Introdução à Criptografia

Cifras Polialfabéticas

Prof. Rodrigo Minetto

rminetto@dainf.ct.utfpr.edu.br Universidade Tecnológica Federal do Paraná Fatos históricos de: O livro dos códigos de Simon Singh.

Sumário

- Introdução
- 2 Cifrando com Vigenère
- 3 Decifrando com Vigenère
- 4 Criptoanálise da Cifra de Vigenère

Cifra de Vigenère

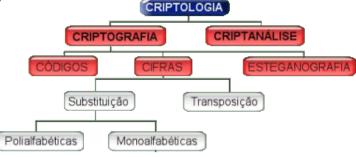
Em 1460, Leon Battista Alberti propôs o uso de dois ou mais alfabetos cifrados, usados alternadamente, para confundir os criptoanalistas. Esse foi o avanço mais significativo em cifras após um período de mil anos.

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

Texto original: **HELLO** → Texto cifrado: **AFPAD**

Cifra de Vigenère

Em uma cifra de **substituição polial- fabética** utilizam-se múltiplos cifrantes para substituir os caracteres de uma única mensagem.



Cifra de Vigenère

Uma cifra polialfabética muito conhecida é atribuída a Blaise de Vigenère (documentos mostram no entanto que a cifra foi primeiramente descrita por Giovan Batista Belaso em 1553). A cifra de Vigenère é um método de criptografia que usa uma série de diferentes cifras de César baseadas em letras e uma **senha**. Os franceses a apelidaram de "le chiffre indéchiffrable"

Sumário

- Introdução
- 2 Cifrando com Vigenère
- 3 Decifrando com Vigenère
- 4 Criptoanálise da Cifra de Vigenère

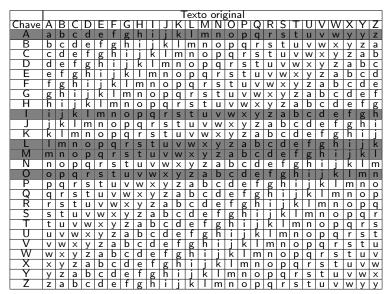
Quadrado de Vigenère

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н		J	K	L	М	N,	O	Р	Q	R	S	Т	U	V	W	X	Υ	Ζ
Α	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	z
В	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a
С	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b
D	d	е	f	g	h	<u>i</u>	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	у	z	a	b	С
E	е	f	g	h	<u>i</u>	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d
F	f	g	h	<u>i</u>	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e
G	g	h	i	j	k	<u> </u>	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f
H	h	i	Ĺ	k	Ш	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g
	İ	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	e	f	g	ĥ
J	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	ш
K	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	z	a	b	С	d	e	t	g	h	İ	لأبا
L_L		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	İ	j	k
M	m	n	0	р	q	r	S	t	и	٧	W	Х	У	z	a	b	С	d	е	f	g	h	Ĺ	į	k	Ш
N	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	е	f	g	h	i	Ĺ	k	ı	m
0	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	i	j	ķ		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	İ	į	k	ı	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	İ	j	k		m	n	0	р
Ŕ	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	İ	j	k		m	n	0	р	q
<u>S</u>	S	t	u	٧	W	Х	У	Z	a	b	c.	d	e	f	g	h	i.	į	ķ	ı	m	n	0	р	q	r
	t	u	٧	W	Х	У	Z	a	b	c.	d	e	t	g	h	į	į	ķ	ı	m	n	0	р	q	r	S
U	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	İ	j	k	ı	m	n	0	р	q	r	S	t
V	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	į	j	k	ı	m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	Ç	d	e	f	g	h	1	لٰہا	ķ		m	n	0	р	q	r	S	t	u	٧
X	Х	У	z	a	b	Ç	d	e	f	g	h	Ĺ	į	ķ	1	m	n	0	р	q	r	S	t	u	٧	w
Y	У	Z	a	b	Ç	d	e	f	g	h	-	Ĺ	ķ		m	n	0	р	q	r	S	t	u	٧	W	X
Z	Z	a	b	С	d	e	f	g	h	İ	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У

Chave = LIMAO

	Π										٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	ΙE	F	G	Н		J	K	L	М	N,	0	P	Q	R	S	T	U	V	W	X	Υ	Z
Α	a	b	С	d	е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	и	٧	w	У	У	z
В	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a
C	С	d	е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b
D	d	е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	а	b	С
E	e	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d
F	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e
G	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f
H	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f	g
	i	j	k	П	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d	е	f	ъ	h
J	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	f	g	h	i
K	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	Ь	U	d	е	f	g	h	-	j
L		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	U	d	е	f	g	h	i	۰.	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	ψ	f	g	h	i	j	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	ψ	f	g	h	i	j	k	_	m
0	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р
Ŕ	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k	1	m	n	0	р	q
S	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r
T	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k	ı	m	n	0	р	q	r	S
U	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	<u>i</u>	j	k	1	m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	С	d	е	f	g	h	<u>i</u>	<u>j</u>	k		m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	С	d	е	f	g	h	i	<u>_i</u> _	k		m	n	0	р	q	r	s	t	u	V
X	Х	У	z	a	b	С	d	е	f	g	h	l i	j	k		m	n	0	р	q	r	S	t	u	٧	w
_ Y _	у	Z	a	b	С	d	е	f	g	h	i	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	X
_ Z	z	а	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	V	w	у	у

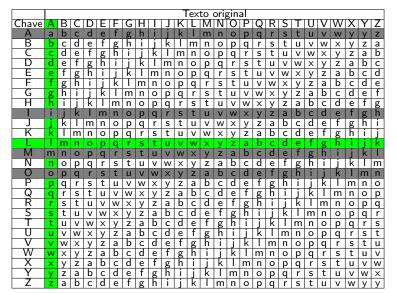
Chave = LIMAO



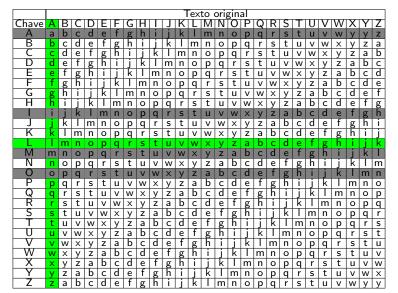
Texto = ATACARBASESUL e **Chave** = LIMAO

											٦	ex	to	orig	gin	al										
Chave	Α	В	C	D	E	F	G	Н	П	J	K	L	М	N.	0	Р	Q	R	S	Т	U	V	W	Χ	Y	Z
A	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a
С	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	w	Х	У	Z	a	Ь
D	d	е	f	g	h	<u>i</u>	j	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	у	z	а	b	С
E	е	f	g	h	i	<u>j</u>	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d
F	f	g	h	<u>i</u>	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	е
G	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f
H	h	i	<u>j</u>	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	_i_
K	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	از
L	Ш	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	_i_	j	k	
N	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	<u>i</u>	j	k		m
0	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	е	f	g	h	į į	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k	ı	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	f	g	h	i	j	k		m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q
S	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r
T	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	ı	m	n	0	р	q	r	S
U	u	٧	w	Х	У	Z	а	b	U	d	е	f	g	h	i	j	k	—	m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	C	а	е	f	g	h	i	j	k	_	m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	V
X	Х	У	z	a	b	С	d	υ	f	g	h	i	j	k	Г	m	n	0	р	q	r	S	t	а	٧	W
Υ	У	Z	a	b	С	d	е	f	g	h	i	j	k	Г	m	n	0	р	q	r	S	t	u	>	W	X
Z	Z	а	b	С	d	е	f	g	h	i	j	k	Г	m	n	0	р	q	r	S	t	u	٧	W	У	У

