

Cifra de Hill

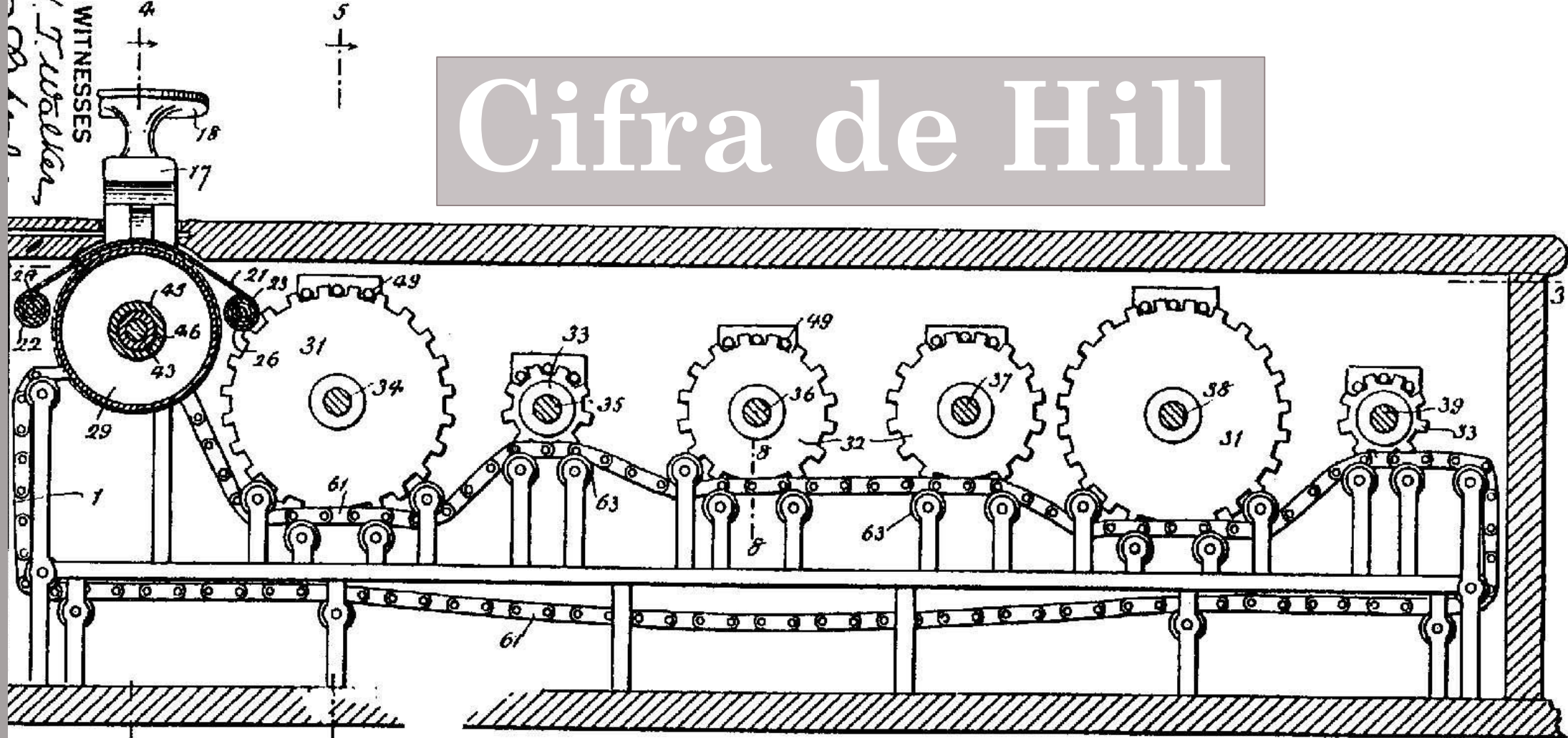
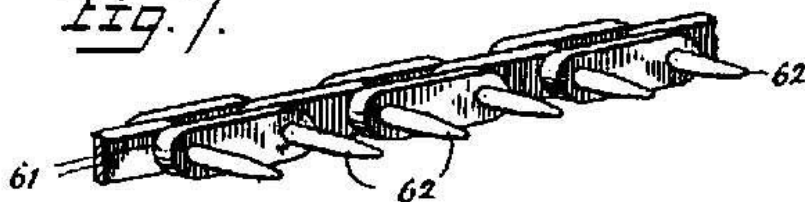


Fig. 7.



Grupo: André Vasconcelos
 Guilherme A. S. Pereira
 João Vitor V. Moraes
 Marcos Prysthon

BY

Louis Weisner and
 Lester S. Hill
 INVENTORS

Definição

A cifra de Hill é uma cifra de substituição baseada em álgebra linear em que se utiliza matrizes $n \times n$ para codificar mensagens. Nos slides a seguir, faremos uma demonstração da 2-cifra de Hill.

