434425	Failed
4. Test for the Longest Run of Ones in a Block	0.6159437597350765	Passed
5. Binary Matrix Rank Test	0.2377706733994799	Passed
6. Non-overlapping Template Matching Test	0.554036242568517	Passed
7. Overlapping Template Matching Test	0.06056124084979755	Passed
8. Maurer's "Universal Statistical" Test	0.31783981206500345	Passed
9. Linear Complexity Test	0.6147950197040517	Passed
10. Serial Test	P-value 1: 0.3480865928828113 P-value 2: 0.14650159795118806	Passed
11. Approximate Entropy Test	0.6070817178485156	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.5762236567527586 P-value Reverse: 0.6191910083601417	Passed
13. Random Excursions Test	0.21192260126153925	Passed
14. Random Excursions Variant Test	0.5014092297070036	Passed

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.2584762244800356	Passed
2. Frequency Test within a Block	0.16506592273911905	Passed
3. Runs Test	0.7044818919995235	Passed
4. Test for the Longest Run of Ones in a Block	0.3345633805673859	Passed
5. Binary Matrix Rank Test	0.6151166063911337	Passed
6. Non-overlapping Template Matching Test	0.8948718128853981	Passed
7. Overlapping Template Matching Test	0.7287996008715579	Passed
8. Maurer's "Universal Statistical" Test	0.9525530704849474	Passed
9. Linear Complexity Test	0.855743580462208	Passed
10. Serial Test	P-value 1: 0.49206817747986054 P-value 2: 0.7069169106818007	Passed
11. Approximate Entropy Test	0.8318026610561564	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.4902921550347985 P-value Reverse: 1	Passed
13. Random Excursions Test	0.006153773379803178	Failed
14. Random Excursions Variant Test	0.22695334997944938	Passed

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.08081095183956699	Passed
2. Frequency Test within a Block	0.2626387875424427	Passed
3. Runs Test	0.531937965897955	Passed
4. Test for the Longest Run of Ones in a Block	0.015516643759580742	Passed
5. Binary Matrix Rank Test	0.10128201672206202	Passed
6. Non-overlapping Template Matching Test	0.773433279594248	Passed
7. Overlapping Template Matching Test	0.0562339042868398	Passed
8. Maurer's "Universal Statistical" Test	0.6159213503221519	Passed
9. Linear Complexity Test	0.34062457912262895	Passed
10. Serial Test	P-value 1: 0.17970152480426818 P-value 2: 0.5352578101005041	Passed
11. Approximate Entropy Test	0.000012369471548578091	Failed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.15783534703688762 P-value Reverse: 0.5765605938883134	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.4592999943295808	Passed
2. Frequency Test within a Block	0.4089219152311223	Passed
3. Runs Test	0.9820111324793624	Passed
4. Test for the Longest Run of Ones in a Block	0.051831977960479544	Passed
5. Binary Matrix Rank Test	0.5471050303184408	Passed
6. Non-overlapping Template Matching Test	0.7669506203989523	Passed
7. Overlapping Template Matching Test	0.5326128151514115	Passed
8. Maurer's "Universal Statistical" Test	0.714918485700706	Passed
9. Linear Complexity Test	0.2260443571993266	Passed
10. Serial Test	P-value 1: 0.7603320752792931 P-value 2: 0.9840433753017813	Passed
11. Approximate Entropy Test	0.8971135336444286	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.3265774181022765 P-value Reverse: 0.7811150782248921	Passed
13. Random Excursions Test	0.18735326936559776	Passed
14. Random Excursions Variant Test	0.018093842191290288	Passed

MERSENNE TWISTER

Generator bez większych problemów przechodzi (prawie) wszystkie testy.

Dwa razy generator nie przeszedł testu 3, lecz P-value jest tam większa od 1, co jest ciężkie do zinterpretowania i (myślę że) skłaniałoby raczej do spodziewania się błędu po stronie strony internetowej (implementacji testu NIST), aniżeli samej metodologii czy wartości wyrzuconych przez generator.

Raz nie przeszedł testu 4, lecz był bardzo blisko (zabrakło 0,002 w P-value).

Raz nie przeszedł testu 8, lecz był bardzo blisko (zabrakło 0,002 w P-value). Test sprawdza jak bardzo da się skompresować dany ciąg bitów, a Mersenne Twister znany jest z „odporności" na kompresowanie. Nie uznałbym tego negatywnego wyniku za „bardzo" istotny.

W jednej próbie wystąpił błąd w teście 13 i 14 (ciężko mi powiedzieć dlaczego, ale spodziewam się winy po stronie strony).

Raz „oblał" test 14 (zabrakło 0,005). Oznacza to, że w tym teście była lekka tendencja do przebywania w danym „stanie" ciut częściej lub rzadziej niż zakładano od PRNG.

Wnioski z tych testów płyną następujące: Mersenne Twister jest bardzo dobrym generator liczb pseudo losowych, czasami zdarzy mu się wypaść poza „strefę przyzwoitości" i nie przejść danego testu. Jednak wypadki takie nie są ani częste, ani bardzo drastyczne (P-value są bardzo niewiele poniżej zakładanego zakresu).

