

Java Math.random() Combined Validation Report

Bit Based Randomized Entropy System — Scheduler Based RNG

Developed By: Mehul Singh

Bit Sample Size: 10,918,505 bits

Integer Sample Size: 100,000 integers [0..999]

Total Tests Executed: 45

Analysis Date: April 06, 2026

VERDICT: 41/45 TESTS PASSED
REVIEW NEEDED

This report presents a comprehensive independent analysis combining NIST SP 800-22 statistical tests (core and extended including Binary Matrix Rank, Non-Overlapping Template, Overlapping Template, Linear Complexity), distribution uniformity checks, spectral analysis (FFT, compression, binary derivative, turning point), entropy measurements, autocorrelation profiling, pattern detection, cross-segment consistency, adversarial ML attacks (Logistic Regression, Gradient Boosted Trees, MLP Neural Network), cryptographic wrapper validation, and integer-level distribution and sequence tests (including Anderson-Darling, collision, maximum-of-t, Spearman correlation, and median tests) on Java Math.random() output.

PART 1: NIST SP 800-22 Core Tests (Bits)

Test	p-value	Result	Detail
Frequency (Monobit)	0.003218	FAIL	ones=5,454,385 / zeros=5,464,120 (ratio: 0.499554)
Block Frequency (M=128)	0.809584	PASS	85,300 blocks tested
Runs Test	0.294443	PASS	5,457,516 total runs
Longest Run of Ones	0.711833	PASS	M=10,000 block size
Cumulative Sums (Fwd)	0.002812	FAIL	z=10,552
Cumulative Sums (Rev)	0.004243	FAIL	z=10,153
Approximate Entropy (m=2)	0.026163	PASS	ApEn=0.693147
Serial (m=2) — delta1	0.007505	FAIL	delta1=9.7845
Serial (m=2) — delta2	0.293236	PASS	delta2=1.1047

The NIST Special Publication 800-22 defines the gold standard battery of statistical tests for evaluating randomness quality. A p-value above 0.01 (alpha) indicates no statistically significant deviation from ideal random behavior at the 99% confidence level.

PART 2: NIST SP 800-22 Extended Tests

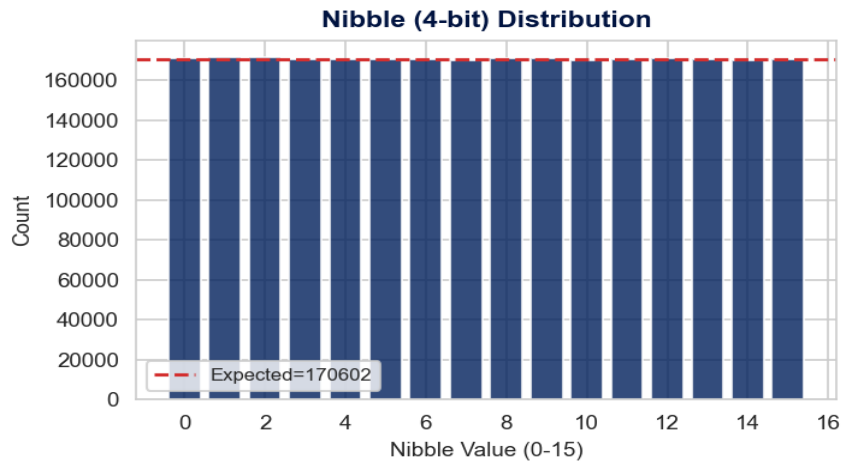
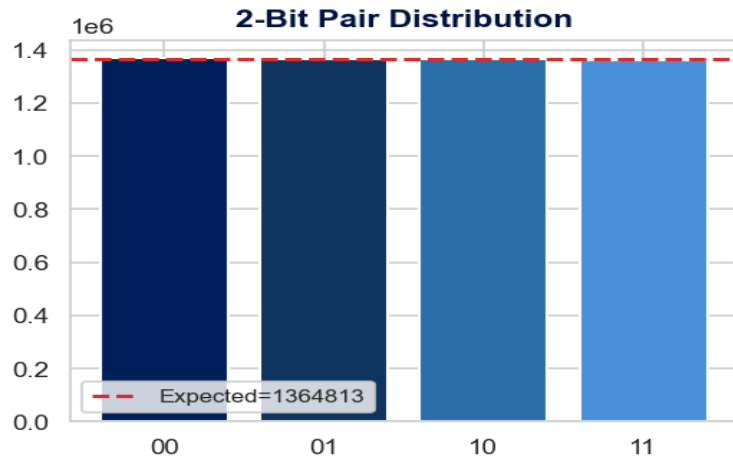
Test	p-value	Result	Detail
Maurer's Universal Statistical	0.358605	PASS	fn=6.1970
Poker Test (m=4)	0.180377	PASS	Chi-sq=19.7840
Random Excursion Variant	0.685598	PASS	Cycles: 1,562
Binary Matrix Rank	0.851951	PASS	Full=567, M-1=1167, rest=266 (n=2000)
Non-Overlapping Template (m=9)	0.396271	PASS	mu=213.24, blocks=100
Overlapping Template (m=9)	1.000000	PASS	lambda=213.24, blocks=100
Linear Complexity	0.920979	PASS	M=500, blocks=1000

