INSTITUTO FEDERAL DO ESPÍRITO SANTO (IFES) *CAMPUS* SERRA

CURSO SUPERIOR DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

RYAN LIMA BACILDO

A ÁLGEBRA LINEAR APLICADA A CRIPTOGRAFIA: CODIFICAÇÃO DE TEXTO UTILIZANDO MATRIZES

Serra - ES

2025

RYAN LIMA BACILDO

ÁLGEBRA LINEAR APLICADA A CRIPTOGRAFIA: CIFRAS DE HILL COMO FORMA DE CODIFICAÇÃO DE TEXTOS POR MEIO DE CÁLCULOS COM MATRIZES

Trabalho proposto para avaliação na matéria de Álgebra Linear do Curso de Bacharelado em Sistemas de Informação do Instituto Federal do Espírito Santo, Campus Serra.
Professor: Dr. Fidelis Zanetti de Castro.

Serra - ES
2025

RESUMO

O presente trabalho aborda a utilização da Álgebra Linear na Criptografia, com foco na implementação da Cifra de Hill, um método tradicional baseado em matrizes invertíveis para codificar e decodificar mensagens. O estudo apresenta conceitos relevantes, tais como: multiplicação de matrizes, inversão modular e determinantes, necessários para a segurança e reversibilidade do processo de codificação. Foi elaborado um programa em linguagem Python com interface interativa para realizar a criptografia e decriptografia de textos, validando a aplicabilidade da técnica. Os resultados evidenciam que a escolha correta das matrizes-chave (invertíveis módulo 26) é fundamental para o sucesso do método. A implementação demonstrou dificuldades, como a geração de matrizes válidas e o tratamento de caracteres não numéricos, indicando áreas para melhorias futuras para atuação em conjunto com outros algoritmos de criptografia.

ABSTRACT

This paper addresses the use of Linear Algebra in Cryptography, focusing on the implementation of the Hill Cipher, a traditional method based on invertible matrices to encode and decode messages. The study presents relevant concepts such as matrix multiplication, modular inversion, and determinants, which are essential for the security and reversibility of the encoding process. A program was developed in Python with an interactive interface to perform text encryption and decryption, validating the applicability of the technique. The results highlight that the correct selection of key matrices (invertible modulo 26) is crucial for the success of the method. The implementation demonstrated challenges, such as generating valid matrices and handling non-numeric characters, indicating areas for future improvements to work in conjunction with other cryptographic algorithms.

ESTRUTURA

1.Introdução:

Exposição do histórico da Álgebra Linear enquanto ferramenta no campo da criptografia e a ideia introdutória da Cifra de Hill;

Argumento da escolha do tema e os objetivos da investigação.

2.Fundamentos Teóricos:

Apresentação dos conceitos matemáticos essenciais, como matrizes invertíveis, transformações lineares e a Cifra de Hill;

Discussão dos critérios a serem seguidos para que a matriz corresponda a uma chave da Cifra de Hill.

3.Aplicação em Python:

Apresentação do desenvolvimento do programa em Python, com explicação do pacote "boxtool" e sua interface interativa;

Exemplos testados de criptografia e descriptografia rodando a partir do programa.

4.Dificuldades e Pontos a Melhorar:

Discussão das dificuldades surgidas durante a implementação, que incluem a geração de matrizes válidas e o tratamento de caracteres especiais;

Sugestões de melhorias para próximas versões do sistema.

5.Conclusão:

Síntese das principais descobertas do trabalho, enfatizando a eficiência da Álgebra Linear na área da criptografia;

Referência às limitações e proposta de continuação do trabalho para futuras investigações.

6.Referências:

Levantamento das fontes consultadas para a elaboração do trabalho.

1.INTRODUÇÃO

A Álgebra Linear constitui um dos alicerces matemáticos de vários domínios da computação, entre os quais se encontra a criptografia. A proteção do sistema de segurança moderna normalmente depende de operações que envolvem matrizes, assim como das propriedades de invertibilidade dessas matrizes, para assegurar a integridade da confidencialidade dos dados. A Cifra de Hill, proposta por Lester Hill em 1929, é uma das aplicações desse princípio ao usar matrizes quadradas invertíveis como chaves para misturar os textos claros com as mensagens cifradas, ao inverso.

