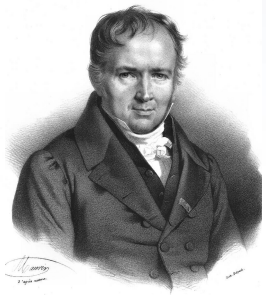
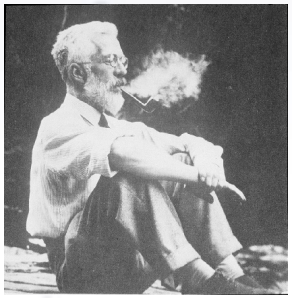
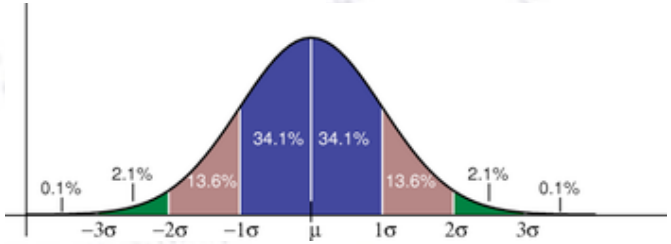
Applied Statistics

Testing random Number




Troels C. Petersen (NBI)

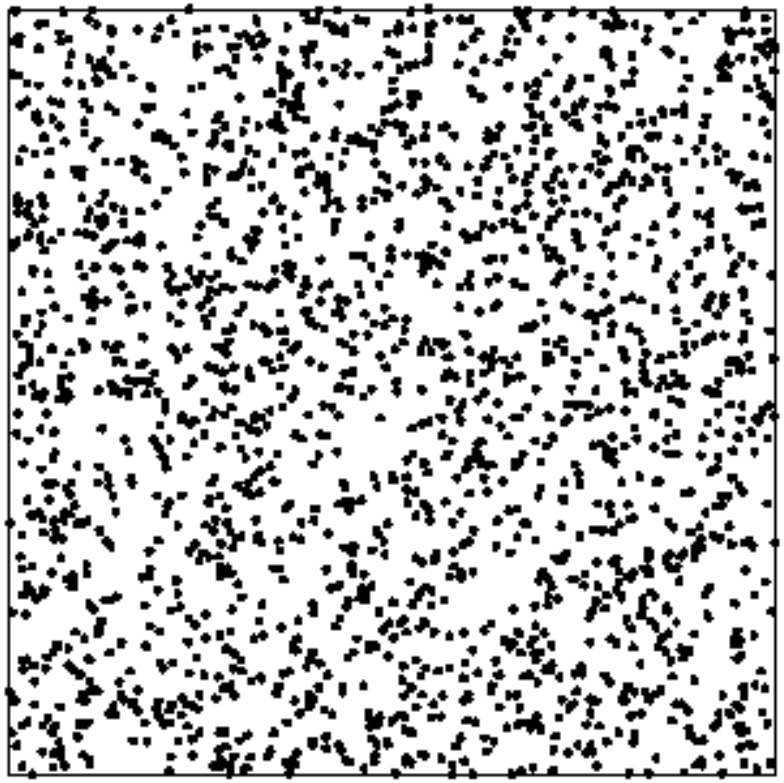


"Statistics is merely a quantisation of common sense"

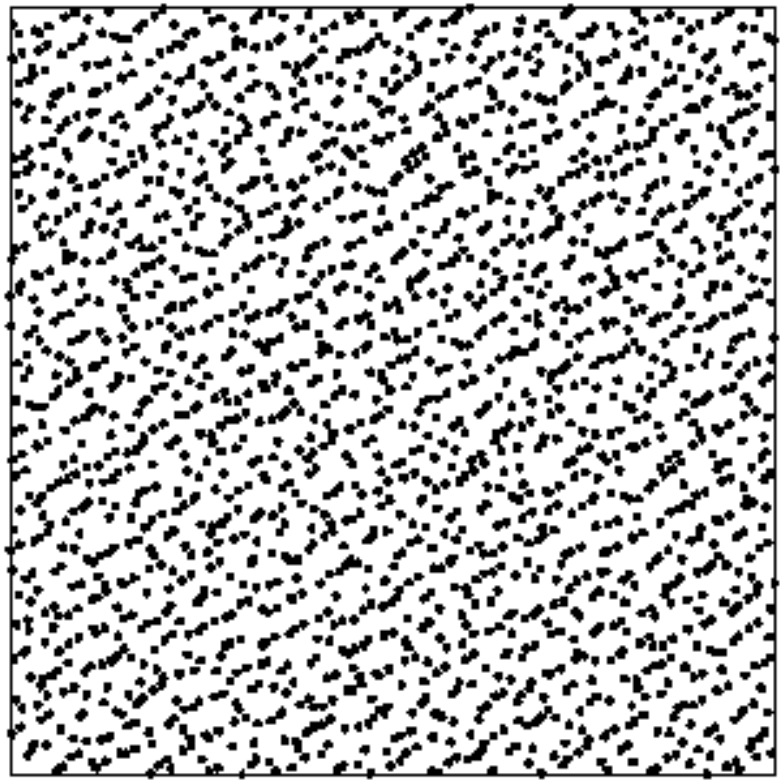
Random numbers

"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." [John Von Neumann]

