

CIFRADOR VERNAN UTILIZANDO LFSR

DIOGO TULER CHAVES
JOÃO MARCOS TOMÁZ
RAFAEL MARTINS GOMES



AGENDA

- *Histórico e motivação*
- *Numeros aleatorios*
- *Implementação*
- *Resultados*
- *Discussão e conclusões*



MOTIVAÇÃO

- A segurança dos dados é uma preocupação cada vez mais constante;
- A criptografia digital é um método que consiste em transformar informações em códigos para evitar o acesso de pessoas não autorizadas ao conteúdo da mensagem.

"O Brasil é o 2º na América Latina com mais ataques cibernéticos em 2022" - Dado da CNN Brasil



"O Brasil registrou no primeiro semestre de 2022, 31,5 bilhões de tentativas de ataques cibernéticos a empresas." - Dado da CNN Brasil

HISTÓRICO



Em meio a crises de segurança e vazamento de dados, a criptografia digital surge como uma forma eficiente de se garantir a restrição de certas informações.



Derivado da cifra de Vernam, o método One Time Pad (OTP) configura um estilo de criptografia praticamente inquebrável. Ele foi aperfeiçoado ao longo dos anos e amplamente usado para o envio de mensagens e informações em contextos de guerra e espionagem.



O LFSR, por sua vez, configura um registrador de deslocamento com feedback linear, e foi desenvolvido na década de 1950. Sua principal função é gerar sequências pseudoaleatórias nas quais os valores são linearmente definidos pelo estado anterior a eles. Tal característica o tornou uma ferramenta valiosa em criptografia que foi amplamente utilizada desde sua criação.

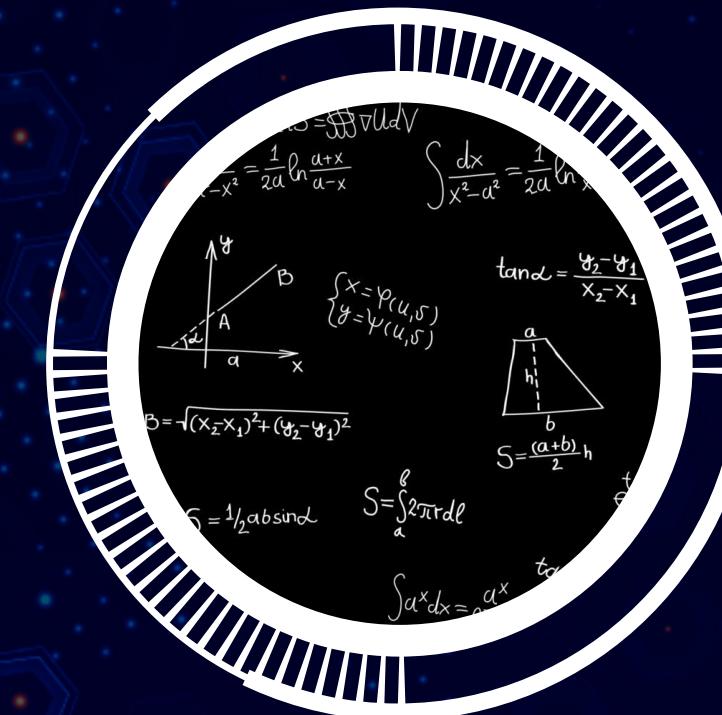
NÚMEROS ALEATÓRIOS



VERDADEIRO

"Que depende de acontecimento incerto."

