UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS APLICADAS E EDUCAÇÃO
DEPARTAMENTO DE CIÊNCIAS EXATAS
CURSO DE LICENCIATURA EM MATEMÁTICA

Letícia Correia Alexandre da Costa

Cifras de Hill: A utilização da Álgebra Linear em Sistemas Criptográficos

Rio Tinto – PB
2022

Letícia Correia Alexandre da Costa

Cifras de Hill: A utilização da Álgebra Linear em Sistemas Criptográficos

Trabalho Monográfico apresentado à Coordenação do Curso de Licenciatura em Matemática como requisito parcial para obtenção do título de Licenciado em Matemática.

Orientador(a): Prof. Dr. Carlos Alberto Gomes de Almeida

Rio Tinto – PB
2022

Catalogação na publicação
Seção de Catalogação e Classificação

C838c Costa, Leticia Correia Alexandre da.
Cifras de Hill: A utilização da álgebra linear em sistemas criptográficos / Leticia Correia Alexandre da Costa. - Rio Tinto, 2022.
35 f. : il.

Orientação: Carlos Alberto Gomes de Almeida.
TCC (Graduação) - UFPB/CCAE.

1. Álgebra Linear. 2. Lester S. Hill. 3. Cifras de Hill. I. Gomes de Almeida, Carlos Alberto. II. Título.

UFPB/CCAE CDU 512.64

Elaborado por CATIA CRISTINA DA SILVA COSTA - CRB-15/837

Letícia Correia Alexandre da Costa

Cifras de Hill: A utilização da Álgebra Linear em Sistemas Criptográficos

Trabalho Monográfico apresentado à Coordenação do Curso de Licenciatura em Matemática como requisito parcial para obtenção do título de Licenciado em Matemática.

Orientador(a): Prof. Dr. Carlos Alberto Gomes de Almeida

Aprovado em: 15 /12/2022

BANCA EXAMINADORA

_____

Prof. Dr. Carlos Alberto Gomes de Almeida (Orientador) – UFPB/DCX

_____

Prof. Dr. José Laudelino de Menezes Neto – UFPB/DCX

_____

Prof. Ma. Agnes Liliane Lima Soares de Santana – UFPB/DCX

Dedicatória

A minha avó materna Maria Correia de Sousa *(em memória).*

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela força e pelas bençõe para que me permitiram chegar até aqui.

À minha mãe, Ana Lucia, que sempre buscou o melhor para seus filhos e sempre estava apoiando todos nós, mesmo diante das dificuldades ela não desistia. Ao pai, Severino, que fez perguntava como estava indo as coisas e sempre fala da filha com orgulho.

Aos meus irmãos, Thais e Pedro Afonso, que me faziam rir no momento que eu queria desistir de tudo, as brincadeiras, os filmes e as series ao lado deles se tornavam engraçadas e ajudavam a esquecer os problemas.

Aos meus avôs, Francisco e Pedro, não pude conhece-los mas espero que eles tenham orgulho de mim. À minha avó paterna, Aorora, que sempre pergunta como estou e como está a faculdade, mesmo que ela nem lembre disso as vezes. À minha avó, Maria (em memória), aquela sempre perguntava como estava indo o TCC, mesmo sem entender ela achava legal, ela não pode chegar a ver a versão final, mas onde quer que esteja, ela verá.

Aos meus professores da UFPB, pois foram eles os responsáveis por ensinar tudo que aprendi, um destaque especial ao meu orientador, Carlos Alberto, pela confiança e por ter aceitado entrar nessa aventura do mundo criptográfico, só tenho a agradecer.

Ao meu Quarteto Fantástico, Ana Carolina, Luana e Lucas, sem vocês não seria nada fácil enfrentar esses anos todos na UF, apoiávamos uns nos outros e olha onde isso trouxe cada um de nós.

Ao pessoal do ônibus: Ana Carolina, Daniel, Isleny, Wellington, Laura, Maria Thays, Daiane e Francielly, sem vocês as idas até a UFPB seria entediante, as músicas e conversas ajudavam muito.

Aos meus colegas de classe, que começaram com muitos e ficamos só alguns mas isso unia a turma em várias maneiras, só tenho a gradecer a todos vocês.

Aqueles que ajudaram indiretamente, muito obrigado, sem vocês eu não conseguiria.

Uma criptografia robusta é capaz de resistir a uma aplicação ilimitada de violência. Nenhuma força repressora poderá resolver uma equação matemática.

Julian Assange

RESUMO

O Trabalho de TCC a seguir, tem como objetivo, apresentar como funciona as Cifras de Hill, como elas foram criadas, além da sua necessidade de ser utilizada, ressaltando que utilizaremos as aplicações seguindo as diretrizes da Álgebra Linear tanto para codificar, quanto para decodificar uma mensagem, apresentando o seu contexto histórico e quem foi Lester S. Hill, citando os seu feitos, mais a frente falaremos sobre as aplicações de Hill numa mensagem e apresentaremos um motivo do qual as Cifra Hill possui uma certa dificuldade na hora de decifra-la.

Palavras-chave: Álgebra Linear. Lester S. Hill. Cifras de Hill.

ABSTRACT

The following TCC Work aims to present how the Hill Ciphers work, how they were created, in addition to their need to be used, emphasizing that we will use the applications following the guidelines of Linear Algebra both to encode and to decode a message, presenting its historical context and who Lester S. Hill was, citing his accomplishments, later on we will talk about Hill's applications in a message and present a reason why the Hill Cipher has a certain difficulty when deciphering it. there.

Keywords: Linear Algebra. Lester S. Hill. Hill Ciphers.

SUMÁRIO

Introdução

Quando optamos por manter nossas vidas privadas, gostamos de pensar que não queremos ninguém se intrometendo nos nossos assuntos pessoais. Pensando nisso, a humanidade buscou uma maneira de "camuflar" seus segredos importantes. Não importava como, a verdade era que segredos não podiam ser revelados.

Mas como guardar essas informações preciosas, sendo que, apenas o remente e a pessoa que irá receber sejam os únicos que saibam como decifra-la?

