João Paulo P. Flor
Jucemar Luis Monteiro
Stephan Hebeda

Um método criptográfico utilizando geometria analítica - Cifra de Hill

21 de novembro de 2007

João Paulo P. Flor
Jucemar Luis Monteiro
Stephan Hebeda

Um método criptográfico utilizando geometria analítica - Cifra de Hill

Apresentado como trabalho final da disciplina
MTM5512 - Geometria Analítica

Professor: César Raitz

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

21 de novembro de 2007

Sumário

Introdução p. 4

1 Noções básicas de criptografia p. 6

1.1 Cifras de substituição . . . . . p. 6

1.2 Criptografia de chave simétrica . . . . . p. 8

1.3 Criptografia de chave assimétrica . . . . . p. 8

1.4 Criptoanálise . . . . . p. 9

2 Alguns conceitos matemáticos importantes p. 11

2.1 Função e Função Bijetora . . . . . p. 11

2.2 Aritmética Modular . . . . . p. 13

2.2.1 Operação Módulo e congruência . . . . . p. 13

2.2.2 Aritmética modular . . . . . p. 14

3 Matrizes p. 15

3.1 Definição formal de matrizes . . . . . p. 15

3.2 Principais operações matriciais utilizadas na Criptografia . . . . . p. 16

4 A Cifra de Hill p. 18

4.1 Operação de encriptação . . . . . p. 18

4.2 Operação de decriptação . . . . . p. 19

4.3 Interpretação geométrica - Mudança de base . . . . . p. 19

4.4 Exemplo passo-a-passo . . . . . p. 19

5 Vulnerabilidades da Cifra de Hill p. 21

5.1 Número de possíveis chaves . . . . . p. 21

5.2 Linearidade da cifra . . . . . p. 22

5.3 Sugestões para adicionar segurança à cifra . . . . . p. 23

5.3.1 Escolha da função bijetora entre caracteres e números . . . . . p. 23

5.3.2 Permutações entre os blocos de texto encriptados (vetores) . . . . . p. 23

6 Influência da Cifra de Hill nos métodos criptográficos atuais p. 24

Considerações Finais p. 26

Bibliografia p. 27

Introdução

O método estudado nessa pesquisa será a Cifra de Hill. Ela é uma cifra de substituição em blocos e usa a multiplicação matricial como operação de codificação e decodificação de um texto, assim como a aritmética modular (principalmente adição *mod* n). Para se codificar um texto qualquer usando a Cifra de Hill, inicialmente o dividimos em blocos de n símbolos cada. A cada símbolo do alfabeto utilizado no texto se atribui um inteiro positivo (correspondência biunívoca). Cada um desses blocos forma então um vetor multidimensional ou matriz coluna.

Se o texto foi dividido em blocos de n símbolos cada, então a chave para o processo de codificação deve ser uma matriz quadrada de ordem n, a qual deve ser *inversível*. O processo de cifragem do texto é feito então de maneira repetitiva: A cifragem de cada bloco é feita multiplicando-se a matriz chave pelo mesmo. Obtém-se então o total do texto cifrado concatenando-se os blocos individualmente cifrados.

Essa concatenação pode ser feita usando os blocos na mesma ordem em que eles estavam originalmente (antes da cifragem), ou pode-se então reorganizá-los em alguma outra ordem. Caso se faça esse procedimento extra após a multiplicação (uma *transposição*), o processo deixa de ser simplesmente uma Cifra de Hill e torna-se um sistema *multinível*.

Notação para Codificação: Sendo A um bloco e K a matriz chave, está representada abaixo a operação de codificação

$$KA = B$$

Essa operação é feita iterativamente, ou seja, a mesma operação é realizada em todos os blocos. Ela é realizada como uma multiplicação usual entre matrizes, com a exceção de que, caso o resultado kij x aij ultrapasse o número correspondente ao último símbolo do alfabeto, é tomado cij = bij mod n.

Para decodficar um bloco de texto B:

$$A = K^{-1}B$$

Usa-se na decodificação a matriz inversa da chave, por isso havíamos ressaltado que a matriz escolhida aleatóriamente como chave fosse inversível.

A cifra de Hill foi inventada por Lester S. Hill em 1929 e foi largamente utilizada até meados da Segunda Guerra Mundial. Atualmente, ela é bastante obsoleta devido ao enorme poder computacional disponível, além dos eficientes algoritmos na área de álgebra linear, que resolvem grandes sistemas de equações sem esforço.

Neste trabalho pretendemos explorar profundamente o funcionamento da Cifra de Hill à luz dos conceitos de vetores e matrizes, assim como possivelmente generalizar o tratamento a outras cifras de substituição em bloco. Pretendemos também analisar os apectos (relacionados à geometria analítica) que tornam a cifra de Hill vulnerável, o que pode ser feito para melhorá-la, além de sua importância histórica e a influência nos métodos criptográficos atuais.

1 *Noções básicas de criptografia*

Criptografia (Kriptós = escondido, oculto; grapho = escrita) é o estudo de maneiras de se transmitir mensagens através de um meio inseguro, na qual alguém que consiga interceptá-la no meio do caminho tenha uma probabilidade praticamente nula de descobrir a mensagem original.