- dicionario.priberam.org



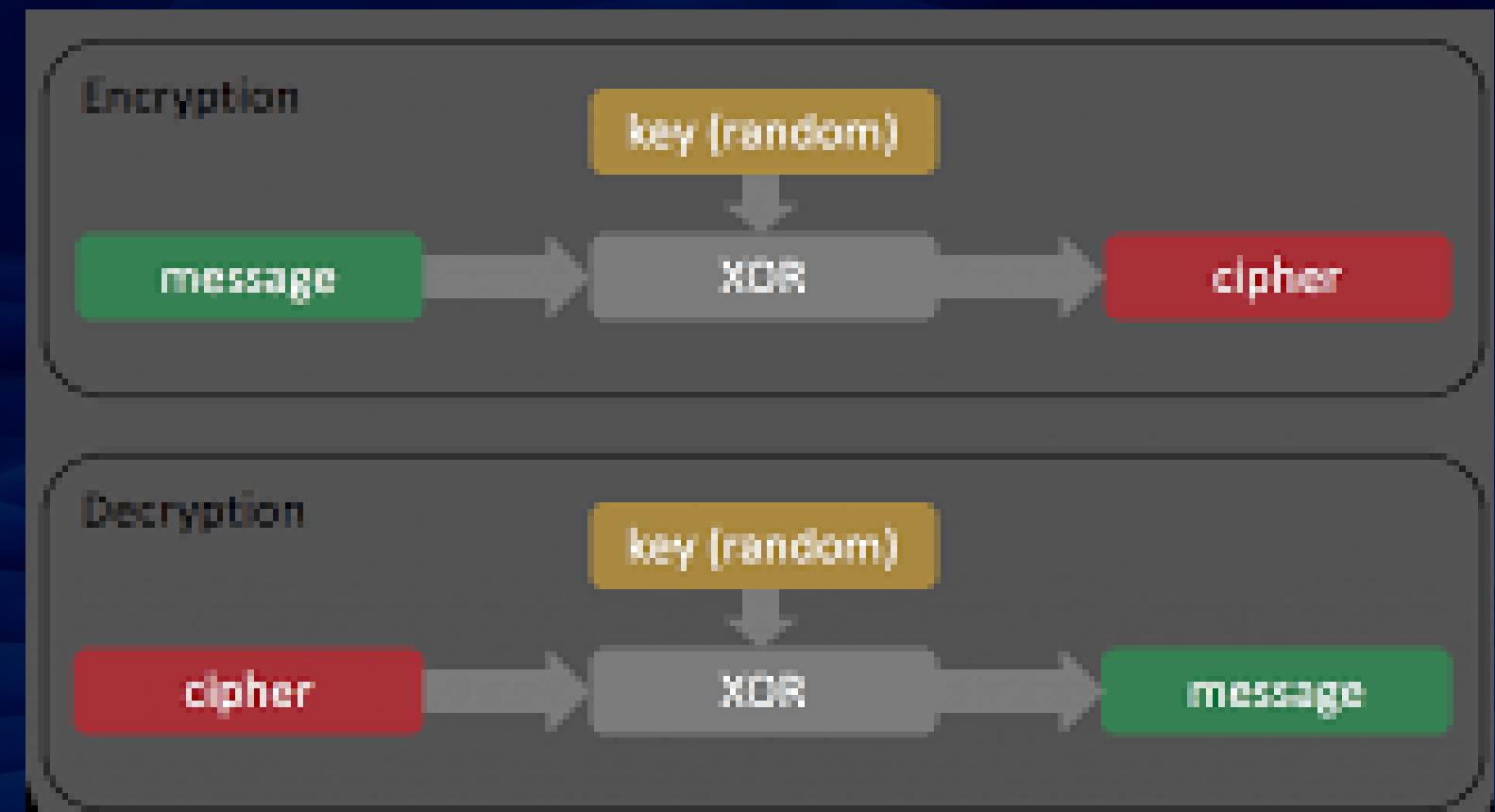
PSEUDO

"Que satisfaz testes de aleatoriedade estatística, mas é resultado de um procedimento matemático definido"
- dicionario.priberam.org

IMPLEMENTAÇÃO

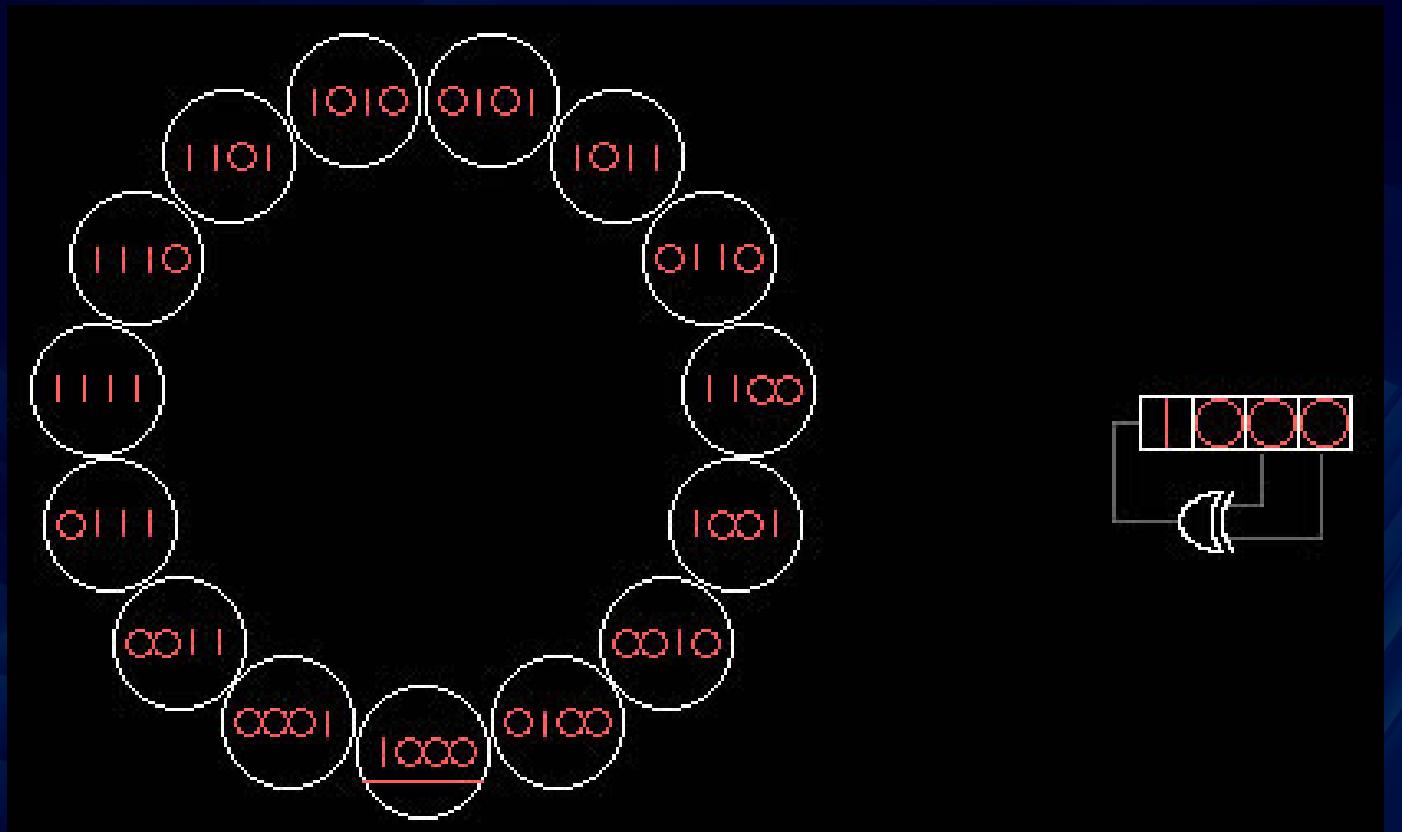
ONE-TIME PAD

- Um estilo de criptografia praticamente inquebrável;
- As mensagens cifradas com OTP não fornecem nenhuma informação sobre a mensagem original a um criptoanalista e sua segurança foi provada matematicamente;
- Consiste num algoritmo em que a mensagem é combinada, caractere por caractere, a uma chave secreta aleatória que para isso deve ter, no mínimo, o mesmo número de caracteres da mensagem. A chave pode ser usada uma única vez;