Extended tests include Maurer's Universal Statistical test (compressibility), Poker test (block uniformity), Random Excursion Variant (cycle analysis), Binary Matrix Rank (linear dependence), Non-Overlapping and Overlapping Template Matching (pattern occurrence), and Linear Complexity (LFSR complexity).

PART 3: Distribution and Uniformity Analysis (Bits)

Test	p-value	Result	Detail
Byte-Level Chi-Square	0.772120	PASS	256 bins: min=5128, max=5577, exp=5331.3
Nibble-Level Chi-Square	0.180377	PASS	16 bins tested
2-Bit Pair Distribution	0.031013	PASS	00:1,367,499 / 01:1,364,495 / 10:1,364,627 / 11:1,362,631

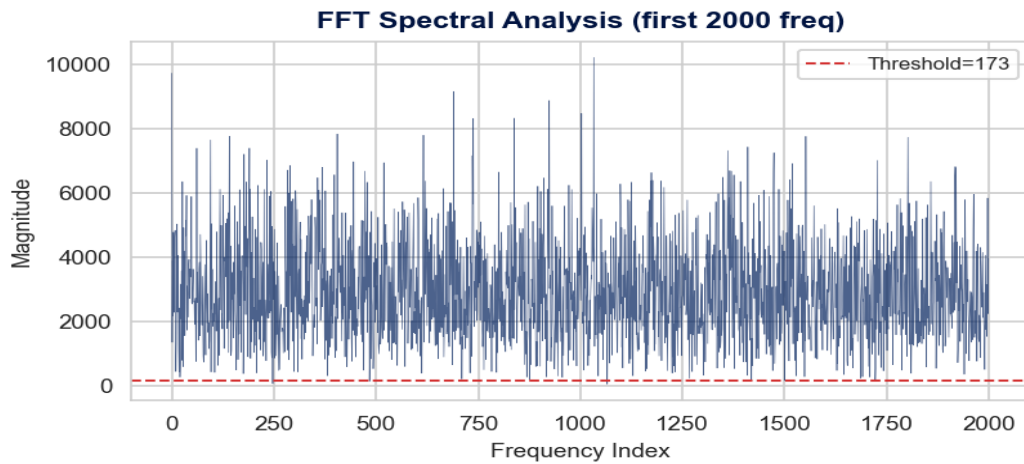
Uniformity tests verify that all possible bit patterns occur with expected frequency at 2-bit, 4-bit (nibble), and 8-bit (byte) granularities.



PART 4: Spectral and Structural Analysis (Bits)

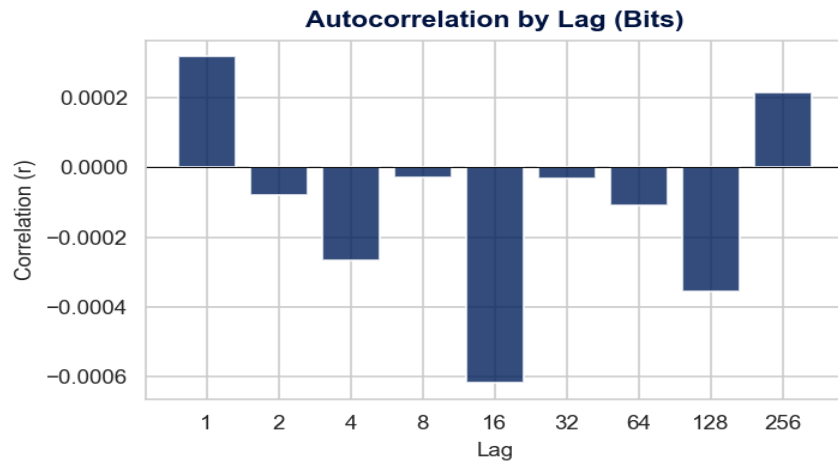
Test	p-value	Result	Detail
Spectral FFT (Periodicity)	0.102548	PASS	peaks below threshold: 5,185,702/5,459,252
Compression Ratio (zlib)	0.218963	PASS	Ratio=1.000312 (1,365,239/1,364,813)
Binary Derivative (1st order)	0.293097	PASS	ones=5,457,515/10,918,504 (ratio=0.499841)
Turning Point Test	0.558081	PASS	TPs=454732, Expected=454936.0

The Discrete Fourier Transform test checks for periodic components in the bitstream. peaks below threshold: 5,185,702/5,459,252. p-value: 0.102548 — No detectable periodicity.



