CIFRA DE HILL

Autor: Maycon Pereira de Souza

Instituto Federal de Goiás – Campus Uruaçu.

maycon.souza@ifg.edu.br

Resumo

Vamos falar sobre um método criptográfico conhecido como Cifra de Hill, método este que foi inventado pelo matemático americano Lester S. Hill em 1929, e que se utiliza da Álgebra Linear para codificar e decodificar uma mensagem através da multiplicação de matrizes.

Figura 1: Lester S. Hill

Palavras-chave: Cifra de Hill; Matrizes; Criptografia; Aritmética Modular.

Preliminares

Em grego, *cryptos* significa secreto, oculto. A criptografia estuda os métodos para codificar e decodificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. A Criptografia é uma técnica de escrever mensagens cifradas que, ao longo da História, teve larga aplicação militar. O cidadão comum, contudo, até pouco tempo, talvez só tenha ouvido falar em criptografia ao assistir a filmes de guerra ou espionagem.

Mais recentemente, esta técnica passou silenciosamente a integrar o cotidiano, sem que se perceba, sistemas de caixas eletrônicos, home-banking, pay-per-view, entre outros, utilizam a criptografia como meio de conferir segurança às suas operações.

Neste artigo iremos tratar do método de Cifra de Hill (Criptografia em um alfabeto algébrico, 1929).

Conceitos

Uma mensagem codificada com uma matriz n x n é chamada de "n-Cifra de Hill". Logo, uma mensagem codificada com uma matriz 2x2 é chamada "2-Cifra de Hill, caso este que será o tratado aqui.

Método para codificar uma mensagem

Primeiro converte-se as letras em números, logo após agrupa-se os números 2 a 2 e multiplicam-se cada grupo por uma matriz quadrada de ordem 2, que seja inversível (ou seja, com determinante $\neq 0$). Os números resultantes são novamente passados para letras, e assim tem-se a mensagem codificada.

Caso algum resultado da multiplicação seja um número maior que o número de letras do alfabeto utilizado, assim utiliza-se o resto da divisão desse número pelo número de letras do alfabeto, que no nosso caso é 26, pois estamos considerando o alfabeto Inglês.

Supõe-se que cada letra de texto comum (mensagem que ainda não foi codificada) e de texto cifrado, excetuando o Z, tem o valor numérico que especifica sua posição no alfabeto padrão (Tabela 1).

Tabela 1: Alfabeto Padrão.

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
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

Passo 1. Escolhe-se uma matriz 2×2 com entradas inteiras para efetuar a codificação, $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ que seja inversível, e que seu determinante seja coprimo com 26, isto é, não possua fatores primos em comum, esta condição é importante para podermos encontrar a inversa dessa matriz módulo 26.

Passo 2. Agrupam-se letras sucessivas do texto comum em pares, adicionando uma letra fictícia para completar a mensagem, caso o texto comum tenha um número ímpar de letras, e substituem-se cada letra de texto comum pelo seu valor numérico.

Passo 3. Converte-se cada par sucessivo de letras de texto comum em um vetor-coluna $p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ e forma-se o produto *A.p*, que será o correspondente vetor cifrado**.**

Passo 4. Converte-se cada vetor cifrado em seu equivalente alfabético.

Antes de darmos um exemplo de codificação de uma mensagem, vamos falar um pouco sobre aritmética modular.

Aritmética Modular

Seja *m* um inteiro positivo e *a*, *b* dois inteiros quaisquer. Dizemos que *a* é congruente a *b* módulo *m* se *m* divide *a* - *b*. Quando *a* for congruente a *b* módulo *m*, escrevemos $a \equiv b (\text{mod } m)$.

Exemplos:

a) $19 \equiv 1(\text{mod } 3)$, pois (19 – 1) é múltiplo de 3, ou então 19 dividido por 3 deixa resto 1.

b) $47 \equiv 5(\text{mod } 6)$, pois (47 – 5) é múltiplo de 6, ou então 47 dividido por 6 deixa resto 5.

Dado um módulo *m*, pode-se provar que qualquer inteiro *a* é equivalente, módulo *m*, a exatamente um dos inteiros: 0, 1, 2, ..., *m*-1. Este inteiro é chamado o resíduo de *a* módulo *m* e escrevemos $Z_m = (0,1,2, ,m -1)$ para denotar o conjunto dos resíduos de *a* módulo *m*.

Observação: Se *a* é um inteiro não-negativo, então seu resíduo módulo *m* é simplesmente o resto da divisão de *a* por *m*.

Teorema

Dados um inteiro *a* e um módulo *m*, quaisquer, se $R = \text{resto de } \frac{|a|}{m}$ então o resíduo *r* de módulo *m* é dado por.

$$r = \begin{cases} R & \text{se } a \geq 0 \\ m - R & \text{se } a < 0 \text{ e } R \neq 0 \\ 0 & \text{se } a < 0 \text{ e } R = 0 \end{cases}$$

Vejamos como aplicar este teorema no exemplo a seguir.