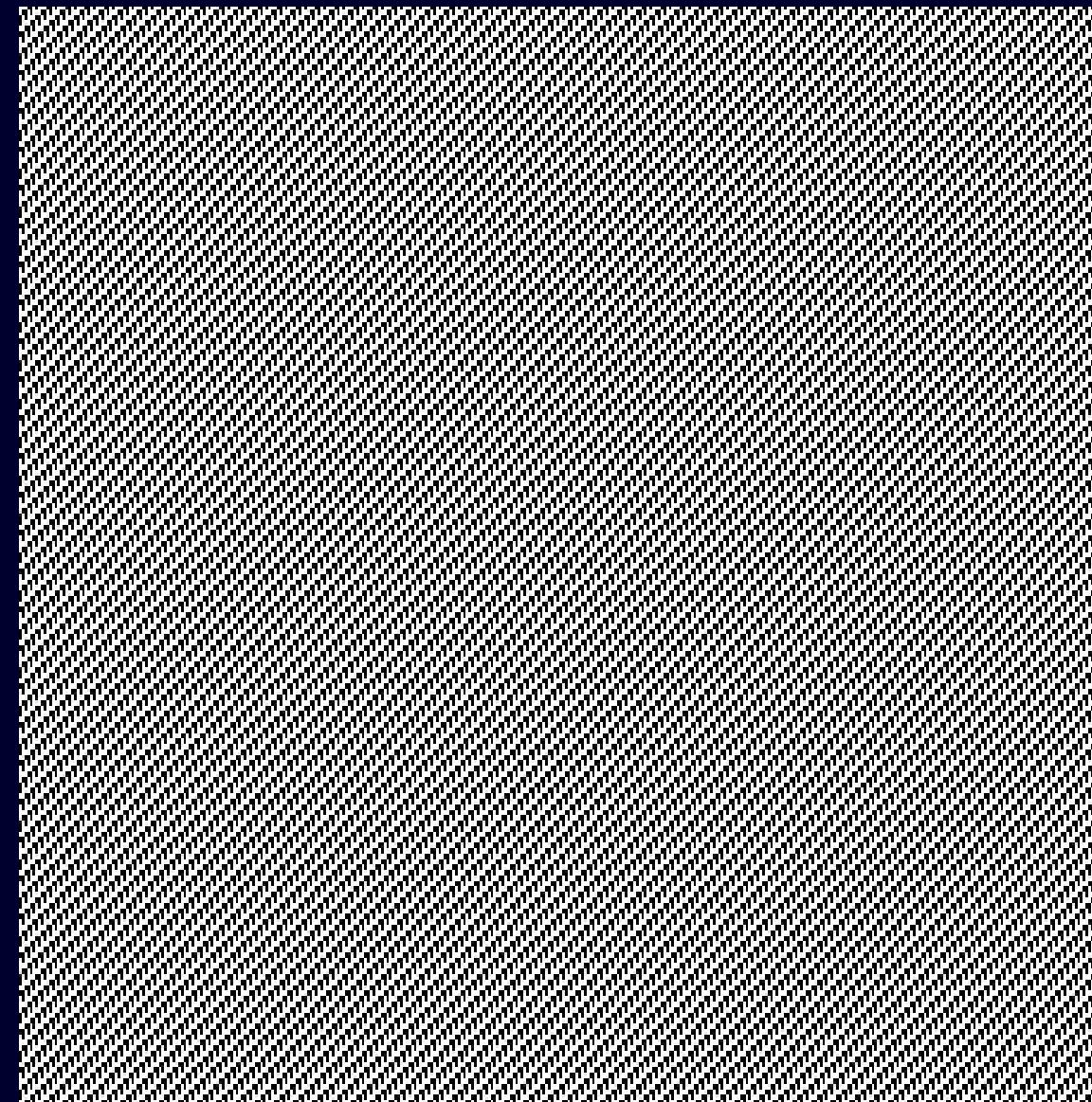
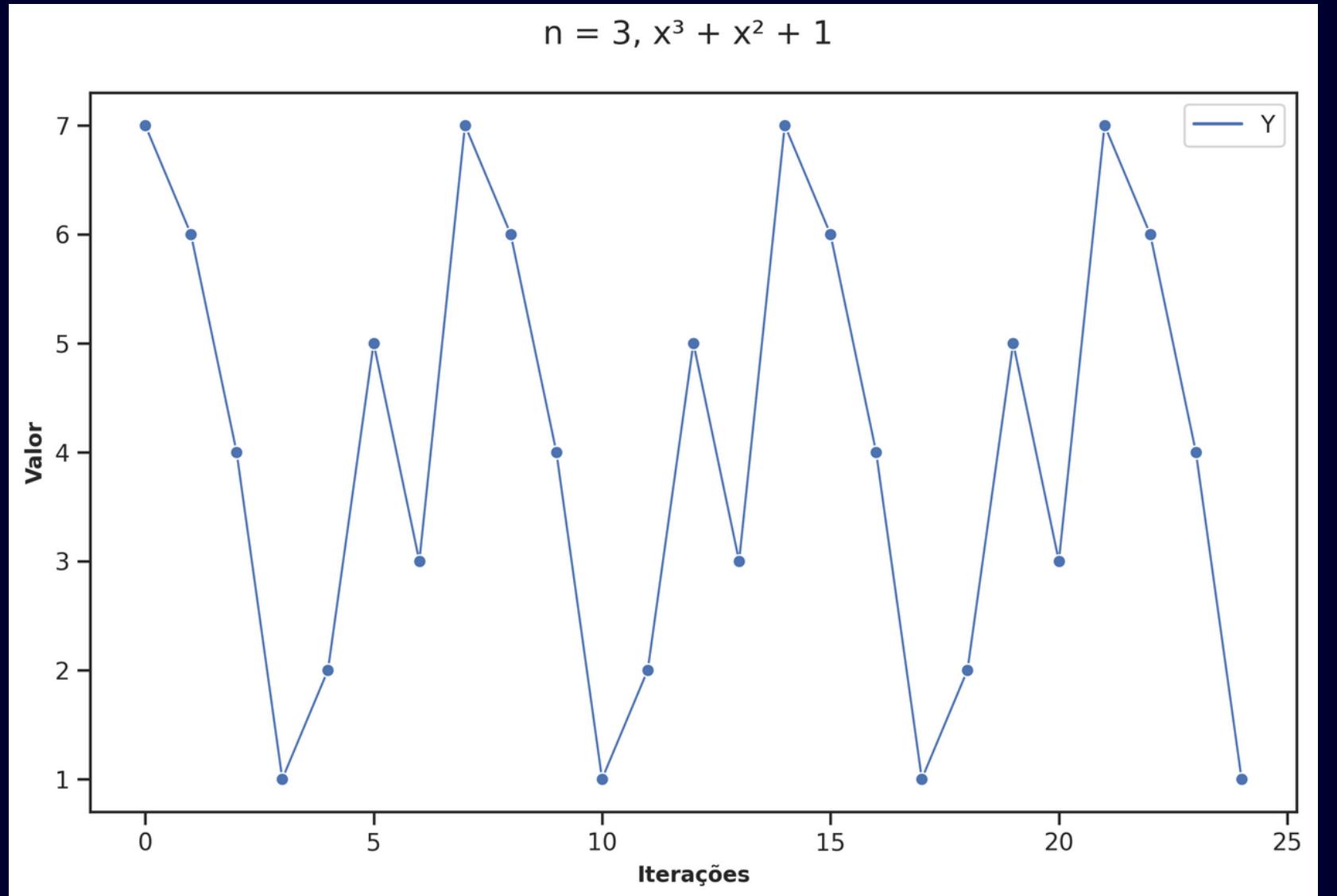
LFSR