Autocorrelation Profile

Lag	1	2	4	8	16	32	64	128	256
r	+0.0003	-0.0001	-0.0003	-0.0000	-0.0006	-0.0000	-0.0001	-0.0004	+0.0002

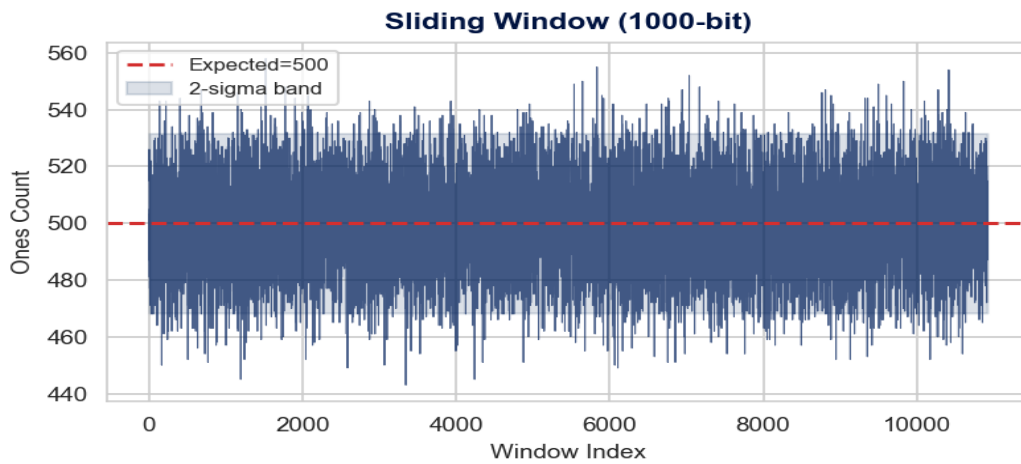
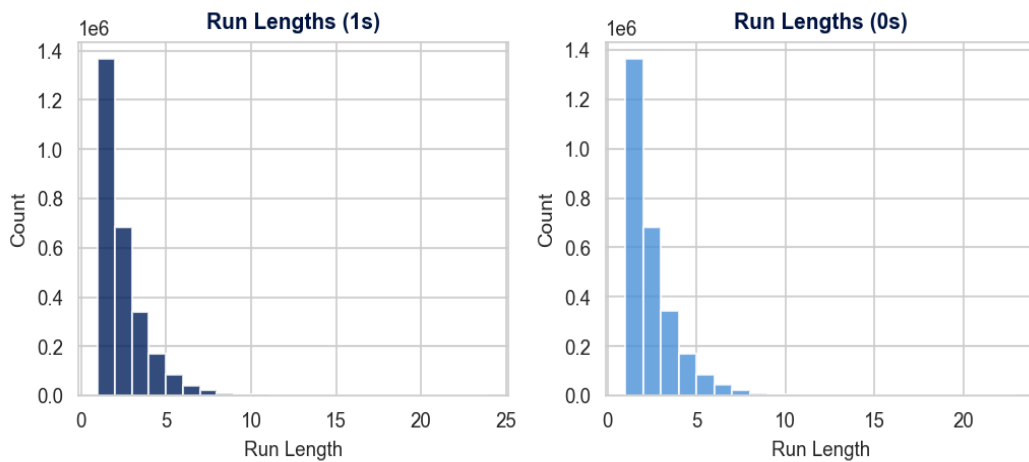


PART 5: Entropy Analysis (Bits)

Metric	Value	Theoretical Max	Assessment
Shannon Entropy (8-bit)	7.999874	8.000000	99.998% of max
Min-Entropy (8-bit)	7.934998	8.000000	99.19%
Transition Rate	0.499841	0.500000	Near-ideal

PART 6: Pattern and Run-Length Analysis (Bits)

