UFC - Quixadá
QXD0170 – Criptografia - 2017.2 - Prof. Cristiano

Trabalho – Geração de números aleatórios

Descrição

1) Implementar um gerador de números aleatórios com base em algum processo/evento a ser utilizado como fonte de entropia, à escolha do aluno.

2) Realizar algum teste de aleatoriedade descrito pelo NIST SP 800-22.

- Devem ser testados dois grupos de amostras:
a) Amostra com números gerados diretamente pelo processo escolhido;
b) Amostra com números gerados por alguma PRF, sendo o processo escolhido utilizado apenas para a geração da semente.

- O documento com a descrição dos testes encontra-se no link:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf

- Conforme acordado, os testes foram atribuídos da seguinte forma:

Aluno	**Teste**
Enoque Alves	01 – Frequency (Monobit) Test
Fernando César	07 – Non-overlapping Template Matching Test
Francisco Leonardo	03 – Runs Test
João Vitor	02 – Frequency Test within a Block
Joaquim da Silva	04 – Test for the Longest Run of Ones in a Block
Pedro Henrique	11 – Serial Test
Pedro Olímpio	12 – Approximate Entropy Test
Raul de Araújo	05 – Binary Matrix Rank Test
Robert de Almeida	08 – Overlapping Template Matching Test
Tharsis Salathiel	09 – Maurer's "Universal Statistical" Test
Vinícius Teixeira	10 – Linear Complexity Test
Wallinson Deives	06 – Discrete Fourier Transform (Spectral) Test

3) Escrever um breve relatório sobre o projeto, contendo uma descrição do processo no qual o gerador se baseou. O relatório deve incluir um gráfico de distribuição das amostras, incluindo as medidas estatísticas necessárias para o teste de aleatoriedade.

4) Apresentação em sala (máx. 5 minutos) do projeto e dos resultados.

5) Data limite para entrega via SIPPA e apresentação em sala no dia 15/09/2017.