1.1.JUSTIFICATIVA

A criptografia baseada em matrizes oferece vantagens como escalabilidade e resistência a ataques de frequência, sendo relevante em aplicações que exigem segurança ágil e robusta. A compreensão de conceitos como inversão modular e dependência linear é essencial para implementar algoritmos eficazes.

1.2.**Objetivos**:

O artigo visa:

. Demonstrar a relação entre Álgebra Linear e criptografia através da Cifra de Hill.

. Implementar um sistema de criptografia/descriptografia em Python utilizando matrizes.

. Analisar desafios práticos, como a geração de matrizes-chave válidas.

2.FUNDAMENTOS TEÓRICO

2.1.Matrizes Invertíveis: Uma matriz é invertível se existir outra matriz que, multiplicada por ela, resulte na matriz identidade.

$$A^{-1}\ tal\ que\ A * A^{-1} = I$$

Na Cifra de Hill, a matriz-chave deve ser invertível módulo 26 (26 pois são 26 as letras do alfabeto). Na prática, isso significa que a matriz deve atender outros requisitos para ser uma chave de criptográfica.
São eles: todos os seus elementos precisam ser menores que 26 e seu determinante deve ser coprimo (não possuir divisores em comum) com 26.

Obs.:Para fins de praticidade, foi utilizado uma função em python para testar e gerar matrizes 3x3 válidas como chaves exemplo.

```python
import numpy as np
import math

def gerar_matriz_valida(dimensao):
    while True:
        # Gera uma matriz aleatória com valores entre 0 e 25
        matriz = np.random.randint(0, 26, size=(dimensao, dimensao))
        det = int(np.round(np.linalg.det(matriz)))  # Calcula o determinante
        det = det % 26  # Reduz o determinante módulo 26
        if math.gcd(det, 26) == 1:  # Verifica se o determinante é coprimo com 26
            return matriz

# Exemplo de uso
matriz_valida = gerar_matriz_valida(3)
print("Matriz válida:\n", matriz_valida)
```

```
PROBLEMAS  SAÍDA  CONSOLE DE DEPURAÇÃO  TERMINAL  PORTAS  GITLENS

PS C:\Users\ryanl\OneDrive\Desktop\Estudos\Álgebra Linear\Trabalhos\Projetos\Projetos\Álgebra Linear\boxtool> python chaves.py
Matriz válida:
 [[10  9 15]
 [ 0 22 23]
 [ 5  6 16]]
PS C:\Users\ryanl\OneDrive\Desktop\Estudos\Álgebra Linear\Trabalhos\Projetos\Projetos\Álgebra Linear\boxtool>
```

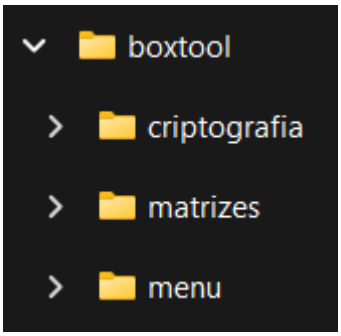
O código se encontra na pasta pacote “boxtools”, mas não está vinculada ao código em si diretamente.

2.2.Transformações Lineares: Cada bloco de texto foi convertido em uma matriz e transformado pela matriz chave A, para encriptar ou por sua inversa mod 26 A^{-1}, para decodificar.

2.3.Cifra de Hill: Método criado por Lester S. Hill em 1929. Consiste em separar o texto em blocos de tamanho n sendo este a complexidade da matriz chave escolhida. Caso algum bloco fique com caracteres a menos, é inserido um caracter fora de contexto para auxiliar o entendimento. Cada caracter é convertido em um número (A=1, B=2, …, Z=25). e os blocos são transformados através da multiplicação como descrito acima.

3.APLICAÇÃO EM PYTHON

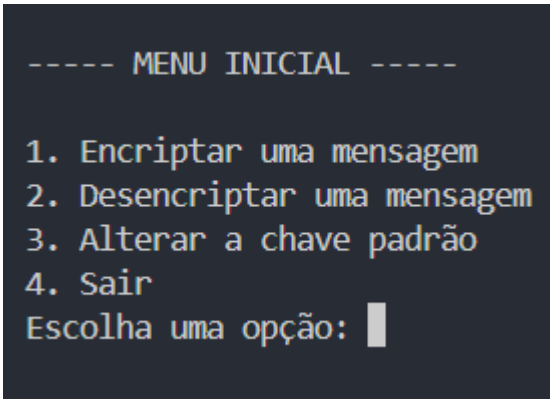
O programa utilizado para demonstração do tema foi desenvolvido em Python 3.
Foi criado um pacote com subpacotes anexados chamado "*boxtool"* onde as funções específicas requeridas foram anexadas, como demonstra a imagem abaixo:



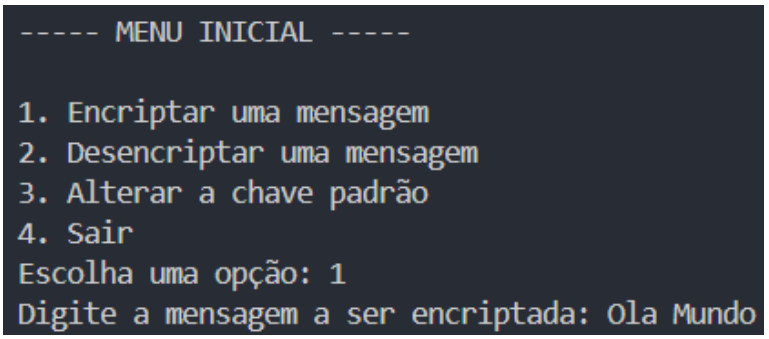
Existe o arquivo da aplicação "programa.py" que contém apenas o inicializador da aplicação.

```
1  from boxtool import menu as mn
2
3  def main():
4      mn.start_menu()
5
6  if __name__ == "__main__":
7      main()
```

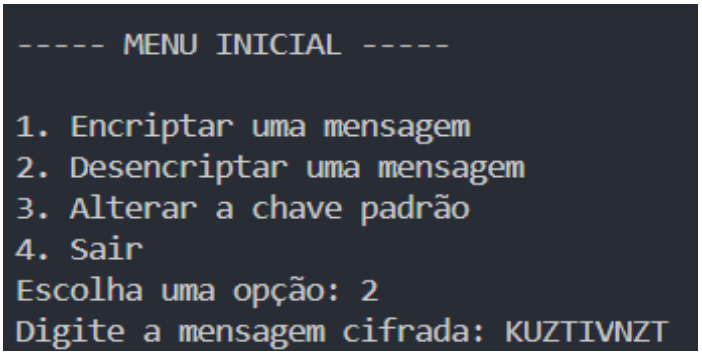
Quando executado, exibe uma interface simples que oferece opções para operações no sistema, sendo bastante intuitivo.



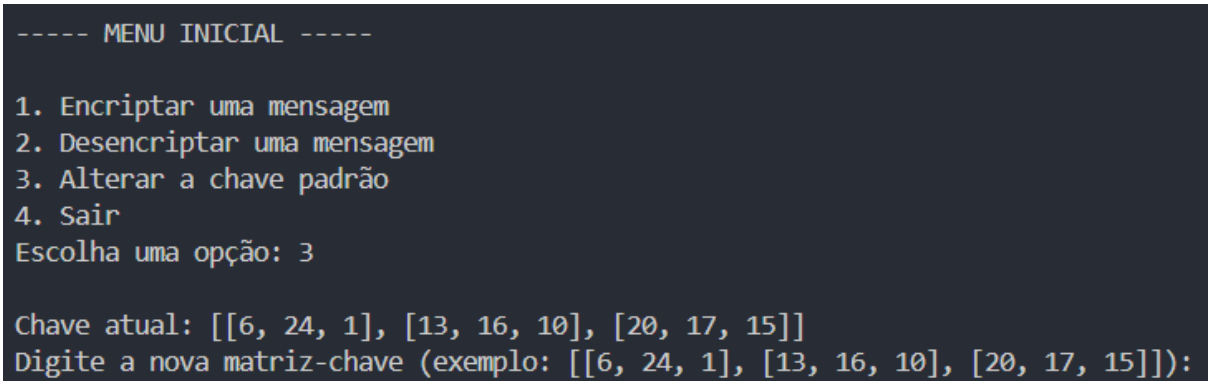
Selecionando as opções 1 ou 2, o usuário é orientado a digitar a mensagem a ser criptografada ou descriptografada respectivamente (imagens 1 e 2), que será exibida na tela após a devida transformação. O programa vem com uma matriz chave já por padrão, que pode ser alterada selecionando a opção 3 (imagem 3 e 4) ou após ter digitado as mensagens nas opções 1 ou 2 (imagens 5 e 6). Após qualquer um desses casos, a aplicação retorna ao MENU INICIAL, possibilitando múltiplas operações sem a necessidade da reinicialização do sistema. Caso seja selecionada a opção 4, a aplicação é devidamente encerrada (imagem 7).