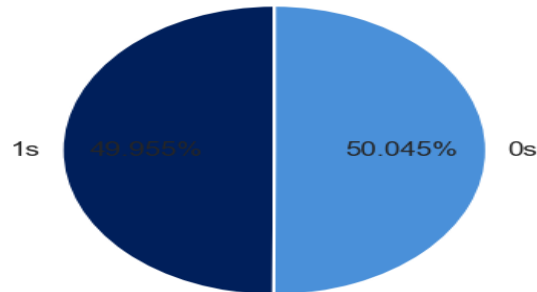
Metric	Ones Runs	Zeros Runs	Expected
Count	2,728,758	2,728,758	~2,729,626
Mean Length	1.9989	2.0024	2.0000
Max Length	23	22	~23



PART 7: Bit-Level Visual Analysis

Visual inspection provides an intuitive layer of validation. A truly random bitstream should show no visible patterns in its matrix representation, uniform density in scatter plots, and a symmetric random walk in cumulative sums.

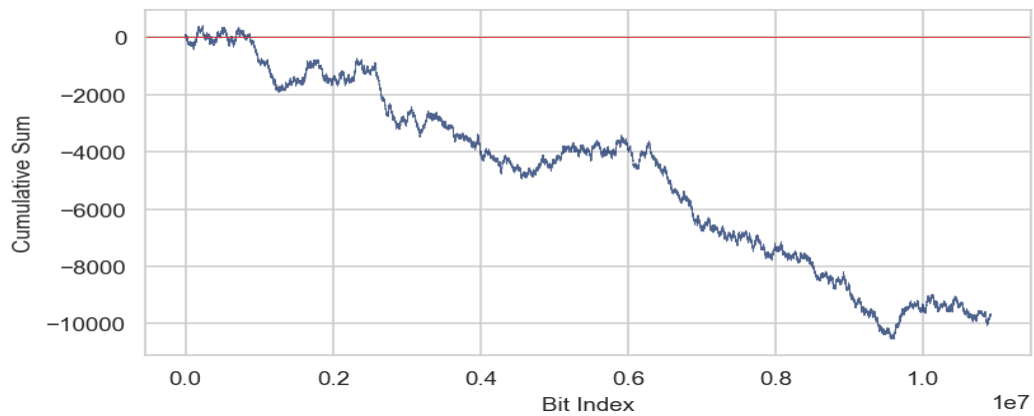
Bit Balance (0 vs 1)



Bit Matrix (100x100)



Cumulative Sum Random Walk

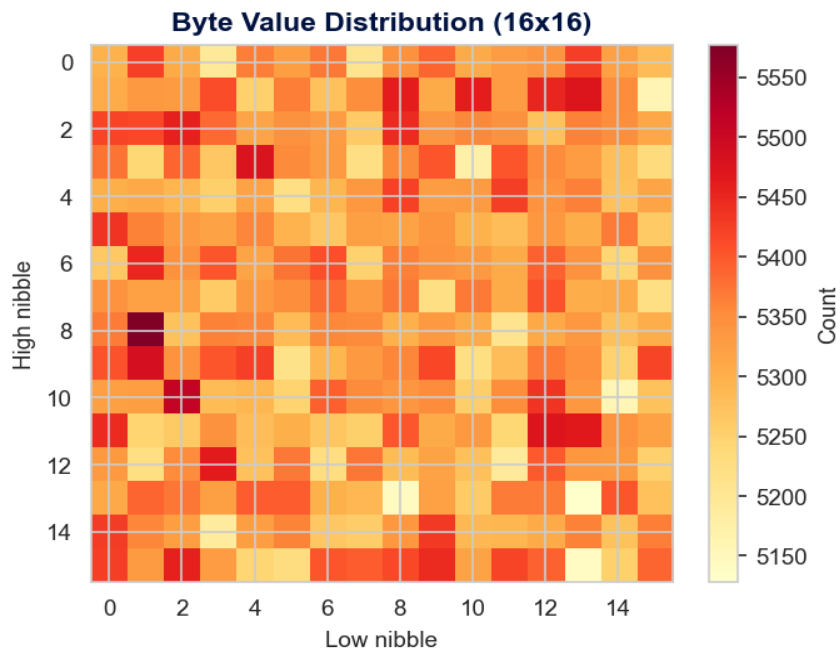
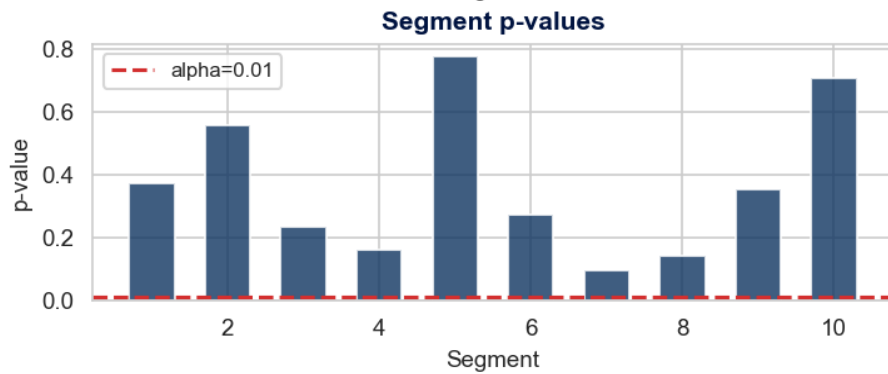
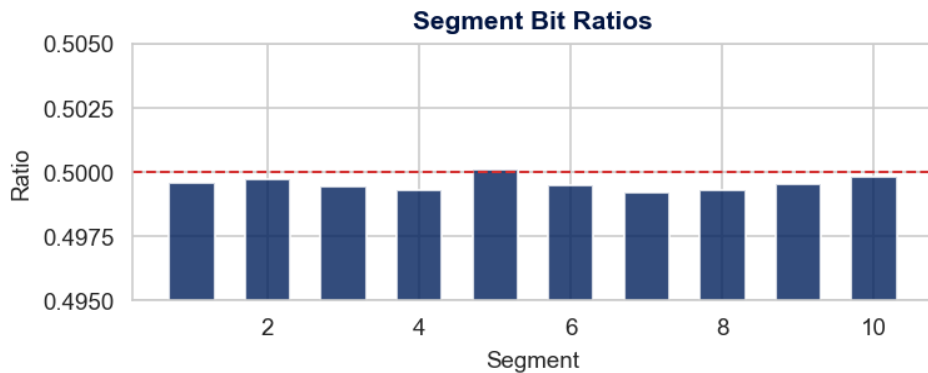


