

	a	b	c	d	e
num_zeros	4992	5085	4957	5055	5005
num_ones	5008	4915	5043	4945	4995
longest_zeros	10	13	11	12	11
longest_ones	13	12	10	11	11
100001's	145	152	157	154	150
1000001's	78	67	62	79	75
10000001's	26	46	38	39	32

overall distribution of 1s and 0s

Frequency of 0s and 1s is good because evenly distributed

get the longest sequence of 0s and 1s

the average length or a run is 11.

the probability of just the 11 0s or 1s $*0.5^{11}$ (0.000488281)

chance is 0.5% so it should not be happening this consistently indicating our lfsr is not very random.

if we include the leading and trailing inverse bit it is $*0.5^{13}$ (0.00012207)

we really should not be seeing this length of sequential bits consistently.

frequency of length $3 < i < 7$

according to the NIST SP 800-22:

- the likelihood of a 1 should be 50% regardless of the previous outputs. like a true coinflip
- We can mathematically calculate the longest run of a 0 or 1 and compare the expected to our lfsr output. This is an indicator of the random performance of our lfsr
- in practice, calculate the expected length(i) repetitions of runs from 3 to 7 and compare to lfsr output.

In our case, we are looking for repetitions of 0's with lengths 4,5 and 6. You made this section very easy because of your *hint*

using this formula $*0.5^{\text{length}+2}$ we can calculate the probability of 100001 when length=4.

so there should be:

- 15.6 occurrences for length=4 sequences (0.015625)
- 7.8 occurrences for length=5 sequences (0.0078125)
- 3.9 occurrences for length=6 sequences (0.00390625)