4ª EDIÇÃO Science & Business Connection by colmeia

ANÁLISE DA QUALIDADE DE NÚMEROS ALEATÓRIOS UTILIZANDO O NIST STATISTICAL TEST SUITE

Izabella Albuquerque P. M. de Souza[1]; Sergio Tavares[2]; Marcello M. Correia[3];

Alessandro A. R. Athie[4]; Jorge O. Echeimberg[5]

[1] Centro Universitário Senac - São Paulo (izabella.apmsouza@senacsp.edu.br).
[2] Centro Universitário Senac - São Paulo (sergio.tavares@spsenac.edu.br).
[3] Centro Universitário Senac - São Paulo (marcello.mcorreia@spsenac.edu.br).
[4]Centro Universitário Senac - São Paulo (alessandro.arathic@spsenac.edu.br).
[5]Centro Universitário Senac - São Paulo (jorge.oecheimberg@spsenac.edu.br).

Resumo: Este artigo apresenta uma análise aprofundada sobre a qualidade da aleatoriedade de números gerados por três fontes amplamente utilizadas em pesquisas científicas e aplicações computacionais: Random.org (site online de geração de números aleatórios verdadeiros), Estatística Fácil (site online de geração de números aleatórios) e Python (algoritmo Mersenne Twister). A investigação se fundamenta na relevância crescente da aleatoriedade para áreas como criptografia, simulações, modelagem estatística, segurança da informação e inteligência artificial, campos que dependem fortemente da imparcialidade, independência e imprevisibilidade de sequências numéricas. Assim, o estudo busca não apenas avaliar o desempenho individual de cada fonte, mas também demonstrar como metodologias híbridas e grandes volumes de dados podem oferecer diagnósticos mais robustos e confiáveis. O objetivo central da pesquisa é comparar, de forma sistemática, a consistência estatística dessas fontes por meio da aplicação combinada da suíte NIST Statistical Test Suite e de métricas quantitativas complementares, como entropia de Shannon, autocorrelação, compressibilidade e distância de Hamming. Para isso, foram coletados 1 milhão de números inteiros por fonte, convertidos em sequências de 32 milhões de bits (números inteiros uniformes serializados em 32 bits por palavra, sem truncamento), volume adequado para testes rigorosos, como recomendado pelo NIST SP 800-22 e pela literatura contemporânea. O método resulta em uma avaliação multidimensional capaz de identificar nuances e padrões que testes isolados não revelariam. Os resultados obtidos evidenciam diferenças significativas entre os geradores. Random.org apresentou o melhor desempenho global (score 0,742), com elevadas taxas de aprovação nos testes NIST, alta entropia e mínima autocorrelação, indicando robustez para aplicações criptográficas. O Python (Mersenne Twister) também demonstrou desempenho estável e altamente consistente (score 0,717), consolidando sua reputação como PRNG confiável para simulações e pesquisas. Estatística Fácil obteve uma performance intermediária (score 0,657), compatível com cenários de menor criticidade, mas apresentando padrões que limitam seu uso em contextos sensíveis. A partir da integração de todas as métricas, foi desenvolvido um score composto normalizado que confirmou a seguinte hierarquia de qualidade: Random.org, Python e Estatística Fácil. Esses achados reforçam a importância da escolha criteriosa de geradores conforme o nível de rigor exigido. Conclui-se que Random.org e Python são adequados para aplicações críticas; Estatística Fácil deve ser reservado a tarefas menos sensíveis.

Palavras-chave: Aleatoriedade; Criptografia; NIST; Entropia; Segurança da Informação.

4ª EDIÇÃO Science & Business Connection by colmeia

ANALYSIS OF RANDOM NUMBER QUALITY USING THE NIST STATISTICAL TEST SUITE

Izabella Albuquerque P. M. de Souza[1]; Sergio Tavares[2]; Marcello M. Correia[3];

Alessandro A. R. Athie[4]; Jorge O. Echeimberg[5]

[1] Centro Universitário Senac - São Paulo (izabella.apmsouza@senacsp.edu.br).
[2] Centro Universitário Senac - São Paulo (sergio.tavares@spsenac.edu.br).
[3] Centro Universitário Senac - São Paulo (marcello.mcorreia@spsenac.edu.br).
[4]Centro Universitário Senac - São Paulo (alessandro.arathic@spsenac.edu.br).
[5]Centro Universitário Senac - São Paulo (jorge.oecheimberg@spsenac.edu.br).

Abstract: This article presents an in-depth analysis of the quality of randomness in numbers generated by three sources widely used in scientific research and computational applications: Random.org (an online true random number generator), Estatística Fácil (an online random number generator), and Python (the Mersenne Twister algorithm). The investigation is grounded in the growing relevance of randomness to fields such as cryptography, simulations, statistical modeling, information security, and artificial intelligence, all of which depend heavily on the impartiality, independence, and unpredictability of numerical sequences. Thus, the study seeks not only to evaluate the individual performance of each source, but also to demonstrate how hybrid methodologies and large data volumes can provide more robust and reliable diagnostics. The central objective of the research is to systematically compare the statistical consistency of these sources through the combined application of the NIST Statistical Test Suite and complementary quantitative metrics such as Shannon entropy, autocorrelation, compressibility, and Hamming distance. To this end, 1 million integers were collected from each source and converted into 32-million-bit sequences (uniform integers serialized into 32-bit words, without truncation), a volume suitable for rigorous testing, as recommended by NIST SP 800-22 and the contemporary literature. The method results in a multidimensional evaluation capable of identifying nuances and patterns that isolated tests would not reveal. The results obtained highlight significant differences among the generators. Random.org showed the best overall performance (score 0.742), with high pass rates in the NIST tests, high entropy, and minimal autocorrelation, indicating robustness for cryptographic applications. Python (Mersenne Twister) also demonstrated stable and highly consistent performance (score 0.717), consolidating its reputation as a reliable PRNG for simulations and research. Estatística Fácil achieved intermediate performance (score 0.657), compatible with less critical scenarios, but showing patterns that limit its use in sensitive contexts. From the integration of all metrics, a normalized composite score was developed that confirmed the following quality hierarchy: Random.org, Python, and Estatística Fácil. These findings reinforce the importance of carefully selecting generators according to the level of rigor required. It is concluded that Random.org and Python are suitable for critical applications, whereas Estatística Fácil should be reserved for less sensitive tasks.

Keywords: Randomness; Cryptography; NIST; Entropy; Information Security.