

TP2 ISL

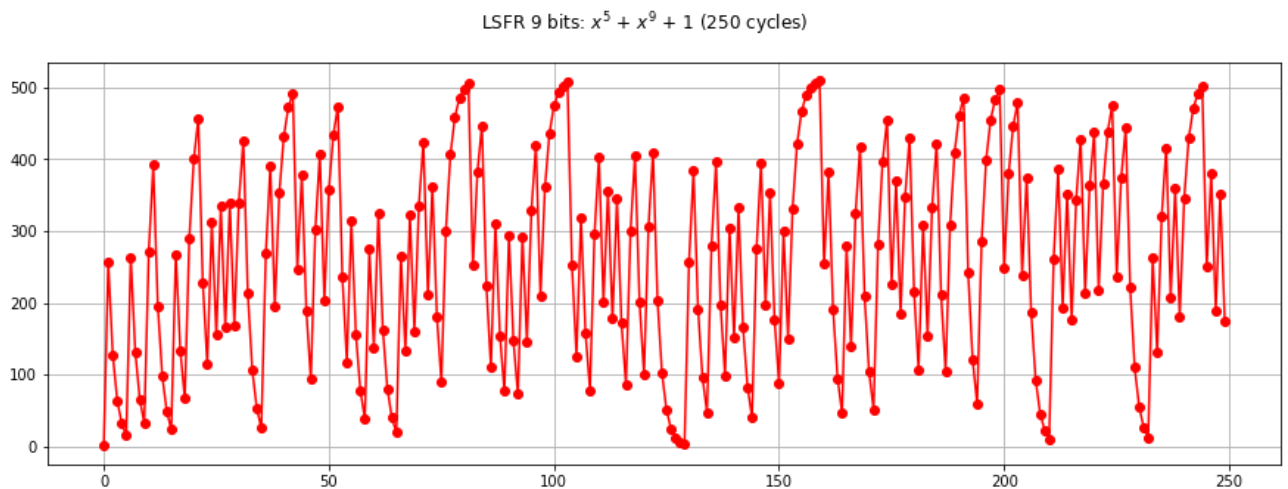
Aluno: Henrique Daniel de Sousa

Matrícula: 2021031912

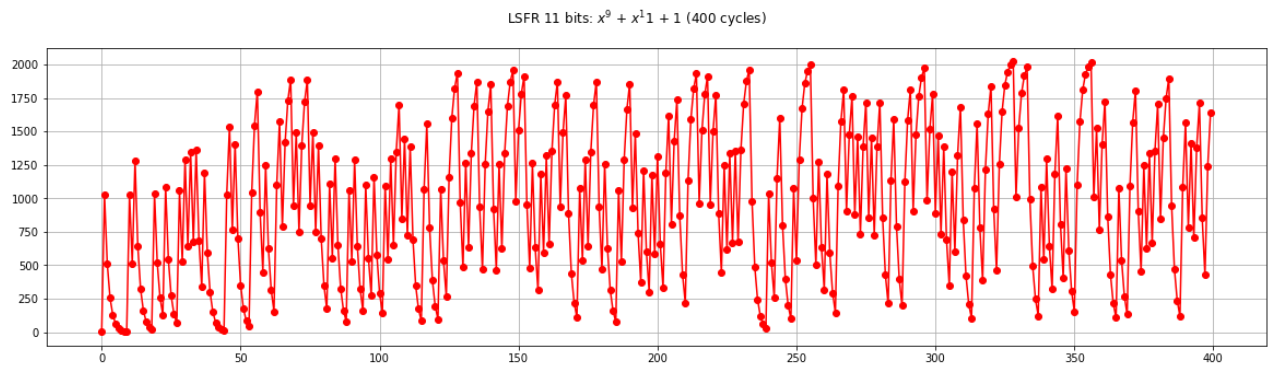
1) Plotagem dos gráficos dos LSFR pequeno e médio e do bitmap do LSFR grande

Os gráficos foram gerados a partir do output dos testbenchs de cada LFSR, por meio das funções das bibliotecas 'Numpy' e 'Matplotlib', em Python. Para o LFSR de 17 bits foi criado um bitmap, no qual é possível observar o caráter cíclico do LFSR.

