

# Java SecureRandom 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: 43/45 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 SecureRandom output.

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

Test	p-value	Result	Detail
Frequency (Monobit)	0.048856	PASS	ones=5,462,507 / zeros=5,455,998 (ratio: 0.500298)
Block Frequency (M=128)	0.110198	PASS	85,300 blocks tested
Runs Test	0.579055	PASS	5,458,334 total runs
Longest Run of Ones	0.427768	PASS	M=10,000 block size
Cumulative Sums (Fwd)	0.088586	PASS	z=6,646
Cumulative Sums (Rev)	0.068020	PASS	z=7,005
Approximate Entropy (m=2)	0.320284	PASS	ApEn=0.693147
Serial (m=2) — delta1	0.123109	PASS	delta1=4.1894
Serial (m=2) — delta2	0.578252	PASS	delta2=0.3091

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

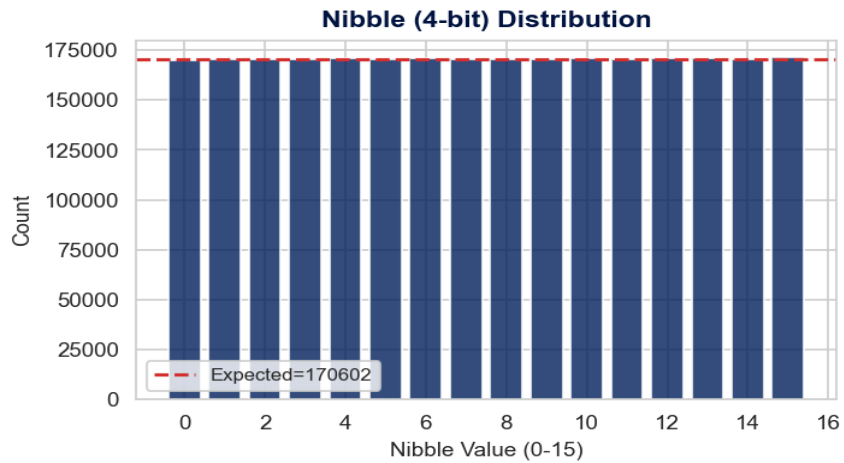
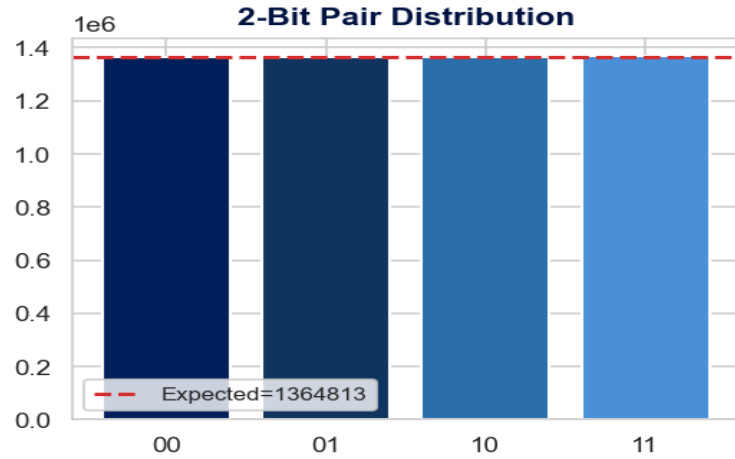
Test	p-value	Result	Detail
Maurer's Universal Statistical	0.160903	PASS	fn=6.1951
Poker Test (m=4)	0.788168	PASS	Chi-sq=10.4851
Random Excursion Variant	0.798999	PASS	Cycles: 987
Binary Matrix Rank	0.849861	PASS	Full=584, M-1=1157, rest=259 (n=2000)
Non-Overlapping Template (m=9)	0.497842	PASS	mu=213.24, blocks=100
Overlapping Template (m=9)	1.000000	PASS	lambda=213.24, blocks=100
Linear Complexity	0.622727	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	0.431626	PASS	256 bins: min=5161, max=5599, exp=5331.3
Nibble-Level Chi-Square	0.788168	PASS	16 bins tested
2-Bit Pair Distribution	0.231106	PASS	00:1,363,338 / 01:1,365,150 / 10:1,364,172 / 11:1,366,592