- Gerador pseudo-aleatório de números binários, podendo ser muito útil para se obter a segurança das informações;
- As posições de bit que afetam o próximo estado são chamadas de taps. O bit mais à direita do LFSR é chamado de bit de saída;
- A sequência de números gerada por um LFSR ou sua contraparte XNOR pode ser considerada um sistema numérico binário tão válido quanto o código Gray ou o código binário natural.



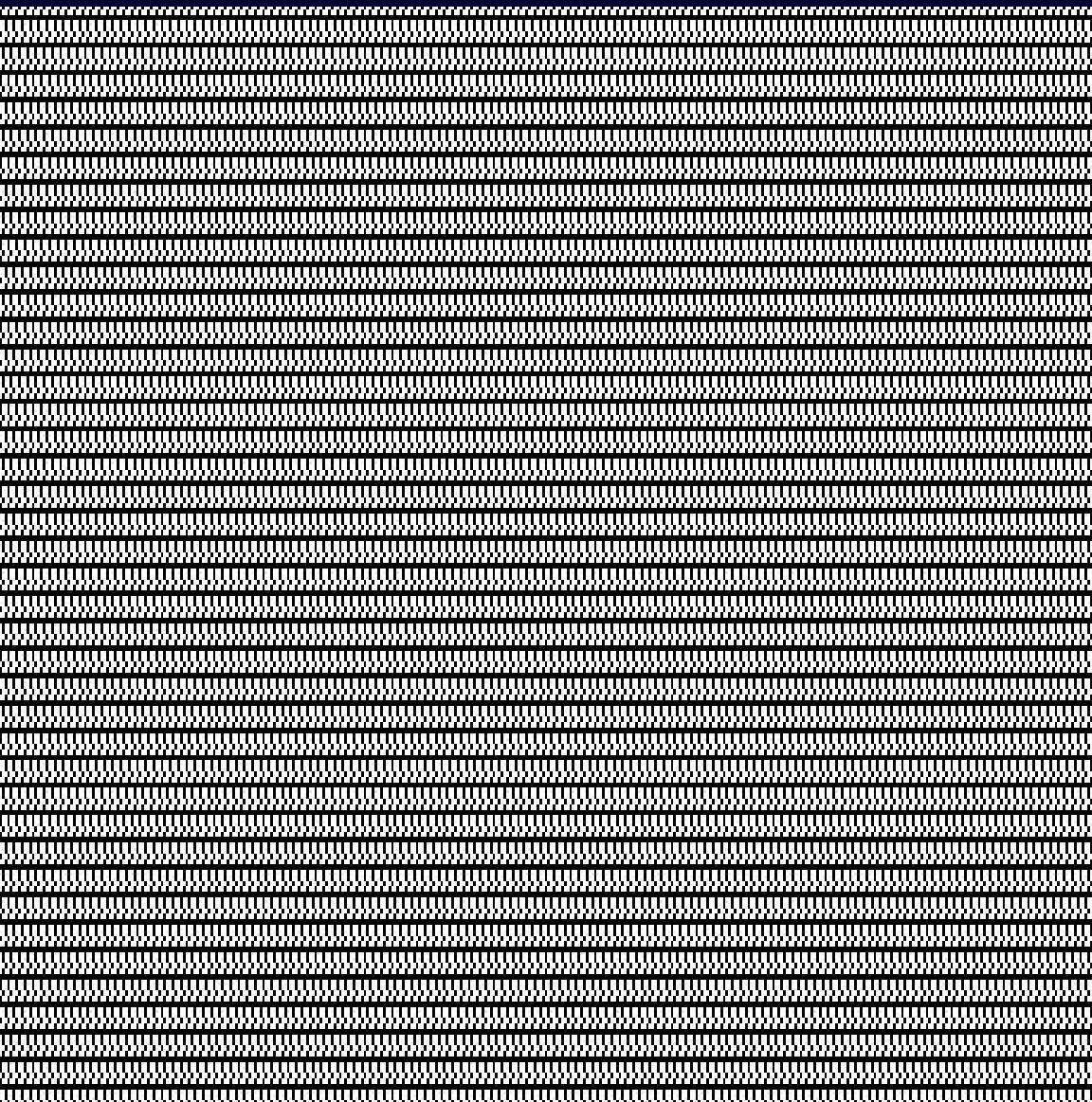
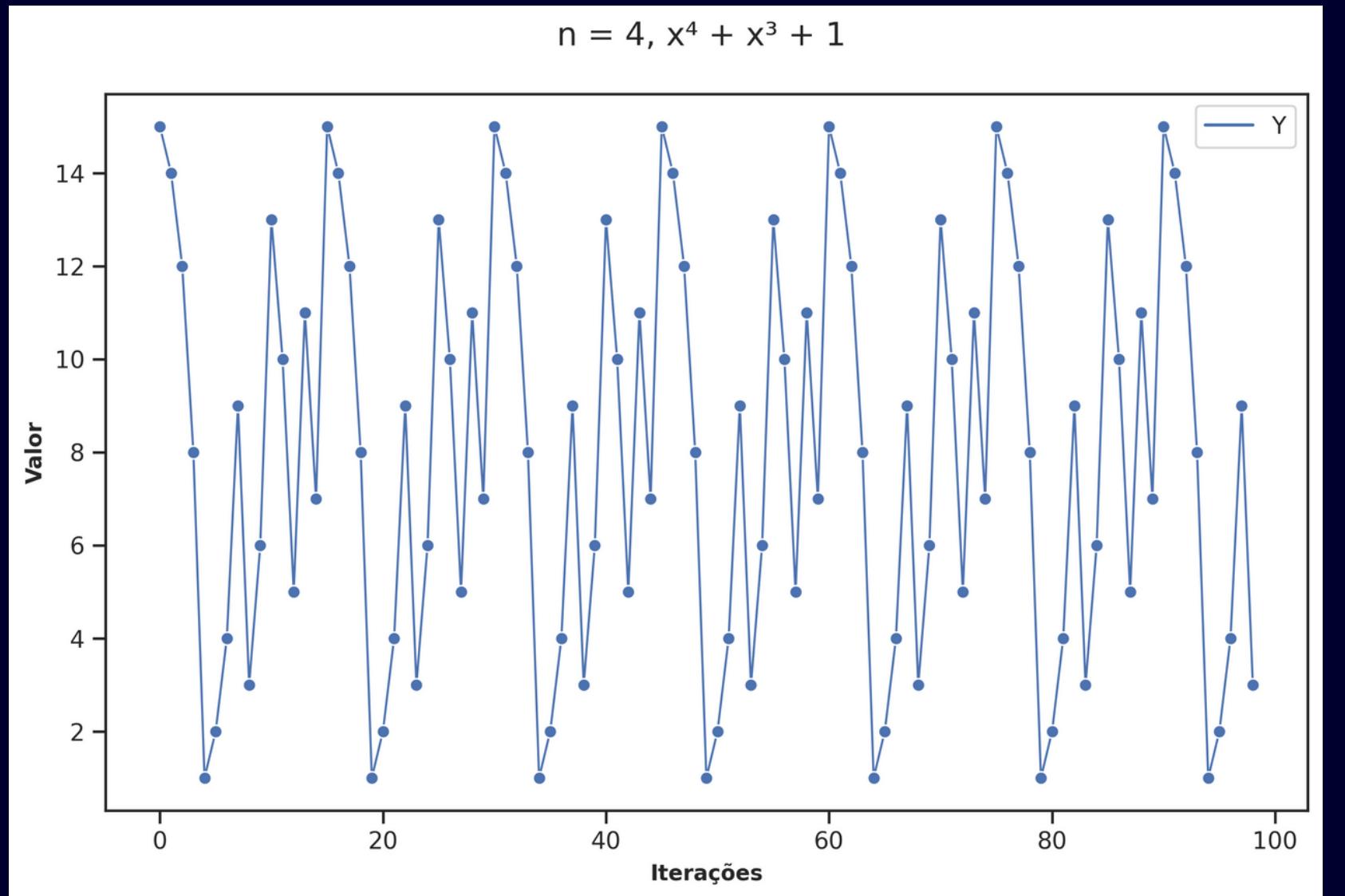
RESULTADOS