Texto = ATACARBASESUL e **Chave** = **L**IMAO



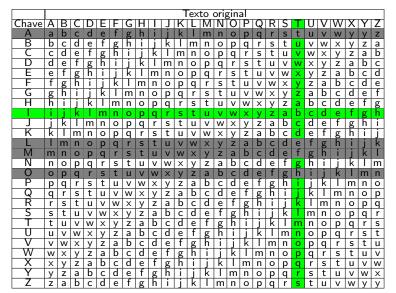
Texto = ITACARBASESUL e Chave = LIMAO



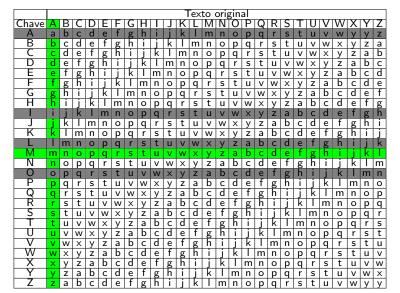
Texto = ITACARBASESUL e **Chave** = LIMAO

A a B b C C C C C C C C C C C C C C C C C C	Bbcdefghijk—mn		D d e f g h i j k I m n o p	<u>в е н ш ж — <mark>т</mark> п о р</u>	F	G mhijk — m n o p q r	H		k m n o p q	K k l m o p q r	L m n o p q r s t u	M n o p q r s t u v	Nnopqrstuv	O o p q r s t u v	P q r s t u v w	Q q r s t u v w x	R r s t u v w x y	S	t u v w x y z a b	U v w x y z a b	V W X y z a b	W X y z a b c	X Y Y Z Z Z Z Z Z Z Z Z Z	Y z a b c d e f	z a b c d e f
B b C c c D d E e e F f G g H h h I i J J J K k L I M m N n O O O P P P Q q q	c d e f g h i j k m n	def ghijken	e f g h i j k l m n	f	h i j k m n o p	hijk Imnopq		m n o p q r	m n o p q r	n o p q r	n o p q r s	n o p q r s t	o p q r s t u	p q r s t u v	q r s t u v w	r s t u v w	t u v w x y	t u v w x y z	v w x y z a	v w x y z a b	w x y z a b	y z a b	z a b c d	z a b c d e	a b c d e f
C c C D d E e e F f G g H h I i J J K k L I M m N n O O O P P P Q q q	d e f gh i j k m n	e f gh i j k m n	f g h i j k l m n		h i j k m n o p	i j k m n o p q	m n o p	m n o p q r	m n o p q r	n o p q r	n o p q r s	o p q r s t	p q r s t u	q r s t u v	r s t u v w	t u v w	t u v w x y	u v w x y z	v w x y z a	w x y z a b	y z a b	y z a b	z a b c d	a b c d e	b c d e f
D d E e F f f G g H h I I J J K K L I M M N n O O P P Q q q	e f ghi	f ghills	g h i j k l m n	h - - - - - - - - - - - - -	i j k m n o p	m n o p	m n o p	m n o p q r	n o p q r	n o p q r	o p q r s	p q r s t	q r s t u	r s t u v	t u v w	t u v w	u v w x	v W X y z	W X y z a	y z a b	y z a b c	z a b c	a b c d	b c d e	c d e f
E e F f G g H h I i J j K k L I M m N n O O P P Q q q	f gh:	m n	h i j k l m n	i-i-j-k-m m n o	m n o	m n o p	m n o p	n o p q r	n o p q r	o p q r	p q r s	q r s t	r s t u	s t u v	t u v w	u v w	v w x y	W X y z	y z a	y z a b	z a b c	a b c	b d	c d e	d e f
F f G g H h l i J j J J J J J J J J J J J J J J J J J	g h: j k m n	h i k m n	i k l m n	T m n o	m n o	m n o p	n o p q	n o p q r	o p q r	p q r	q r s	r s t	t u v	t u v	u v w	V W X	w x y	y z	y z a	z a b	a b c	b c	c d	d e	e
G g H h h i i j j j j j j j j j j j j j j j j	h j k m n	i k m n	j k l m n	T m n o	m n o	n o p q	n o p q	o p q r	p q r s	q r s	r s t	s t u	t u v	u v w	V W X	W X	x y	y z	z a	a b	b c	С	d	е	f
H h i i j j j K k L l M m N n O O O P P Q q	i k m n	n	n o	T m n o	n o p	n o p q	0 p q	p q r	q r s	r	s	t	u	V W	W X	Х	у	z	a	b	С		_		-
	m n	n	n o	n o	n o p	o p q	p q	q	r	S	t	u	٧	W	Х							d	е	†	g
M m N n O o P p Q q	m n	n	n o	n o	o p	p q	q	r	_		_		_			У	Z	a	b						
M m N n O o P p Q q	m n	n	n o	0	р	q	_		_	t	u	V	١٨/	~							d	е	f	g	h
M m N n O o P p Q q	n	n	0	_	_	_	r	S					**	Х	У	Z	a	b	С	d	e	f	g	h	ப்
M m N n O O P P P Q q	n	=		р	q	· ·		_	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	لل
N n O o P p Q q		0	n			1	S	t	u	٧	W	Χ	У	Z	a	b	С	d	е	f	g	h	i	j	k
O 0 P P Q q			р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	
P p Q q	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	<u>i</u>	j	k		m
Qq	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n
	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k		m	n	0
	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	е	f	g	h	i	j	k		m	n	0	р
R r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q
S s	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r
T t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S
Uu	٧	W	Х	У	z	a	b	c	d	e	f	g	h	i	j	ķ	1	m	n	0	р	q	r	S	t
	w	Х	у	Z	a	b	c	d	e	f	g	h	ĺ	j	k	ı	m	n	0	р	q	r	S	t	u
	Х	У	z	a	b	c	d	e	f	g	h	į	į	ķ	1	m	n	0	р	q	r	S	t	u	٧
X x	у	z	a	b	С	d	е	f	g	h	i	j	k	Т	m	n	0	р	q	r	S	t	u	٧	W
Yy	z	a	b	С	d	e	f	g	h	i	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х
Z z		lbl	l c l	d	e	f	g	h	i	Ιi	k l	-1	m	n	0	р	q	r	S	t	u	v	w	у	v