Desde as sociedades antigas (babilônicos, egípcios, etc) sentiu-se a necessidade de manter informações secretas. Os métodos amplamente usados desde esse período até o final da Segunda Guerra Mundial eram baseados essencialmente na simples substituição de caracteres (permutações).

A partir da década de 1950, com o aumento do poder computacional, as cifras usadas até então passaram a ser mais facilmente quebradas. Então houve a necessidade de se criar novos modelos não tão frágeis como os anteriores. Esses novos modelos se baseiam sobretudo nas chamadas *funções de uma direção*; São funções computacionalmente fáceis de serem computadas, mas que se acredita ser extremamente complexo de se inverter. Um desses modelos é o RSA, muito popular atualmente. O RSA se baseia no fato de que realizar o produto de dois inteiros primos é muito fácil, mas decompor enormes inteiros em seus fatores primos é computacionalmente inviável. Os números usados no RSA são de ordem de grandeza igual ou maior a 10^{100}.

Na sequência comentaremos um pouco sobre alguns modelos de codificação chamados de Cifras de substituição, Criptografia de chave simétrica e de chave assimétrica.

1.1 Cifras de substituição

A cifra de substituição faz a codifição da mensagem de acordo com uma regra pré-definida (chamada de chave), de acordo com uma tabela, na qual se estabelece a correspondência entre o símbolo orginal e o criptografado. As cifras de substituição são assim meras funções permutação. Para se fazer a decriptação é necessário saber a chave (e portanto a tabela de substituição) e fazer a substituição. Algumas das principais cifras de substituição:

- Cifras monoalfabéticas ou de substituição simples;
- Cifras polialfabéticas;
- Cifras homofônicas;
- Cifras poligráficas ou de múltiplos símbolos.

Cifras monoalfabéticas A codificação de mensagens é feita através de uma tabela, em que o alfabeto na sua ordem usual é colocado em uma linha, e uma das possíveis permutações desse alfabeto é colocada na linha logo abaixo. A codificação se faz com uma função bijetora, na qual um $f(a)$ corresponde a um a' e a decodificação faz-se com a função inversa.

Exemplo Cifra de Cesar:

a	b	c	d	e	f	g	h	...	r	s	t	u	v	w	x	y	z
d	e	f	g	h	i	j	k	...	u	v	w	x	y	z	a	b	c

Cifras polialfabéticas A tabela de codificação é montada contendo n linhas por n colunas, onde n é o número de símbolos do alfabeto. As linhas da tabela são preenchidas com algumas das possíveis permutações sobre o alfabeto. A encriptação é feita transformando-se cada bloco de texto usando uma linha da tabela.

Exemplo: Mensagem original - cada decada

X	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

A palavra “cada” foi cifrada com a linha e (cada = bece) e “decada” foi cifrada com a linha c (decada = abecac)

Cifras homofônicas Nesse tipo de cifra, os caracteres com incidência acima da média (por ex: a no português) têm mais de uma opção de substituição quando a encriptação é feita. Isso visa diminuir os riscos da mensagem ser descoberta por análise estatística, que será explicada mais adiante.

Cifras poligráficas A encriptação de uma mensagem é feita substituindo o caractere original por um conjunto de símbolos. Assume-se que esse conjunto de símbolos seja conhecido por poucas pessoas.

1.2 Criptografia de chave simétrica

Um modelo de criptografia em que o emissor e o receptor têm a mesma chave, ou seja, a codificação e a decodificação são feitas com uma única chave, ou então a chave de codificação e a de decodificação têm uma relação matemática trivial (uma pode ser muito facilmente obtida tendo-se a outra). A Cifra de Hill é uma cifra simétrica, e algumas cifras simétricas modernas são o DES e o AES.

DES (Data Encryption Standard) O modelo opera sobre blocos de texto com 64 bits cada, e usa uma chave de 56 bits (72 quadrilhões de chaves possíveis). A codificação é feita usando-se uma função inversível sob blocos de bits representando a mensagem. A função que encripta a mensagem é parametrizada pela chave, o que fornece a segurança do sistema, mesmo o algoritmo em si sendo público.

AES (Advanced Encryption Standard) Esse padrão de criptografia surgiu em 1998 após um concurso promovido pelo governo americano para substituir o DES, padrão internacional até então.

A codificação do texto plano utiliza operações matriciais sobre blocos de bytes armazenados em matrizes 4×4. A encriptação começa combinando cada byte com uma subchave (derivada da chave principal], depois cada byte é substituído por outro de acordo com uma tabela de referência, em seguida cada linha da matriz é deslocada n posições, então é feita uma multiplicação da matriz original com a resultante desse deslocamento e a matriz resultante multiplicada por $x^4 + 1$.

1.3 Criptografia de chave assimétrica

São modelos de criptografia onde cada pessoa porta duas chaves, uma chamada de *chave pública* (amplamente divulgada) e outra é a chave privada.

Uma mensagem encriptada usando uma chave só poderá ser decriptada usando a outra correspondente. Se desejo enviar uma mensagem secreta a um amigo meu, devo encriptá-la usando a chave pública dele, assim somente ele (o portador de sua chave privada) poderá decifrar a mensagem.

