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