LSRF pequeno: 9 bits

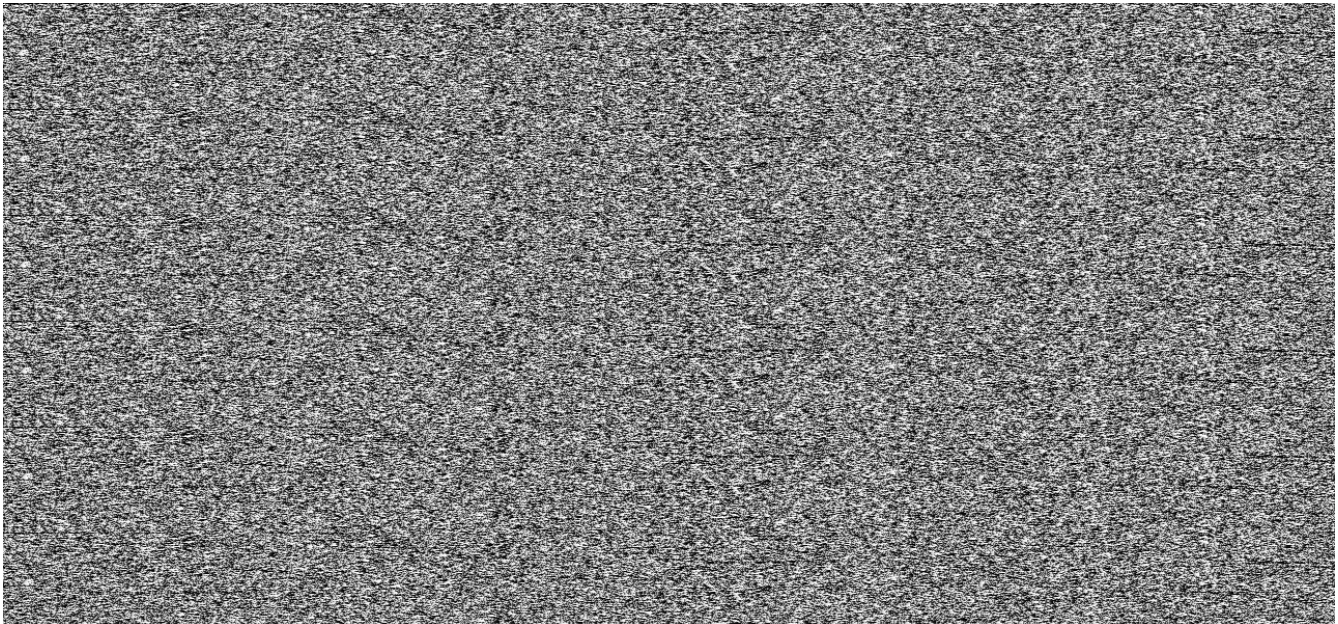


LSFR médio: 11 bits



LSFR grande: 17 bits (771000 cycles)

Bitmap:



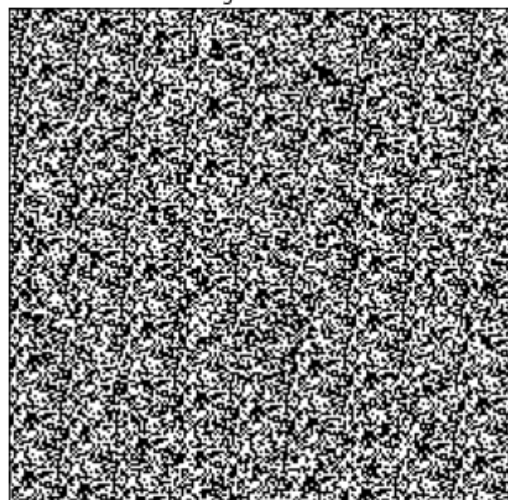
Vernam Cipher

Cifragem de imagem - LFSR (Período: 9)

Imagem original



Imagem cifrada

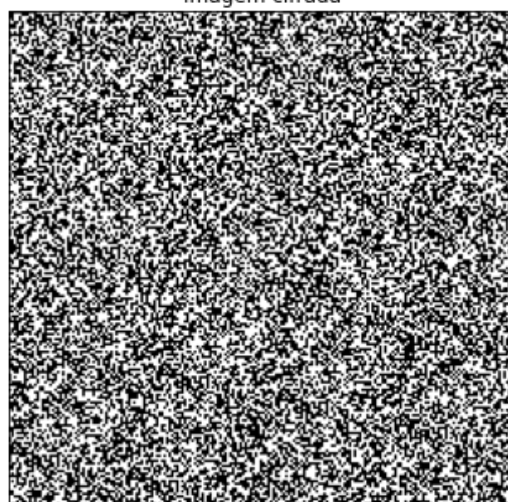


Cifragem de imagem - LFSR (Período: 11)

Imagem original



Imagem cifrada

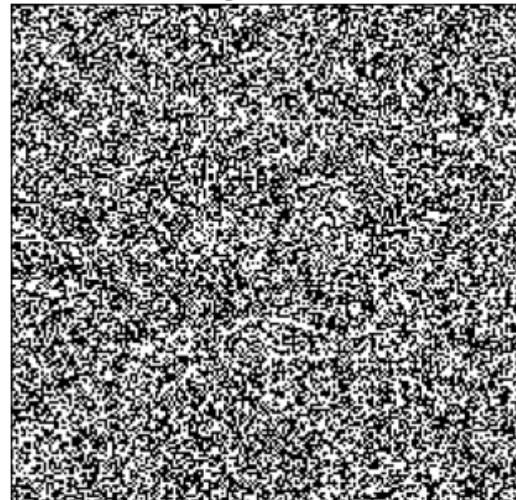


Cifragem de imagem - LFSR (Período: 17)

Imagem original



Imagem cifrada



Decriptação

O processo para decriptar uma imagem criptografada com a cifra de Vernam é simplesmente fazer o processo reverso da encriptação. Logo, os bits criptografados devem ser aplicados no algoritmo de encriptação para serem decriptados, usando a mesma chave utilizada para a encriptação.