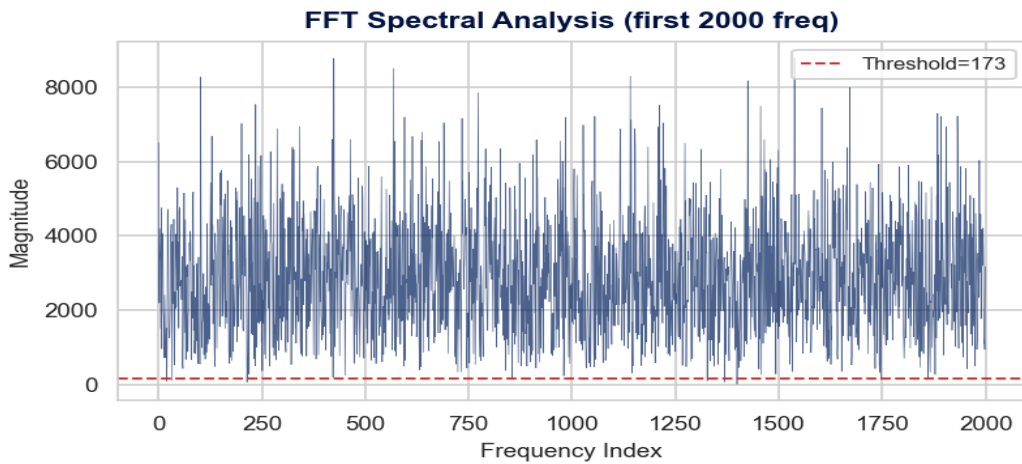
Uniformity tests verify that all possible bit patterns occur with expected frequency at 2-bit, 4-bit (nibble), and 8-bit (byte) granularities.



## PART 4: Spectral and Structural Analysis (Bits)

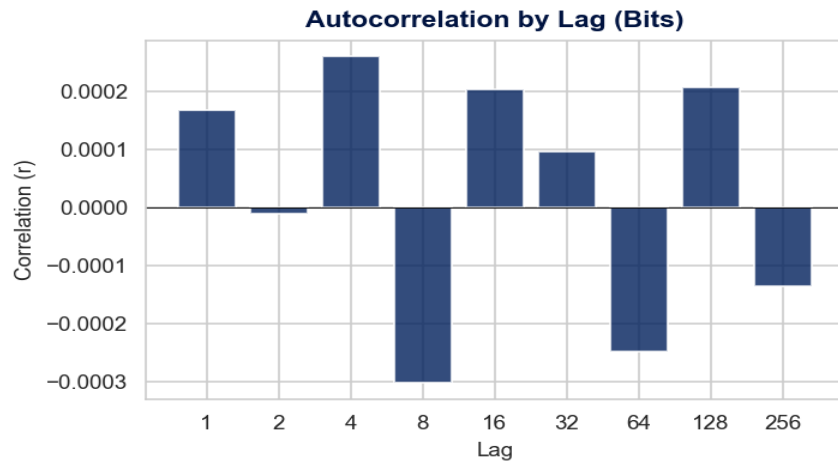
Test	p-value	Result	Detail
Spectral FFT (Periodicity)	0.003836	<b>FAIL</b>	peaks below threshold: 5,187,331/5,459,252
Compression Ratio (zlib)	0.218963	<b>PASS</b>	Ratio=1.000312 (1,365,239/1,364,813)
Binary Derivative (1st order)	0.578045	<b>PASS</b>	ones=5,458,333/10,918,504 (ratio=0.499916)
Turning Point Test	0.499869	<b>PASS</b>	TPs=455171, Expected=454936.0

The Discrete Fourier Transform test checks for periodic components in the bitstream. peaks below threshold: 5,187,331/5,459,252. p-value: 0.003836 — PERIODIC COMPONENTS DETECTED.