Random



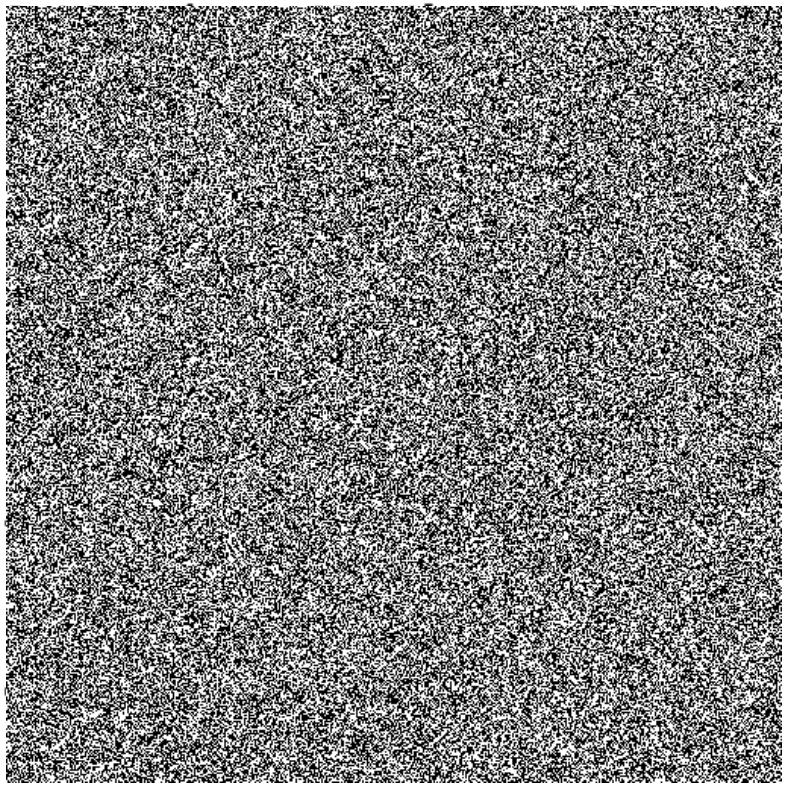
Quasi-Random



Random numbers

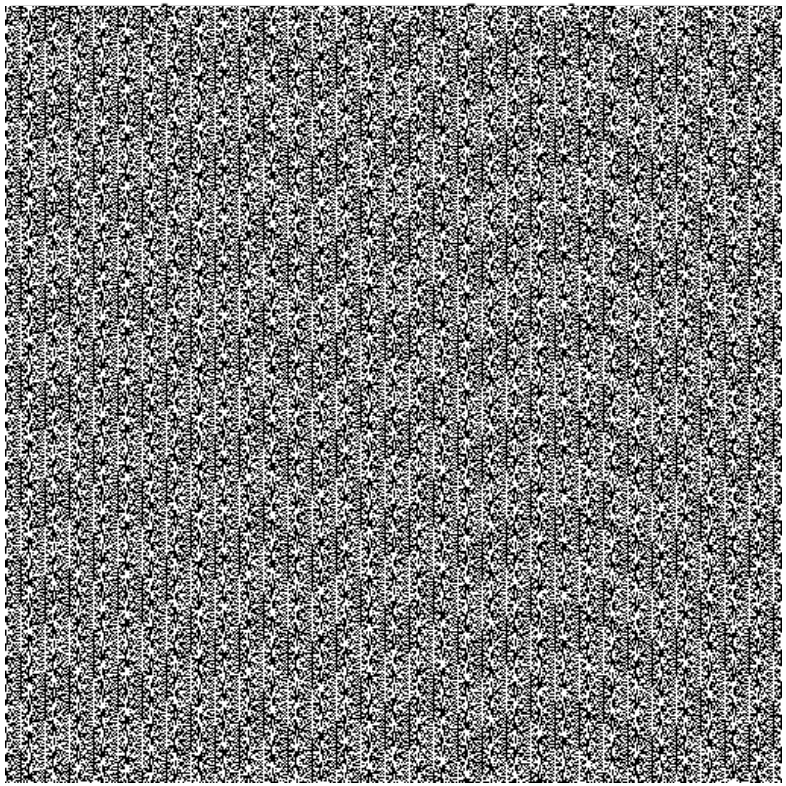
"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." [John Von Neumann]

Random



RANDOM.ORG

Quasi-Random



PHP rand() on Microsoft Windows

Random numbers

"Most studies find that human subjects have some degree of non randomness when attempting to produce a random sequence of e.g. digits."