De modo semelhante, posso enviar uma mensagem cifrada com minha chave privada, e todos que possuem minha chave pública (TODOS) poderão lê-la. O grande benefício é que

assim posso provar que FUI EU quem escrevi a mensagem, e isso faz com que a criptografia de chave assimétrica também dê autenticidade.

O algoritmo mais usado para implementar a criptgrafia assimétrica é o RSA, inventado por Rivest, Shamir e Adleman. Ele será descrito a seguir:

RSA A codificação da mensagem é feita multiplicando-se dois números primos muito grandes (da ordem de 10^{100}). A segurança do RSA vem do fato de que decompor um grande número em seus fatores primos é impraticável computacionalmente. Para se decompor um número da ordem de 10^{100} em seus dois fatores primos se levaria um tempo maior que a IDADE DO UNIVERSO, usando todo o poder computacional atualmente disponível na Terra.

1.4 Criptoanálise

A criptoanálise estuda maneiras de se chegar a mensagem original (plaintext) sem o conhecimento da chave (key) a partir do texto cifrado (ciphertext), assim como também maneiras de se descobrir a chave. Algumas das técnicas de criptoanálise são:

- Brute force
- Ciphertext only
- Known text
- Timing
- Análise estatística

Brute force Tenta-se chegar à chave testando-se todas as possibilidades. A eficácia desse método depende do tamanho e da complexidade da chave. Já se conseguiu descobrir uma chave do DES por força bruta em cerca de 20h.

Ciphertext only Tenta-se chegar à chave ou ao texto original conhecendo-se apenas uma parte da mensagem codificada. Nas cifras de substituição simples é relativamente fácil descobrir a chave apenas com papel e caneta.

Known text Tenta-se chegar à chave conhecendo-se uma pequena parte do texto original e do cifrado correspondente. A Cifra de Hill é *bastante* vulnerável à ataques desse tipo.

Timing Tenta-se descobrir a chave de acordo com o tempo de execução do algoritmo que criptografa a mensagem.

Análise Estatística Busca na mensagem criptografada a freqüência com que os símbolos aparecem a compara com a distribuição de freqüências dos símbolos na língua em que se supõe estar a mensagem original. A partir de então tenta chegar à algumas prováveis mensagens originais (usando o Teorema de Bayes). A Cifra de Hill também é vulnerável a esse tipo de ataque.

2 *Alguns conceitos matemáticos importantes*

A cifra de Hill utiliza matrizes quadradas como modelo para a chave de cifragem, e vetores como modelo para os blocos de texto a serem cifrados. As operações da cifra de Hill são operações matriciais, que no fundo se resumem a operações com números. Os elementos das matrizes devem ser números inteiros pois o processo utiliza também de aritmética modular, uma operação que só faz sentido com inteiros, e será revisada na seção seguinte. Agora, porém, surge uma questão: Como *associar* símbolos a números?

2.1 Função e Função Bijetora

A palavra *associar* sugere o uso do conceito matemático de função. Uma função pode ser vista como uma *regra* que associa cada elemento de um conjunto, chamado de domínio da função, a somente um elemento do outro conjunto, o contra-domínio. Para nossa necessidade, de associar letras a números, teremos uma função do tipo:

$$f : A \to \mathbb{Z}_n$$

onde A é um alfabeto qualquer (conjunto finito de símbolos), e $\mathbb{Z}_n$ é o conjunto dos inteiros de 0 a n-1.

Exemplo 1: Seja $f : A \to \mathbb{Z}_{26}$ onde A=$\{$alfabeto de 26 letras$\}$ e Z=$\{0,1,\ldots,25\}$ dada por:

$$a \mapsto 0$$
$$b \mapsto 1$$
$$c \mapsto 2$$
$$\ldots$$
$$z \mapsto 25$$

Para executar as operações da Cifra de Hill sobre um dado texto, precisamos aplicar uma função que leve de letras para inteiros não-negativos, mas se quisermos saber o ”resultado”da cifragem, ou se quisermos decifrar uma mensagem cifrada usando o processo de Hill, precisamos *inverter* essa função que leva para números, ou seja, precisamos de: $f^{-1} : \mathbb{Z}_n \to A$, ou seja, precisamos da *função inversa* de f. Invertendo a função do Exemplo 1, ficamos com:

Função inversa do Exemplo 1: Tomando a função f^{-1} inversa de f, temos:

$$0 \mapsto a$$
$$1 \mapsto b$$
$$2 \mapsto c$$
$$\dots$$
$$25 \mapsto z$$

Por definição, uma função qualquer f é inversível se e somente se ela for *bijetora*, o que é sinônimo de um mapeamento um-para-um. Uma função dita bijetora, e portanto INVERSÍVEL, satisfaz duas condições:

$$x \neq y \longrightarrow f(x) \neq f(y) \tag{2.1}$$

$$Im(f) = Contradom(f) \tag{2.2}$$

A primeira condição diz que elementos diferentes do domínio estão associados a elementos diferentes no contradomínio. A segunda condição diz que cada elemento do contradomínio deve ter um elemento do domínio associado a ele. A segunda condição também pode ser expressa da seguinte maneira (talvez mais explícita): $|Dom(f)| = |Contradom(f)|$, ou seja, o domínio e o contradomínio devem ter o mesmo *número* de elementos; não podem “sobrar” elementos não associados.