Pensando nisso, grandes influenciadores de suas épocas criaram diversas maneiras de manterem os seus segredos salvos entre eles mesmos. Com o passar dos anos, matemáticos e cientistas buscavam novas maneiras de manter os segredos salvos. Com a Primeira Guerra Mundial, parecia evidente a necessidade de manter sigilo entre os seus aliados e com o surgimento da Segunda Guerra Mundial, ficou mais que claro. Nesse momento da história mundial, o segredo se torna tão importante quanto as batalhas travadas entre os rivais. O uso da matemática aparece com o intuito de melhorar o segredo das mensagens e descobrir os segredos rivais. A Álgebra se faz presente, pois devido ao grau de complexidade que os cálculos pediam, ela se torna fundamental para a construção de computadores que iriam criptografar mensagens inimigas.

A Álgebra Linear pode ser utilizada em alguns métodos criptográficos, como as Cifras de Hill que apresentaremos nesse trabalho. Quando unida com a Teoria dos Números, ela é capaz de auxiliar nas estruturas dos programas que mantém os sigilos de informações e mensagens de toda uma população. O nosso principal objetivo é apresentar um método de criptografar mensagens utilizando as Cifras de Hill através das diretrizes da Álgebra Linear, descrevendo a importância da criptografia no contexto histórico assim como a de Lester S. Hill. Mostraremos a utilização da Álgebra Linear e como ela influenciou a criptografia. Utilizaremos as Cifras de Hill na codificação e decodificação de mensagens.

No primeiro capítulo, iremos abordar a história da criptografia e o seu desenvolvimento com os anos. No segundo capítulo, abordaremos o criador das Cifras de Hill, Lester S Hill e seus feitos enquanto estava vivo, no terceiro capítulo, será abordado como iremos realizar a criptografia das mensagens segundo as diretrizes que Hill nos propõe e no capítulo 4 comentamos sobre as criptografias atuais e como elas funcionam.

1 - Histórico da Criptografia

1.1 – O que é Criptografia?

Criptografia é a área de estudo que envolve conjuntos de técnicas com o objetivo de ocultar uma mensagem. Entretanto, a criptografia também refere-se à construção e a análise de dados permitindo que os segredos fiquem a salvos do público. Matsumoto (2014, p.4) diz que "desde quando o homem se organizou para viver em grupo, ele sentiu a necessidade de guardar informações. [...] Sejam segredos individuais ou coletivos." A criptografia surgiu tendo como intuito o "secreto" – guardar as nossas informações, segredos, tudo que consideramos valioso – sendo assim, os inimigos não devem descobrir o que queremos manter guardado.

Dentro disso, a criptografia possui um objetivo de transformar um texto qualquer, num texto cifrado para que assim ele possa ser decifrado pelo portador da chave decodificadora.

Diferentes tipos de cifras fazem parte da criptografia, entre elas estão as cifras simétricas e cifras assimétricas. As cifras simétricas utilizam a mesma chave tanto para codificar quanto para decodificar, isso resulta em resultados mais rápidos e uteis mas possuem menos segurança justamente por utilizarem a mesma chave, já cifras assimétricas utilizam dois tipos de chave, neste caso, uma chave que conhecemos, pois é pública, utilizamos ela para codificar a mensagem, enquanto isso, a sua segunda chave é secreta e quem a possui é o receptor da mensagem, sendo assim, apenas ele pode decodificar a mensagem. Nas cifras assimétricas, encontramos uma forte influência da Álgebra Linear e da Teoria dos Números, pois suas aplicações ajudam nessa área de estudo que é criptografia.

1.2 – Antiga História da Criptografia

A palavra criptografia vem do grego Kryptós, que significa secreto, para a criptografia isso seria escrever uma mensagem ou código de uma maneira ao qual o receptor e remetente são os únicos capazes de decifrá-la. Resumindo, a criptografia é a uma ferramenta capaz de codificar e decodifica mensagens. Singh (2003, p.12) diz que a "A história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de código e os decifradores, uma corrida armamentista intelectual que teve um forte impacto na história humana". Com essa citação, podemos descrever o uso da criptografia em algumas situações.

Por volta de 4000 a.C., os egípcios já faziam uso da criptografia em alguns de seus hieróglifos. Há registros que mostram que os espartanos (século V a.C.) usavam esse método

para esconder fatos. O Imperador Romano Júlio César (100-44 a.C.), usava desse conhecimento para esconder os acontecimentos em Roma e enviava mensagens codificadas a seus aliados, ao qual, apenas quem recebia podia entender a mensagem. Esta cifra é chamada atualmente de "Cifra de César", a qual consistiu em trocar uma letra do alfabeto por uma que estava 3 casas a frente, ou seja, a letra A seria substituída pela letra D. Entretanto, essa cifra podia ser decifrada facilmente se um inimigo receber e observar o padrão que Júlio César utilizava.

O uso da criptografia foi bastante importante no cenário histórico, principalmente quando falamos sobre guerras. No decorrer da história da humanidade, passamos por conflitos, guerras, pandemias entre outras coisas. Quando não tínhamos a tecnologia a nosso favor, as mensagens enviadas por grandes potências de sua época, como por exemplo da Roma antiga para o antigo Egito, eram escritas de formas criptográficas, no qual, apenas o portador da chave decodificadora poderia traduzir a mensagem. No século passado, um dos responsáveis pela criação de um computador foi o matemático Alan Turing (1912-1954) que auxiliou na "quebra" de mensagens que os alemães usavam, assim os cálculos matemáticos ajudaram a decifrar a a criptografia da máquina conhecida como Enigma.

Utilizar estratégias em combate é essencial quando se quer vencer uma simples batalha ou uma Grande Guerra, se pensarmos que muitos usavam mais o corpo do que a mente. Com o passar dos anos, o ser humano percebeu que a melhor maneira de vencer conflitos políticos é utilizando de estratégias que o favoreciam. Segundo Bruno (2017, p.1) "a estratégia está diretamente ligada a um importante componente: a informação. [...] a troca de informação é vital para coordenar exércitos". Se pararmos para pensar, o método de comunicação tinha suas limitações por causa da grande distância entre um país e outro, independentemente se falamos do antigo Egito ou do povo da Pérsia, o que dificultava bastante enviar uma mensagem simples, e ainda tinha a chance dessa mensagem chegar a mãos inimigas, o que seria pior ainda. Então, qual estratégia foi utilizada para esconder essas mensagens? Isso vai depender de qual povo antigo estamos falando. Em alguns casos, o mensageiro nem sabia que mensagem estava transportando, enquanto os Espartanos, na Grécia Antiga, usavam o Bastão de Licurgo. Para ler a mensagem nesse bastão, era necessário enrolar a tira no bastão que vinha enrolada na forma espiral junto com o bastão. Este método foi um dos primeiros sistemas de criptografia, apesar de alguns estudiosos acreditarem que não se passa de um mito.