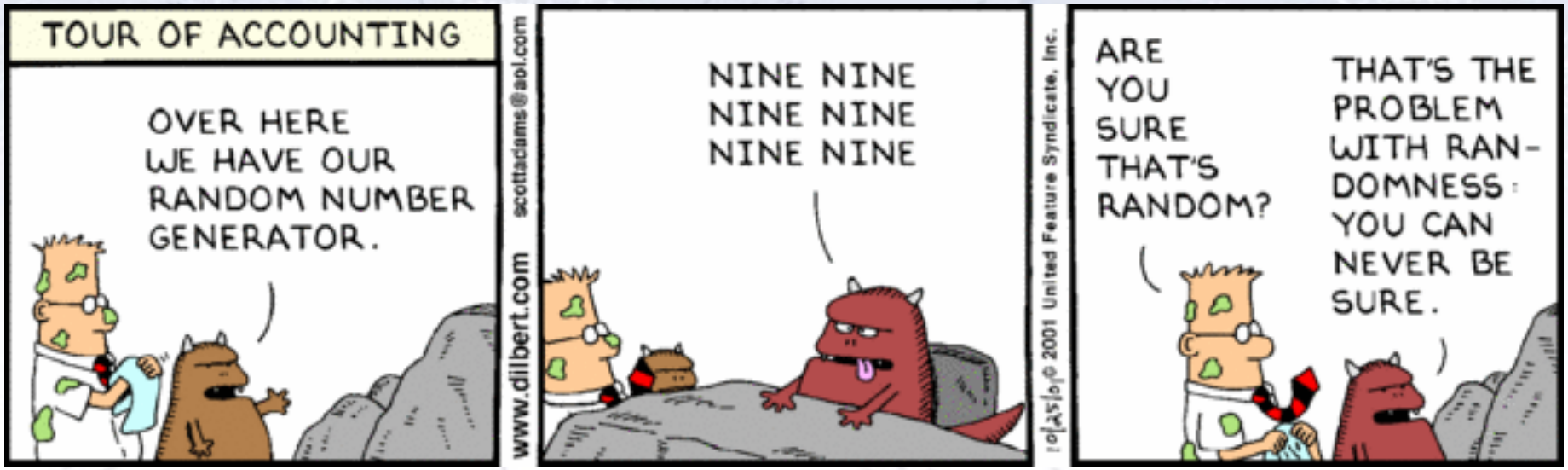
[Wikipedia, On random numbers produced by humans]

Random numbers

"Most studies find that human subjects have some degree of non randomness when attempting to produce a random sequence of e.g. digits."

[Wikipedia, On random numbers produced by humans]