Texto = IbACARBASESUL e Chave = LIMAO



Texto = IbACARBASESUL e Chave = LIMAO



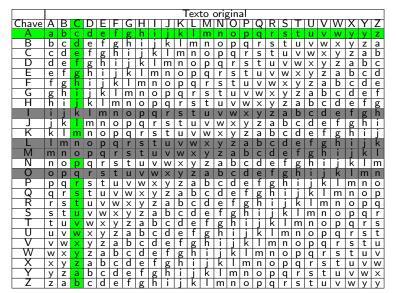
Texto = IbmCARBASESUL e Chave = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	H		J	K	L	M	N	0	Р	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	С	d	e	f	g	h	į	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a
C	С	d	e	f	g	h	İ	j	k		m	n	0	p	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	e	f	g	h	į	j	ķ	1	m	n	0	p	q	r	S	t	u	٧	W	Х	У	Z	a	b	С
Ē	e	f	g	h	1	Ţ	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d
F	t	g	h	ļ	Ţ	ķ		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e
G	g	h	1	Ţ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f
H	h	1	J	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	t	g
	Ţ	J	k	1	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	f	g	h
J	Į.	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	X	У	z	a	b	С	d	e	f	g	h	ĻĻ
K	ķ	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	z	а	b	С	d	e	f	g	h	1	L,
L	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	Ť	g	h	Ţ	Ţ	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	Ť	g	h		,	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	ļ.	Į.	k	_	m
0	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	Ť	g	h	ļ	J	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	t	g	h	-	Į.	k	1	m	n	0
Q	q	r	S	t	u	V	W	Х	У	Z	a	b	C	d	e	f	g	h	1	Į.	k	1	m	n	0	р
R	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	f	g	h	1	Į.	k	1	m	n	0	р	q
S	S	t	u	V	W	Х	У	Z	a	b	С	d	e	T	g	h	+	Į.	k	1	m	n	0	р	q	r
	t	u	V	W	X	У	Z	a	b	С	d	e	T	g	h.	ļ.	Į.	k	1	m	n	0	р	q	r	S
V	u	٧	W	X	<u>y</u>	Z	a	b	С	d	e	f	g	h	ļ.	Į.	k	1	m	n	0	р	q	r	S	t
W	V	W	X	У	Z	a	b	С	d	e f	T	g	h	ļ!	Ц.	k	1	m	n	0	р	q	r	S	t	u
X	W	X	У	z	a	b	C	d	e	-	g	h	H	H.	k	1	m	n	0	р	q	r	S	t	u	V
HŶ	X	У	z	a	b	C	d	e f	f	g	h	ļ!	Į,	k	1	m	n	0	p	q	r	S	t	u	V	W
T	У	Z	a	b	C	d	e	·	g	h	!	Į,	k		m	n	0	p	q	r	S	t	u	V	W	X
L	Z	а	b	С	d	e	<u> </u>	g	h		J	K		m	n	0	р	q	r	S	t	u	V	W	У	У

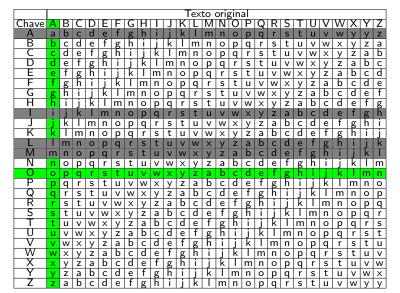
Texto = IbmCARBASESUL e Chave = LIMAO

											٦	ex	to	orig	gin	al										
Chave	Α	В	C	D	E	F	G	Н	П	J	K	L	M	N.	0	Р	Q	R	S	Т	U	V	W	X	Y	Ζ
Α	а	b	С	d	е	f	g	h	i	j	k	Т	m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	С	d	е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	V	w	Х	У	z	a
C	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	е	f	g	h	i	j	k	Т	m	n	0	р	q	r	S	t	и	٧	W	Х	У	z	а	Ь	С
E	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d
F	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e
G	g	h	Т	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	Ь	С	d	е	f
H	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	Ь	С	d	е	f	g
	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h
J	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	Ь	U	d	е	f	g	h	i
K	k		m	n	0	р	q	r	s	t	u	٧	W	Х	У	Z	а	Ь	U	d	е	f	g	h	i	j
L		m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	C	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	е	f	g	h	i	j	k	
N	n	0	р	q	r	S	t	u	>	W	Х	У	Z	a	b	С	d	ψ	f	ъ	h	i	j	k		m
0	0	р	q	r	S	t	u	٧	8	X	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	bg	h	-	j	k		m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	П	m	n	0	р
R	r	S	t	u	V	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	П	m	n	0	р	q
S	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	-	٠.	k	_	m	n	0	р	q	r
Т	t	u	٧	W	Х	у	Z	а	Ь	С	d	е	f	g	h	-	j	k	—	m	n	0	р	q	r	S
U	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u
W	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧
X	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	w
Y	У	Z	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	w	Х
Z	Z	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У

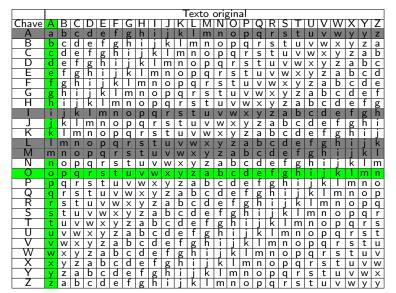
Texto = IbmcARBASESUL e Chave = LIMAO



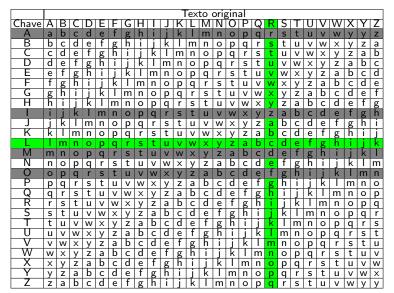
Texto = IbmcARBASESUL e Chave = LIMAO



Texto = IbmcoRBASESUL e Chave = LIMAO



Texto = IbmcoRBASESUL e Chave = LIMAO



Texto = IbmcocBASESUL e Chave = LIMAO

											٦	ex	to	orig	gin	al										
Chave	Α	В	C	D	E	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Τ	U	V	W	X	Υ	Ζ
_ A	а	b	С	d	е	f	g	h	i	j	k	Ш	m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	c	d	e	f	g	<u>h</u>	i	j	ķ		m	n	0	р	q	r	S	t	u	٧	w	Х	У	Z	a
С	С	d	e	f	g	h	Ĺ	j	k		m	n	0	p	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	е	f	g	h	İ	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С
E	е	f	g	h	Ĺ	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d
F	f	g	h	Ĺ	Ĺ	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e
G	g	h	i	Ĺ	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f
H	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	w	Х	У	z	а	b	С	d	е	f	g
	į	j	k	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	٧	w	Х	У	z	a	b	c	d	e	f	g	h	Li.
K	k	-	m	n	0	р	q	r	S	t	и	٧	W	Х	У	z	а	b	С	d	е	f	g	h	i	j
L	<u> </u>	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	i		k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	t	g	h	İ	j	k	
N	n	0	р	q	r	S	t	и	٧	W	Х	У	z	a	b	С	d	е	f	g	h	<u>i</u>	j	k	Ш	m
0	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	İ	į	k	ı	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	t	g	h	İ	j	k		m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	i	j	ķ		m	n	0	р	q
<u>S</u>	S	t	u	٧	w	Х	У	Z	a	b	С	d	e	f	g	h	Ĺ	į	ķ	1	m	n	0	р	q	r
I	t	u	٧	W	Х	У	Z	a	b	С	d	e	†	g	h	ļ.	Ĺ	ķ	ı	m	n	0	р	q	r	S
U	u	٧	w	Х	У	Z	a	b	c	d	e	f	g	h	į	Ĺ	ķ		m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	c	d	e	f	g	h	Ĺ	Ĺ	ķ	1	m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	c	d	e	f	g	h	L į	Ĺ	ķ	1	m	n	0	р	q	r	S	t	u	V
X	Х	У	z	a	b	С	d	e	f	g	h	Í	j	ķ	1	m	n	0	р	q	r	S	t	u	٧	w
Y	У	Z	a	b	c	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	X
_ Z	Z	а	b	С	d	e	f	g	h	i	∣ j	k		m	n	0	р	q	r	S	t	u	٧	W	У	у