N = 3



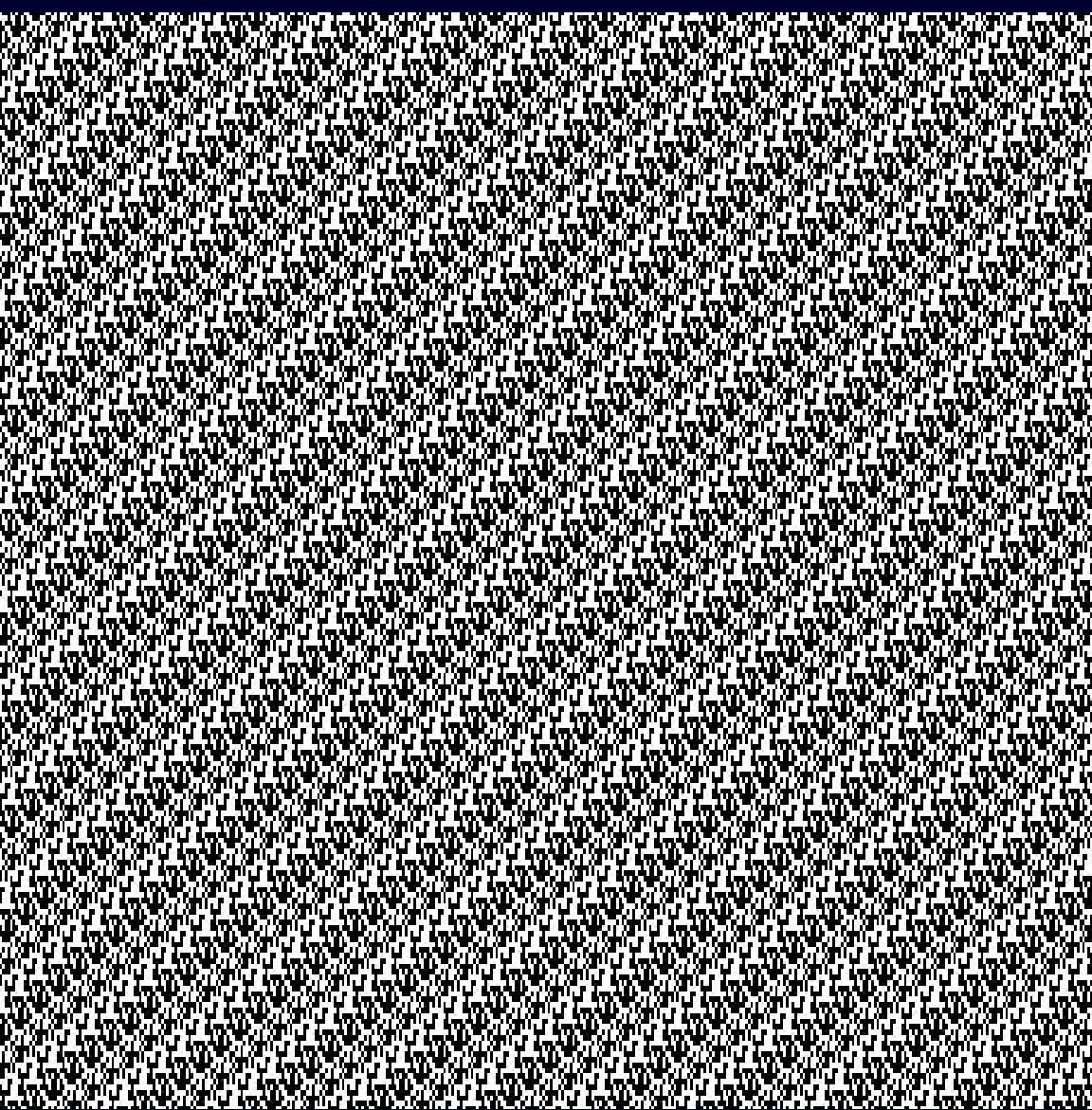
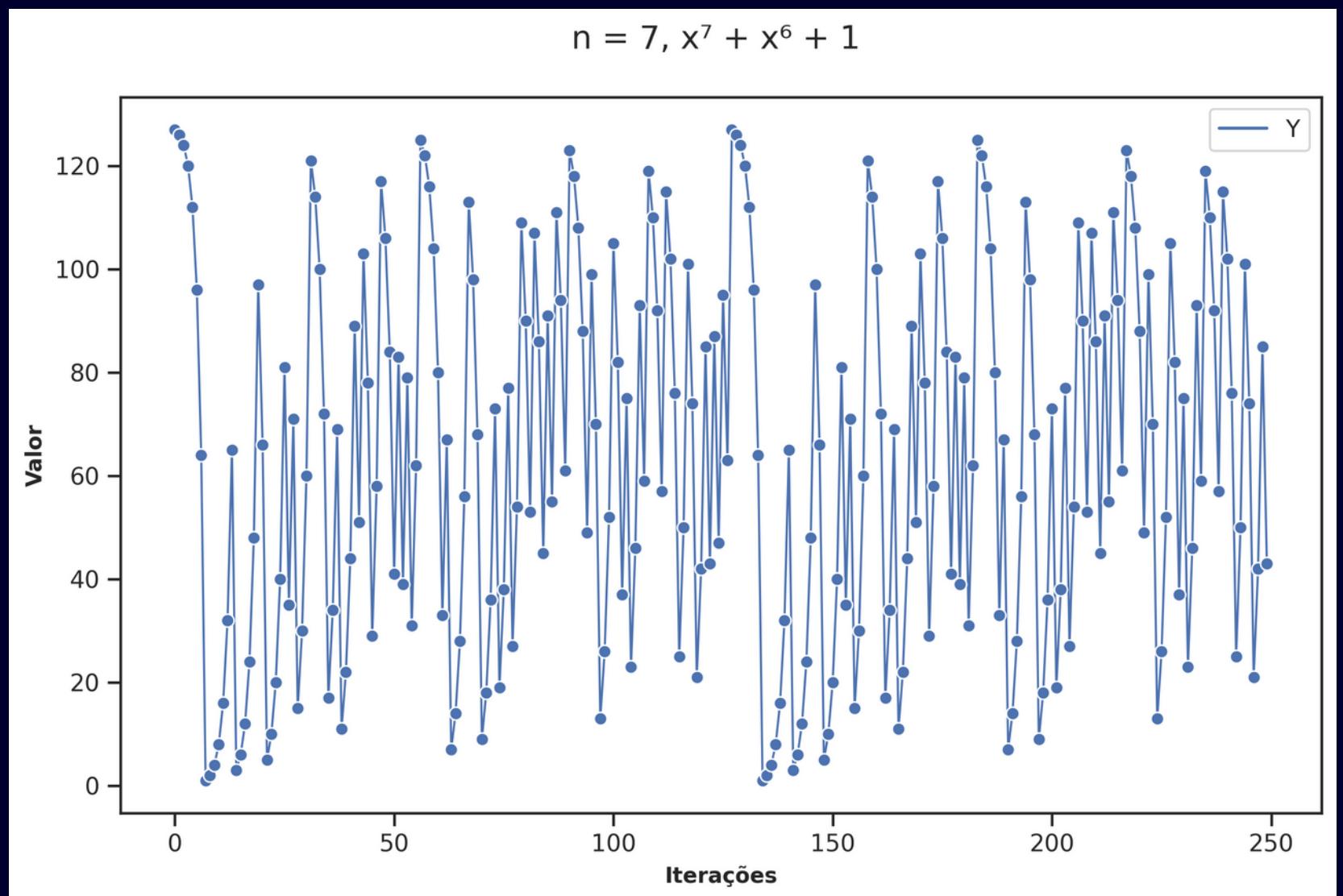
Entropy, bits
0.9854