### Autocorrelation Profile

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

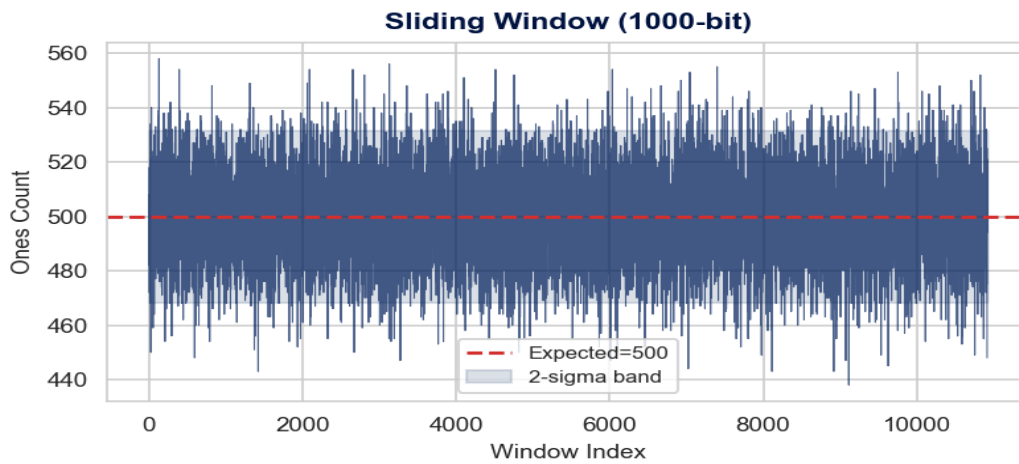
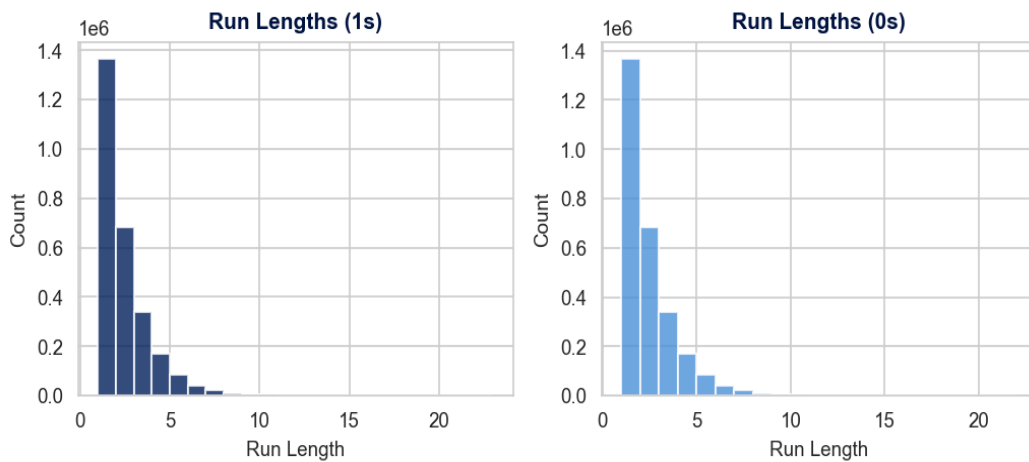


## PART 5: Entropy Analysis (Bits)

Metric	Value	Theoretical Max	Assessment
Shannon Entropy (8-bit)	7.999864	8.000000	99.998% of max
Min-Entropy (8-bit)	7.929318	8.000000	99.12%
Transition Rate	0.499916	0.500000	Near-ideal

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

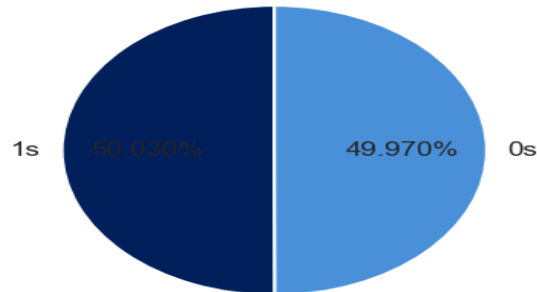
Metric	Ones Runs	Zeros Runs	Expected
Count	2,729,167	2,729,167	~2,729,626
Mean Length	2.0015	1.9991	2.0000
Max Length	22	21	~23