Se tivermos um texto fonte, e desejarmos criptografá-lo usando a Cifra de Hill, devemos então associar as *n* letras do alfabeto aos inteiros de 0 até n-1. Não há nenhuma função específica que deva ser usada para fazer essa associação. Porém devemos ter certeza de que a função usada é inversível, para depois podermos realizar o processo inverso.

2.2 Aritmética Modular

Como já foi mencionado anteriormente, os métodos criptográficos - e em particular a Cifra de Hill - trabalham sobre *alfabetos*, que são conjuntos FINITOS de símbolos. Associando esses símbolos a um conjunto de números podemos usar operações aritméticas úteis sobre estes números. Porém, ao usar uma cifra, nós queremos que ao final do processo encriptação - transmissão - decriptação nós tenhamos a mensagem no mesmo alfabeto do texto original.

Assim, se fizermos a associação de letras com inteiros e chegarmos a um conjunto $\mathbb{Z}_n$, devemos GARANTIR que todas as operações realizadas na cifragem (operações entre elementos desse conjunto $\mathbb{Z}_n$) resultem em elementos desse mesmo conjunto, ou seja, as operações devem ser *fechadas*; só assim poderemos voltar à mensagem no alfabeto original. Essa garantia se obtém pelo uso da *aritmética modular*.

2.2.1 Operação Módulo e congruência

Em várias situações, estamos interessados apenas no *resto* da divisão entre dois inteiros. Um exemplo clássico é quando perguntamos: "Que horas serão daqui a 30 horas", nesse caso nos interessa apenas o resto de (50 + hora atual)/24. Existe uma operação binária entre inteiros, chamada *módulo*, definida da seguinte maneira:

$$a \bmod n = r \Longrightarrow a = qn + r$$

Ou seja, *a mod n* é o resto da divisão inteira de a por n. A operação módulo define uma relação muito útil sobre os inteiros, semelhante à igualdade: é a CONGRUÊNCIA. A relação de congruência é definida usando a operação módulo da seguinte maneira:

$$a \equiv b \pmod{n} \Longleftrightarrow a \bmod n = b \bmod n$$

Ou seja, a é congruente a b módulo n se e somente se a e b tiverem o mesmo resto (módulo) quando divididos por n. A relação de congruência sobre os inteiros é a base que estrutura a aritmética modular. A aritmética modular foi desenvolvida pelo grande matemático Carl Friedrich Gauss e é o fundamento da teoria dos números. A aritmética modular tem muitas aplicações práticas, incluindo música, artes visuais, química, e sendo a criptografia uma das mais importantes. Vamos revisá-la com mais detalhes então.

2.2.2 Aritmética modular

A aritmética modular é um conjunto de operações que estão definidas (fazem sentido) somente para os números inteiros. Elas são semelhantes às operações usuais de adição e multiplicação, mas funcionam como se fossem operações "circulares" em torno de um conjunto finito de inteiros de 0 a n-1. Para ilustrar melhor esse conceito intuitivo, voltemos ao exemplo do relógio:

Suponha que sejam 4h da manhã. Nesse caso a pergunta: "Que horas serão daqui a 30h?" (usando x como incógnita) equivale à seguinte expressão usando adição módulo 24:

$$4 + 30 \equiv x \pmod{24}$$

Ora, somando-se usualmente 30 e 4 obtemos 34, mas não usando uma adição módulo 24. Usando a adição modular nós temos: $4 + 30 \equiv x \pmod{24} \iff x = (30 + 4) \bmod 24$. Generalizando, uma *adição módulo n* pode ser definida da seguinte forma:

$$a + b \equiv x \pmod{n} \iff x = (a + b) \bmod n$$

A mesma definição, apenas substituindo o símbolo da operação, vale para a multiplicação modualar. Enfim, há várias definições formais e complexas das operações da aritmética modular, mas para nossos propósitos basta a seguinte:

Aritmética modular Realizar uma operação entre dois inteiros em *aritmética modular* não é nada mais do que primeiramente realizar a operação usual entre os inteiros e, em seguida, tomar o resultado *mod n*

3 *Matrizes*

Dada a importância do conceito de matriz para a Cifra de Hill, é necessária uma revisão desse conceito, abordado de forma conveniente. É também importante rever algumas das operações matriciais mais usadas na criptografia.

3.1 Definição formal de matrizes

Tomando por base o conjunto $\mathbb{N}$ dos números naturais, o produto cartesiano de $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$ indicará o conjunto de todos os pares ordenados (a,b), então um subconjunto importante de $\mathbb{N}^2$ é obtida como sendo:

$$S_{mn} = \{(i, j) | 1 \leq i \leq m \text{ e } 1 \leq j \leq n\}$$

Com base nisso, uma Matriz é uma função que a cada par ordenado (i,j) no conjunto S_{mn} associa um número real.

$$f : S_{mn} \rightarrow \mathbb{R}$$

Uma matriz, também pode ser definida simplesmente como uma "tabela" de m x n números reais, representada sob a forma de um quadro com m linhas e n colunas e utilizado, entre outras coisas, para a resolução de sistema de equações lineares e transformações lineares.