Exemplo: Encontre o resíduo módulo 26 de:

a) 87

$R = \text{resto de } \frac{|a|}{m}$, como $a \geq 0$, tem-se: $r = R$.

$R = \text{resto de } \frac{|87|}{26}$, dividindo-se 87 por 26 dá um resto de $R = 9$, ou seja, $r = 9$. Assim, $87 \equiv 9 \pmod{26}$.

b) -38

$R = \text{resto de } \frac{|a|}{m}$, como $a < 0$ e $R \neq 0$, tem-se: $r = m - R$.

$R = \text{resto de } \frac{|-38|}{26}$, dividindo-se 38 por 26 dá um resto $R = 12$ e $r = 26 - 12 = 14$. Assim, $-38 \equiv 14 \pmod{26}$.

Pronto, já estamos aptos a dar um exemplo de codificação de mensagem.

Exemplo

Vamos codificar a mensagem: **CONFIRMADO**, com a matriz codificadora: $A = \begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix}$.

C	**O**	**N**	**F**	**I**	**R**	**M**	**A**	**D**	**O**
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
3	**15**	**14**	**6**	**9**	**18**	**13**	**1**	**4**	**15**

Após aplicarmos os passos 1, 2, 3 e 4, temos:

$$\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 15 \end{bmatrix} = \begin{bmatrix} 21 \\ 57 \end{bmatrix} = \begin{bmatrix} 21 \\ 5 \end{bmatrix} \begin{matrix} \text{U} \\ \text{E} \end{matrix}$$

Assim CO corresponde ao par UE, pois 5 é o resto da divisão de 57 por 26, isto é, $57 \equiv 5 \pmod{26}$.

$$\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 6 \end{bmatrix} = \begin{bmatrix} 34 \\ 10 \end{bmatrix} = \begin{bmatrix} 8 \\ 10 \end{bmatrix} \begin{matrix} \text{H} \\ \text{J} \end{matrix}$$

Assim NF corresponde ao par HJ.

$$\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} . \begin{bmatrix} 9 \\ 18 \end{bmatrix} = \begin{bmatrix} 36 \\ 63 \end{bmatrix} = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \begin{matrix} \text{J} \\ \text{K} \end{matrix}$$

Assim IR corresponde ao par JK.

$$\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} . \begin{bmatrix} 13 \\ 1 \end{bmatrix} = \begin{bmatrix} 27 \\ -9 \end{bmatrix} = \begin{bmatrix} 1 \\ 17 \end{bmatrix} \begin{matrix} \text{A} \\ \text{Q} \end{matrix}$$

Assim MA corresponde ao par AQ.

$$\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} . \begin{bmatrix} 4 \\ 15 \end{bmatrix} = \begin{bmatrix} 23 \\ 56 \end{bmatrix} = \begin{bmatrix} 23 \\ 4 \end{bmatrix} \begin{matrix} \text{W} \\ \text{D} \end{matrix}$$

Assim DO corresponde ao par WD.

Logo a mensagem codificada é **UE HJ JK AQ WD**, que seria normalmente transmitida como uma única cadeia sem espaços: **UEHJJKAQWD**.

Método para decodificar uma mensagem

Sabemos que na Aritmética usual, cada número não-nulo *a*, tem um inverso multiplicativo, denotado por a^{-1}, tal que $aa^{-1} = a^{-1}a = 1$.

Já, na Aritmética modular, tem-se o seguinte conceito correspondente: Dado um número *a* em Z_m, diz-se que um número a^{-1} é inverso multiplicativo de *a* módulo *m* se $aa^{-1} = a^{-1}a \equiv 1 (\text{mod}\, m)$. Pode ser provado que se *a* e *m* não têm fatores primos comuns, então *a* tem um único inverso multiplicativo módulo *m*; analogamente, se *a* e *m* têm fator primo comum, então *a* não tem inverso multiplicativo módulo *m*.

Para uma referência futura, fornece-se a seguinte tabela de inversos módulo 26:

Tabela 2: Inversos Módulo 26.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Para decifrar as Cifras de Hill, usa-se a inversa (mod 26) da matriz codificadora. Ou seja, se *m* é um inteiro positivo, pode-se dizer que uma matriz *A* com entradas em Z_m é invertível módulo *m* se existir uma matriz B com entradas em Z_m tal que $AB=BA \equiv I$ (mod *m*).

Suponha-se que: $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ é invertível módulo 26. Se $p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ é um vetor comum, então $c = A.p$ é o correspondente vetor cifrado e $p = A^{-1}c$.

Assim, cada vetor comum pode ser recuperado do correspondente vetor cifrado pela multiplicação à esquerda por $A^{-1} \pmod{26}$.