## 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.

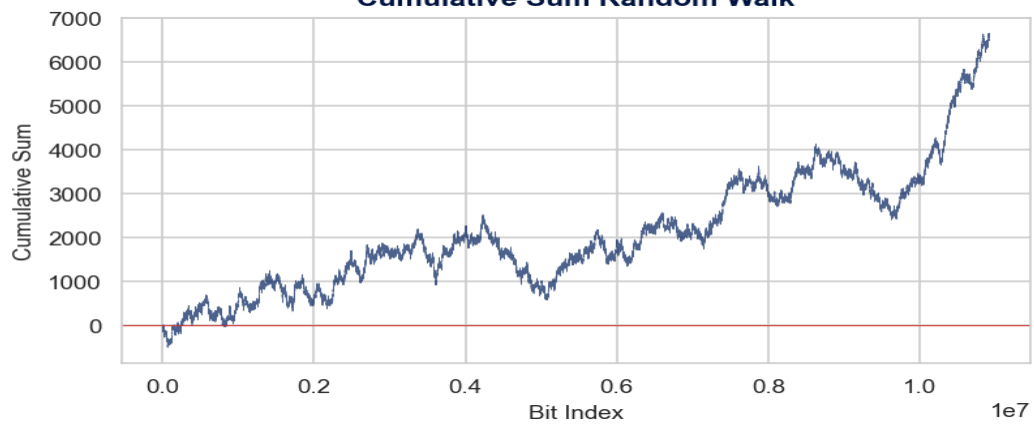
**Bit Balance (0 vs 1)**



**Bit Matrix (100x100)**



**Cumulative Sum Random Walk**

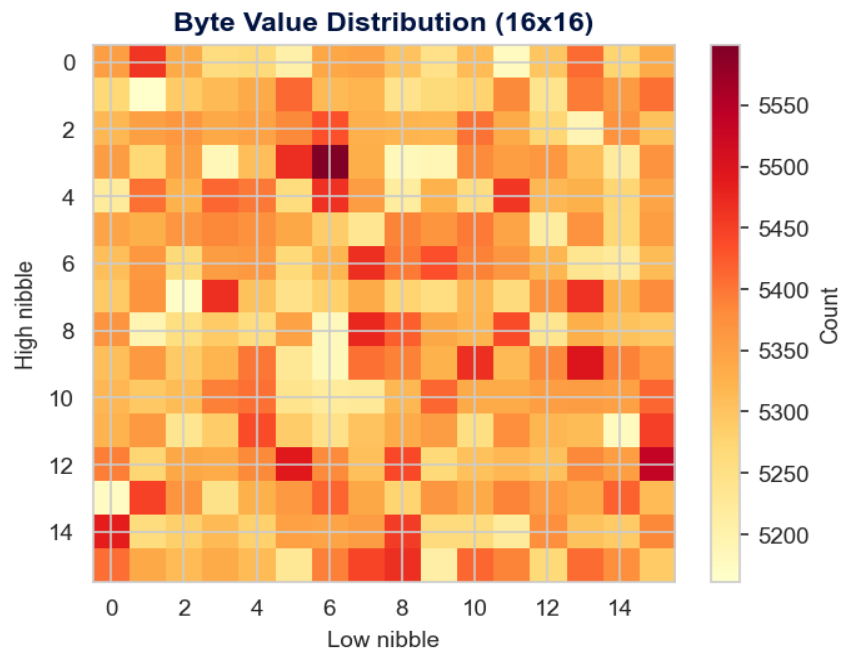
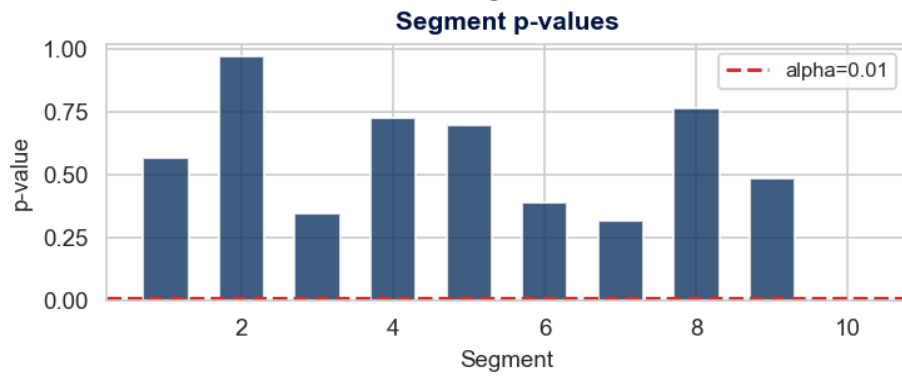
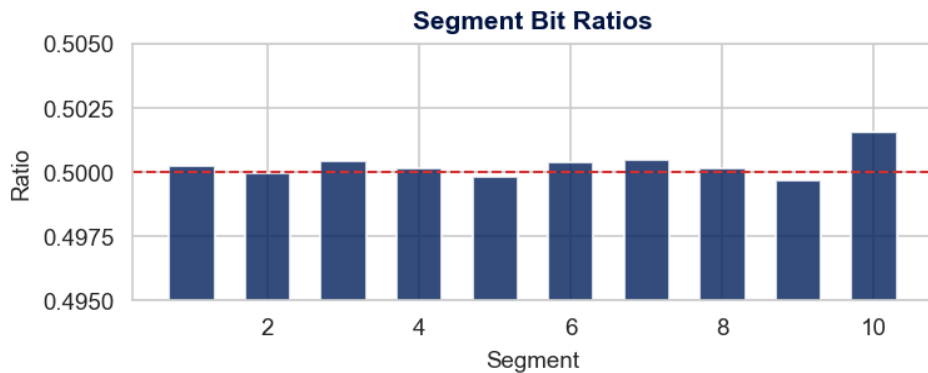