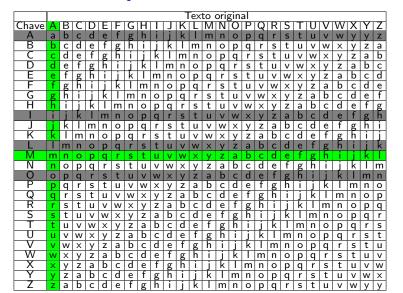
Texto = IbmcocBASESUL e Chave = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Τ	U	V	W	X	Y	Z
A	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	C	d	e	f	g	<u>h</u>	i	j	ķ		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а
C	С	d	е	f	g	h	Ĺ	j	k		m	n	0	p	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	е	f	g	h	İ	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	z	a	b	С
E	е	t	g	h	Ĺ	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d
F	f	g	h	İ	Ĺ	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e
G	g	h	j	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f
H	h	1	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	у	Z	а	b	С	d	е	f	g
	i	j	k	Т	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	t	g	h
J	j	k	Ш	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	f	g	h	Ĺ
K	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	t	g	h	Ĺ	لر
Ļ	Ш	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	Ç	d	e	f	g	h	į	į	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	t	g	h	İ	j	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k	Щ	m
0	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	e	t	g	h	ļ	J	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	z	a	b	Ç	d	e	f	g	h	1	Ļ	k	ı	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	t	g	h	_	Ţ	ķ	1	m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	1	Ţ	ķ	1	m	n	0	р	q
<u>S</u>	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	†	g	h	į	Ţ	k	ı	m	n	0	р	q	r
	t	u	٧	W	Х	У	z	a	b	c	d	e	†	g	h	1	Į.	ķ	1	m	n	0	р	q	r	S
U	и	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	1	Į,	k	1	m	n	0	р	q	r	S	t
V	٧	W	Х	У	Z	a	b	С	d	e	t	g	h	ļ.	Į,	k	1	m	n	0	р	q	r	S	t	u
W	W	Х	У	Z	a	b	c	d	e	f	g	ķ	!	Į,	k	1	m	n	0	р	q	r	S	t	и	٧
X	Х	У	z	a	b	C	d	e	f	g	h	1	Į,	k	1	m	n	0	р	q	r	S	t	и	٧	W
Y	У	Z	a	b	Ç	d	e	f	g	ḥ	!	Ţ	k		m	n	0	р	q	r	S	t	u	٧	W	Х
L	Z	a	b	С	d	e	<u> </u>	g	h	ı	J	K		m	n	0	р	q	r	S	t	u	V	W	у	У

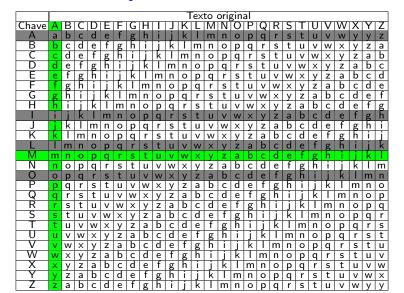
Texto = IbmcocjASESUL e **Chave** = LIMAO

	П										٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н	П	J	K	L	M	N	0	Р	Q	R	S	Τ	U	V	W	X	Y	Ζ
A	a	b	С	d	е	f	g	h	i	j	k		m	n	0	p	q	r	S	t	u	٧	W	У	у	Z
В	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Χ	У	Z	a
C	С	d	е	f	g	h	<u>i</u>	j	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b
D	d	е	f	g	h	i	j	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	у	Z	a	b	С
E	е	f	g	h	<u>i</u>	<u>j</u>	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d
F	f	g	h	i	j	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	у	z	a	b	С	d	e
G	g	h	į	j	ķ		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	е	f
H	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	t	g
	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	t	g	h
J	j	k	П	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	t	g	h	Ĺ
K	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	Ĺ	į
Ļ	Ш	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	C	d	e	f	g	h	į	į	k
M	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	e	†	g	h	ļ	Į	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e	t	g	h	1	LJ.	k		m
0	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	t	g	h	ļ	Į	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	z	a	b	Ç	d	e	t	g	ḥ	1	J	k	1	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e	Ť	g	h	-	J	k	1	m	n	0	р
Ŕ	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	T	g	h	-	Ţ	k	1	m	n	0	р	q
S	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	-	Ţ	k	1	m	n	0	р	q	r
<u> </u>	t	u	٧	W	X	У	z	a	b	С	d	e	f	g	ļ ḥ	1	Į.	k	1	m	n	0	р	q	r	S
U	u	٧	W	Х	У	z	a	b	С	d	e	f	g	ḥ	ļ.	J	k	-	m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	С	d	e	Ť	g	ḥ	ļ.	Ų.	k	_	m	n	0	р	q	r	S	t	u
W	W	Х	У	Z	a	b	C	d	e	Ť	g	h	ļ!	Ц.	ķ	1	m	n	0	р	q	r	S	t	u	V
X	Х	У	Z	a	b	С	d	e	Ť	g	h	ļ!	IJ.	k	Ц.	m	n	0	р	q	r	S	t	u	٧	W
Y 7	У	Z	a	b	C	d	e	T	g	h	!	Į.	k	1	m	n	0	р	q	r	S	t	u	٧	W	X
L	Z	а	b	С	d	е	<u> </u>	g	h	1	IJ	k		m	n	0	р	q	r	S	t	u	V	W	У	У

Texto = IbmcocjASESUL e Chave = LIMAO



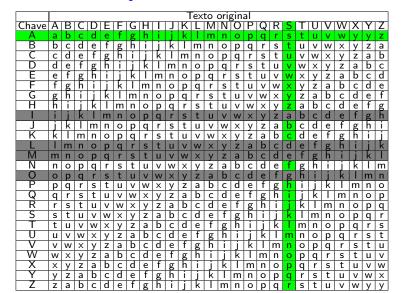
Texto = IbmcocjmSESUL e Chave = LIMAO



Texto = IbmcocjmSESUL e Chave = LIMAO

	П										٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	X	Y	Ζ
Α	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	X	У	Z	а
С	c	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	u	٧	w	Х	У	Z	a	b
D	d	e	f	g	h	i	j	k	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С
E	e	f	g	h	į	Ĺ	k	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d
F	t	g	h	į.	Ĺ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e
G	g	h	!	Ļ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f
H	h	1	Į.	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	t	g
	ļ	Į	k	L	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	а	b	С	d	e	f	g	h
Į.	Ļ	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	!
K	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	z	а	b	С	d	e	t	g	h		J
L		m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	C-	d	e	Ť	g	h	!	1	k
M	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	t	g	h		Į	K	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	T	g	h	ı.	Į.	k		m
P	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	е	Ť	g	h	Ļ	Ļ	k		m	n
	р	q	r	S	t	u	V	W	Х	У	z	a	b	C	d	e	f	g	h	!	J	k	1	m	n	0
Q R	q	r	S	t	u	V	W	X	У	Z	a	b	C	d	e	f	g	h	÷	J L	k	1	m	n	0	p
5	r	t	t	u	V	W	V	У	z	a b	b	d	d e	f	1	g h	h	+	J	k	I	m	n	0	p	ď
	t	-	u	V	w	X		z	a b	_	d	_	f	-	g	+	+	Ţ	k	m	m	n	0	p	q	r
l U	u	u	V	W	v	y z	Z	a b	b	d	e	e		g h	h	۱÷	k	k	m	m	n	0	р	q	r s	s t
$\frac{1}{V}$	v	<u> </u>	W	X	y Z	a	a b	C	đ	e	f		g h	۳.	H.	J k	Ĥ	m	m	n	0	р	q	r	t	_
- W	W	X	V	y z	a	b	C	đ	e	f	_	g h	!!	H	k	۱÷	m	m n	n	0	p	q	r	t	ι u	u v
X	X	V	y Z	a	b	C	đ	e	f	4	g h	+	H	k	۱÷	m	n	= 0	0	р	q	r	t	u u	u V	w
FŶ	V	y Z	a	b	C	d	e	f	_	g h	 ''	+	k	⊬	m	n	0	_	р	q	S	t	u u	u V	w	×
$\frac{1}{Z}$	y Z	a	-	C	đ	e	f	-	g	+	H	Ţ	Ť	m	-	0	_	р	q	S	t	_	v	w	۷۷	v
	<u>LZ</u>	a	b	L	u	Le		g	h		IJ	ĸ	<u> </u>	ш	n	LO	р	q		3	L	u	V	٧V	у	У