Em Aritmética Modular, uma matriz quadrada é invertível se, e somente se, det A ≠ 0. A inversa de det *A*(mod 26) é dada por:

$$A^{-1} = (a_{11}a_{22} - a_{12}a_{21})^{-1}.\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} (\text{mod} 26).$$

Então, para se encontrar a inversa de $\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix}$ módulo 26, faz-se:

det *A* = ad − bc = 2.4- 1.(-1) = 9, logo pela tabela 2, temos que o inverso multiplicativo de 9 módulo 26 é 3, assim temos:

$$A^{-1} = 3.\begin{bmatrix} 4 & -1 \\ 1 & 2 \end{bmatrix} (\text{mod} 26) = \begin{bmatrix} 12 & -3 \\ 3 & 6 \end{bmatrix} (\text{mod} 26) = \begin{bmatrix} 12 & 23 \\ 3 & 6 \end{bmatrix} (\text{mod} 26).$$

Portanto a inversa de *A* (mod 26) é $\begin{bmatrix} 12 & 23 \\ 3 & 6 \end{bmatrix}$.

Se quisermos decifrar a mensagem codificada para mensagem comum, basta aplicar a matriz inversa em cada um dos vetores cifrados, isto é, multiplicamos a esquerda a matriz inversa de *A* por cada um dos vetores cifrados, e assim obtemos os equivalentes alfabéticos destes vetores que fornecem a mensagem já decifrada.

Decodificando a mensagem **UEHJJKAQWD.**

Para decodificar o par UE, que corresponde aos números 21 e 5, temos:

$$\begin{bmatrix} 12 & 23 \\ 3 & 6 \end{bmatrix}.\begin{bmatrix} 21 \\ 5 \end{bmatrix} = \begin{bmatrix} 367 \\ 93 \end{bmatrix} = \begin{bmatrix} 3 \\ 15 \end{bmatrix} \begin{matrix} \text{C} \\ \text{O} \end{matrix}$$

Para decodificar o par HJ, que corresponde aos números 8 e 10, temos:

$$\begin{bmatrix} 12 & 23 \\ 3 & 6 \end{bmatrix}.\begin{bmatrix} 8 \\ 10 \end{bmatrix} = \begin{bmatrix} 326 \\ 84 \end{bmatrix} = \begin{bmatrix} 14 \\ 6 \end{bmatrix} \begin{matrix} \text{N} \\ \text{F} \end{matrix}$$

Para decodificar o par JK, que corresponde aos números 10 e 11, temos:

$$\begin{bmatrix}12 & 23\\ 3 & 6\end{bmatrix}.\begin{bmatrix}10\\ 11\end{bmatrix} = \begin{bmatrix}373\\ 96\end{bmatrix} = \begin{bmatrix}9\\ 18\end{bmatrix}\begin{matrix}\mathrm{I}\\ \mathrm{R}\end{matrix}$$

Para decodificar o par AQ, que corresponde aos números 1 e 17, temos:

$$\begin{bmatrix}12 & 23\\ 3 & 6\end{bmatrix}.\begin{bmatrix}1\\ 17\end{bmatrix} = \begin{bmatrix}403\\ 105\end{bmatrix} = \begin{bmatrix}13\\ 1\end{bmatrix}\begin{matrix}\mathrm{M}\\ \mathrm{A}\end{matrix}$$

Para decodificar o par WD, que corresponde aos números 23 e 4, temos:

$$\begin{bmatrix}12 & 23\\ 3 & 6\end{bmatrix}.\begin{bmatrix}23\\ 4\end{bmatrix} = \begin{bmatrix}368\\ 93\end{bmatrix} = \begin{bmatrix}4\\ 15\end{bmatrix}\begin{matrix}\mathrm{D}\\ \mathrm{O}\end{matrix}$$

Sendo assim temos a mensagem decodificada: **CO NF IR MA DO.**

E agrupando convenientemente as letras temos a mensagem decodificada: **CONFIRMADO.**

Referências

CASTRO, Elisangela R. D. de. **Álgebra linear e teoria dos números na criptografia**. 2012. 46 f. Trabalho de Conclusão de Curso (Especialização)- Universidade Tecnológica Federal do Paraná, Campo Mourão, 2012. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/handle/1/483>. Acesso em: 01 Jan. 2015.

COUTINHO, S.C.: **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

COUTINHO, S. C. **Criptografia**. Programa de Iniciação Científica OBMEP, IMPA, SBM, 2009.

Lester S. Hill, **Cryptography in an Algebraic Alphabet**, *The American Mathematical Monthly* Vol.36, June–July 1929, pp. 306–312.

SILVA. Sógenes G. P. da. **CRIPTOGRAFIA.** Disponível em: <http://pt.slideshare.net/sogenes/criptografia-1805777>. Acesso em: 02 Jan. 2015.

ZATTI, Sandra Beatris; BELTRAME, Ana Maria. **A presença da álgebra linear e teoria dos números na criptografia.** Disponível em: <http://www.unifra.br/eventos/jornadaeducacao2006/2006/pdf/artigos/matem%C3%A1tica/A%20PRESEN%C3%83A%20DA%20-LGEBRA%20LINEAR%20E%20TEORIA%20DOS%20N+MEROS%20NA%20CRIPT%C3%A0.pdf>. Acesso em: 01 Jan. 2015.