PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ
Escola Politécnica

Curso: Ciência da Computação
Disciplina: Métodos Quantitativos

Atividade A16 –Geração de Variáveis Aleatórias

**TAREFA INDIVIDUAL** – **TDE1** – Parte 2.

Nome: Gabriel Augusto Martins de Araujo

Faça uma pesquisa sobre o tema Geração de Variáveis Aleatórias e responda às seguintes questões:

1. Apresente duas situações que usam geradores de números aleatórios.
    a Jogos online, especialmente aqueles que apresentam apostas de algum tipo, como loot boxes usam geradores de números aleatórios para determinar os resultados dessas apostas.
    b Criptografia, na hora de gerar valores criptografados é importante o uso de geradores de números aleatórios para evitar previsibilidade e padrões de aparecerem em senhas e chaves de acesso e tornar esses elementos mais fáceis de se descobrir.
2. Escolha um método da literatura e explique como se pode gerar números aleatórios.
    a TRNG (*True Random Number Generador*) usam eventos reais para gerar o número, esses eventos são em sua maioria eventos físicos, como a medição de radiação, ruído, ou até movimento de materiais flutuantes em lâmpadas de lava, como esses elementos não estão sobre controle de um indivíduo ou fórmula matemática – pelo menos uma que não podemos prever – isso resulta em valores verdadeiramente aleatórios.
3. Como se pode avaliar a qualidade de uma sequência de números aleatórios gerados?
    a É preciso verificar a uniformidade, previsibilidade e tempo até repetição do gerador, isso é, se os números estão distribuídos dentro do intervalo de geração, se é possível usar um dos números para prever o número seguinte e se o período que demora para os números se repetirem é longo o suficiente.
4. Descreva como funciona o gerador de números aleatórios Mersenne Twister.
    a O gerador Mersenne Twister é um gerador pseudoaleatório que utiliza uma *seed* para gerar um vetor de número, onde o intervalo dos valores é $[0,2^w-1]$, com w sendo a quantidade de bits na *seed*, após o vetor original ser usado um novo é gerado, usando *twist* para gerar números diferentes, twist é um sistema que basicamente pega bit mais e menos significativos e os mistura e dependendo da paridade do resultado ele aplica o XOR com um valor especifico.s