PART 8: Cross-Segment Consistency (Bits)

The bitstream was divided into 10 equal segments and each independently tested.

Seg	1	2	3	4	5	6	7	8	9	10
Ratio	0.4996	0.4997	0.4994	0.4993	0.5001	0.4995	0.4992	0.4993	0.4996	0.4998
p-val	0.372	0.558	0.234	0.161	0.777	0.275	0.097	0.143	0.352	0.706

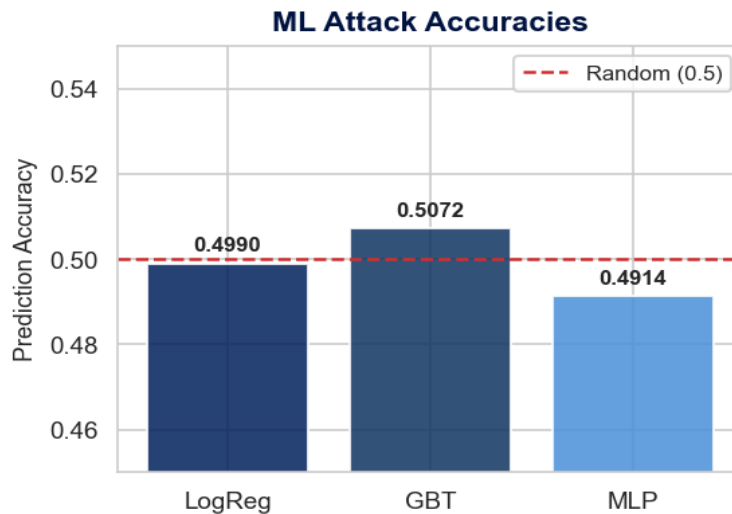
KS test on segment p-values: stat=0.3276, p=0.1864. Cross-half correlation: $r = 0.000046$.



PART 9: Adversarial and Predictability Tests (Bits)

Test	p-value	Result	Detail
Frequency Prediction (w=8)	0.588510	PASS	Acc: 0.5020 (expected ~0.5019)
ML Attack (LogReg, w=16)	0.579260	PASS	Accuracy: 0.4990
ML Attack (GBT, w=16)	0.097329	PASS	Accuracy: 0.5072
ML Attack (MLP, w=16)	0.938571	PASS	Accuracy: 0.4914
Pattern Repetition (w=59)	1.000000	PASS	No repetition detected

These tests attempt to predict the next bit using frequency-based pattern matching and machine learning (Logistic Regression, Gradient Boosted Trees, MLP Neural Network). An accuracy near 50% indicates the output is unpredictable. Pattern repetition checks for repeated subsequences.