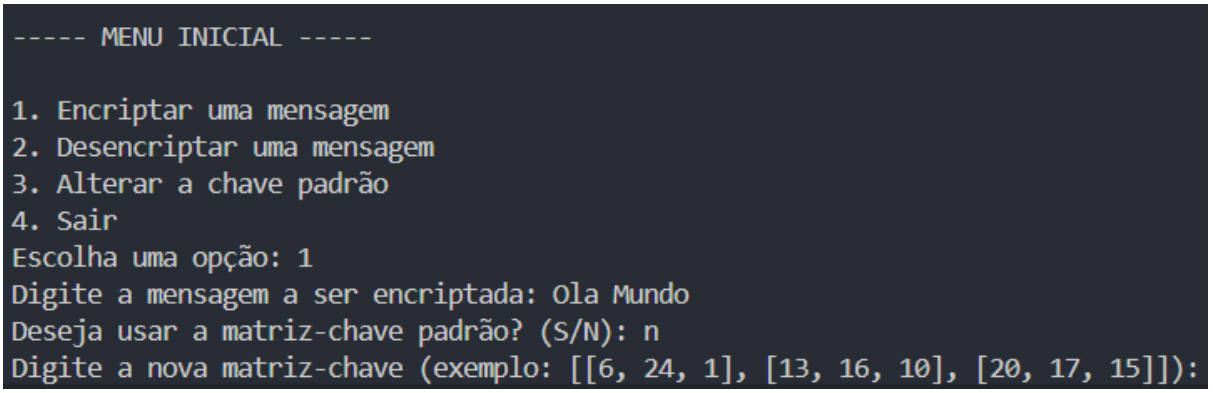
(Imagem 1)



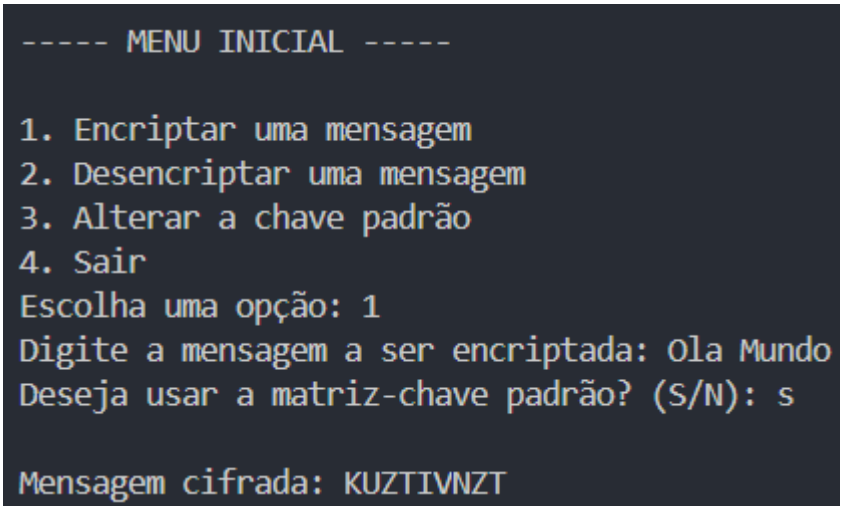
(Imagem 2)



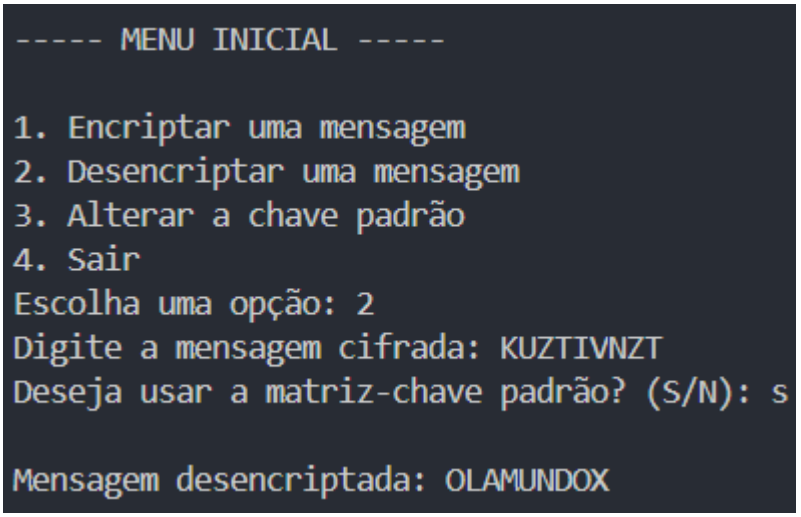
(Imagem 3)