N = 4



Entropy, bits
0.9972

$N = \mathbb{P}$

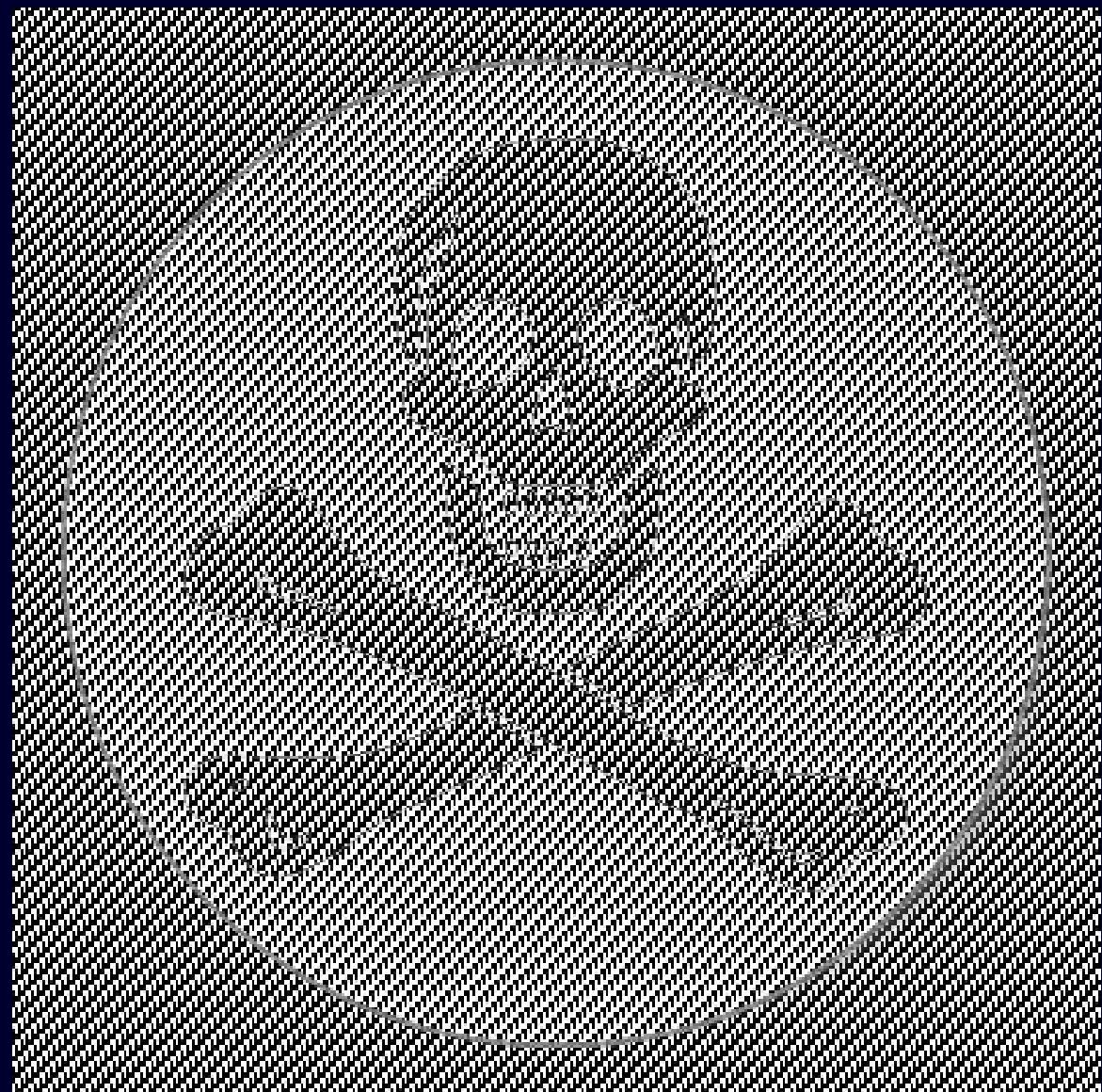


Entropy, bits
1.0000

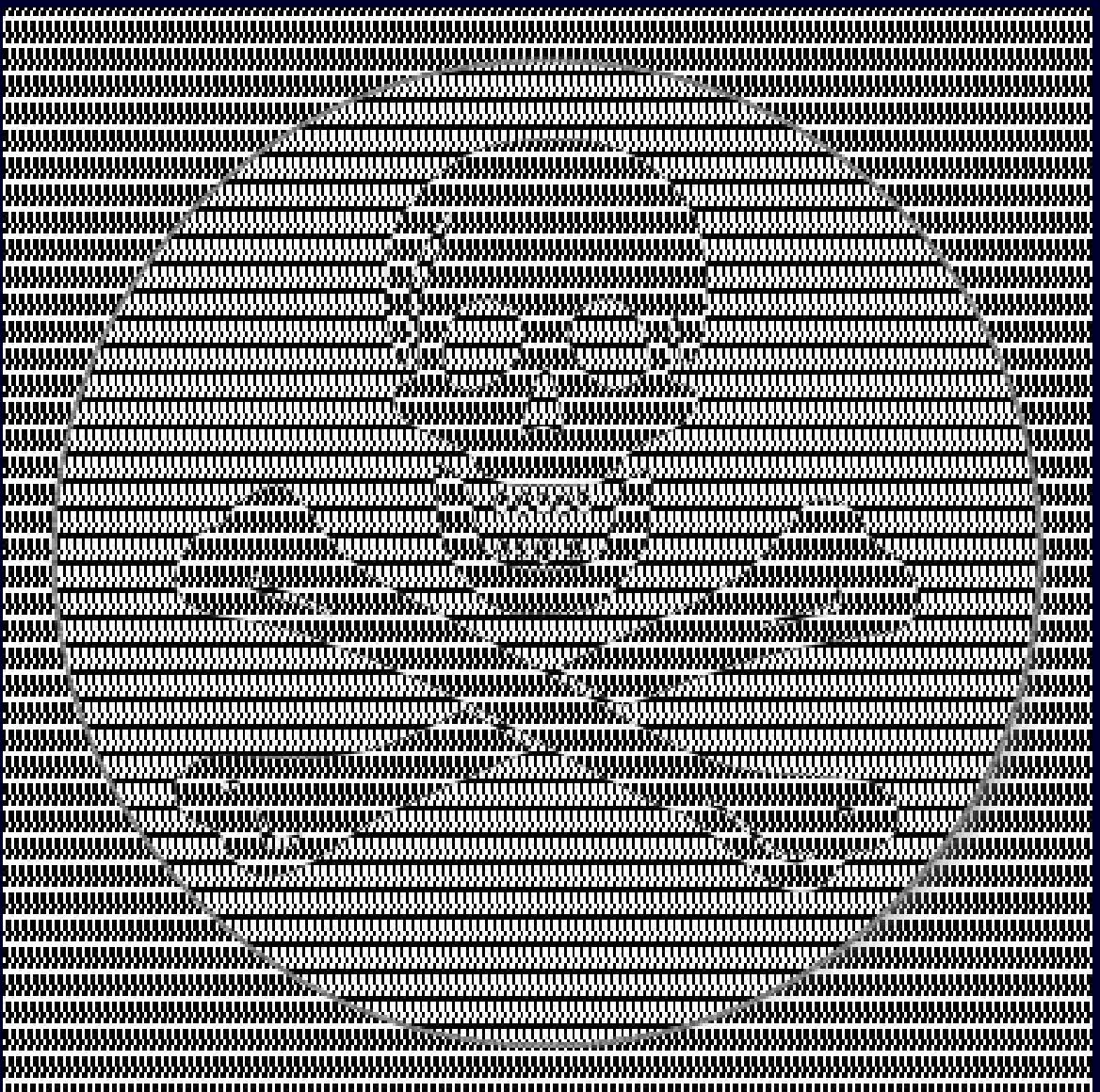
IMAGEM ORIGINAL
ESCOLHIDA



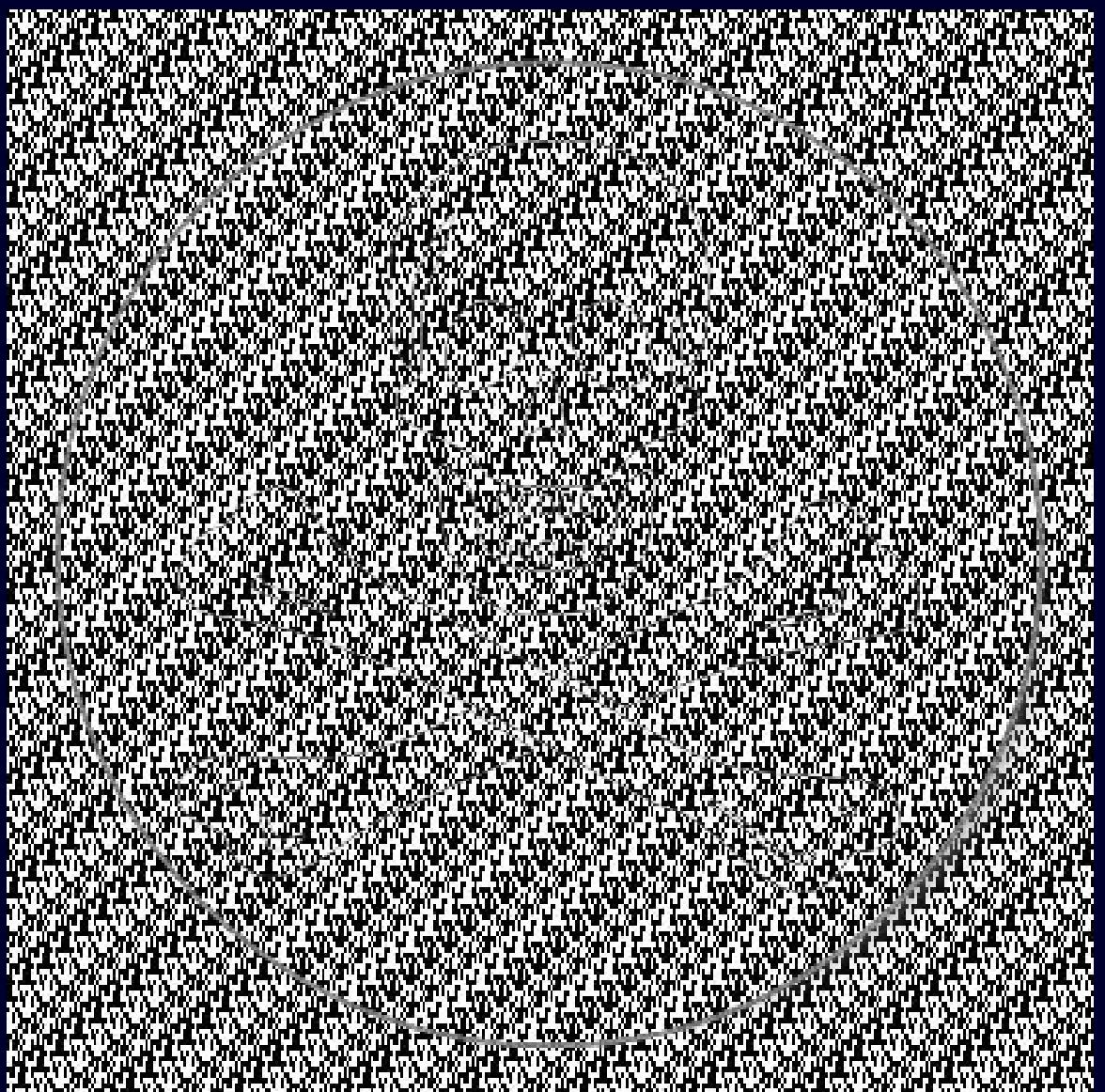
$N = 3$



$N = 4$



N = P



DISCUSSÃO

Podemos perceber que o n interfere diretamente com a entropia dos valores, sendo ambos diretamente proporcionais. Além disso, quando o n é alto a imagem criptografada fica muito difícil de ser identificada.

Maior desvantagem

Sua qualidade depende diretamente do valor do n escolhido.

Maior vantagem

Implementação e funcionamento muito simples.

CONCLUSÃO

Após os estudos necessários, foi concluído que a segurança dos dados é uma das grandes preocupações em um mundo cada vez mais tecnológico. Os métodos apresentados neste trabalho são exemplos significativos da relevância desse assunto. Além disso, as aulas gravadas e o curso de introdução aos sistemas lógicos ministrado pelo professor Gilberto Medeiros Ribeiro (UFMG) foram de grande ajuda para a realização do projeto. O projeto não apenas permitiu a aplicação prática de conteúdos aprendidos em sala, mas também expandiu o conhecimento dos alunos com novos tópicos relacionados ao campo de hardware.



OBRIGADO
PELA ATENÇÃO