Texto = IbmcocjmsESUL e Chave = LIMAO



Texto = IbmcocjmsESUL e Chave = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	Ε	F	G	Н	П	J	K	L	M	N	0	Р	Q	R	S	Τ	U	V	W	Χ	Υ	Z
Α	a	b	С	d	е	f	g	h	i	l j	k		m	n	0	p	q	r	S	t	u	٧	W	У	у	z
В	Ь	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	s	t	а	٧	W	Х	У	Z	a
C	C	d	е	f	g	h	-	j	k		m	n	0	р	q	r	s	t	а	>	W	Х	У	Z	а	b
D	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	а	>	W	Х	у	Z	а	Ь	С
E	е	f	g	h	i.	j	k		m	n	0	р	q	r	S	t	u	>	٧	Х	У	Z	а	Ь	U	d
F	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	٧	Х	У	z	a	b	U	d	e
G	g	h	i	j	k		m	n	0	р	q	r	s	t	u	٧	W	Х	У	Z	a	b	С	d	е	f
Н	h	i	j	k	Ш	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	f	g	h	i
K	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	ازا
<u> </u>	Ш	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	
N	n	0	р	q	r	s	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k		m
O	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	į	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	1	J	k	ı	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	1	J	k		m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q
<u>S</u>	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	t	g	h	-	J	ķ	ı	m	n	0	р	q	r
!_	t	u	٧	W	Х	У	z	a	b	С	d	e	f	g	h	1	Ţ	k	ı	m	n	0	р	q	r	S
U	u	٧	w	Х	У	z	a	b	С	d	е	f	g	h	<u> i</u>	j	k		m	n	0	р	q	r	S	t
V	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	Ļ	Ĺ	ķ	1	m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	Ç	d	e	t	g	h	ļ.	Į,	ķ	1	m	n	0	р	q	r	S	t	и	V
X	Х	У	z	a	b	Ç	d	e	t	g	h	İ	Ĺ	ķ	ய	m	n	0	р	q	r	S	t	u	٧	w
Y	У	Z	a	b	С	d	e	t	g	h	Į.	j	k	ш	m	n	0	р	q	r	S	t	u	٧	W	Х
L	Z	a	b	С	d	е	<u> </u>	g	h	ı	J	K		m	n	0	р	q	r	S	t	u	٧	W	У	у

Texto = IbmcocjmssSUL e Chave = LIMAO

	П										٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	Е	F	G	H	П	J	K	L	M	M.	0	Р	Q	R	S	Т	U	V	W	X	Y	Z
Α	a	b	С	d	е	f	g	h	-	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	С	d	е	f	g	h	i	٠.	k	_	m	n	0	р	q	r	s	t	а	٧	W	Х	У	Z	a
С	С	d	е	f	g	h	i	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	у	Z	а	b	С
E	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d
F	f	g	h	<u>i</u>	j	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е
G	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f
H	h	<u>i</u>	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k		m	n	0	p	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i
K	k	<u> </u>	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	е	t	g	h	Ĺ	j
<u> </u>	Ш	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	C.	d	e	t	g	h	į	į	k
M	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	t	g	h	ļ	Ţ	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e	f	g	h	1	Į.	k		m
O	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	Ť	g	ḥ	Ļ	Į.	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	z	a	b	Ç	d	e	f	g	h	-	Ţ	k	1	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e	f	g	h	-	Ţ	k	1	m	n	0	р
R	r	S	t	u	V	W	X	У	z	a	b	С	d	e	Ť	g	h	+	J	k	1	m	n	0	р	q
<u> </u>	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	+	J.	k	1	m	n	0	р	q	r
l t	t	u	٧	W	Х	У	z	a	b	С	d	e	f	g	h	1	J.	k	1	m	n	0	р	q	r	S
	u	٧	W	X	У	z	a	b	С	d	e	f	g	h.	!	J.	k	1	m	n	0	р	q	r	S	t
W	٧	w	X	У	Z	a	b	С	d	e	T	g	h	Ļ.	Į.	k	1	m	n	0	р	q	r	S	t	u
	W	X	У	z	a	b	C	d	e	f	g	h	!	.	k	1	m	n	0	р	q	r	S	t	u	٧
X	X	<u>y</u>	Z	a	b	C	d	f	ſ	g	h	ļ!	Į,	k	1	m	n	0	p	q	r	S	t	u	V	W
Y	У	z	a	b	C	d	e	_	g	h	ļ.	Į.	k	<u> </u>	m	n	0	p	q	r	S	t	u	V	W	X
LZ	Z	a	b	С	d	е	_լ	g	h	П	J	k	<u> </u>	m	n	0	р	q	r	S	t	u	V	W	у	у

Texto = IbmcocjmssSUL e **Chave** = **L**IMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Τ	U	V	W	X	Υ	Ζ
A	a	b	С	d	е	f	g	h	-	l j	k		m	n	0	р	q	r	S	t	u	٧	W	У	у	z
В	b	С	d	е	f	g	h	-	٦.	k		m	n	0	р	q	r	s	t	а	٧	W	Х	у	Z	a
C	С	d	е	f	g	h	-	j	k		m	n	0	р	q	r	s	t	u	>	W	Х	У	Z	а	b
D	d	е	f	g	h	i	j	k	_	m	n	0	р	q	r	S	t	а	>	W	Х	у	Z	a	Ь	С
E	e	f	g	h	i	j	k	_	m	n	0	р	q	r	S	t	u	>	8	Х	У	Z	а	b	U	d
F	f	g	h	i	j	k	_	m	n	0	р	q	r	S	t	u	٧	٧	Х	У	Z	a	b	С	d	e
G	g	h	i	j	k	П	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d	е	f
Н	h	i	j	k		m	n	0	р	q	r	s	t	u	V	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	а	b	С	d	е	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	V	w	Х	У	Z	а	b	С	d	e	f	g	h	i
K	k		m	n	0	р	q	r	S	t	u	٧	w	Х	У	z	а	b	С	d	е	f	g	h	i	j
L	Ш	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	<u>b</u>	С	d	е	f	g	h	i	j	k		m
0	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	C	d	e	f	g	h	İ	j	k	ı	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	1	j	k		m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q
S	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r
	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	Ĺ	j	k	Т	m	n	0	р	q	r	S
U	u	٧	w	X	У	Z	a	b	С	d	е	f	g	h	<u> i</u>	Ĺ	k		m	n	0	р	q	r	S	t
V	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	<u> i</u>	Ĺ	k		m	n	0	р	q	r	S	t	u
W	W	Х	У	Z	a	b	c	d	е	t	g	h	i	Ĺ	<u>k</u>		m	n	0	р	q	r	S	t	u	V
X	Х	У	z	a	b	c	d	e	f	g	h	Į į	Ĺ	ķ	\perp	m	n	0	р	q	r	S	t	u	٧	w
Y	У	z	a	b	c	d	e	f	g	h	i	į	k	\perp	m	n	0	р	q	r	S	t	u	٧	W	X
Z	Z	а	b	С	d	е	†	g	h	İ	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	у