## PART 8: Cross-Segment Consistency (Bits)

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

Seg	1	2	3	4	5	6	7	8	9	10
Ratio	0.5003	0.5000	0.5004	0.5002	0.4998	0.5004	0.5005	0.5001	0.4997	0.5016
p-val	0.566	0.971	0.347	0.726	0.698	0.390	0.320	0.762	0.485	0.001

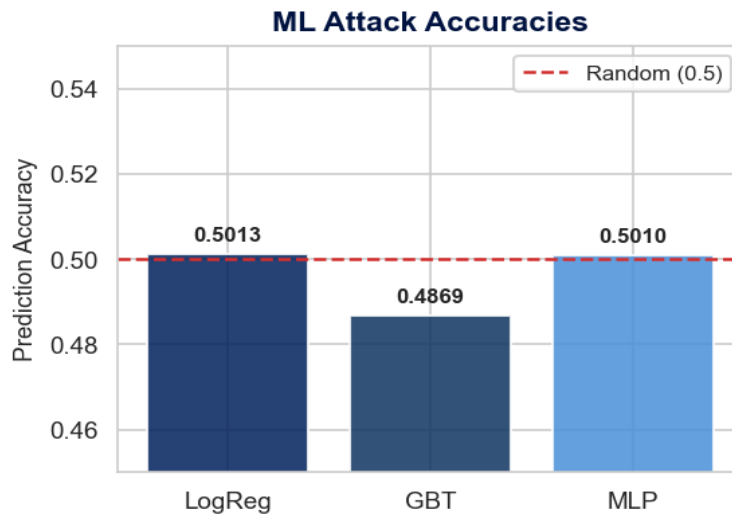
KS test on segment p-values: stat=0.2196, p=0.6447. Cross-half correlation:  $r = -0.000179$ .



## PART 9: Adversarial and Predictability Tests (Bits)

Test	p-value	Result	Detail
Frequency Prediction (w=8)	0.904993	PASS	Acc: 0.5019 (expected ~0.5019)
ML Attack (LogReg, w=16)	0.397432	PASS	Accuracy: 0.5013
ML Attack (GBT, w=16)	0.990559	PASS	Accuracy: 0.4869
ML Attack (MLP, w=16)	0.429014	PASS	Accuracy: 0.5010
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