Vários matemáticos e cientistas foram importantes quando falamos na construção de sistemas criptográficos que utilizamos para manter a nossa privacidade no mundo virtual. Antes da tecnologia avançar para a situação atual a qual a conhecemos, os cálculos eram feitos de

forma escrita para evitar que vazassem informações. Neste momento, os cientistas matemáticos se tornam importantes para o desenvolvimento e para a criação desses códigos e algoritmos. A busca por informações se torna mais necessária no momento em que a Segunda Grande Guerra já havia iniciado. Como o ataque a Pearl Harbor, os Estados Unidos optam por contra-atacar o Japão com as bombas atômicas em Hiroshima e Nagasaki, causando assim o desfecho da Segunda Grande Guerra.

Sobre as guerras e os matemáticos, Singh fala que:

> Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, que a Segunda Guerra Mundial foi a guerra dos físicos devido à bomba atômica. De modo semelhante se fala que uma Terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não nos surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos. (SINGH, 2003, p.13)

Com o uso da Matemática, é possível observar a complexidade desses cálculos. Suas estruturas algébricas são utilizadas para melhorar a segurança, pode ser usado operações fáceis com conjuntos numéricos, porém em outros pontos, podem ter uma complexidade maior em seus cálculos.

Dentre vários métodos de codificação, o uso de matrizes está presente em equações que podem ser utilizadas na codificação de uma mensagem. Quando utilizamos as matrizes, usamos processos de multiplicação entre matrizes, para codificar utilizamos uma matriz A, e para decodificar utilizamos a inversa de A. Nesse ponto podemos calcular a inversa de duas maneiras: usando Sistemas Lineares ou através da Eliminação Gaussiana, isso quando trabalhamos com os números reais e através da inversa de A pelo grupo fechado em Z_n, o qual será apresentado neste trabalho.

Nesse momento a Álgebra se faz presente para a utilização no processo de codificação e decodificação, principalmente a Álgebra Linear que por muitos é considerada bem abstrata, entretanto ela se faz presente em sistemas computacionais que usam sistemas criptográficos para preservar a sua segurança.

Com a utilização da Álgebra Linear para a criptografia, um método se destaca que são as Cifras de Hill. As Cifras de Hill foram criadas por Lester S. Hill em 1929, esta cifra se encaixa nas cifras de substituição em bloco, se baseiam na Álgebra Linear e podem ser

quebradas utilizando também a Álgebra Linear. Este método de codificação é um método antigo com ênfase a transformações lineares e congruência.

1.3 – Vida e Obra de Lester S. Hill

Nascido no dia 18 de Janeiro de 1891 na cidade de Nova York nos Estados Unidos, Lester S. Hill foi um matemático e educador norte-americano. Aos 20 anos formou na Universidade de Columbia e anos depois conseguiu o seu PHD pela Universidade de Yale. Hill dedicou sua vida ao ensino da Matemática, lecionando em escolas estadunidense e em Universidade como a Princeton e Yale.

Durante a Segunda Guerra Mundial, Hill esteve envolvido com as forças armadas estadunidense com o intuito de codificar mensagens entre os Aliados. Seus esforços foram muito elogiados pelo Governo Norte americano devido aos seus resultados em relações as cifras e aos códigos algébricos que foram utilizados antes e durante o decorrer na Segunda Grande Guerra pelo Exército Estadunidense.

Figura1.1: Lester S. Hill em 1956

Fonte: Murray Eisenberg [8]

Devido a seu grande interesse em desenvolver aplicações da matemática avançada nos sistemas de comunicações, Hill desenvolveu vários métodos de decodificar as comunicações. Lester S. Hill possui uma notável influência sobre a criptografia, a arte de codificar e decodificar códigos.

Na área da Matemática existem vários tipos de criptografia, entretanto falaremos sobre as Cifras de Hill, criadas por Lester S. Hill (1891-1961) e publicadas em 1929 e 1931 chamadas respectivamente: “Cryptography in the Algebraic Alphabet” e ”Concerning Certain Linear Transformation Apparatus of Cryptography”. Em seus trabalhos, Hill aborda um Sistema

Poligráfico que é um sistema criptográfico no qual o texto a ser criptografado é dividido em conjuntos de n letras, no qual cada um desse conjuntos será substituído por um conjunto diferente de letras cifradas.

Este tipo de criptografia aborda o uso de matrizes em suas resoluções através de multiplicação e cálculo de matriz inversa para realizar a decodificação, em alguns casos pode-se usar módulo, além do uso de transformação e independência linear. Esse campo de investigação é voltado para os estudantes de Álgebra Linear que tem como propósito mostrar as contribuições da Matemática para o avanço dessa ciência que hoje conhecemos como criptografia. Entretanto, é possível trazer os cálculos dos computadores para essas equações já mencionadas para o que muitos chamam de criptografia matemática.

Em 9 de Janeiro de 1961 na cidade Nova York, Lester S. Hill faleceu 70 anos de causa desconhecida. Suas obras possuem uma certa complexidade por envolverem algo abstrato e beleza, sobre isso o filosofo e matemático Bertrand Russell (1872-1970) diz que "A matemática, vista corretamente, possui não apenas verdade, mas também uma beleza suprema – uma beleza fria e austera, como a de uma escultura.", com isso ele diz que a matemática é bela pois ela não mente e com isso acabamos ficando encantados com essa ferramenta de auxílio.

2.1 FUNDAMENTAÇÃO TEÓRICA

A partir deste ponto, apresentaremos a ideia fundamental no qual a pesquisa será baseada, logo usaremos Singh, Anton e Rorres e Eisenberg como os principais no referencial teórico da pesquisa. Será mostrado como cada um deles se faz presente na construção da pesquisa e sua relação com ela.

A importância de esconder segredos sempre foi necessária, pois contém a intenção de proteger quem envia e quem recebe a mensagem. O autor ainda fala que do ponto de vista da história, a criptografia é precedida pela esteganografia, que consiste na ocultação da mensagem enquanto a criptografia altera a forma da mensagem, ocultando assim o seu significado.

