**Segurança da Informação CC8130**

**Validação de chaves aleatórias**

**The Monobit Test**

Neste teste, conta-se a quantidade de 1s que estão nos 20.000 bits. Esta quantidade será chamada de X.

O teste é verdadeiro se 9.654 < X < 10.346.

**The Poker Test**

Neste teste, divide-se os 20.000 bits em 5.000 segmentos contínuos de 4 bits cada um. Então, deve-se armazenar a quantidade de ocorrências de cada uma das combinações dos 16 possíveis valores de 4 bits. As 16 combinações são: ['0000', '0001', '0010', '0011', '0100', '0101', '0110', '0111', '1000', '1001', '1010', '1011', '1100', '1101', '1110', '1111']

Determine f(i) como sendo o número de cada valor de 4 bits i em que 0 ≤ i ≤ 15.

Então, com a seguinte equação X é determinado.

X = (16/5000) \* ( - 5000

O teste é aprovado se 1.03 < X < 57.4

**The Run Test**

Neste teste de verifica-se sequência máxima de bits consecutivos de 1s ou 0s da amostra de 20.000 bits. As incidências de execução para 0 e 1 que tiverem comprimento maior ou igual a 1, são contabilizadas e armazenadas.

O teste é aprovado se o número de execuções cujo comprimento é de 1 a 6 estiverem dentro dos intervalos correspondentes abaixo. Isto vale para 0 e 1, ou seja, todas as 12 contagens devem estar no intervalo especificado. Neste teste, todo comprimento maior que 6 será truncado com tamanho 6.

|  |  |
| --- | --- |
| **Comprimento** | **Intervalo** |
| 1 | 2.267 – 2.733 |
| 2 | 1.079 – 1.421 |
| 3 | 502 - 748 |
| 4 | 223 - 402 |
| 5 | 90 - 223 |
| 6+ | 90 - 223 |

**The Long Run Test**

Neste teste, verifica-se a existência de sequências de bits cujo comprimento seja maior que 34.

Este teste é aprovado, se não houver tais sequências na amostra de 20.000 bits.

**Resultados:**

Para a execução dos testes, foi utilizado um documento txt, com 20 chaves, cada uma com tamanho de 20.000 bits.

A tabela a seguir representa as chaves e em quais testes elas passaram.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CHAVE** | **THE MONOBIT TESTE** | **THE POKER TEST** | **THE LONG RUN TEST** | **THE RUN TESTE** |
| **1** | Não | Não | Sim | Sim |
| **2** | Não | Não | Sim | Sim |
| **3** | Não | Não | Sim | Sim |
| **4** | Não | Não | Sim | Não |
| **5** | Não | Não | Sim | Não |
| **6** | Não | Não | Sim | Não |
| **7** | Não | Não | Sim | Sim |
| **8** | Não | Não | Sim | Sim |
| **9** | Não | Não | Sim | Sim |
| **10** | Não | Não | Sim | Não |
| **11** | Sim | Sim | Sim | Não |
| **12** | Sim | Sim | Sim | Sim |
| **13** | Sim | Sim | Sim | Sim |
| **14** | Sim | Sim | Sim | Não |
| **15** | Sim | Sim | Sim | Não |
| **16** | Sim | Sim | Sim | Não |
| **17** | Sim | Sim | Sim | Não |
| **18** | Sim | Sim | Sim | Sim |
| **19** | Sim | Sim | Sim | Sim |
| **20** | Sim | Sim | Sim | Não |

Link para o código: <https://github.com/thyagomelo02/Chaves-Aleat-rias>