Cryptographic Wrapper Validation

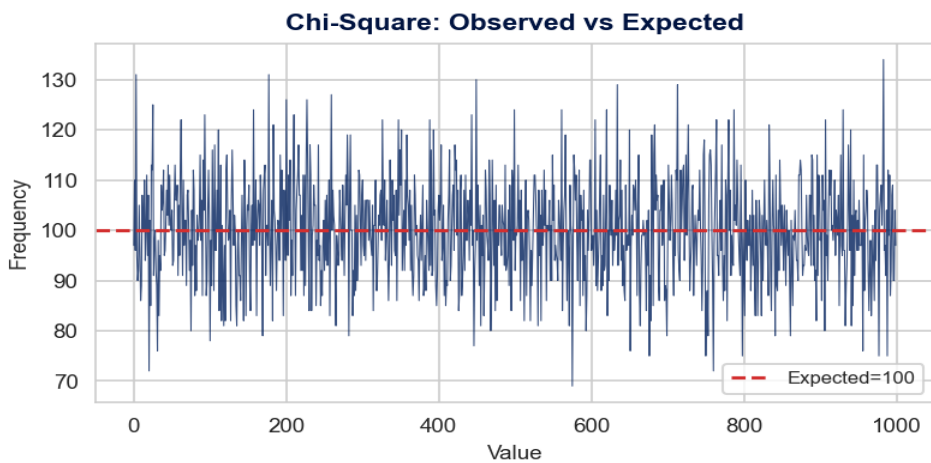
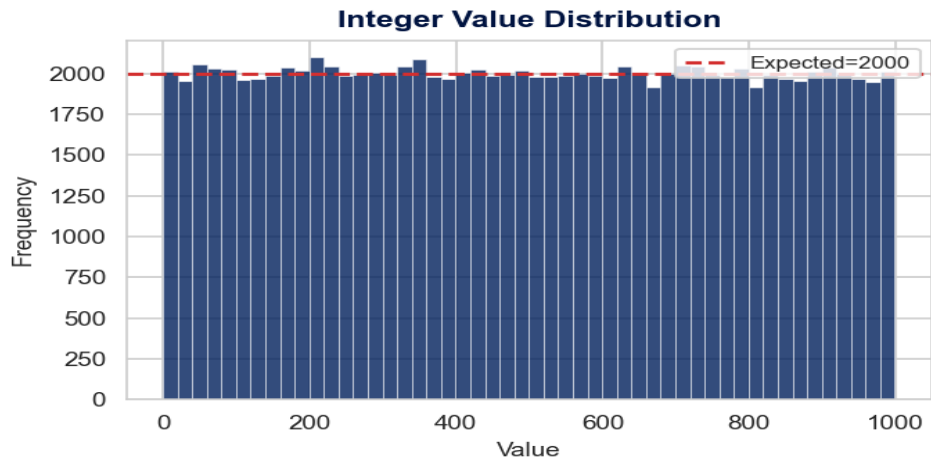
Test	p-value	Result	Detail
SHA-256 CSPRNG Wrapper	1.000000	PASS	Post-hash prediction: 0.5320

The Java Math.random() output is seeded into a SHA-256 based CSPRNG wrapper, and the resulting secure bits are re-tested for predictability. This validates the suitability of Java Math.random() output as entropy source for cryptographic applications.

PART 10: Integer Distribution Tests

Test	p-value	Result	Detail
Chi-Square Uniformity	0.145997	PASS	k=1000, chi-stat=1046.16
Mean (Z-test)	0.161835	PASS	Actual=498.2230, Expected=499.5000
Variance (Chi-sq)	0.860876	PASS	Actual=83267.3962, Expected=83333.2500
Binned Goodness-of-Fit	0.944039	PASS	Chi-sq=34.3590, bins=50
Birthday Spacing	1.000000	PASS	Collisions=4092, lambda=17179869.18
Coupon Collector	0.500000	PASS	Range 1000 too large
Collision Test	0.999851	PASS	Expected=15384.0, Actual=15384.0
Anderson-Darling	0.219754	PASS	A2*=0.4909

