INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO

CAMPUS SÃO PAULO

AMANDA JEN, FELIPE TEIXEIRA DE LIMA, JULIANA XAVIER DOS SANTOS ARAUJO

VETORES, GEOMETRIA ANALÍTICA E ÁLGEBRA LINEAR (SPOMVAL) - TRABALHO FINAL

SÃO PAULO - SP

2025

Amanda Jen, Felipe Teixeira de Lima, Juliana Xavier dos Santos Araujo

TRABALHO FINAL

Trabalho apresentado à disciplina de Vetores, Geometria Analítica e Álgebra Linear do Instituto Federal de Educação, Ciência e Tecnologia Campus São Paulo como nota parcial para aprovação na disciplina do curso Bacharelado em Sistemas de Informação.

Professora: Josceli Maria Tenorio

SÃO PAULO – SP

2025

1. INTRODUÇÃO

O presente trabalho tem como objetivo aplicar e aumentar os aprendizados de Álgebra Linear no desenvolvimento de um sistema de criptografia baseado na Cifra de Hill. A cifra utiliza vetores, matrizes, operações modulares e transformações lineares para codificar mensagens, demonstrando como conceitos matemáticos são aplicados em Sistemas de Informação.

A implementação foi desenvolvida em Python, incluindo testes, validações e análise de invertibilidade de matrizes módulo m, requisito essencial para o processo de decodificação.

2. FUNDAMENTAÇÃO TEÓRICA

A Cifra de Hill é um método de criptografia clássica baseado em operações matriciais e transformações lineares, desenvolvido por Lester S. Hill em 1929. Foi um dos primeiros algoritmos que utilizou conceitos de Álgebra Linear para codificar mensagens, demonstrando como as matrizes podem ser aplicados ao tratamento e segurança de dados. Para tanto, são necessários entendimentos acerca dos fundamentos matemáticos, incluindo vetores, matrizes, operações modulares, determinantes e inversa de matrizes em aritmética modular.

2.1 Vetores e Representação Numérica do Texto

Para aplicar a Cifra de Hill, cada caractere do alfabeto é transformado para um número inteiro. Em geral, utiliza-se o módulo $m = 26$, de modo que:

$$A \rightarrow 0,\ B \rightarrow 1,\ \ldots,\ Z \rightarrow 25$$

Assim, uma mensagem de texto pode ser representada como um vetor coluna de inteiros. De acordo com LAY, David (2012), esses vetores são agrupados em blocos de tamanho *n*, sendo *n* a ordem da matriz de codificação. Esse agrupamento reflete diretamente o princípio de operação da cifra, no qual cada bloco é transformado linearmente pela matriz geradora.

2.2 Matrizes e Transformações Lineares

A Cifra de Hill opera através de uma transformação linear aplicada aos vetores que representam a mensagem. Seja:

- P: vetor bloco da mensagem (plaintext)
- A: matriz quadrada de ordem *n* usada para codificação
- C: vetor criptografado (ciphertext)

A codificação é realizada por:

$$C = A \cdot P (mod m)$$

2.3 Aritmética Modular

Todas as operações da cifra são realizadas módulo *m*.
A aritmética modular é utilizada em criptografia e sistemas de segurança, já que permite operar sobre conjuntos finitos, garantindo que todos os resultados permaneçam dentro do intervalo $0 \leq x < m$.

A operação central é:

$$x \equiv y (mod\ m)$$

Ou seja, *x* e *y* deixam o mesmo resto quando divididos por *m*.

2.4 Determinante e Invertibilidade da Matriz

Para que a cifra funcione corretamente, a matriz deve ser invertível modulo *m*. Isso significa que existe uma matriz A^{-1}tal que:

$$A^{-1} \cdot A \equiv I (mod m)$$

Para que essa inversa exista, é necessário que:

$$gcd(det(A), m) = 1$$

Ou seja, o determinante da matriz deve ser inversível no conjunto dos inteiros módulo m.

Se o determinante da matriz e *m* não forem coprimos, a matriz não possui inversa modular, impossibilitando a decodificação da mensagem. Esse critério é fundamental na validação da matriz escolhida pelo usuário.

2.5 Matriz inversa de Matriz Módulo *m*

A decodificação da Cifra de Hill depende da matriz inversa:

$$P = A^{-1} \cdot C (mod m)$$

Para matrizes 2×2, a inversa modular segue:

$$A = (a\ b\ c\ d) \Rightarrow A^{-1} = det(A)^{-1} (d\ -b\ -c\ a) (mod m)$$

onde $det(A)^{-1}$é o inverso multiplicativo de $det(A)$modulo m.

Esse processo pode ser generalizado para matrizes maiores utilizando adjunta e cofatores, desde que a condição de que sejam coprimos esteja satisfeita.

2.6 Aplicação da Álgebra Linear na Criptografia

A Cifra de Hill é fundamental no uso de operações lineares em criptografia. Mesmo sendo simples e vulnerável a ataques pela análise moderna, seu valor acadêmico é alto, pois demonstra:

- Utilização de vetores e matrizes para transformação de dados;
- Demonstra a importância da matriz inversa e do determinante;
- Aplicação direta de transformações lineares em um sistema real;
- Conexão entre matemática abstrata e segurança da informação.