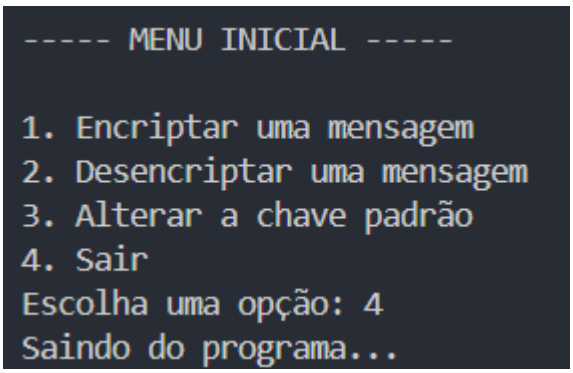
(Imagem 4)



(Imagem 5)



(Imagem 6)


----- MENU INICIAL -----
1. Encriptar uma mensagem
2. Desencriptar uma mensagem
3. Alterar a chave padrão
4. Sair
Escolha uma opção: 4
Saindo do programa...

(Imagem 7)

4.DIFICULDADES E PONTOS A MELHORAR

A principal dificuldade na implementação das Cifras de Hill no programa foi a obtenção de matrizes viáveis para chave, problema solucionado com a adição do programa “chave.py”. Existiram outras dificuldades, como a criação das matrizes dos blocos correspondentes de caracteres, problema apenas parcialmente resolvido. Infelizmente o sistema apresenta a falha de não poder representar os espaços após a decodificação da frase, o que pode ser resolvido com uma implementação mais complexa do pacote matriz também para essa conversão.

5.CONCLUSÃO

Neste estudo, foi investigada a utilização da Álgebra Linear na implementação da Cifra de Hill, que é um dos métodos clássicos em criptografia que utiliza matrizes invertíveis para codificação e decodificação. Na implementação prática, em Python, observou-se como os conceitos matemáticos de matrizes invertíveis, determinante no módulo e transformação linear são vitais para garantir a segurança e a reversibilidade do processo de criptografia. A Cifra de Hill provou ser eficiente e escalável, além de conseguir resistir a ataques de frequência, razão pela qual ela pode ser vista como uma ferramenta muito prática para o uso em sistemas de Informação. No entanto, foram observadas algumas limitações, tais como a dificuldade encontrada para gerar matrizes-chave que sejam válidas, de forma especial se relacionadas a matrizes de maior dimensão (ex: 3x3), e a impossibilidade de tratar espaços ou caracteres especiais pela implementação atual. Além disso, o fato de o texto ser dividido em blocos de tamanho fixo, pode exigir algum tipo de preenchimento, o que pode se tornar inadequado em certos cenários.
Para trabalhos futuros recomenda-se combinar as técnicas utilizadas com métodos de aprendizado de máquina para gerar matrizes-chave mais complexas e mais robustas, expandir o alfabeto para incluir caracteres especiais, números e espaços, otimizar o desempenho para lidar com matrizes de maior dimensão assim como textos grandes, e elaborar uma interface gráfica mais amigável. Embora a cifra de Hill seja um método antiquado, permanece atual como uma ferramenta educacional e uma ferramenta de prática para aprendizados sobre a intersecção de Álgebra Linear e criptografia, evidenciando a importância da Matemática na Computação e abrindo espaço para futuras melhorias e aplicações mais avançadas.

6.REFERÊNCIAS:

https://repositorio.ufpb.br/jspui/bitstream/123456789/27681/1/Let%C3%ADciacorreiaalexandredacosta_TCC.pdf

https://www.ime.unicamp.br/~marcia/AlgebraLinear/aplicacao_criptografia.html

https://www.youtube.com/watch?v=rEKjkrIdYH0