Criando uma cifra

Para a criação de uma cifra de Hill, é necessário uma matriz (senha) e fazer a conversão de cada letra para seu respectivo número usando a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	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	0

Exemplo de uma 2-cifra de Hill

Senha: A matriz formada pela senha deve ser invertível módulo 26

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix}$$

Para que a matriz cumpra a condição é necessário que sua determinante esteja na tabela abaixo:

Det	1	3	5	7	9	11	15	17	19	21	23	25
Det ⁻¹	1	9	21	15	3	19	7	23	11	5	17	25

Tabela de recíprocas módulo 26 da determinante

Divisão da frase em pares de letras

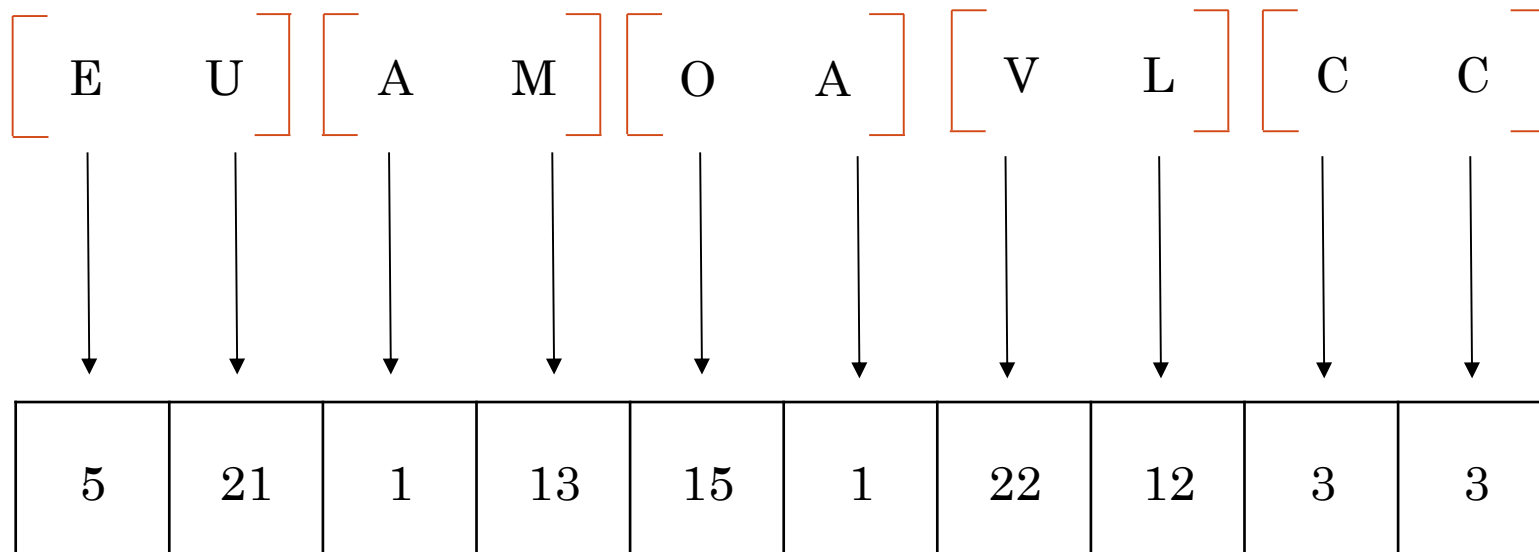
- A frase "Eu amo avlc" será dividida em:

[E U] [A M] [O A] [V L] [C C]

Quando a quantidade de letras de uma frase é ímpar, duplicaremos a última letra para formar um par.

Fazendo a correspondência das letras


Com os vetores de letras em mãos, vamos convertê-los em números:



Multiplicação da matriz senha pelos vetores

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 5 \\ 21 \end{bmatrix} = \begin{bmatrix} 47 \\ 110 \end{bmatrix}$$

Aplica mod 26 à matriz (pois os números não possuem equivalente alfabético na tabela)


$$\begin{bmatrix} 21 \\ 6 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

Multiplicação da matriz senha pelos vetores

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 13 \end{bmatrix} = \begin{bmatrix} 27 \\ 66 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 1 \\ 14 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

$$\begin{bmatrix} 21 & 6 \end{bmatrix}$$

Multiplicação da matriz senha pelos vetores

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 15 \\ 1 \end{bmatrix} = \begin{bmatrix} 17 \\ 20 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 17 \\ 20 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

$$\begin{bmatrix} 21 & 6 \end{bmatrix} \begin{bmatrix} 1 & 14 \end{bmatrix}$$

Multiplicação da matriz senha pelos vetores

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 22 \\ 12 \end{bmatrix} = \begin{bmatrix} 46 \\ 82 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 20 \\ 4 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

$$\begin{bmatrix} 21 & 6 \end{bmatrix} \begin{bmatrix} 1 & 14 \end{bmatrix} \begin{bmatrix} 17 & 20 \end{bmatrix}$$