Esse modelo serve como ponte entre cifras clássicas e a criptografia moderna, que também se fundamenta fortemente em álgebra matricial, modular e estruturas algébricas. A importância e as principais aplicações dessa cifra serão ressaltadas no tópico a seguir.

3. Aplicações

A Cifra de Hill ainda possui relevância conceitual no estudo e na prática de Segurança da Informação. Embora não seja utilizada diretamente como mecanismo de proteção em sistemas modernos devido às vulnerabilidades já conhecidas frente a ataques de criptoanálise linear e análise de frequência, seus princípios matemáticos continuam fundamentais em diversos componentes presentes em Sistemas de Informação contemporâneos.

Em primeiro lugar, a Cifra de Hill introduz de forma didática o uso de álgebra linear como base para operações criptográficas, especialmente o emprego de matrizes inversíveis para transformar blocos de dados. Esse conceito é essencial para compreender algoritmos atuais que operam por meio de transformações matemáticas semelhantes, como o AES (Advanced Encryption Standard), que utiliza operações matriciais e transformações lineares em espaços vetoriais finitos para garantir confidencialidade. Assim, a Cifra de Hill é frequentemente utilizada no ensino e na modelagem inicial de mecanismos criptográficos dentro de disciplinas de Sistemas de Informação e Segurança.

Além disso, ao trabalhar com blocos de caracteres ou bytes, a Cifra de Hill introduz o conceito de criptografia em bloco, ideia presente em praticamente todos os sistemas modernos de comunicação segura — como conexões HTTPS, redes corporativas protegidas por VPNs, sistemas de autenticação e tokens de sessão. Mesmo que o algoritmo em si não seja empregado na prática, o entendimento de sua estrutura auxilia no desenvolvimento, avaliação e implementação de soluções que envolvem a criptografia de dados sensíveis.

No contexto de Sistemas de Informação voltados para análise forense, auditoria e conformidade, a Cifra de Hill também serve como recurso pedagógico importante para compreender como vulnerabilidades podem ser exploradas quando chaves são mal gerenciadas ou quando métodos de cifragem apresentam dependência excessiva de propriedades matemáticas

previsíveis. Essa compreensão auxilia profissionais a adotarem técnicas robustas de gestão de chaves e a evitarem padrões previsíveis nos sistemas que desenvolvem ou administram.

Por fim, a Cifra de Hill se mostra útil em aplicações experimentais, simulações e testes acadêmicos que envolvem códigos automáticos, manipulação de matrizes, integração com bancos de dados e pipelines de processamento de dados. Sistemas de Informação frequentemente integram módulos que exigem transformações lineares, normalização de dados e operações vetoriais — aspectos que podem ser explorados ou demonstrados utilizando a lógica matemática presente na cifra.

Desse modo, mesmo não sendo adotada como mecanismo de segurança em ambientes produtivos, a Cifra de Hill desempenha papel relevante como instrumento educacional, conceitual e experimental, contribuindo diretamente para a formação de profissionais e para o desenvolvimento de tecnologias seguras no campo dos Sistemas de Informação.

4. Casos de teste:

Caso de Teste 1 – Entrada e Saída

Entrada:

modulo = 26

ordem = 2

Matriz:

A=[3, 3]

[2, 5]

Saída esperada:

“Mensagem original: TESTE

Mensagem criptografada: RGHBDT

Mensagem descriptografada: TESTEX”

```
Mensagem original: TESTE
Mensagem criptografada: RGHBDT
Mensagem descriptografada: TESTEX
```

Caso de Teste 2 – Matriz não invertível

Entrada:

modulo = 26

ordem = 2

Matriz:

A=[2, 4]

[6, 8]

Saída esperada:

mensagem: "A matriz não é invertível módulo 26"

```
A matriz não é inversível módulo 26.
```

5. Conclusão:

A partir do conteúdo aplicado no presente projeto, fica evidente a importância da criptografia para a segurança de dados. Além disso, o projeto ressaltou como as matrizes e a matemática estão ligadas à informática.

A Cifra de Hill é um exemplo de criptografia de dados, principalmente em formato de texto que se baseia em matrizes e álgebra linear. Apesar de ser considerada simples quando comparada às tecnologias atuais, foi essencial para o surgimento de novos métodos e é utilizada em sistemas mais simplificados até os dias atuais.

6. Referências bibliográficas

SINGH, Simon. *O Livro dos Códigos e Cifras*. São Paulo: Record, 2001.
LAY, David C. *Álgebra Linear e Suas Aplicações*. 4. ed. São Paulo: Pearson, 2012.

VITORINO, Alfredo; RUGGIERO, Márcia Aparecida Gomes. *Álgebra Linear e Aplicações: Criptografia*. 2015. Disponível em: https://www.ime.unicamp.br/~marcia/AlgebraLinear/aplicacao_criptografia.html. Acesso em: 28 nov. 2025.