É descrito por Simon Singh (2003) que o empenho dos criptógrafos e criptoanalistas ao longo de anos em busca de um código mais e mais difícil de ser "quebrado" e qual a melhor estratégia a ser utilizada. O autor ainda compara os códigos com as bactérias e seus decifradores com os antibióticos, pois o fortalecimento de um leva ao fortalecimento do outro, criando assim um ciclo sem fim.

Ainda em sua obra, Singh (2003) fala da importância da cifra e como uma cifra fraca é pior do que não contém nenhum tipo de cifra para a proteção. Como exemplo, ele nos mostra a condenação e execução da Rainha da Escócia, Mary Stuart, em 1587. Em seu livro ele diz:

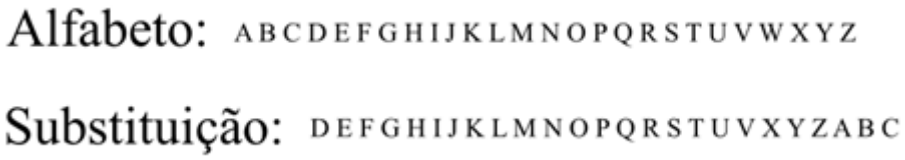
> A correspondência que ela trocava com seus seguidores, que conspiravam para a morte de sua prima, a Rainha Elizabeth, e sua posterior ascensão ao trono da Inglaterra, foi interceptada e corretamente decifrada pelo secretário de segurança do palácio e chefe da espionagem inglesa, Sir Francis Walsingham. (SINGH, 2003, p.13)

A área da Matemática é bastante utilizada na construção de sistemas computacionais, nela encontramos subáreas que auxiliam na construção de sistemas criptográficos. No caso da criptografia, podemos trabalhar com duas: Teoria dos Números e Álgebra Linear, mas o matemático Lester S. Hill (1891- 1961) desenvolveu uma cifra que utilizava apenas a Álgebra Linear, essas cifras são conhecidas como Cifras de Hill.

Em sua obra, Anton e Rorres (2012) dizem e explicam processos de cifrar uma mensagem. Eles explicam que este estudo é chamado de criptografia, os códigos são chamados de cifras e seus textos são chamados de criptogramas. O primeiro exemplo citado é a cifra de

substituição que acaba sendo chamada de Cifra de César por causa do Imperador Romano Júlio César (100 - 44 a.C), devido a sua grande utilização durante o tempo em que esteve no comando do Império Romano. A figura abaixo mostra como seria feita a substituição baseada no método de César.

Figura 2: Cifra de César



Fonte: Criada pela autora

É possível observar que a letra A acaba sendo substituída pela letra D, ou seja, três letras à sua frente no alfabeto e assim sucessivamente. O exemplo que Anton e Horres (2012) citam é 'ROMA NÃO FOI CONSTRUÍDA EM UM DIA' com a utilização das Cifras de César fica 'URPD QRD IRL FRQVWUXLGD HP XP GLD'. Eles dizem que é fácil de decifrar esta cifra, pois é uma questão de observar os padrões que ela tem e assim fica fácil de descobrir o método utilizado.

A partir desse ponto, tanto Anton e Rorres (2012) quanto Eisenberg (1998) descrevem como utilizar o sistema poligráfico de Hill. As cifras de Hill constituem na utilização da Álgebra especificamente, a Álgebra Linear. Eisenberg (1998) se refere a esta cifra como uma cifra de difícil decifração se a pessoa que tentar decifrá-la não tiver um conhecimento prévio de Álgebra Linear ou o auxílio de um computador para a sua decodificação.

Tanto Eisenberg (1998) quanto Anton e Rorres (2012) utilizam matrizes, porém elas possuem ordem diferentes, neste momento iremos trabalhar com uma matriz de ordem 2X2.

Para realizar a codificação deve se seguir os seguintes passos:

Passo 1: Escolhemos uma matriz de ordem quadrada (A) para realizar a codificação.

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Passo 2: Agrupamos o texto que será utilizado em pares ordenados, caso ocorra de a quantidade ser ímpar, deve-se dobrar a última letra, contanto que não altere o sentido do texto.

Passo 3: Montaremos cada par ordenado de letras ficará na forma de uma matriz coluna

que chamaremos de p. Sendo p um vetor normal, logo a multiplicação de Ap será o vetor cifrado.

Passo 4: Converteremos o vetor cifrado ao seu equivalente no alfabeto. Por exemplo: se os números cifrados forem 5 e 8, as letras correspondentes no alfabeto serão E e H.

O método mais utilizado pelas cifras de Hill é com uma matriz de ordem 2X2, entretanto é possível trabalhar com uma matriz de ordem 3 como mostra Eisenberg (1998).

É provável que em algum momento dos cálculos acabe surgindo um número maior que 26 que é a quantidade de letras que temos no alfabeto. Quando isso ocorrer trabalharemos com a Aritmética Modular, já que ela trabalha com os restos de uma divisão matemática tendo bastante importância em criptografia.

Na Aritmética Modular temos um número positivo que chamaremos de módulo (m) o qual o usaremos para realizar a divisão e o seu resto é a nossa resposta. A definição formal de módulo está logo abaixo.

Definição: Dados um número inteiro positivo m e dois inteiros a e b quaisquer, dizemos que a é equivalente a b módulo m, e escrevemos:

$$a=b \bmod.(m)$$

se a-b for um múltiplo inteiro de m.

Para a decodificação de uma mensagem, Hill utiliza dois métodos para encontrar a chave decodificadora. Ambas irão envolver cálculos para encontrar a matriz inversa de A.

1º método (através dos grupos dos Reais): através do conhecimento prévio obtido no ensino médio como a utilização de equações ou com o método da substituição. Temos a matriz quadrada A de ordem n, para descobrir a sua inversa usaremos uma matriz quadrada B com variáveis a, b, e assim adiante, tal que a multiplicação entre eles terá como resultado uma matriz identidade de ordem n, então B será a inversa de A ou através da Eliminação Gaussiana, que os estudantes de Álgebra Linear conhecem mais como escalonamento. Este método consiste em transformar o sistema de matrizes em uma matriz estendida do sistema em uma matriz triangular (matriz escalonada).

2º método (pelo método de Hill): através de um grupo fechado em Z_n onde utilizaremos uma fórmula diferente para encontrarmos a inversa de A.

Após encontrar a matriz inversa a usaremos do mesmo modo que foi na codificação.

Multiplicaremos a chave decodificadora (matriz inversa de A) como os pares ordenados codificados. Se necessário, usaremos Aritmética Modular. Desse modo teremos a mensagem decodificada.

