A MATEMÁTICA E OS OUTROS

A CIFRA DE HILL

Maria de Lourdes R. de A. Jeanrenaud

Da Antiguidade à Idade Contemporânea, o homem desenvolve pesquisas na busca de técnicas para ocultar a comunicação de informações sigilosas. O estudo destas técnicas, a arte da *Criptografia* ou da *Estenografia*, faz parte de nossas preocupações diárias. Cada vez que vamos ao banco acessar nossa conta corrente através de algum meio eletrônico, utilizamos senhas e códigos para impedir o acesso de terceiros. Estamos desta forma "praticando" Criptografia.

Ao mesmo tempo, formas de se quebrarem algoritmos criptográficos, revelando o conteúdo de uma mensagem sem a necessidade de se ter a chave apropriada, surgem a cada segundo.

Do bastão de Licurgo, passando pela *cifra de Vigenère* até chegar ao sistema *RSA*, a Criptografia esteve presente em vários fatos marcantes da história. Alan Turing e uma equipe de cientistas ingleses juntaram todos os seus esforços na quebra do código da máquina *ENIGMA*, utilizada pelos alemães na codificação de mensagens durante a II Guerra Mundial,

No início do século XX, iniciam-se as primeiras tentativas de mecanização das técnicas criptográficas, pois os sistemas existentes, mono e polialfabéticos, estavam vulneráveis à análise de frequências. Uma das alternativas apresentadas consistia em agrupar as letras do texto normal, formando blocos com um número *n* de caracteres e, a cada conjunto formado, substituí-las por um conjunto *n* de letras cifradas. Esta técnica clássica de substituição, utilizando conceitos da Álgebra Linear e da Aritmética Modular, aprimorada por Lester S. Hill em 1929, deu origem ao que se denomina a *Cifra de Hill*.

As operações com matrizes terão por base uma tabela de substituição, como por exemplo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z	.
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Tabela 1

Como os resultados obtidos podem ser superiores a 27, é conveniente operarmos no corpo $\mathbf{Z_{27}}$ através da relação de congruência módulo 27.

Vamos **cifrar** o texto:

MATEMÁTICA E DIVERSÃO.

Procedendo por etapas, iremos:

- Separar o texto, da esquerda para a direita, em um número *k* de grupos com n letras cada um. Se o texto a ser cifrado possuir um número par de letras, podemos escolher arbitrariamente qualquer símbolo para preencher o último grupo. Podemos ou não ignorar o espaço entre as palavras. No nosso exemplo, teremos 10 grupos com 2 letras cada um.

MA TE MÁ TI CA ED IV ER SA O.

- Numerar cada grupo separado de acordo com a tabela escolhida para alfabeto.

13,1 – 20,5 – 13,1 – 20,9 – 3,1 – 5,4 – 9,22 – 5,18 – 19,1 – 15,27

- Colocar cada grupo de n números como colunas de uma matriz P com k colunas. Teremos a matriz 2 x 10 abaixo:

$$P = \begin{pmatrix} 13 & 20 & 13 & 20 & 3 & 5 & 9 & 5 & 19 & 15 \\ 1 & 5 & 1 & 9 & 1 & 4 & 22 & 18 & 1 & 27 \end{pmatrix}$$

- Escolher uma matriz A de ordem n (no caso, n=2), que será a *matriz de codificação,* fazendo o papel de *chave.* Para garantir o processo inverso, a decodificação do texto, o processo matricial deve ser reversível, isto é, A deve ser *inversível* $(\det A \neq 0)$. Vamos utilizar, em nosso exemplo, a matriz

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

- Codificar o texto através da multiplicação das matrizes A e P em $\mathbf{Z_{27}}$**,** obtendo a matriz C = A.P (mod 27).

$$C = \begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 13 & 20 & 13 & 20 & 3 & 5 & 9 & 5 & 19 & 15 \\ 1 & 5 & 1 & 9 & 1 & 4 & 22 & 18 & 1 & 27 \end{pmatrix}$$

$$\Rightarrow C = \begin{pmatrix} 2 & 15 & 2 & 13 & 9 & 22 & 3 & 10 & 14 & 3 \\ 15 & 12 & 15 & 16 & 25 & 26 & 13 & 13 & 9 & 12 \end{pmatrix}$$

Teremos então:

2,15 – 15,12 – 2,15 – 13,16 – 9,25 – 22,26 – 3,13 – 10,13 – 14,9 – 3,12

Retornando à tabela 1, o texto cifrado será:

BOOLBOMPIYVZCMJMNICL

O processo inverso, a **decifragem,** consiste em realizar a mesma operação com outra chave, a matriz inversa A^{-1}. Porém, quando a ordem de A aumenta, consequência direta do número de letras do "alfabeto" e da tabela de símbolos utilizados, este processo é demorado e mais complexo.

É bastante trabalhoso inverter matrizes de ordem muito grande sem auxílio computacional adequado. Por esse motivo, na época de sua criação, tal tipo de cifra não foi desenvolvido na prática.

Por outro lado, é uma escrita enigmática bastante vulnerável já que, conhecendo-se uma pequena parte do texto original e o tamanho do bloco de letras utilizado (a ordem da matriz chave), é possível "quebrar" o algoritmo. Outra condição importante é que o alfabeto utilizado tenha um número primo de caracteres, garantindo a inversibilidade no corpo Z_m.

Mesmo assim, a *cifra de Hill* é um excelente instrumento didático, servindo como um sistema prático para aplicação de ferramentas matemáticas como: operações com matrizes, inversão de matrizes, cálculo de Determinantes e Aritmética modular.

BIBLIOGRAFIA

[1] - **SINGH**, Simon. O Livro dos Códigos. Rio de Janeiro: Record, 2001.

[2] - **COUTINHO**, S. C. Números Inteiros e Criptografia RSA. Rio de Janeiro: Série Computação e Matemática, SBM, 1997.

[3] - **TKOTZ**, Viktoria. Criptografia. Segredos Embalados Para Viagem. São Paulo: Novatec Editora, 2005.

[4] - **ANTON**, Howard. et al. Álgebra Linear com Aplicações. Porto Alegre: Bookman, 2005