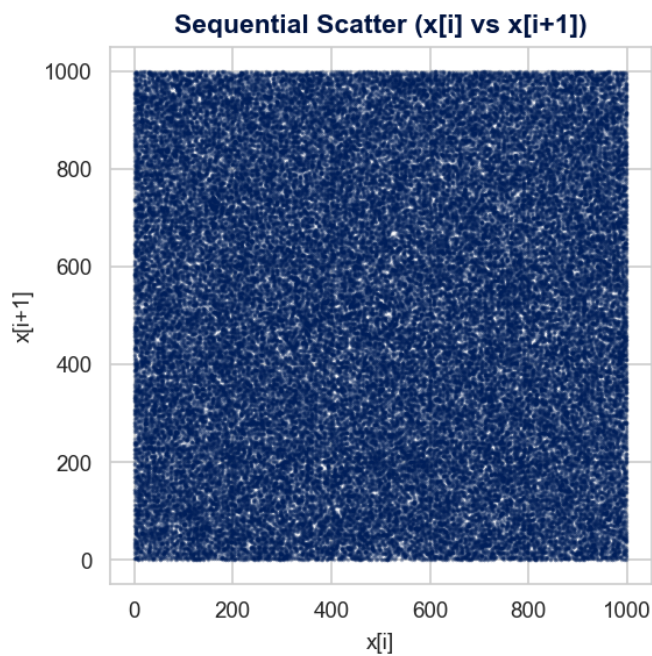
Integer output tested across range [0..999] (1000 values). Tests include Chi-Square uniformity, binned goodness-of-fit, KS test, Birthday Spacing, Coupon Collector, Collision, Anderson-Darling, and moment analysis.

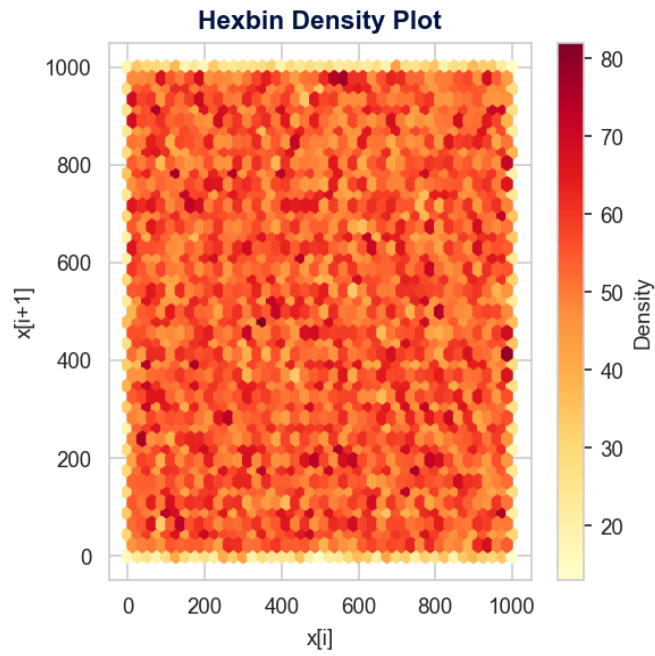


PART 11: Integer Sequence Tests

Test	p-value	Result	Detail
Skewness/Kurtosis	0.660445	PASS	Skew=0.0071, Kurt=-1.2000
Maximum-of-5	0.491337	PASS	KS=0.005883, groups=20000
Runs Up/Down	0.343097	PASS	Runs=66462, Expected=66588.3
Lag-1 Autocorrelation	0.861625	PASS	r=-0.000551
Gap Test (KS)	0.523680	PASS	Mean gap=1035.45, Expected=1000
Permutation (t=5)	0.186477	PASS	120/120 patterns observed
Spearman Rank Correlation	0.860647	PASS	rho=-0.000555
Median Test	0.844479	PASS	Above=49977, Below=49914, Median=497.0

Sequence tests verify that consecutive integers show no patterns, memory, or predictability. Includes runs test, multi-lag autocorrelation, gap test, permutation test, Spearman rank correlation, maximum-of-t, skewness/kurtosis, and median test.