3 – Matrizes e Cifras de Hill

A utilização de matrizes se relaciona com o contexto número, com o objetivo de apresentar um certo dado estatístico ou mostra a sua importância quando falamos sobre o desenvolvimento de programas computacionais, pois eles possuem a habilidade de manipular as tabelas com as informações numéricas.

Podemos ver as matrizes como objetos matemáticos vivos devido a sua bela teoria e importância que associamos a elas que possuem uma grande variação de aplicações. Na criptografia, utilizaremos as matrizes como objetivo de codificação e decodificação através de seus sistemas polinomiais, eliminação gaussiana, módulo e houver necessidade, sistemas lineares.

Podemos trabalhar com matrizes de ordem 2X2 ou 3X3, vale ressaltar que a matriz chave deve ser de ordem quadrática – possuir a mesma quantidade de linhas e colunas – pois desta maneira descreve Lester S Hill.

Para realizarmos a codificação e decodificação seguiremos alguns passos para que assim ela possa ser realizada.

3.1 - Codificação de Mensagens

Hill utilizou da ideia inicial a respeito da criação de tabelas, portanto para este trabalho utilizaremos 26 números que corresponderão as letras do alfabeto sem o acréscimo de sinais de pontuação e traços para o espaço, se houver necessidade, dobraremos a última letra da mensagem contanto que a frase ou texto não perca sentindo.

Para a criação da tabela de letras usaremos o módulo, neste caso o modulo 26 conforme as tabelas abaixo demonstrarão:

Tabela 1: Tabela de Correspondência 1

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	2	3	4	5	6	7	8	9	10	11	12	13

Tabela 2: Tabela de Correspondência 2

N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

14	15	16	17	18	19	20	21	22	23	24	25	0

Para codificar as mensagens seguiremos alguns procedimentos, vale ressaltar que a codificação e decodificação pelo método de Hill utiliza sistemas de matrizes que segue as diretrizes da Álgebra Linear, portanto é necessário compreender os seus conceitos básicos que remetem a Álgebra Linear.

3.2 - Matriz Quadrada

Para ser a chave codificadora e decodificadora a matriz deve ter ordem quadrada e ser inversível, ou seja, possuir o mesmo número de linhas e colunas. Para simplificar os cálculos, usaremos uma matriz de ordem 2x2, que possua como sua inversa uma matriz de com números inteiros.

$$A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{vmatrix} 1 & 2 \\ 0 & 3 \end{vmatrix}$$

A matriz que usaremos para codificar as nossas mensagens será denominada de A. A qual utilizaremos durante todo o processo para realizar a codificação e decodificação.

3.3 - Matriz Inversa

Depois que a mensagem for criptografada e for enviada para o remetente, a mensagem passará pelo processo de decifrada pelo receptor da mensagem. Para isso, será necessário que ele possua a matriz inversa de A, pois somente ela poderá decifrar a mensagem. Muitos matemáticos acreditam que por esse motivo as Cifras de Hill possui uma certa dificuldade pois apenas a inversa de sua matriz codificadora poderá decodificar qualquer mensagem que for codificada por ela.

Para encontrarmos a matriz inversa, usaremos a Eliminação Gaussiana para encontrar a matriz A^{-1}. Lembrando que ela só pode ser usada se trabalharmos com o conjunto dos números Reais.

$$\text{Det A} = \begin{vmatrix} 1 & 2 \\ 0 & 3 \end{vmatrix}$$

Antes, precisamos saber se matriz A possui determinante ≠ 0, pois se ela tiver, então ela pode ter sua inversa calculada. Para isso o seu determinante deve ser ≠ 0.

Para realizar o cálculo do determinante usaremos a seguinte formula:

$$\text{Det A} = a_{11} \,.\, a_{22} - a_{12} \,.\, a_{21}$$

Logo a nossa equação ficará da seguinte maneira:

$$\text{Det A} = 1 \,.\, 3 - 2 \,.\, 0 = 5 - 6 = 3$$

Portanto, o determinante da nossa matriz A é 3. Agora que possuímos essa informação, podemos iniciar o processo de codificação e decodificação.

Primeiro, escreveremos a matriz de forma aumentada, com uma matriz identidade ao seu lado.

$$\text{A} = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$$

Com a matriz aumentada, iremos encontrar o pivô que vai estar na primeira coluna na primeira linha e igualar ele a 1. Entretanto, o nosso pivô já é o número 1 e o seu número que seria necessário zerar já é 0, então buscaremos o pivô da próxima coluna.

Para que isso ocorra, iremos dividir a segunda linha por 3, ou seja:

$$\text{A} = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \qquad \rightarrow L_2 = {}^{L_2}/_{3} \rightarrow \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{matrix} 1 & 0 \\ 0 & {}^{1}/_{3} \end{matrix}$$

Agora, iremos zera o 2 que está na primeira linha. Subtraindo ele por duas vezes a segunda linha. Então, teremos:

$$\rightarrow L_1 = L_1 - 2 \,.\, L_2 \quad \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{matrix} 1 & {}^{-2}/_{3} \\ 0 & {}^{1}/_{3} \end{matrix}$$

Com o pivô da segunda linha encontrado, eliminaremos a segunda coluna por completo subtraindo por duas vezes o valor da segunda linha. Portanto, iremos ter:

$$\rightarrow L_1 = L_1 - 2\,.\,L_2 \qquad \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{matrix} -5 & 2 \\ 3 & -1 \end{matrix}$$

Logo, a nossa matriz inversa de A será:

$$A^{-1} = \begin{pmatrix} 1 & -2/3 \\ 0 & 1/3 \end{pmatrix}$$

Com a nossa matriz inversa calculada, podemos iniciar os processos para codificar e decodificar uma mensagem.

3.4 – Codificando uma mensagem.

Quando falamos de codificar uma mensagem, podemos utilizar diversas maneiras, entretanto as Cifras de Hill consiste basicamente num sistema em que podemos utilizar principalmente a multiplicação de matrizes.

Para codificar uma mensagem é necessário seguir alguns passos:

Primeiro iremos escolher a nossa matriz A de ordem quadrática. Em seguida, agruparemos as letras em pares ordenados, se ocorrer do último par no ficar completo, dobraremos a última letra contanto que a frase não irá perder o seu sentido original. Após essas etapas, cada letra será substituída por seu valor numérico correspondente – seguindo as tabelas de referências já apresentadas – logo realizaremos as operações necessárias para realizar a codificação.