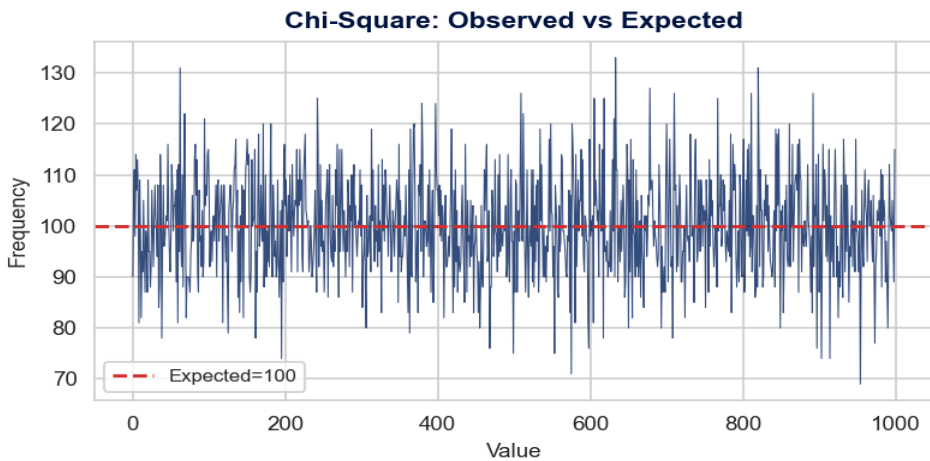
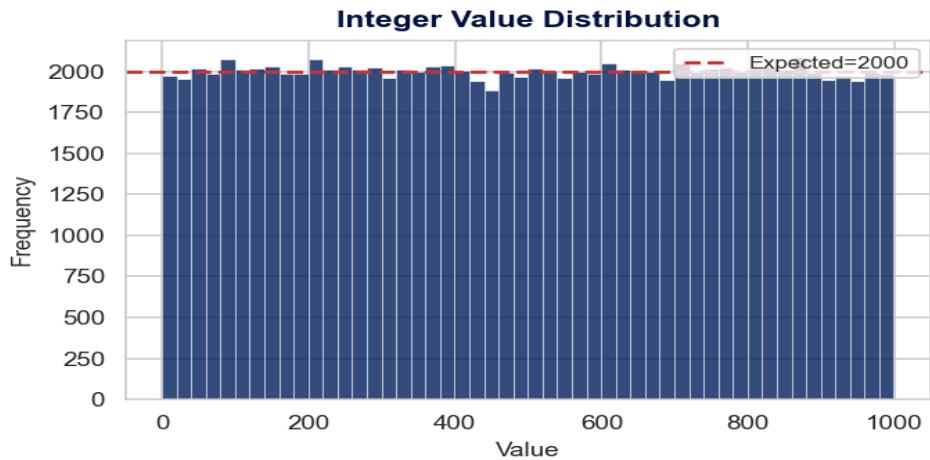
Test	p-value	Result	Detail
SHA-256 CSPRNG Wrapper	1.000000	PASS	Post-hash prediction: 0.5291

The Java SecureRandom 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 SecureRandom output as entropy source for cryptographic applications.

## PART 10: Integer Distribution Tests

Test	p-value	Result	Detail
Chi-Square Uniformity	0.799222	PASS	k=1000, chi-stat=961.32
Mean (Z-test)	0.513985	PASS	Actual=498.9042, Expected=499.5000
Variance (Chi-sq)	0.946617	PASS	Actual=83307.7441, Expected=83333.2500
Binned Goodness-of-Fit	0.959479	PASS	Chi-sq=33.1650, 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	0.000520	FAIL	A2*=1.5590