Texto = IbmcocjmssdUL e **Chave** = LIMAO

											٦	ex	to	ori	gin	al										\Box
Chave	Α	В	C	D	E	F	G	H	\Box	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	X	Υ	Ζ
A	a	b	С	d	е	f	g	h	į	j	ķ	1	m	n	0	р	q	r	S	t	и	٧	W	У	У	Z
В	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	X	У	Z	a
C	c	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	c
E	e	f	g	h	į	Ĺ	k	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	c	d
F	f	g	h	į	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e
G	g	h	Ì	j	k	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	е	f
H	h	Ĺ	Ĺ	k	<u> </u>	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	f	g
	ļ	J	k	Ш	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	†	g	h
J	Ţ	ķ		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	1
K	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	у	z	a	b	U.	d	е	t	g	h	1	Ų.
L	Ш	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	e	Ť	g	ḥ	1	Ţ	k
M	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	е	t	g	h	ļ	Į	k	
N	n	0	p	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	1	Į.	k	1	m
0	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	Ť	g	h	ļ	J	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	z	a	b	Ç	d	e	f	g	ḥ	-	Ţ	k	1	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e	f	g	h	-	Ţ	k		m	n	0	р
R	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	ļ ţ	g	h	_	J.	k	1	m	n	0	р	q
S	S	t	u	٧	W	X	У	z	a	b	С	d	e	f	g	h.	+	J	ķ	1	m	n	0	р	q	r
	t	u	V	W	X	У	z	a	b	С	d	e	f	g	ļ ḥ	ļ.	J.	k	_	m	n	0	р	q	r	S
U	u	٧	W	X	У	z	a	b	С	d	e	f	g	h.	ļ.	Į.	k	1	m	n	0	р	q	r	S	t
V	٧	w	X	У	z	a	b	С	d	e	f	g	h	Ļ.	Į.	ķ	1	m	n	0	р	q	r	S	t	u
W	W	X	У	z	a	b	C	d	e	Ť	g	h	ļ!	Ц.	ķ	1	m	n	0	р	q	r	S	t	u	٧
X	X	У	Z	a	b	C	d	e	f	g	h	ļ!	Į,	k	<u> </u>	m	n	0	p	q	r	S	t	u	V	W
Y	У	Z	a	b	C	d	e	T	g	h	ļ!	Į.	k	1	m	n	0	p	q	r	S	t	u	V	W	X
L	Z	a	b	С	d	e	<u> </u>	g	h	1	IJ	K	<u> </u>	m	n	0	р	q	r	S	t	u	V	W	У	у

Texto = IbmcocjmssdUL e **Chave** = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н	Т	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	Χ	Υ	Ζ
<u> </u>	a	b	С	d	е	f	g	h	i	j	ķ		m	n	0	р	q	r	S	t	u	٧	W	У	у	z
В	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	X	У	Z	a
C	c	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	у	Z	a	b	c
E	e	f	g	h	į	j	k	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	c	d
F	f	g	h	į.	لٰہ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e
G	g	h	!	Ļ	ķ		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f
H	h	1	J	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	t	g
	ļ	Į	k	Ш	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	t	g	h
J	Ţ	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	†	g	h	1
K	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d	e	t	g	h	1	1
L	ш	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	C	d	e	Ť	g	h		Ţ	k
M	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	f	g	h	ļ	Į	k	4
N	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	1	J	k	1	m
P	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	Ť	g	h	1	Į.	k		m	n
	р	q	r	S	t	u	V	W	X	У	z	a	b	C	d	e	f	g	h	1	Į.	k	1	m	n	0
Q R	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	f	g	h	-	J	k	1	m	n	0	р
5	r	S	t	u	V	W	X	У	Z	a	b	C	d	e	†	g	h	+	J	k		m	n	0	p	q
 }	s t	t	u	V	w	X	<u>y</u>	z	a	b	d	d	e	f	g	h	+	J	k	1	m	n	0	p	q	r
Ü	-	u	V	W	X	У	z	a b	b	d	_	e	f	g h	h	+	Ţ	k	1 2	m	n	0	p	ď	r	s t
V	u	V	W	X	y	z	a	_	d	_	f		g h	111	۱÷	J	k	1 2	m	n	0	p	ď	r	S	_
- W	V	W	X	y	Z	a	b	d	_	e	_	g h	111	H÷.	H	k	<u></u>	m	n	0	p	ď	r	s t	t	u
X	W	v	y	z a	a b	b	d c	e	e f	1	g h	+	H	k	k	m	m n	n	0	р	q	r	s t	L U	u v	W
$\vdash \hat{\lor}$	V		Z	b	_	d	_	f	_	g	11	÷	H	۱÷	١			0	р	q	_	t	_	-	-	-
7	z	z a	a	C	C d	_	e	<u>_</u>	g	h	H	1	k	<u>ا</u>	m	n	0	р	q r	r	S +	_	u	V	W	×
	Į Z	а	b	L	d	е		g	h		IJ	ĸ	<u> </u>	m	n	0	р	q	1	S	L	и	V	W	У	у

Texto = lbmcocjmssdcL e **Chave** = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Η		7	K	L	M	N	0	Р	Q	R	S	Н	U	V	W	X	Υ	Z
A	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	Ь	С	d	е	f	g	h	-	j	k	_	m	n	0	р	q	r	s	t	а	٧	W	Х	У	Z	а
С	C	d	е	f	g	h	-	j	k	_	m	n	0	р	q	r	S	t	а	>	W	Х	У	Z	а	b
D	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	а	>	W	Х	у	Z	а	Ь	С
E	е	f	g	h	i	j	k	_	m	n	0	р	q	r	S	t	u	>	٧	Х	У	Z	а	Ь	U	d
F	f	g	h	i	j	k	_	m	n	0	р	q	r	S	t	u	٧	٧	Х	У	Z	а	b	U	d	е
G	g	h	i	j	k		m	n	0	р	q	r	s	t	u	٧	W	Х	У	Z	а	b	С	d	е	f
Н	h	i	j	k		m	n	0	р	q	r	s	t	u	V	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	V	w	Х	У	Z	а	b	С	d	е	f	g	h	i
K	k		m	n	0	р	q	r	S	t	u	٧	w	Х	У	z	а	b	С	d	е	f	g	h	i	j
L		m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	е	f	g	h	i	j	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	<u>b</u>	С	d	е	f	g	h	i	j	k		m
0	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	C	d	e	f	g	h	İ	j	k	ı	m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	İ	j	k		m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k	1	m	n	0	р	q
S	S	t	u	٧	w	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k	ı	m	n	0	р	q	r
_ l	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	Ĺ	j	k		m	n	0	р	q	r	S
U	u	٧	w	Х	У	Z	a	b	С	d	е	f	g	h	<u> i</u>	Ĺ	k		m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	С	d	е	f	g	h	<u> i</u>	Ĺ	k		m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	Ç	d	e	t	g	h	Ļ	للا	ķ		m	n	0	р	q	r	S	t	u	٧
X	Х	У	z	a	b	c	d	e	t	g	ḥ	Į į	Ĺ	ķ	\perp	m	n	0	р	q	r	S	t	u	٧	W
<u>Y</u>	У	Z	a	b	Ç	d	e	t	g	h	İ	Ĺ	ķ	Ш	m	n	0	р	q	r	S	t	u	٧	W	Х
L	Z	a	b	С	d	е	<u> †</u>	g	h	İ	j	k		m	n	0	р	q	r	S	t	и	٧	W	У	У