Para apresentar o que foi descrito acima, usaremos a seguinte frase:

O TCC NÃO SE FAZ SOZINHO

Se ordenamos essa frase em pares ordenados teremos:

OT CC NÃ OS EF AZ SO ZI NH OO

É possível observar que a frase possui letras impares, neste caso, foi necessário dobrar a última letra para que todos tivessem o seu par. Também é possível observar que a frase não perdeu o sentido por causa disso.

Utilizando as tabelas de referências, iremos substituir cada letra por seu número correspondente.

O	T	C	C	N	Ã	O	S	E	F	A	Z	S	O	Z	I	N	H	O
15	20	3	3	14	1	15	19	5	6	1	0	19	15	0	9	14	8	15

Agora que cada letra possui o seu número correspondente, iremos realizar a parte de codificar a mensagem. Para isso iremos realizar uma multiplicação de matrizes, ou seja, multiplicaremos as linhas pelas colunas. Se o nosso resultado for maior que 26, então usaremos o modulo.

Então, calcula-se:

$$OT = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 20 \end{bmatrix} = \begin{bmatrix} 55 \\ 60 \end{bmatrix}$$

$$CC = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 9 \\ 9 \end{bmatrix}$$

$$NA = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 1 \end{bmatrix} = \begin{bmatrix} 16 \\ 3 \end{bmatrix}$$

$$OS = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 19 \end{bmatrix} = \begin{bmatrix} 53 \\ 57 \end{bmatrix}$$

$$EF = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 6 \end{bmatrix} = \begin{bmatrix} 17 \\ 18 \end{bmatrix}$$

$$AZ = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$SO = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 15 \end{bmatrix} = \begin{bmatrix} 49 \\ 15 \end{bmatrix}$$

$$ZI = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 9 \end{bmatrix} = \begin{bmatrix} 18 \\ 27 \end{bmatrix}$$

$$NH = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} . \begin{bmatrix} 14 \\ 8 \end{bmatrix} = \begin{bmatrix} 30 \\ 24 \end{bmatrix}$$

$$OO = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} . \begin{bmatrix} 15 \\ 15 \end{bmatrix} = \begin{bmatrix} 45 \\ 45 \end{bmatrix}$$

Como é possível observar, alguns números estão maiores que 26, neste caso usaremos a aritmética modular para simplificar esses números pelos seus correspondentes nas tabelas de referências, ou seja, usaremos o resto das divisões desses números pelo 26 para assim obter uma equivalência.

55 mod 26 = 3
60 mod 26 = 8
53 mod 26 = 1
57 mod 26 = 5
27 mod 26 = 1
30 mod 26 = 4
45 mod 26 = 19
49 mod 26 = 23

Sendo assim, temos os nosso números de pares ordenados da seguinte maneira:

3 8 9 9 16 3 1 5 17 18 1 0 23 15 18 1 4 24 19 19

Portanto, só nos resta substituir os números que conseguimos pelo seu correspondente nas tabelas:

3	8	9	9	16	3	1	5	17	18	1	0	23	15	18	1	4	24	19	19
C	H	I	I	P	C	A	E	Q	R	A	Z	W	O	R	A	D	X	S	S

Logo, a mensagem a ser transmitida seria CHIIPCAEQRAZWORADXSS.

3.5 – A inversa de A pelo método de Hill

Como Hill trabalha com um sistema em $\mathbb{Z}_m$, sendo esse m o valor de 26, visto que é correspondente a quantidade de letras do alfabeto. Portanto, o nosso conjunto $\mathbb{Z}_m$ será:

$$\mathbb{Z}_{26} = \{ 0, 1, 2, 3, 4, \ldots, 25\}$$

Com isso a nossa matriz inversa tem que respeitar a seguinte associação:

$$A \cdot B = B \cdot A = I_{\mathbb{Z}_{26}} ; = I_{\mathbb{Z}_{26}} = I \pmod{26}$$

Isso é proposto devido à complexidade que Hill utilizou em seu método criptográfico. Por esta trabalhando com um grupo fechado em $\mathbb{Z}_{26}$, isso permite com que possua uma dificuldade em suas resoluções, por isso, muitos matemáticos consideram esta cifra difícil de decodificada, pois se a pessoa que tentar codifica-la não possuir um conhecimento prévio, não irá conseguir fazer a resolução pois a sua inversa – que é necessária para a decodificação – possui uma formula única voltada para o grupo dos números inteiros. Isso fica mais claro com a seguinte definição:

Definição: Dado um número α em $\mathbb{Z}_m$, dizemos que um número α^{-1} em $\mathbb{Z}_m$ é um recíproco, ou inverso multiplicativo, de α módulo m se $\alpha\alpha^{-1} = \alpha^{-1}\,\alpha = 1 \pmod{m}$.

Sendo assim, a e m não podem possuir fatores primos em comum, desde modo, os múltiplos de 26 também não considerados.

Com a definição acima, podemos encontrar o inverso multiplicativo pelo módulo de m. Como estamos trabalhando com um grupo fechado em $\mathbb{Z}_{26}$, podemos ir substituindo número por número para encontrar o inverso multiplicativo. Usaremos o det (A) = 3 para encontramos o mesmo.

Iremos atribuir alguns valores para encontramos o inverso multiplicativo. Primeiro usaremos o número 9.

$$3x = 1 \pmod{26}$$
$$3 \cdot 9 = 1 \pmod{26}$$
$$3 \cdot 9 = 27 = 1 \pmod{26}$$
$$3^{-1} = 9 \pmod{26}$$

Logo, 9 é o inverso multiplicativo de 3 no grupo $\mathbb{Z}_{26}$. Não será necessário aprofundar-

se mais nessa parte pois estamos trabalhando com um grupo fechado quando vamos além disso já estamos entrando numa definição da Álgebra Abstrata, por isso podemos consultar o quadro abaixo que irá mostrar os inversos multiplicativos pelo módulo 26.

a	1	3	5	7	9	11	...
a^{-1}	1	9	21	15	3	19	...

