História da Criptografia

(ou quase isso)

Eduardo Mendes (z4r4tu5tr4)

z4r4tu5tr4@babbge: screenfetch

Nome: Eduardo Mendes
Instituição: Fatec Americana
Uptime: 12097080s
Email: mendexeduardo@gmail.com
git: github.com/z4r4tu5tr4

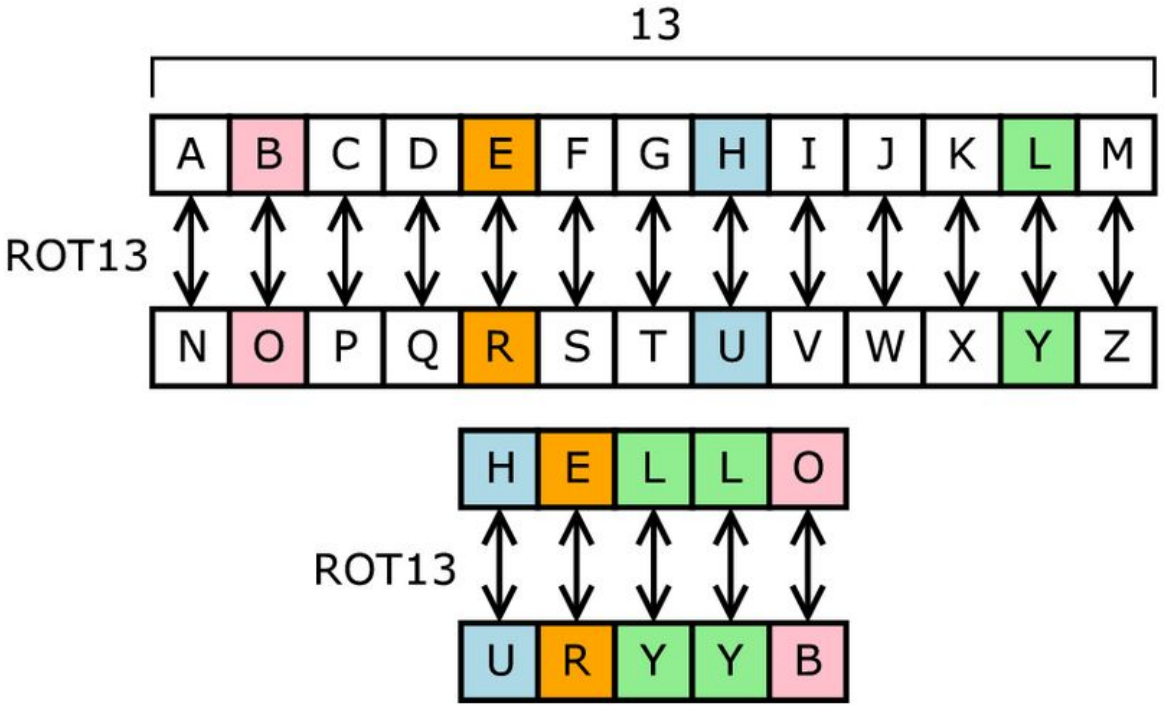
Sexo e substituição

Noções básicas de Kama-Sutra

Kama-Sutra, como assim?

- Criador: Vatsyayana
- Idade: 320 - 540 dc.
- Conteúdo: Posições sexuais
  Mulheres casadas
  Promiscuidade
  Prostituição
  Criptografia