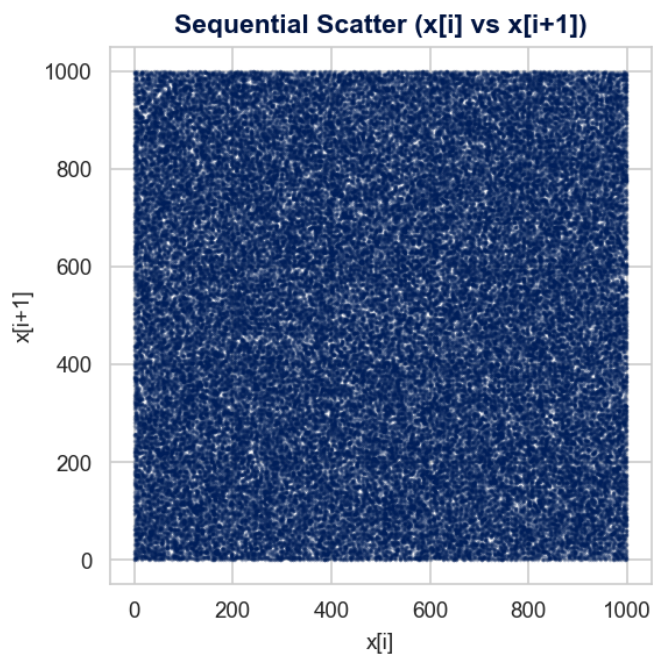
Integer output tested across range [0..999] (1000 values). Tests include Chi-Square uniformity, binned goodness-of-fit, KS test, Birthday Spacing, Coupon Collector, Collision, Anderson-Darling, and moment analysis.

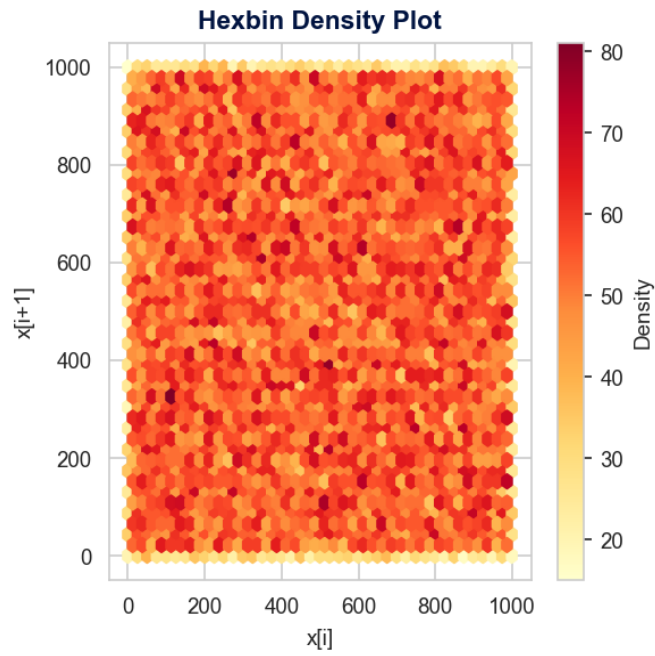


## PART 11: Integer Sequence Tests

Test	p-value	Result	Detail
Skewness/Kurtosis	0.934826	PASS	Skew=0.0017, Kurt=-1.2046
Maximum-of-5	0.300128	PASS	KS=0.006871, groups=20000
Runs Up/Down	0.212016	PASS	Runs=66776, Expected=66609.7
Lag-1 Autocorrelation	0.612490	PASS	r=0.001602
Gap Test (KS)	0.606236	PASS	Mean gap=1111.07, Expected=1000
Permutation (t=5)	0.170469	PASS	120/120 patterns observed
Spearman Rank Correlation	0.613677	PASS	rho=0.001596
Median Test	0.819826	PASS	Above=49999, Below=49926, Median=499.0

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.