Com isso em mãos, podemos calcular a inversa de A (mod 26), utilizando o inverso multiplicativo que vai multiplicar a matriz adjunta de A pelo módulo 26. A formula do inversa fica da seguinte maneira:

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (mod\ 26)$$

Agora iremos substituir os valores na formula.

$$A^{-1} = 9 \begin{bmatrix} 3 & -2 \\ 0 & 1 \end{bmatrix} (mod\ 26)$$

Agora, multiplicaremos o 9 pela matriz adjunta, se algum número ficar maior que 26, usaremos a Aritmética Modular para que ele fique dentro das regras.

$$A^{-1} = \begin{bmatrix} 27 & -18 \\ 0 & 9 \end{bmatrix} (mod\ 26)$$
$$A^{-1} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} (mod\ 26)$$

Agora que temos a nossa matriz inversa pelo módulo 26, podemos dar início ao processo de decodificação da mensagem.

3.6 – Decodificando uma mensagem

Agora, como já temos a nossa matriz inversa, iremos realizar os mesmos passos da codificação para realizar a decodificação.

O nosso texto cifrado será dividido em pares ordenados e terá como valores os seus correspondentes na tabela:

CH	II	PC	AE	QR	AZ	WO	RA	DX	SS
3 8	9 9	16 3	1 5	17 18	1 0	23 15	18 1	4 24	19 19

Sendo assim, para obter a mensagem que originalmente foi escrita, iremos multiplicar os vetores acima pela matriz inversa. Portanto, teremos:

$$\text{CH} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 8 \end{bmatrix} = \begin{bmatrix} -141 \\ 72 \end{bmatrix}$$

$$\text{II} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 9 \\ 9 \end{bmatrix} = \begin{bmatrix} -153 \\ 81 \end{bmatrix}$$

$$\text{PC} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 16 \\ 3 \end{bmatrix} = \begin{bmatrix} -38 \\ 27 \end{bmatrix}$$

$$\text{AE} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 5 \end{bmatrix} = \begin{bmatrix} -89 \\ 45 \end{bmatrix}$$

$$\text{QR} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ 18 \end{bmatrix} = \begin{bmatrix} -307 \\ 162 \end{bmatrix}$$

$$\text{AZ} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\text{WO} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 23 \\ 15 \end{bmatrix} = \begin{bmatrix} -247 \\ 135 \end{bmatrix}$$

$$\text{RA} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 9 \end{bmatrix}$$

$$\text{DX} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 24 \end{bmatrix} = \begin{bmatrix} -428 \\ 216 \end{bmatrix}$$

$$\text{SS} = \begin{bmatrix} 1 & -18 \\ 0 & 9 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 19 \end{bmatrix} = \begin{bmatrix} -323 \\ 171 \end{bmatrix}$$

Como é possível observar, alguns desses valores ficaram na forma negativada, com isso será necessário realizar a aritmética modular, entretanto somaremos 26 ao valores que ficarem negativos. Dado isso, temos:

$-141 \bmod 26 = -11 \rightarrow -11+26 = 15$

$-153 \bmod 26 = -23 \rightarrow -23 + 26 = 3$

$-38 \bmod 26 = -12 \rightarrow -12 + 26 = 14$

$-89 \bmod 26 = -11 \rightarrow -11+26 = 15$

$-307 \bmod 26 = -21 \rightarrow -21 + 26 = 5$

$-247 \bmod 26 = -13 \rightarrow -13+26 = 13$

$-428 \bmod 26 = -12 \rightarrow -12 + 26 = 14$

$-323 \bmod 26 = -11 \rightarrow -11 + 26 = 15$

Com a parte negativa já calculada, iremos efetuar os cálculos do valores positivos, seguindo o mesmo padrão que foi usado no processo de codificação.

$$72 \bmod 26 = 20$$
$$81 \bmod 26 = 3$$
$$27 \bmod 26 = 1$$
$$45 \bmod 26 = 19$$
$$162 \bmod 26 = 6$$
$$135 \bmod 26 = 5$$
$$216 \bmod 26 = 8$$
$$171 \bmod 26 = 15$$

Agora, com o módulo já calculado, podemos usar as tabelas de referências para relacionar os números com as letras. Sendo assim, os pares ordenados são:

15 20 3 3 14 1 15 19 5 6 1 0 13 5 0 9 14 8 15 15

Relacionando os pares com as letras teremos:

15 20	3 3	14 1	15 19	5 6	1 0	13 5	0 9	14 8	15 15
OT	CC	NA	OS	EF	AZ	SO	ZI	NH	OO

Como podemos observar, a mensagem passou a ser novamente O TCC NÃO SE FAZ SOZINHO, lembrando que a última letra pode ser descartada pois ela foi dobrada com o intuito de termos pares ordenados. E desse modo, se dá a criptografia pelo método de Hill.

3.7 – Criptografia Atual

No século XXI, a nossa privacidade se torna algo que almejamos independente do que queremos. Afinal, a nossa privacidade é o que nos permite realizar certas atividades. Como por exemplo uma pessoa que trabalha com investigações, ou uma pessoa que seja responsável por nós juridicamente. Privacidade é algo que permite aos humanos uma certa "liberdade".

Com a pandemia da Covid-19, passamos a utilizar métodos diferentes para repassar dinheiro por exemplo. O Pix se tornou uma ferramenta de troca de dinheiro rápida e eficaz, isso foi ganhando mais força com o decorrer da pandemia, pois podemos usar o smatphone para realizar este pagamento, com isso, foi necessário uma segurança maior com os nossos dados pessoais.

Os aplicativos de bancos possuem acesso aos nosso dados pessoais e é nesse momento que a criptografia entra, com o objetivo de manter nossos dados salvos e seguros. Esses tipos de criptografias possuem uma requintada matemática atrás de seu simples "click". Isso porque, são através desses cálculos que nossos dados ficam protegidos e para quebra-los requer um avançado conhecimento matemático pois estamos falando de cálculos que possuem a sua forma um pouco mais abstrata.

Os sistemas atuais possuem uma complexidade, quanto maior a quantidade de bits, maior será a quantidade de chaves necessárias para decifrar um documento ou outra coisa. Dentre os diversos tipos de criptografia, ressaltaremos algumas.

- Criptografia RC4

A criptografia RC4, também conhecida como Rivest Cipher 4, é uma cifra de fluxo criada nos anos 80. Ela opera os seus dados um byte por vez, atualmente essa cifra não é utilizada pois possuía uma fácil vulnerabilidade para ser decodificada.

- Criptografia Twofish

Esta cifra é uma evolução da Blowfish, a Twofish é uma cifra simétrica – ou seja, tanto o emissor quanto o receptor da mensagem utilizam a mesma chave – com bastante utilidade e segurança.