Texto = IbmcocjmssdcL e Chave = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н		J	K	Ļ	М	N	0	Р	Q	R	S	Т	U	V	W	Χ	Υ	Z
A	a	b	С	d	е	f	g	h	i	j	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	X	У	Z	a
C	С	d	e	f	g	h	i	j	k		m	n	0	p	q	r	S	t	и	٧	W	Х	У	Z	a	b
D	d	е	f	g	h	i	j	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	у	Z	а	b	С
E	е	f	g	h	<u>i</u>	<u>j</u>	k		m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d
F	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	٧	Х	У	z	a	b	U	d	е
G	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f
Н	h	i	j	k		m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	а	b	С	d	е	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	V	w	Х	У	Z	а	b	С	d	e	f	g	h	i
K	k		m	n	0	р	q	r	S	t	u	٧	w	Х	У	z	а	b	С	d	e	f	g	h	i	j
L		m	n	0	р	q	r	S	t	u	V	W	×	У	Z	a	b	С	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	<u>b</u>	С	d	е	f	g	h	<u>i</u>	j	k		m
0	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n
Р	р	q	r	S	t	u	V	W	Х	У	z	а	b	С	d	e	f	g	h	Ì	j	k		m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	İ	j	k		m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q
S	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	ı	m	n	0	р	q	r
T	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	ı	m	n	0	р	q	r	S
U	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	<u>i</u>	j	k	1	m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k	1	m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	С	d	е	f	g	h	i	<u>j</u>	k		m	n	0	р	q	r	S	t	и	٧
X	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W
Y	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х
Z	Z	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	у

Texto = Ibmcocjmssdcx e Chave = LIMAO

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 b c d e f g h i												٦	ex	to		gin	al										
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 b c d e f g h i	Chave	Α	В	C	D	E	F	G	Н		J	K	L	М	N	0	Р	Q	R	S	Т	U	V	W	X	Υ	Ζ
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 c d e f g h i j		a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	V	W	У	У	Z
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 d e f g h i j k	В	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	X	у	Z	а
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 e f g h i j k l	C	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	w	X	У	z	a	b
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 f 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 g 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 h i j k		d	е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С
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 g h i j k l m n		е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	а	b	С	d
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 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 h i 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 j k l m n o p		f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	у	Z	a	b	С	d	е
	G	g	h	i	j	k	П	m	n	0	р	q	r	s	t	u	٧	W	Х	У	Z	a	b	С	d	е	f
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 j k L I m n o p q r s t u v w x y z a b c d e f g h i j k M m n o p q r s t u v w x z a b c d e f g h i j k I m n s t u v w x z a b c d e f g h i j k I m n	H	h	i	j	k	Т	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g
K K I m n o p q r s t u v w x y z a b c d e f g h i j k M m n o p q r s t u v w x y z a b c d e f g h i j k M m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a b c d e f g h i j k J m n o p q r s t u v w x y z a		i	j	k	T	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h
L I m n o p q r s t u v w x y z a b c d e f g h i j k I M n o p q r s t u v w x y z a b c d e f g h i j k I N n o p q r s t u v w x y z a b c d e f g h i j k I m n o p q r s t u v w x y z a b c d e f g h i j k I m n o p q r s t u v w x y z a b c d e f g h i j k I m n o p q r s t u v w x y z a b c d e f g h i j k I m n o p q r s t u v w x y z a b c d e f g h i j k I m n o p q r s t u v w x y z a b c d e f g h i j k I m n o p q r s t u v w x y z a b c d e f g h i j k I m n o p q r s t u v w x y z a b c d e f g h i j k I m n o p q r T t u v w x y z a b c d e f g h i j k I m n o p q r s t u v w x y z a c x x y z a b c d e f g h i j k I m	J	j	k	П	m	n	0	р	q	r	s	t	u	٧	w	Х	У	z	а	b	С	d	е	f	g	h	i
M m n o p q r s t u v w x y z a b c d e f g h i j k l m n o p q r s s t u v w x y z a v x y z a b c d e f g h i j k l m n	K	k	П	m	n	0	р	q	r	s	t	u	٧	w	Х	У	z	а	b	С	d	е	f	g	h	i	j
N n o p q r s t u v w x y z 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 c z a b c d e f g m o q n o c d e f g m o q n o c d e f g m o q n o c d e f g m o q n o c d	L		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k
O o p q r s t u v w x y z a b c d e f g h i j k l m n c Q q r s t u v w x y z a b c d e f g h i j k l m n c Q q r s t u v w x y z a b c d e f g h i j k l m n c Q q r s t u v w x y z 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 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 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 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 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 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 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 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 b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x x y z a b c d e f g h i j k l m n o p q r s t u v x x x x x y z a b c d e		m	n	0	р	q	r	S	t	u	٧	w	Х	У	Z	а	b	С	d	е	f	g	h	i	j	k	
P p q r s t u v w x y z a b c d e f g h i j k I m n o p Q q r s t u v w x y z a b c d e f g h i j k I m n o p q r s t u w x y z a b c d e f g h i j k I m n o p q r s t u w x y z a b c d e f g h i j k I m n p q r		n	0	р	q	r	s	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k	П	m
Q q r s t u v w x y z a b c d e f g h i j k l m n o p q S t u v w x y z a b c d e f g h i j k l m n o p q S s t u v w x y z 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 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 b c d e f g d 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 d 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 d h i j k l m n o p q r s t u v	0	0	р	q	r	S	t	u	٧	W	X	У	Z	а	b	С	d	е	f	g	h	i	i	k	П	m	n
Q q r s t u v w x y z a b c d e f g h i j k l m n o p q S s t u v w x y z 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 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 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 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 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 x y z 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 c x y z 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 c x y z 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 c x y z 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 c x y z 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 c x y z 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 c x y z 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 c x a b c c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g g h i v y w x y z a c x a b c c d e f g g h i v y x x a c x a b c c d e f g g h i v y x a c x a b c c d e f g g h i v y x a c x a b c c d e f g g h i v y x a c x a b c c d e f g g h i v y x a c x a b c c d e f g g	Р	р	q	r	s	t	u	٧	w	Х	У	z	а	Ъ	С	d	е	f	g	h	T	j	k	П	m	n	0
S		q	r	s	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g		i	j	k	Т	m	n	0	р
T t u v w x y z a b c d e f g h i j k l m n o p q r s t U u v w x y z a b c d e f g h i j k l m n o p q r s t V v w x y z a b c d e f g h i j k l m n o p q r s t u W w x y z a b c d e f g h i j k l m n o p q r s t u X x y z 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 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 b c d e f g h i j k l m n o p q r s t u v w X x y z 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g g h i i j k l m n o p q r s t u v w x x y z a b c d e f g g h		r	S	t	u	٧	w	Х	У	Z	а	Ь	С	d	е	f	g	h	i	j	k	Т	m	n	0	р	q
U u v w x y z a b c d e f g h i j k l m n o p q r s t u V v w x y z a b c d e f g h i j k l m n o p q r s t u W w x y z 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 b c d e f g h i j k l m n o p q r s t u v w X x y z a b c d e f g h i j k l m n o p q r s t u v w Y y z a b c d e f g h i j k l m n o p q r s t u v w x	S	S	t	u	٧	w	Х	У	Z	а	b	С	d	е	f	g	h	i	j	k	Т	m	n	0	р	q	r
V v w x y z 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 b c d e f g h i j k l m n o p q r s t u v x x y z a b c d e f g h i j k l m n o p q r s t u v w Y y z a b c d e f g h i j k l m n o p q r s t u v w Y y z a b c d e f g h i j k l m n o p q r s t u v w x	T	t	u	٧	w	Х	У	Z	a	b	С	d	е	f	g	ĥ	i	j	k	Т	m	n	0	р	q	r	S
V v w x y z 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 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 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 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 b c d e f g h i j k l m n o p q r s t u v w x	U	u	V	w	Х	У	z	a	Ь	С	d	е	f	g	ĥ	i	i	k	Т	m	n	0	р	q	r	s	t
W w x y z a b c d e f g h i j k l m n o p q r s t u v w x x y z 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 b c d e f g h i j k l m n o p q r s t u v w x x y z a b c d e f g h i j k l m n o p q r s t u v w x x x x x x x x x	V	٧	w	Х	У	z	а	Ь	С	d	е	f	g		ī	T	k	Т	m	n	0	р	q	r	S	t	u
X x y z 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 b c d e f g h i j k l m n o p q r s t u v w x	W	w	х	У	z	a	Ь	С	d	е	f	g		i	Ιī	k	Т	m	n	0	р	_	_	s	t	и	V
Y y z a b c d e f g h i j k l m n o p q r s t u v w x	X	Х	٧	z	a	Ь	С	d	е	f	g		i	i	k	Т	m	n	0	р	_	_	s	t	и	٧	w
	Y	٧	ź	а	Ъ	С	d	е	f	g		i	Ť	k	Т	m	n	0	р	_	_	s	t	u	٧	w	X
	Z	z	а	Ь	С	d	е	f	g	h	i	i	k	Т	m	n	0	р	q	r	s	t	u	V	w	У	У