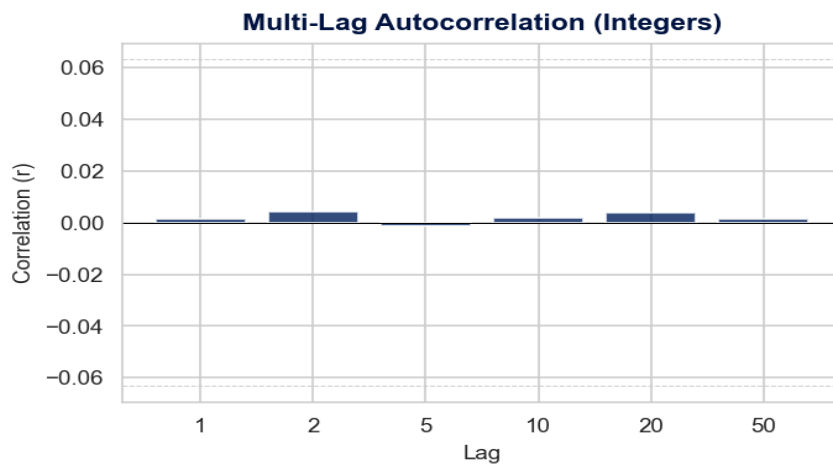


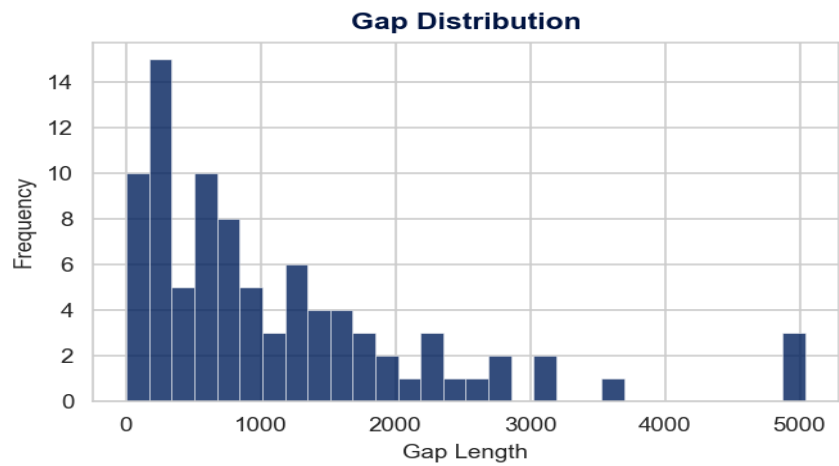
### Integer Statistical Moments

Metric	Expected	Actual	Diff	p-value
Mean	499.5000	498.9042	0.5958	0.513985
Variance	83333.2500	83307.7441	25.5059	0.946617

### Multi-Lag Autocorrelation (Integers)

Lag	1	2	5	10	20	50
r	+0.0016	+0.0042	-0.0014	+0.0020	+0.0041	+0.0015





## FINAL ASSESSMENT

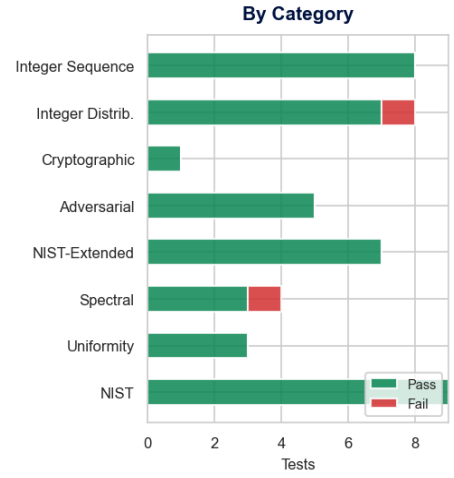
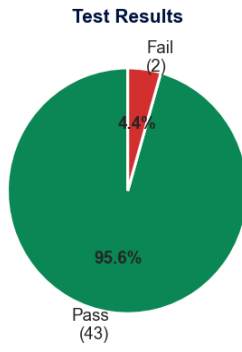
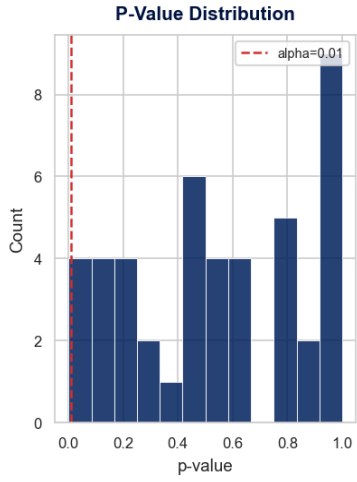
---

Category	Tests	Passed	Status
NIST	9	9	PASS
Uniformity	3	3	PASS
Spectral	4	3	FAIL
NIST-Extended	7	7	PASS
Adversarial	5	5	PASS
Cryptographic	1	1	PASS
Integer Distribution	8	7	FAIL
Integer Sequence	8	8	PASS
<b>GRAND TOTAL</b>	<b>45</b>	<b>43</b>	<b>2 FAIL</b>

## REVIEW NEEDED

**Failed tests (2):** Spectral FFT (Periodicity), Anderson-Darling

# Java SecureRandom 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

