TESTES DE ALEATORIEDADE DO NIST

Orientador: Faleiros, A. C.; Aluno:Alves, E. P. S.

Nos dias atuais diversos processos importantes podem ser executados por meio de acessos remotos ou via internet, um fator muito importante para esses tipos de procedimento é a segurança. Para assegurar a integridade dos dados utiliza-se a criptografia, que por sua vez, é dependente de números aleatórios que garante maior confiabilidade estatística para o processo.
Existem diversas técnicas de se criar um gerador de números aleatórios e para garantir sua confiabilidade o NIST − Instituto Nacional de Padrões e Tecnologia − criou alguns padrões de testes baseados em processos estatísticos.
O objetivo principal dessa pesquisa é analisar algumas técnicas atribuídas a alguns testes e com a implementação de um gerador e testes, em linguagem JAVA, verificar a eficiência do gerador em determinadas circunstâncias.
A metodologia aplicada ao projeto foi o estudo prévio de alguns tipos de geradores de números aleatórios, seus requisitos mínimos para um bom desempenho assim como a maneira correta de implementá-los, desde parametros iniciais à semente para geração. Em seguida o estudo base de alguns testes do NIST, na implementação foram necessárias bibliotecas especiais para calcular alguns testes estatísticos, utilizamos o SSJ - Simulation Stochastic for Java - da Universidade de Montreal. Dos testes para analise de eficiência de geradores, foram implementados dois, o de freqüência (monobit) e o de bloco de freqüência, e um gerador de números aleatórios do tipo Blum Blum Shub. E em seguida o gerador de números aleatórios foi testado em ambos os testes se utilizando de parametros iniciais padrões exigido pelo gerador e novamente testados utilizando outros parametros que não teriam resultados satisfatórios diante daquele gerador.
O resultado obtido entrou de acordo ao esperado e estudado na bibliografia sobre geradores de números aleatórios, sendo de inicio apenas testado o gerador com os parametros confiáveis no gerador foram alteradas suas sementes 30 vezes e gerados por vez 100000 números, a média obtida foi de 49.659 (zero) e 50.341(um).
A segunda etapa ainda utilizando parametros confiáveis, foram alteradas as sementes randomicamente e foram aplicadas 1000 sementes randômicas em seis diferentes parametros e nos testes os que não passaram foram aproximadamente 6% no primeiro e 8% no segundo. Utilizando parametros divergentes aos indicados, como números não primos entre si ou com resíduo quadrático diferente de zero, esses valores subiram para 25% no primeiro e 36% no segundo.
A partir dos resultados podemos concluir que o estudo desses testes e geradores são de extrema importância, ao passo que, ao aplicar um gerador bem estudado e testado em criptografia, por exemplo, pode-se minimizar significativamente a vulnerabilidade dos dados.

Testes de aleatoriedade, NIST, criptografia, geradores pesudoaleatórios.