Uma matriz com m linhas e n colunas é chamada de uma matriz m por n (escreve-se $m \times n$) e m e n são chamadas de suas dimensões, tipo ou ordem. Um elemento de uma matriz A que está na i-ésima linha e na j-ésima coluna é chamado de elemento i,j ou (i,j)-ésimo elemento de A. Ele é escrito como A_{ij} ou A(i,j), reforçando o significado como função.

Uma matriz onde uma de suas dimensões é igual a 1 é geralmente chamada de vetor. Uma matriz $1 \times n$ (uma linha e n colunas) é chamada de vetor linha ou matriz linha, e uma matriz $m \times 1$ (uma coluna e m linhas) é chamada de vetor coluna ou matriz coluna.

Exemplo: Tomando a Matriz A com m = 2 e n = 3 pode-se obter um elemento qualquer através

da função f.

$$A = \begin{bmatrix} 4 & 0 & 9 \\ 1 & 7 & 3 \end{bmatrix}$$

onde $f(1,1) = 4; f(1,2) = 0$ e assim por diante ...

Nesse exemplo, temos $Dom(f) = \{(1,1);(1,2);\ldots;(2,3)\}$ e $Contradom(f) = \mathbb{R}$.

3.2 Principais operações matriciais utilizadas na Criptografia

Adição e subtração Esta operação só faz sentido entre matrizes que têm o mesmo número de linhas e colunas (mesma ordem). Sejam duas matrizes $A_{m,n}$ e $B_{m,n}$. Então a matriz $R = A \pm B$ é uma matrix $m \times n$ tal que cada elemento de R é dado por:

$$r_{ij} = a_{ij} \pm b_{ij}$$

Multiplicação por um escalar Seja a matriz $A_{m,n}$ e c um escalar $(c \in \mathbb{R})$. A matriz $P = cA$ é uma matriz $m \times n$ tal que cada elemento de P é dado por:

$$p_{ij} = c \cdot a_{ij}$$

Multiplicação de matrizes Sejam as matrizes $A_{m,p}$ e $B_{p,n}$ (o número de colunas da primeira deve ser igual ao número de linhas da segunda). O produto AB é dado pela matriz $C_{m,n}$ cujos elementos são calculados por:

$$c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj}$$

Pode-se ainda fazer uma interpretação da multiplicação entre duas matrizes "uma linha por vez", ou "uma coluna por vez". Exemplificarei usando o caso por coluna. Dessa maneira, a primeira coluna de AB é a matriz A multiplicada pela primeira coluna de B, e assim por diante ... Um exemplo seria:

$$\begin{bmatrix} 4 & 0 \\ 1 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 2 \begin{bmatrix} 4 \\ 1 \end{bmatrix} + 1 \begin{bmatrix} 0 \\ 7 \end{bmatrix}$$

Essa definição é totalmente equivalente à anterior, e deixa mais claro a função que as operações matriciais ocupam nas transformações sobre vetores.

Inversão de matrizes Sendo A uma matriz quadrada A^{-1} é dita sua inversa, se e somente se $A^{-1}A = I = AA^{-1}$. Uma outra condição que também determina se uma matriz é inversível é seu determinante: Uma matriz A é inversível se e somente se $det(A) \neq 0$.

Uma vez verificada que uma matriz é inversível, ou seja, possui determinante diferente de zero, existem vários métodos para se obter sua inversa. Um deles se resume em:

$$A^{-1} = \frac{1}{|A|} \cdot cof(A)^t$$

4 A Cifra de Hill

A Cifra de Hill foi inventada por Lester S. Hill em 1929 e é uma cifra de substituição polialfabética *em bloco*. A encriptação e a decriptação são realizadas através de operações com matrizes e vetores, e a chave é uma matriz quadrada inversível (uma base para um espaço vetorial).

4.1 Operação de encriptação

A encriptação de uma determinada mensagem é feita tomando-se cada letra do alfabeto e associando-se a ela um número inteiro de 0 a n-1 de forma biunívoca (onde n é o número de letras do alfabeto). Pode-se, por exemplo, fazer a=0, b=1, c=2, ..., z=25. Divide-se então o texto em blocos de tamanho n, e cada um desses blocos então é considearado um vetor de n dimensões. É escolhida então uma matriz quadrada inversível de ordem n para servir de chave. Essa matriz chave é então multiplicada pelos vetores, um de cada vez, resultando nos "vetores encriptados".

As operações de multiplicação/adição sobre inteiros que estão implícitas na multiplicação matricial são todas realizadas *módulo n*. No caso do alfabeto latino, como temos 26 letras, realizamos adição e multiplicação *módulo 26*.

Ao final das repetidas multiplicações da chave por cada um dos blocos, convertemos os resultados obtidos de volta para as letras usando a inversa da função que converteu letras em números. Assim temos a mensagem criptografada.

A matriz utilizada como chave deve ser inversível. Caso ela não seja inversível, não será possível voltar à mensagem original depois de encriptada.

4.2 Operação de decriptação

Para se obter a mensagem original a partir da encriptada, multiplica-se a INVERSA da matriz chave por cada um dos blocos (vetores) e assim obtém-se os vetores originais, bastando então substituirmos cada número pelo seu caractere correspondente e então teremos a mensagem original de volta.