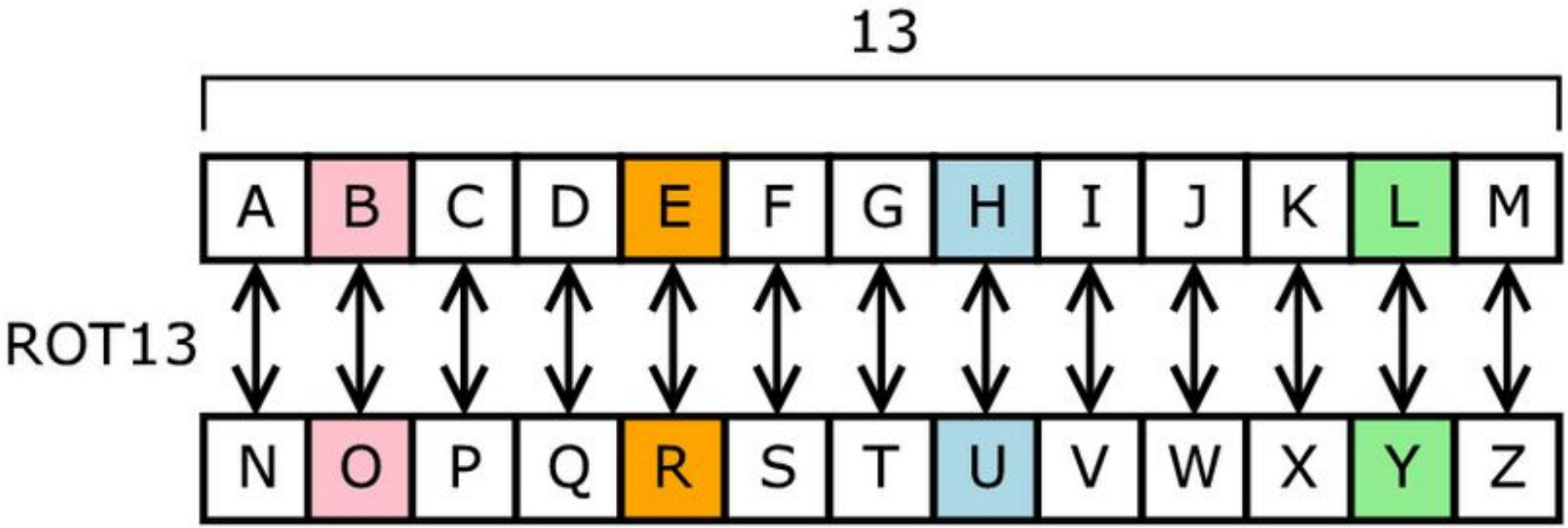
ROT13



Cifra de substituição

Texto claro:
Hello

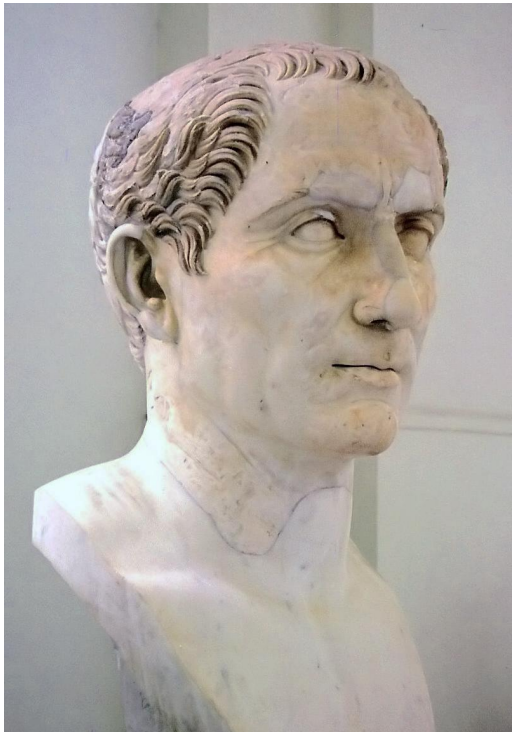
Texto criptografado
URYYB


13
A B C D E F G H I J K L M
ROT13
N O P Q R S T U V W X Y Z

Cesar e a monoalfabetização

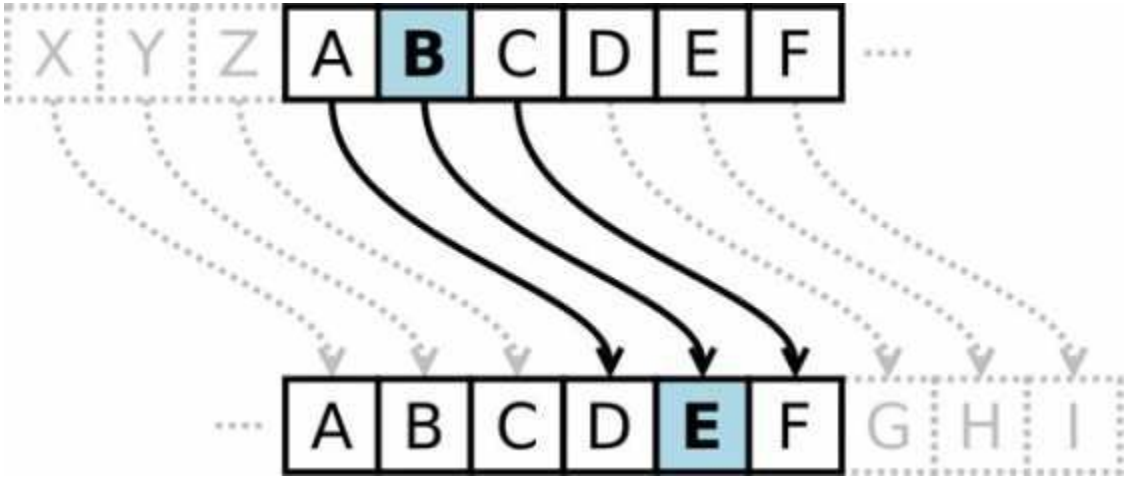
Milhares de variações

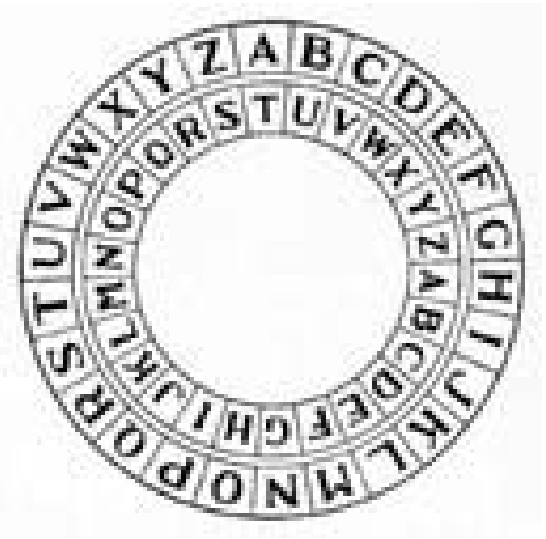
Gaius Julio Cesar



- Patrício
- Líder militar e político
- Responsável pela transformação da republica em império
- De Bello Civili

ROT 3





Belaso usou KY

O que é necessário para deslisar no redondo

Quem foi Belaso?

- 1505 - ?
- University of Padua in 1538
- Criação da cifra 1553

