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.