4.3 Interpretação geométrica - Mudança de base

A operação de encriptação realizada pela Cifra de Hill pode ser interpretada puramente como uma mudança de base realizada sobre um conjunto de vetores. A mudança de base é uma dentre várias transformações lineares, estudadas pela Geometria Analítica e Álgebra Linear.

Consideremos um vetor $\vec{v}$ com n coordenadas e na base usual. Multiplicar uma matriz quadrada de ordem n por esse vetor $\vec{v}$ (vetor coluna) é totalmente análogo (pode ser interpretado como) uma *mudança de base* de $\vec{v}$. Isso significa que agora as coordenadas do vetor v serão a representação de v como combinação linear dessa nova base, e não mais de $\{$i,j,k$\}$.

Se tomarmos uma base $B = \{\vec{b_1}, \vec{b_2}, \vec{b_3}\}$ e situarmos cada um dos vetores dessa base nas colunas de uma matriz, teremos a matriz quadrada M_B. Se tomarmos a *inversa* dessa matriz, temos a matriz que realizará a mudança de base. Representando essa matriz por T, fica: $T = (M_B)^{-1}$

Dizer que T é uma matriz de mudança de base significa que, se a multiplicarmos por um vetor na base usual, teremos como resultado o *mesmo vetor*, mas sendo representado como combinação linear dos vetores da nova base.

Depois dessa explicação, pode-se notar que a matriz chave da Cifra de Hill nada mais é que uma matriz T (transformação), e que ela (a chave) muda a base de cada um dos vetores que estão na mensagem. *Isso* constitui a encriptação realizada pela Cifra de Hill. Na decriptação apenas se usa $K^{-1} = T^{-1} = M_B$, que é a própria matriz contendo nas colunas os vetores que formam a base do "espaço vetorial encriptado".

4.4 Exemplo passo-a-passo

Desejamos encriptar o texto "GEOMETRIA" usando a Cifra de Hill. Primeiramente estabelecemos a função já mencionada entre as letras do alfabeto e números inteiros.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	5	16	2	9	22	15	13	6	8	20	3	10
n	o	p	q	r	s	t	u	v	w	x	y	z
17	21	1	24	18	25	4	11	19	12	7	23	14

Dividimos então o texto em blocos de n componentes (no nosso caso 3). Ficamos então com os vetores do texto original (vetores no $\mathbb{R}^3$). GEO = (6,4,14); MET = (12,4,19); RIA = (17,8,0). Escolhemos (aleatóriamente, com distribuição uniforme) uma matriz quadrada inversível de ordem n para ser a *chave* da cifra. Essa matriz chave é aqui representada por K.

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

Considerando os vetores como colunas (matrizes $n \times 1$) fazemos então a multiplicação da matriz K por cada um dos vetores do texto: Sendo $\vec{v}_1 = (15,9,21)$, $\vec{v}_2 = (10,9,4)$, $\vec{v}_3 = (18,6,0)$, temos:

$$K \cdot \vec{v}_1 = (66,102,39) \quad K \cdot \vec{v}_2 = (27,41,22) \quad K \cdot \vec{v}_3 = (24,42,12)$$

Agora devemos tirar módulo 26 desses vetores resultantes, obtendo assim:

$$\vec{e}_1 = (66,102,39) \bmod 26 = (14,24,13)$$
$$\vec{e}_2 = (27,41,22) \bmod 26 = (1,15,22)$$
$$\vec{e}_3 = (24,42,12) \bmod 26 = (24,16,12)$$

Ao fim do da encriptação, obtemos (14,24,13) = ZQH; (1,15,22) = PGF e (24,16,12) = QCW. O nosso texto encriptado então é "ZQHPGFQCW". (Note que no texto original GEOMETRIA tínhamos duas letras E, mas no texto encriptado o E é substituído por letras diferentes, Q e G. Isso aumenta a segurança de uma cifra.)

Para decriptar o texto "ZQWPGFQCW" basta seguir o mesmo caminho, mas usando agora a inversa da matriz chave. Os vetores voltam a serem representados na base usual.

$$K^{-1} \cdot \vec{e}_1 = (15,9,-5) \quad K^{-1} \cdot \vec{e}_2 = (62,35,-48) \quad K^{-1} \cdot \vec{e}_3 = (-60,-20,52)$$

Tirando o módulo 26 como na encriptação, temos (15,9,21) = GEO; (10,9,4) = MET e (18,6,0) = RIA. Nosso texto secreto "GEOMETRIA" de volta!

5 *Vulnerabilidades da Cifra de Hill*

A Cifra de Hill foi altamente revolucionária quando de sua criação, pois era a primeira cifra de substituição poligráfica com a qual era prática trabalhar em blocos de mais que três caracteres. Porém ela tornou-se obsoleta e suas fraquezas a tornam inutilizável nos tempos modernos. Nesta seção vamos abordar alguns ataques aos quais a Cifra de Hill é vulnerável, e quais são os aspectos da cifra (relacionados à Geometria Analítica) que causam essas vulnerabilidades.

Pretendemos ainda mencionar alguns pequenos "ajustes" que poderiam ser adicionados ao processo de encriptação/decriptação com a Cifra de Hill, e que aumentariam sua segurança.