- Criptografia DES

DES, sigla para Data Encrytion Standard, também é uma chave simétrica, é uma das primeiras a ser criada na década de 70. Por ser uma cifra pequena, atualmente, ela é considerada insegura para algumas aplicações. Atualmente, a DES foi substituída pela AES.

- Criptografia AES

É uma das cifras mais seguras que existe atualmente, sendo utilizada pelo Governo dos Estados Unidos e também por diversos grupos de segurança. Esta cifra possui uma chave extremamente difícil de ser decifrada, por isso ataques cibernéticos não conseguem decifra-la.

- Criptografia RSA

A criptografia RSA é tipo de cifra assimétrica – ou seja, a um primeiro momento ela é privada, mas em seu modelo público pode criar uma chave, assim o seu receptor terá acesso aos seus dados – sendo ela uma das mais seguras e melhor pois utiliza o algoritmo SPN (Rede de Permutação de Substituição), que contitui em várias rodadas para criptografar os dados.

Como vimos, existem diversos tipos de sistemas criptográficos, sendo todos eles envolvidos por cálculos que irão assegurar a nossa privacidade.

4 – Considerações Finais

Com tudo que foi visto sobre a criptografia, é possível observar que a matemática possui uma certa importância quando falamos sobre a ferramenta que é a criptografia. As Cifras de Hill possuem uma certa dificuldade nesse ponto visto que usamos a Álgebra Linear para realizar a codificação e ela só pode ser desfeita pela Álgebra Linear, por isso, muitos estudiosos matemáticos ressaltam a importância dessas Cifras devido ao seu grau de complexidade. Foi possível observar que essa dificuldade está bastante relacionada a parte da decodificação, pois ela possui uma forma diferente de ser feita. Por usar Aritmética Modular, não podemos calcular a sua inversa da forma com a qual estamos habituados, foi necessário entrar brevemente na Álgebra Abstrata para compreender melhor o que se está falando. Imaginemos o quão grande seria realizar essas equações ao trabalharmos com uma matriz 3X3 ou até mesmo 5X5.

A partir desses números estaríamos entrando num mundo mais virtual, estaríamos falando de sistemas computacionais que resolveriam esses cálculos de forma rápida e praticamente instantânea. Nesse momento, vemos que a matemática, mesmo sendo bem abstrata, é essencial para a manter a nossa segurança pessoal.

As Cifras de Hill possuem uma importância histórica, pois se trata de uma cifra bastante utilizada na Segunda Grande Guerra. Hill tinha como objetivo ajudar os Estados Unidos a vencer a Alemanha Nazista. Suas cifras possuem uma certa dificuldade para se decifrar, este foi um dos motivos dela ter sido bastante utilizada. Quando essa cifra é combinada com a Teoria dos Números, pode gerar programas voltados a criptografar mensagens através de um aplicativo por exemplo.

Através da codificação e da decodificação, podemos ver que Hill utiliza a Álgebra Linear como um artificio para dificultar, principalmente, a decodificação. Pois, se um inimigo tivesse acesso a chave codificadora e calcula-se a sua inversa, ele iria obter uma mensagem decodificada de forma errada, pois as Cifras de Hill utilizam de uma formula que envolve a adjunta de A e o inverso multiplicativo do nosso modulo. Hill trabalha com um grupo fechado de 26, pois equivaliam as letras do alfabeto, logo os seus cálculos eram todos feitos de forma manual.

Existem algumas variações das Cifras de Hill que não utilizam o mesmo modo de decodificar, por isso, se tratam de inspirações feitas a partir dessa Cifra.

Com o passar dos anos, técnicas de criptografias avançadas foram criadas com o objetivo de manter a privacidade das pessoas em sigilo, com isso, o mundo foi avançando de

forma tecnológica e as formas mais arcaicas de criptografia foram ficando para trás, mas sempre fazendo parte da criptografia atual, afinal, apesar de serem avançadas elas possuem uma base matemática antiga fazendo com que suas equações passem a serem desenvolvidas por computadores.

REFERÊNCIAS

[1] SINGH, Simon. **O Livro dos Códigos:** A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica. Rio de Janeiro: Record, 2003.

[2] BRUNO, Odemir Martinez. **Criptografia:** de arma de guerra a pilar da sociedade moderna. Brasil: Jornal da USP, 2017. Disponível em: https://jornal.usp.br/artigos/criptografia-de-arma-de-guerra-a-pilar-da-sociedade-moderna/. Acesso em: 25 set. 2021

[3] ANTON, Howard; RORRES, Chris. **Álgebra Linear**: com aplicações. Tradução: Claus Ivo Doering. 10. ed. Porto Alegre: Anton Textbooks, Inc, 2012. 784 p. v. Único. ISBN 9780470432051. *E-book*.

[4] DOS SANTOS, José Luiz. A Arte de Cifrar, Criptografar, Esconder e Salva, guardar como Fontes Motivadoras para Atividades de Matemática Básica.2013. 81 p. Dissertação (Mestrado em Matemática) - PROFMAT-UFBA, Bahia, 2013. PDF.

[5] DUARTE, Felipe de Almeida. **A ÁLGEBRA NA CRIPTOGRAFÍA**. 61 f. Trabalho de Conclusão de Curso - Curso de Licenciatura em Matemática, Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2015

[6] FERNANDES, Cláudio. **"Máquina Enigma"**; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/historiag/maquina-enigma.htm. Acesso em 13 de outubro de 2021.

[7] ZATTI, Sandra Beatriz. Presença da Álgebra Linear e Teoria dos Números na Criptografia. Santa Maria. 2006. Disponível em: https://docplayer.com.br/4947507-A-presenca-da-algebra-linear-e-teoria-dos-numeros-na-criptografia-sandra-beatris-zatti-1-ana-maria-beltrame-2.html. Acesso em: 04 de Out. 2021.

[8] EISENBERG, Murray. Hill Ciphers and Modular Linear Algebra. **Hill Ciphers**, Massachusetts, p. 19, 3 nov. 1998. Disponível em: https://www.apprendre-en-ligne.net/crypto/hill/Hillciph.pdf. Acesso em: 27 out. 2021.

[9] GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de Pesquisa**. 1ª. ed. Rio Grande do Sul: Editora da UFRGS, 2009. 120 p. v. Único. ISBN 978-85-386-0071-8. *E-book*.