Cifra de vigenère

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

O que vamos precisar?

- Aritimética modular (outra vez)

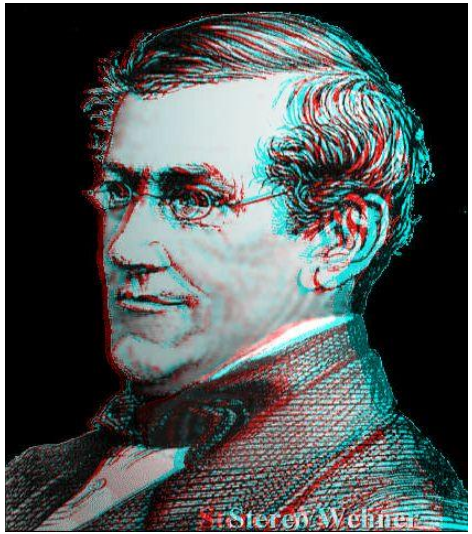
$$\sum_{K=C}^{L} (m + K) mod_A$$

$L =$ *longitud total del mensaje* $\qquad C = \{x | x$ *que sean caracteres de la clave*$\}$

Wheatstone saiu para jantar

Mas o sanfoneiro só toca isso

Quem foi Wheatstone?



- 1802 - 1875
- Inventor:
  - Estereoscópio
  - Cifra de Playfair
  - Ponte de Wheatstone (calculo de resistores)

Cifra de Playfair

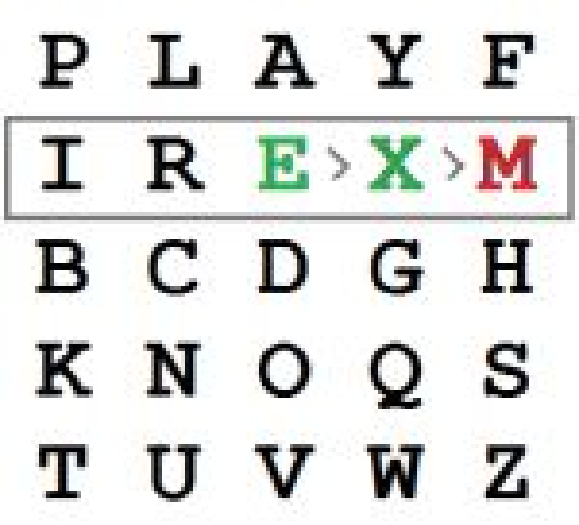
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
J	K	N	O	S
T	U	V	W	Z