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.8949842917488074	Passed
2. Frequency Test within a Block	0.4544117426717819	Passed
3. Runs Test	1.4869935922311206	Failed
4. Test for the Longest Run of Ones in a Block	0.18007894958577042	Passed
5. Binary Matrix Rank Test	0.2526736367987845	Passed
6. Non-overlapping Template Matching Test	0.6498807574603207	Passed
7. Overlapping Template Matching Test	0.04608944943450769	Passed
8. Maurer's "Universal Statistical" Test	0.008329307209860803	Failed
9. Linear Complexity Test	0.1202684013696759	Passed
10. Serial Test	P-value 1: 0.799411057936783 P-value 2: 0.5118241484506787	Passed
11. Approximate Entropy Test	0.8385521851599476	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.9969633143740679 P-value Reverse: 0.9829034542512365	Passed
13. Random Excursions Test	0.08806677816236932	Passed
14. Random Excursions Variant Test	0.3558089413139778	Passed

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.8041344068024324	Passed
2. Frequency Test within a Block	0.926077191507125	Passed
3. Runs Test	0.3964036901024165	Passed
4. Test for the Longest Run of Ones in a Block	0.4030546212940589	Passed
5. Binary Matrix Rank Test	0.7977501173149483	Passed
6. Non-overlapping Template Matching Test	0.4939452419013044	Passed
7. Overlapping Template Matching Test	0.688731801457207	Passed
8. Maurer's "Universal Statistical" Test	0.4529617861598738	Passed
9. Linear Complexity Test	0.17099823080585042	Passed
10. Serial Test	P-value 1: 0.6768510804902736 P-value 2: 0.3964380007139442	Passed
11. Approximate Entropy Test	0.44013124717788554	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.8280351071340093 P-value Reverse: 0.9911716198174783	Passed
13. Random Excursions Test	0.013154135005838615	Passed
14. Random Excursions Variant Test	0.005515428231730013	Failed

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.42836067623307494	Passed
2. Frequency Test within a Block	0.07817375756475911	Passed
3. Runs Test	0.8503848700685468	Passed
4. Test for the Longest Run of Ones in a Block	0.0084671411359036	Failed
5. Binary Matrix Rank Test	0.9032250795541384	Passed
6. Non-overlapping Template Matching Test	0.6418128269196826	Passed
7. Overlapping Template Matching Test	0.45594204448393727	Passed
8. Maurer's "Universal Statistical" Test	0.6350804455284098	Passed
9. Linear Complexity Test	0.85355103398765 9	Passed
10. Serial Test	P-value 1: 0.7179868678583248 P-value 2: 0.8508766586427323	Passed
11. Approximate Entropy Test	0.7963388579150715	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.28691198328412115 P-value Reverse: 0.7720697986119001	Passed
13. Random Excursions Test	0.14552504078731776	Passed
14. Random Excursions Variant Test	0.0925628813746896	Passed

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.46783877055292755	Passed
2. Frequency Test within a Block	0.6074139450164571	Passed
3. Runs Test	1.204729921990532	Failed
4. Test for the Longest Run of Ones in a Block	0.15708222294131882	Passed
5. Binary Matrix Rank Test	0.9268539905343912	Passed
6. Non-overlapping Template Matching Test	0.8087035185112498	Passed
7. Overlapping Template Matching Test	0.8739725402373415	Passed
8. Maurer's "Universal Statistical" Test	0.6376038167912566	Passed
9. Linear Complexity Test	0.7651564359660951	Passed
10. Serial Test	P-value 1: 0.7427929059438263 P-value 2: 0.7948637838609869	Passed
11. Approximate Entropy Test	0.794981460046567	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.6951452782347407 P-value Reverse: 0.6082724599123537	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.3832083775509474	Passed
2. Frequency Test within a Block	0.4909916997461422	Passed
3. Runs Test	0.09126511237842205	Passed
4. Test for the Longest Run of Ones in a Block	0.4625935722158395	Passed
5. Binary Matrix Rank Test	0.08855862078163204	Passed
6. Non-overlapping Template Matching Test	0.7427847389433715	Passed
7. Overlapping Template Matching Test	0.8034349733363868	Passed
8. Maurer's "Universal Statistical" Test	0.05165173055858574	Passed
9. Linear Complexity Test	0.05925878471094482	Passed
10. Serial Test	P-value 1: 0.16449682662352577 P-value 2: 0.09141122440010724	Passed
11. Approximate Entropy Test	0.2789526914961004	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.6137459825796467 P-value Reverse: 0.5983301549986939	Passed
13. Random Excursions Test	0.1056253333072583	Passed
14. Random Excursions Variant Test	0.27333192741126255	Passed

SHA-1

Zacznę od tego, że nie jest on wstanie przejść wielkości testów ze względu na potrzebną ilość bitów do ich przeprowadzania (brakuje kilku rzędów wielkości generowanego hashu).

Nie przejściem testu 3 (P-value powyżej 1, znów obarczyłbym stronę).

Nie przejście testu 4 oznacza, że nie pojawił się odpowiednio długi ciąg 1 (co może występować często, jeśli nasz hash ma zależeć od nazwiska).

Test 11 wskazał niską entropię => stosunkowo dużą „powtarzalność" możliwych wzorów.

Wnioski: O ile hashowanie ma swoje niewątpliwe plusy i zastosowania, o tyle nie uznałbym go za dobry sposób generowania liczb losowych.

Tests

Start Test

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.6170750774519738	Passed
2. Frequency Test within a Block	0.8553453273074225	Passed
3. Runs Test	1.1854840696952003	Failed
4. Test for the Longest Run of Ones in a Block	0.0013003420142660568	Failed
5. Binary Matrix Rank Test		Error
6. Non-overlapping Template Matching Test		Error
7. Overlapping Template Matching Test		Error
8. Maurer's "Universal Statistical" Test		Error
9. Linear Complexity Test		Error
10. Serial Test		Error
11. Approximate Entropy Test	0.0004515650794936126	Failed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.9458885209237415 P-value Reverse: 0.9458885209237415	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error