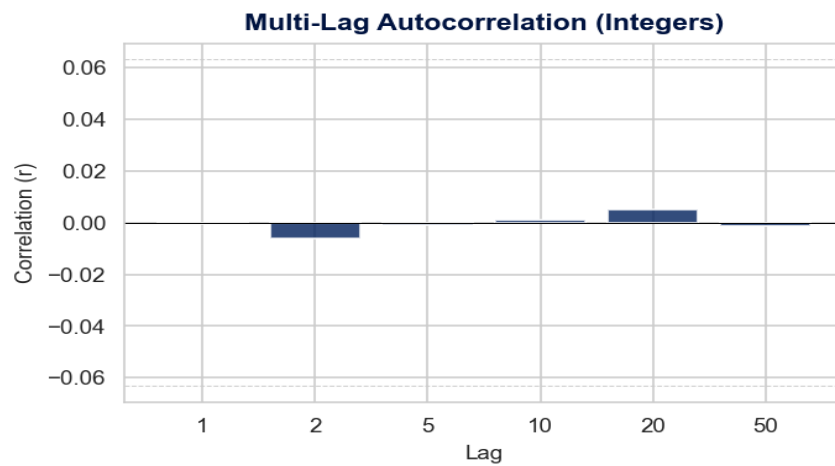


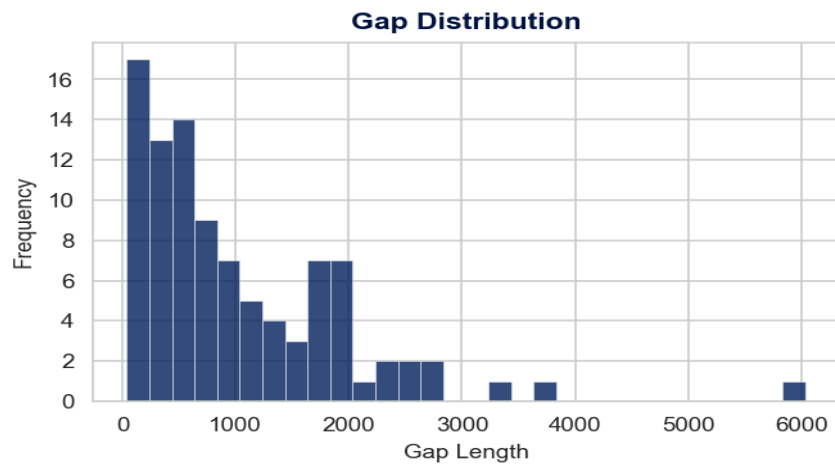
Integer Statistical Moments

Metric	Expected	Actual	Diff	p-value
Mean	499.5000	498.2230	1.2770	0.161835
Variance	83333.2500	83267.3962	65.8538	0.860876

Multi-Lag Autocorrelation (Integers)

Lag	1	2	5	10	20	50
r	-0.0006	-0.0061	-0.0009	+0.0012	+0.0051	-0.0012





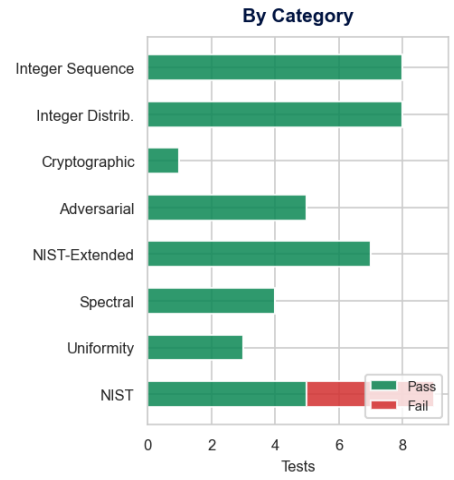
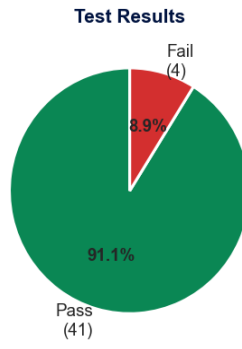
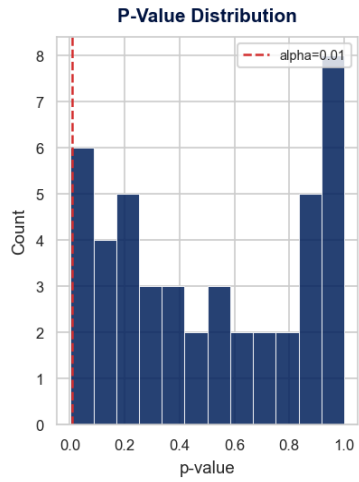
FINAL ASSESSMENT

Category	Tests	Passed	Status
NIST	9	5	FAIL
Uniformity	3	3	PASS
Spectral	4	4	PASS
NIST-Extended	7	7	PASS
Adversarial	5	5	PASS
Cryptographic	1	1	PASS
Integer Distribution	8	8	PASS
Integer Sequence	8	8	PASS
GRAND TOTAL	45	41	4 FAIL

REVIEW NEEDED

Failed tests (4): Frequency (Monobit), Cumulative Sums (Fwd), Cumulative Sums (Rev), Serial (m=2) — delta1

Java Math.random() Validation Dashboard



Complete P-Value Results

Each bar represents one test. Green bars exceed the $\alpha=0.01$ threshold (PASS). Red bars fall below (FAIL).
Numeric p-values shown at bar ends.

Complete Test Results — All P-Values