- Cifra de bloco
- 3 regras
- Realmente usa matriz

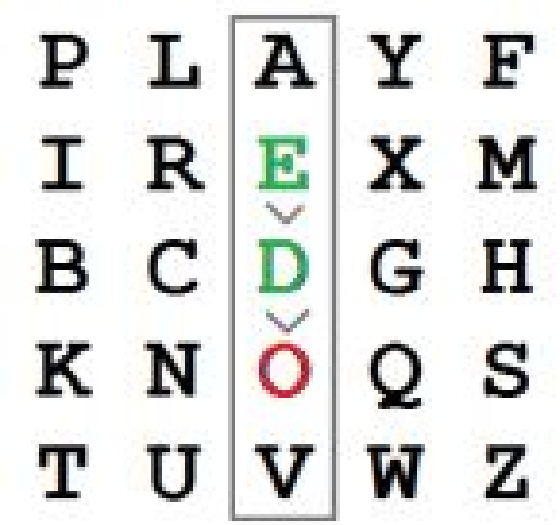
Cifra de Playfair

- Existem 3 operações
  - $\text{Shift}_{1 \bmod 5}$ de linha
  - $\text{Shift}_{1 \bmod 5}$ de coluna
  - $\text{Shift}_{N \bmod 5}^{C \bmod 5}$