5.1 Número de possíveis chaves

O número de chaves possíveis de serem usadas é uma medida importante da segurança de um algoritmo de critografia. Isso porque, com o imenso poder computacional disponível nos dias de hoje, a busca de uma chave por força bruta (tentativa de todas as opções possíveis) é muito rápida. Portanto um padrão criptográfico deve ter um grande número de possíveis chaves, tornando inviável uma busca por força bruta.

Se temos um conjunto de k números, e uma matriz quadrada de ordem $n \times n$, então o número de matrizes diferentes que podemos formar, *escolhendo livremente* dentre esses k elementos é:

$$k^{n^2}$$

Essa quantidade é encontrada facilmente usando o conceito de arranjos. Se usarmos o alfabeto usual com 26 letras, teremos um limite superior de 26^{n^2} possíveis chaves. Esse número é apenas um limite superior pois dentre esse grupo, devemos escolher como chave somente as matrizes *inversíveis em módulo 26*.

Mas e o que significa uma matriz ser inversível módulo 26? Relembrando a fórmula para

inverter uma matriz:

$$A^{-1} = \frac{1}{|A|} cof(A)^t$$

Usamos o determinante para encontrar a inversa de uma matriz. E como usamos aritmética modular na Cifra de Hill, a matriz inversa A^{-1} deve conter somente números inteiros. Isso implica que a o determinante deve ser divisor dos elementos da matriz adjunta. Com essa restrição reduzimos bastante o número de possíveis chaves. Apesar disso, aumentando a ordem da matriz chave, aumentamos esse número, mas então a encriptação começa a se tornar inviavelmente lenta.

De fato, esse aspecto (número de chaves) contribui para a vulnerabilidade da Cifra de Hill. O número de chaves possíveis não é suficiente para tornar extremamente impraticável um ataque por força bruta. Porém ele não é o mais problemático. A Cifra de Hill sofre também de *linearidade*.

5.2 Linearidade da cifra

A Cifra de Hill também é vulnerável a ataques de "Texto plano conhecido". Esses ataques ocorrem quando alguém "escutando" o canal da mensagem consegue ter acesso a alguns (poucos) pares de caracteres originais/cifrados. Alguém com acesso a esses pares tem grandes chances de descobrir a chave sendo usada, isso pois a Cifra de Hill é completamente *linear*.

Diz-se que a Cifra de Hill é linear pois suas operações são lineares (multiplicação por escalares e adição); A própria "natureza" da cifra é linear pois ela usa dos conceitos da Álgebra Linear e Geometria Analítica.

Um interceptador, "escutando" uma mensagem sendo transmitida com Cifra de Hill de ordem 2 precisa de apenas 4 pares de caracteres original/cifrado para descobrir a chave. Por exemplo:

$$\begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 7 \end{bmatrix} \quad \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \begin{bmatrix} 17 \\ 3 \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix} \Longrightarrow \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \begin{bmatrix} 4 & 17 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 12 \\ 7 & 5 \end{bmatrix}$$

Da multiplicação matricial mais à direita pode-se montar um sistema de equações lineares, que resolvido nos dá a chave sendo usada. Claramente esse exemplo com chaves de ordem 2 é apenas didático. Mesmo em 1929 a Cifra de Hill já usava matrizes chave de ordem 6 ou superior. O fato, porém, é que mesmo assim a linearidade continua, e como resolver sistemas

lineares se tornou trivial com computadores, a Cifra de Hill ficou vulnerável.

De modo geral, para descobrir a chave de ordem n da Cifra de Hill basta que o atacante conheça n^2 pares de caracteres originais/cifrados. Ele poderá montar um sistema lineares de n^2 equações e n^2 incógnitas, e ao resolvê-las terá descoberto a chave.

5.3 Sugestões para adicionar segurança à cifra

Quanto ao "núcleo" da Cifra de Hill não se pode fazer nada para aumentar sua segurança; ela é totalmente linear pela própria natureza das operações. O que se pode fazer é adicionar algumas *camadas extras* no processo de encriptação/decriptação usando a Cifra de Hill. Os dois "passos" do processo que podem ser *parametrizados* são:

5.3.1 Escolha da função bijetora entre caracteres e números

Em todos os exemplos deste trabalho considerou-se a associação entre as letras do alfabeto e os inteiros de 0 a n-1 como sendo a usual, ou seja: a=0, b=1, c=2, ..., z=25. Mas também se enfatizou que QUALQUER mapeamento, e não especificamente esse, funcionaria.

Uma possibilidade seria então a de *parametrizar* a escolha dessa função bijetora, ou seja, fornecer ao algoritmo cifrador que usa a Cifra de Hill uma espécie de "chave extra", a qual serviria para identificar qual permutação do alfabeto deve ser usada no mapeamento. Isso aumentaria a segurança pois mesmo conhecendo-se a matriz chave ainda não se sabe quais são os caracteres correspondentes aos números da mensagem.

5.3.2 Permutações entre os blocos de texto encriptados (vetores)

Uma outra operação que poderia ser adicionada à Cifra de Hill para aumentar sua segurança seria mudar a ordem dos blocos de texto encritpados. Novamente seria usado um parâmetro também aleatório nesse processo, e que seria uma terceira "chave", de conhecimento mútuo de quem envia e recebe a mensagem.

