Blum Blum Shub

Os valores de q e s são dependentes do valor de p utilizado, então, por exemplo, se você escolhe o valor de p = 88379, o valor de q vai ser calculado e o mesmo vai ser q = 89387.

A semente s vai ser calcula e seu resultado é s = 5303185940.

A seguir, o exemplo usado:

```
Primos usados:
p => 88379
q => 89387

Semente s usada (secreta em aplicações reais) => 5303185940
n = p * q = 7899933673

Arquivo "bits_bbs.txt" gerado com 100.000 bits.
```

Obs.: O valor de p é via prompt de comando, ou seja, o usuário que define o número, mas nem todos são aceitos para o programa e para o teste no site **Random Bitstream Tester**.

Os bits são gerados em um arquivo .txt. Ao escolher o **Manual bitstream input**, você colará os bits e, assim, startar o teste.

Com esses bits, obtive os seguintes resultados:

Test name	Result value (P-value)	Status
1. Frequency (Monobit) Test	0.21511862812929072	Passed
2. Frequency Test within a Block	0.7499327615835366	Passed
3. Runs Test	0.07788147455226913	Passed
4. Test for the Longest Run of Ones in a Block	0.2646970380375414	Passed
5. Binary Matrix Rank Test	0.001923114804230958	Failed
6. Non-overlapping Template Matching Test		Error
7. Overlapping Template Matching Test		Error
8. Maurer's "Universal Statistical" Test		Error
8. Maurer's "Universal Statistical" Test		Error
9. Linear Complexity Test		Error
10. Serial Test		Error
11. Approximate Entropy Test	0.2894775593762201	Passed
12. Cumulative Sums (Cusum) Test	P-value Forward: 0.21085507108222168 P-value Reverse: 0.6925302678770493	Passed
13. Random Excursions Test		Error
14. Random Excursions Variant Test		Error