Cifra de Playfair

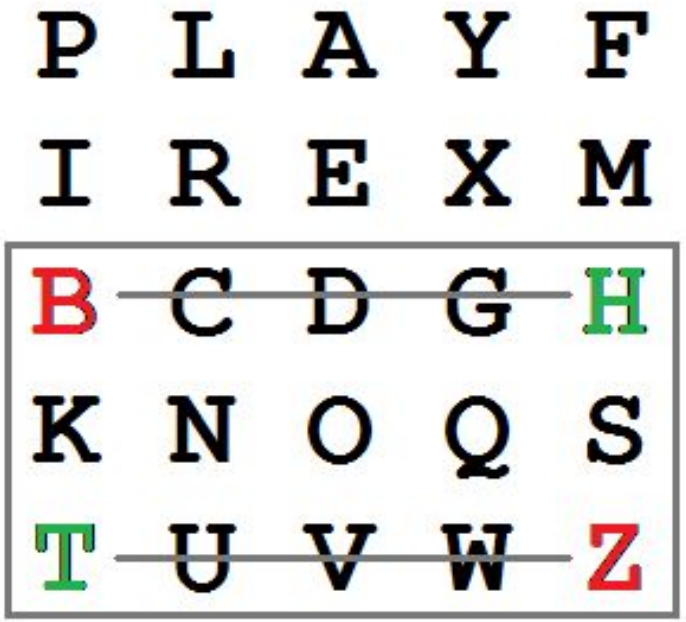


Shift$_1$ de linha



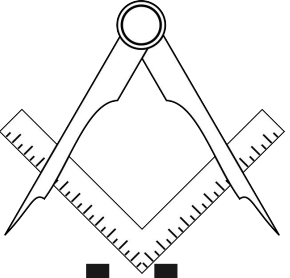
Shift$_1$ de coluna

Cifra de Playfair



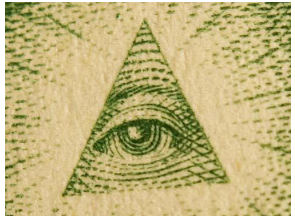
$Shift_N^C$

Onde Shift $_4^5$



Um novo emprego de marçoneiro

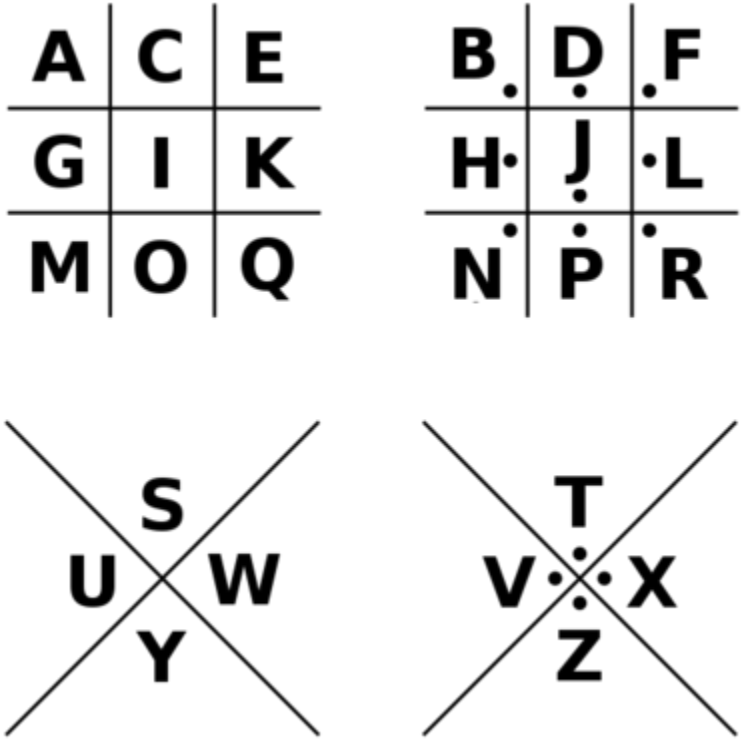
Ou algo que o valha



Cifra Maçonica

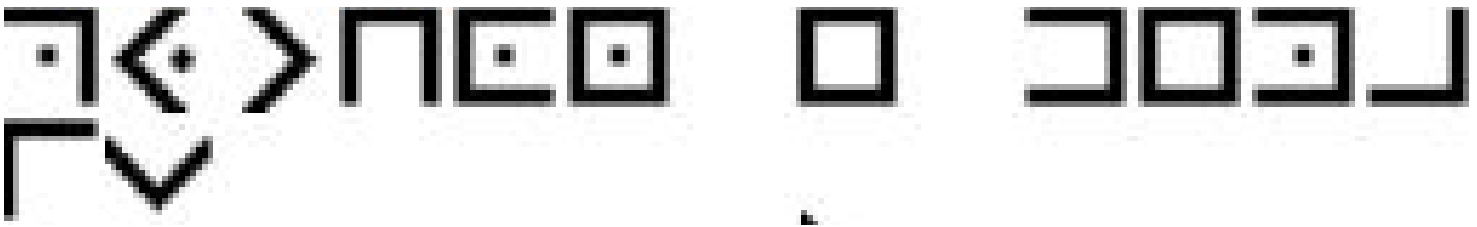
- Quem foram os maçons livres?
- Por que a necessidade de um código?

Cifra Maçonica



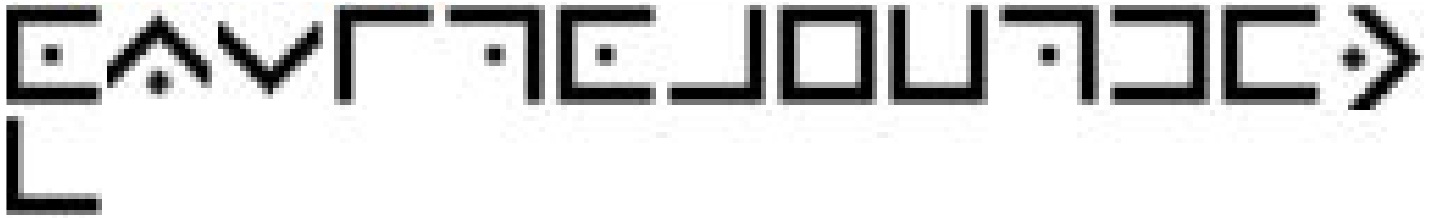
Desafios

1



Desafios

2



Cerca da ferrovia

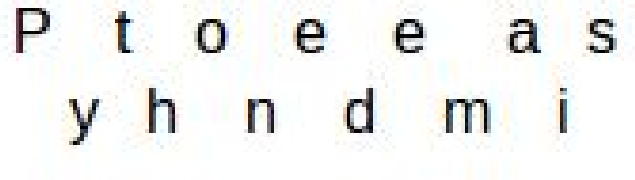
Brincadeira do trenzinho

Origens?

- Nunca se soube ao certo
- Meninos brincando do trilho do trem

Como funciona?

Python é demais



PTOEEASYHNDMI

XOXO

Duvidas?

mendesxeduardo@gmail.com