Tendo k blocos encriptados, o números de possíveis permutações desses k blocos é similarmente k!. Conjuntamente com o processo descrito na subseção anterior, é adicionada uma camada de operações não-lineares à cifra, o que a torna mais segura.

6 *Influência da Cifra de Hill nos métodos criptográficos atuais*

Pode-se dizer que a Cifra de Hill funcionou como um passo na história da criptografia, introduzindo as idéias de proteção de mensagens através de matrizes, mas acabou tornando-se obsoleta uma vez que seus pontos fracos começaram a ser descobertos e suas defesas foram quebradas. Então novos métodos de criptografia foram criados com o passar do tempo. Os grandes responsáveis por essa grande evolução na criptografia no século XX foram os avanços na Ciência da Computação, trazendo algoritmos mais poderosos; e também o uso de novas idéias matemáticas como por exemplo: permutações (uma permutação é uma bijeção, de um conjunto finito X nele mesmo) usadas no DES e Triple DES, operações de rotação (transformação geométrica de um sistema de coordenadas) usadas no RC5 e a o teorema fundamental da aritmética (capacidade de decompor qualquer inteiro em fatores primos) usado como base para o RSA.

O legado da Cifra de Hill, a qual se valia de operações matriciais de multiplicação e inversão para encriptar e decriptar suas mensagens, foi passado adiante. Porém nos novos métodos de criptografia as matrizes com suas operações não executam o papel que tinham na Cifra de Hill, que era o de encriptar e decriptar a mensagem. Nos novos métodos as matrizes armazenam as chaves, subchaves e blocos de texto utilizados, a fim de agilizar e organizar o funcionamento do algoritmo o tornando mais compreensível e confiável. Abaixo seguem alguns métodos criptográficos atuais e como eles usam matrizes:

DES O algoritmo de criptografia simétrica DES gera 16 subchaves a partir da chave fornecida, as quais serão usadas nas 16 "rodadas" de encriptação. A matriz ChavesK armazena essas 16 subchaves, uma por linha. Cada uma dessas subchaves é gerada a partir da anterior por uma rotação de bits.

Blowfish No algoritmo Blowfish, a matriz ChavesP armazena as 18 subchaves que são utilizadas nesse algoritmo, também uma por linha. O algoritmo faz uso de uma função de

Feistel, e a matriz F armazena os resultados gerados pela função após cada iteração sobre o bloco de texto plano.

RC5 A matriz MatrixBlocosHex é uma matriz onde cada linha corresponde a um bloco de texto a ser cifrado. As matrizes SH armazenam as S-boxes (são função permutação que têm a chave como parâmetro). Já a matriz CriptoMatrix armazena os blocos de texto já devidamente criptografados, um por linha.

IDEA K é uma matriz que armazena todas as 52 subchaves utilizadas nesse algoritmo, uma por linha. Já K_{inv} é a matriz que armazena o *inverso* (multiplicativo ou aditivo, conforme o caso) de cada uma das 52 subchaves, também uma por linha.

Considerações Finais

Nesse trabalho constatamos a profundidade e o tremendo nível de abstração dos conceitos da Geometria Analítica e da Álgebra Linear. A Criptografia é uma área freqüentemente associada com conceitos algébricos e sem nenhuma relação com os espaços e formas e sem interpretação geométrica, mas a Cifra de Hill e alguns dos modernos métodos criptográficos demonstram exatamente o contrário: Os conceitos geométricos têm sido cada vez mais importantes para a "arte de esconder", assim como para a Computação como um todo.

A Cifra de Hill é atualmente obsoleta, mas representou uma revolução em sua época. Ela usou conceitos da teoria de matrizes e vetores até então não aplicados em criptografia. Além disso, ela foi a primeira cifra de substituição poligráfica em que era praticável trabalhar com blocos de mais de 3 caracteres.

Apesar de ser um modelo até certo ponto ultrapassado, pesquisar a Cifra de Hill foi para nós de grande valia. Ao procurar compreender seu mecanismo de funcionamento, aplicamos os conceitos aprendidos durante a disciplina, e os relacionamos com outros os quais pensávamos serem independentes. Especialmente interessante foi estudar as próprias *características* da Cifra de Hill, relacionadas à Geometria Analítica, que fornecem um nível já insuficiente para os dias de hoje.

Com este trabalho aumentamos ainda mais nosso interesse pela área da Criptografia, e tivemos a oportunidade de revisar importantes conceitos matemáticos. Esperamos continuar progredindo nessa construção do conhecimento tecnológico, e sempre usando das ferramentas matemáticas apropriadas.

Bibliografia

1) STEINBRUCH, Alfredo; WINTERLE, Paulo. *Geometria analítica*.
São Paulo: McGraw-Hill, 1987.
2) OLIVEIRA, Ivan de Camargo; BOULOS, Paulo. *Geometria analítica: um tratamento vetorial*. São Paulo: McGraw-Hill, 1987.
3) http://www.mat.ufmg.br/ regi/gaalt/gaalt0.pdf
4) http://www.cce.ufes.br/dmat/camara/linear/linear.pdf