Testing random numbers



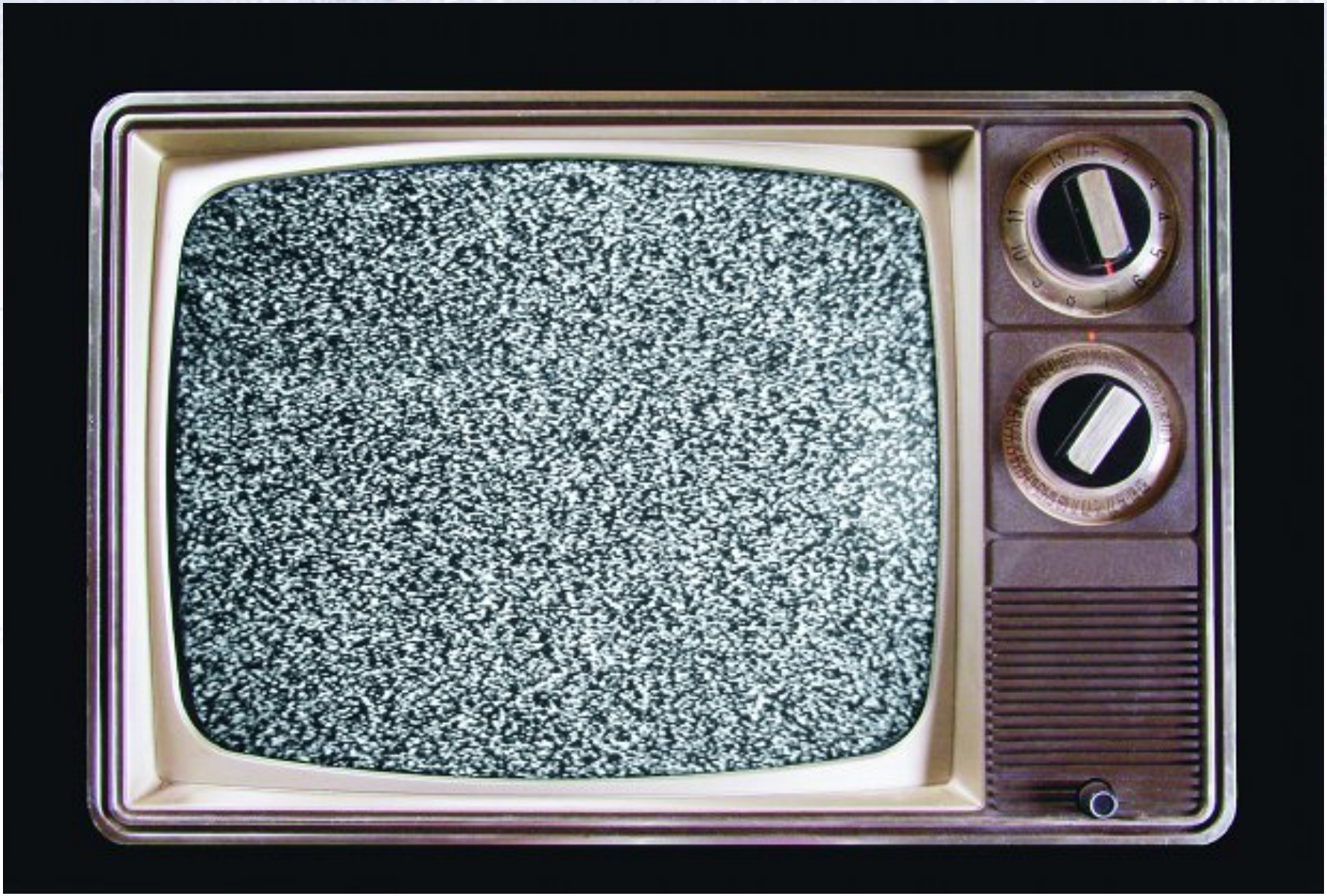
In contrast to popular believe, there are ways of testing random numbers. But it is not easy! A recommended list (Louis Foley, Random.org, 2001) is:

- A chi-square test
- A test of runs above and below the median
- A reverse arrangements test
- An overlapping sums test
- A binary rank test for 32×32 matrices

More tests for randomness

NIST Statistical Test Suite		
Test	**Defect Detected**	**Property**
Frequency (monobit)	Too many zeroes or ones	Equally likely (global)
Frequency (block)	Too many zeroes or ones	Equally likely (local)
Runs test	Oscillation of zeroes and ones too fast or too slow	Sequential dependence (locally)
Longest run of ones in a block	Oscillation of zeroes and ones too fast or too slow	Sequential dependence (globally)
Binary matrix rank	Deviation from expected rank distribution	Linear dependence
Discrete fourier transform (spectral)	Repetitive patterns	Periodic dependence
Non-overlapping template matching	Irregular occurences of a pre-specified template	Periodic dependence and equally likely
Overlapping template matching	Irregular occurences of a pre-specified template	Periodic dependence and equally likely
Maurer's universal statistical	Sequence is compressible	Dependence and equally likely
Linear complexity	Linear feedback shift register (LFSR) too short	Dependence
Serial	Non-uniformity in the joint distribution for m-length sequences	Equally likely
Approximate entropy	Non-uniformity in the joint distribution for m-length sequences	Equally likely
Cumulative sums (cusum)	Too many zeroes or ones at either an early or late stage in the sequence	Sequential dependence
Random excursions	Deviation from the distribution of the number of visits of a random walk to a certain state	Sequential dependence
Random excursions variants	Deviation from the distribution of the number of visits (across many random walks) to a certain state	Sequential dependence

What to use for random seed?



NSA and Dual_EC_DRBG

Cryptography is based on random numbers. One of the four accepted random number generators (RNG) used for cryptography was Dual_EC_DRBG.

Several academics point out, that Dual_EC_DRBG was a very poor and possibly “back-doored” pseudorandom number generator! Nevertheless, one of the large cryptography companies in the US, RSA Security, continued using it.

In 2013, Edward Snowden published papers that showed, that the NSA had put a backdoor in the Dual_EC_DRBG algorithm! The lack of perfect randomness allowed NSA to break the encryption.

Outputs of multiple independent RNGs can be combined (for example, using a bit-wise XOR operation) to provide a combined RNG at least as good as the best RNG used. This is referred to as software whitening.