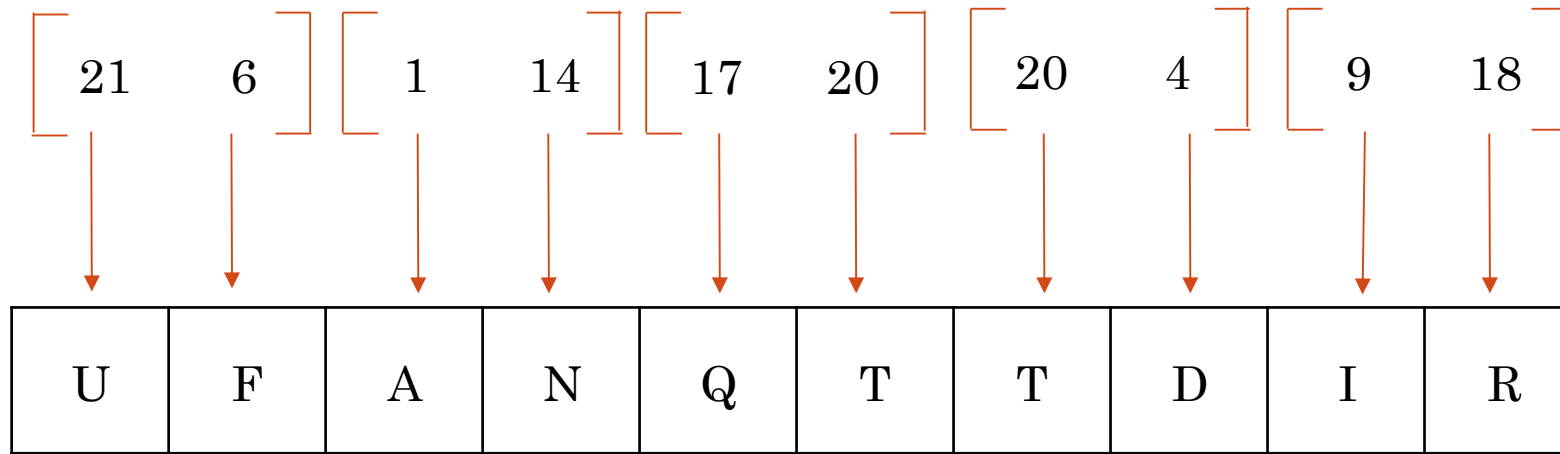
Multiplicação da matriz senha pelos vetores

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 9 \\ 18 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 9 \\ 18 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

$$\begin{bmatrix} 21 & 6 \end{bmatrix} \begin{bmatrix} 1 & 14 \end{bmatrix} \begin{bmatrix} 17 & 20 \end{bmatrix} \begin{bmatrix} 20 & 4 \end{bmatrix} \begin{bmatrix} 9 & 18 \end{bmatrix}$$

Fazendo as correspondências de pares de números



Decifrando a 2-Cifra de Hill

Do exemplo que acabamos de cifrar, pegamos a matriz formada pela senha e os pares de letras:

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix}$$

$$\begin{bmatrix} U & F \end{bmatrix} \begin{bmatrix} A & N \end{bmatrix} \begin{bmatrix} Q & T \end{bmatrix} \begin{bmatrix} T & D \end{bmatrix} \begin{bmatrix} I & R \end{bmatrix}$$

Encontrando a matriz inversa mod 26 da senha

$$A = \begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix} \quad \begin{array}{l} \text{Det}(A) = 1 \times 5 - 2 \times 1 = 3 \\ \text{Logo : } 3^{-1} = 9 \pmod{26} \end{array}$$

$$A^{-1} = 9 \begin{bmatrix} 5 & -2 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 45 & -18 \\ -9 & 9 \end{bmatrix} = \begin{bmatrix} 19 & 8 \\ 17 & 9 \end{bmatrix} \pmod{26}$$

Decifrando a 2-Cifra de Hill

Encontra-se a matriz inversa mod 26 da senha:

$$\begin{bmatrix} 1 & 2 \\ 1 & 5 \end{bmatrix}$$
$$\begin{bmatrix} 19 & 8 \\ 17 & 9 \end{bmatrix}$$

Faz a correspondência dos pares cifrados com os números da tabela:

U	F	A	N	Q	T	T	D	I	R
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
5	21	1	13	15	1	22	12	3	3

Multiplicação da matriz inversa da senha pelos pares

$$\begin{bmatrix} 19 & 8 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 21 \\ 6 \end{bmatrix} = \begin{bmatrix} 447 \\ 411 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 5 \\ 21 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

Multiplicação da matriz inversa da senha pelos pares

$$\begin{bmatrix} 19 & 8 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 1 \\ 14 \end{bmatrix} = \begin{bmatrix} 131 \\ 143 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 1 \\ 13 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

$$\begin{bmatrix} 5 & 21 \end{bmatrix}$$

Multiplicação da matriz inversa da senha pelos pares

$$\begin{bmatrix} 19 & 8 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 17 \\ 20 \end{bmatrix} = \begin{bmatrix} 483 \\ 469 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 15 \\ 1 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

$$\begin{bmatrix} 5 & 21 \\ 1 & 13 \end{bmatrix} \begin{bmatrix} 1 & 13 \end{bmatrix}$$

Multiplicação da matriz inversa da senha pelos pares

$$\begin{bmatrix} 19 & 8 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 20 \\ 4 \end{bmatrix} = \begin{bmatrix} 412 \\ 376 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 22 \\ 12 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

$$\begin{bmatrix} 5 & 21 \\ 1 & 13 \end{bmatrix} \begin{bmatrix} 1 & 13 \end{bmatrix} \begin{bmatrix} 15 & 1 \end{bmatrix}$$

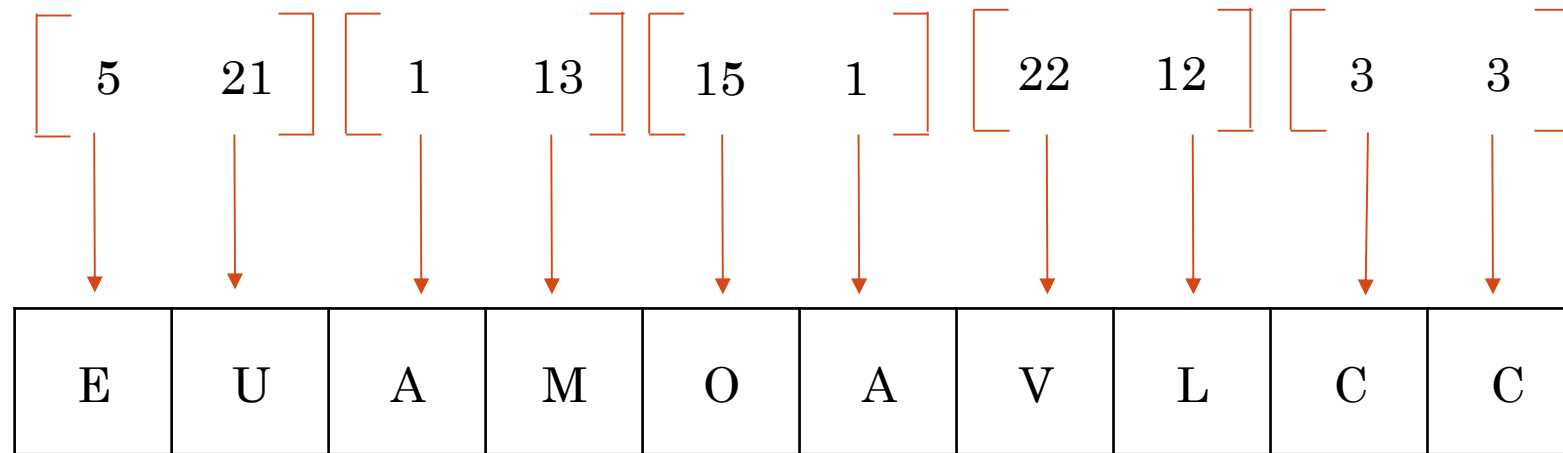
Multiplicação da matriz inversa da senha pelos pares

$$\begin{bmatrix} 19 & 8 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 9 \\ 18 \end{bmatrix} = \begin{bmatrix} 315 \\ 315 \end{bmatrix} \text{ Aplica mod 26 à matriz} \rightarrow \begin{bmatrix} 3 \\ 3 \end{bmatrix}$$

Matrizes resultantes da multiplicação:

$$\begin{bmatrix} 5 & 21 \\ 1 & 13 \end{bmatrix} \begin{bmatrix} 1 & 13 \\ 15 & 1 \end{bmatrix} \begin{bmatrix} 22 & 12 \\ 3 & 3 \end{bmatrix}$$

Fazendo as correspondências de pares de números



Eu amo avlc