Sumário

- Introdução
- 2 Cifrando com Vigenère
- 3 Decifrando com Vigenère
- 4 Criptoanálise da Cifra de Vigenère

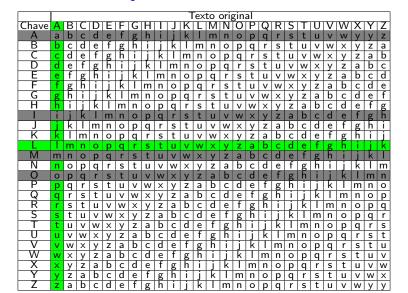
Texto = lbmcocjmssdcx e **Chave** = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	H	Т	J	K	Ļ	M	N	0	Р	Q	R	S	Т	U	V	W	Χ	Υ	Ζ
Α	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	s	t	u	٧	W	у	у	z
В	Ь	С	d	е	f	g	h	i	j	k	_	m	n	0	р	q	r	s	t	а	>	W	Х	у	Z	a
С	C	d	е	f	g	h	i	j	k		m	n	0	р	q	r	s	t	а	>	W	Х	У	Z	a	b
D	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	а	>	W	Х	у	Z	а	b	С
E	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	>	٧	Х	У	Z	а	b	С	d
F	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	٧	Х	У	Z	a	b	С	d	e
G	g	h	i	j	k	П	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d	е	f
Н	h	i	j	k		m	n	0	р	q	r	s	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k		m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	а	b	С	d	е	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	V	w	Х	У	Z	а	b	С	d	e	f	g	h	i
K	k		m	n	0	р	q	r	S	t	u	٧	w	Х	У	z	а	b	С	d	е	f	g	h	i	j
L		m	n	0	p	q	r	S	t	u	٧	w	Х	У	z	a	b	С	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k		m
0	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	c	d	e	f	g	h	i	j	ķ		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k	ı	m	n	0	р	q
S	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	ı	m	n	0	р	q	r
T	t	u	٧	W	Х	у	Z	a	b	С	d	е	f	g	h	i	j	k	ı	m	n	0	р	q	r	S
U	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	1	m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	С	d	е	f	g	h	<u>i</u>	j	k	1	m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	С	d	е	f	g	h	<u>i</u>	j_	k		m	n	0	р	q	r	S	t	и	V
X	Х	У	Z	a	b	С	d	е	f	g	h	l i	L j	k		m	n	0	р	q	r	S	t	и	٧	W
Y	У	Z	a	b	С	d	е	f	g	h	í	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х
Z	Z	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	у	у

Texto = lbmcocjmssdcx e **Chave** = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Н	U	V	W	X	Υ	Z
Α	a	b	С	d	е	f	g	h	i	l j	k		m	n	0	p	q	r	S	t	u	٧	W	У	у	Z
В	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	s	t	а	٧	W	Х	У	Z	а
C	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	а	>	W	Х	У	Z	а	b
D	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	а	>	W	Х	у	Z	а	Ь	С
E	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	>	٧	Х	У	Z	а	Ь	U	d
F	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е
G	g	h	i	j	k	П	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f
Н	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k	Т	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h
J	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	i
K	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	C	d	е	f	g	h	i	j
L	Ш	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m
0	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k		m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	-	j	k		m	n	0	р
R	r	S	t	и	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	-	٦.	k	П	m	n	0	р	q
S	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	i	٦.	k		m	n	0	р	q	r
T	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S
U	и	٧	W	Х	У	Z	a	Ь	С	d	е	f	g	h	ī	j	k	Т	m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	С	d	е	f	g	h	i	j	k	Т	m	n	0	р	q	r	S	t	u
W	w	Х	У	z	a	Ь	С	d	е	f	g	h	i	j	k	Τ	m	n	0	р	q	r	S	t	u	٧
X	Х	У	z	a	Ъ	С	d	е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W
Y	У	Z	a	Ь	С	d	е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х
Z	z	а	b	С	d	е	f	g	h	i	j	k	П	m	n	0	р	q	r	S	t	u	٧	W	У	У

Texto = lbmcocjmssdcx e **Chave** = LIMAO



Texto = Abmcocjmssdcx e **Chave** = **L**IMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	H		J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	X	Υ	Ζ
A	a	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	c	d	e	t	g	h	İ	j	ķ	I	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a
C	С	d	e	t	g	h	į	į	ķ	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b
D	d	e	t	g	h.	į	Ĺ	ķ	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	c
Ē	e	f	g	ḥ	1	Ţ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d
F	t	g	h	!	Ļ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	c	d	e
G	g	h	!	Ļ	ķ		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f
H	h		Į.	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	f	g
	Ţ	Į	k		m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	t	g	h
J	Ţ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	e	f	g	ḥ	1
K	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	t	g	h		J
L	ш	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	C	d	e	Ť	g	ņ	1	1	K
M	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	Ť	g	h	!	Į	k	
N	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	f	g	h	1	J	k	1	m
P	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	T	g	h	÷	Ļ	k	100	m	n
-	p	q	r	S	t	u	V	W	X	У	z	a	b	C	d	e	f	g	h	+	J.	k	1	m	n	0
Q R	q	r	t	t	u	V	W	X	У	Z	a	b	d	d	f	f	g h	h	-	J	k	1	m	n	0	p
S	r	t	u	u	V	X	V	y z	z a	a b	b	d	e	e f		g h	:	+	J k	k	m	m	n o	0	p	q
1	t	u	v	W	W X	v	y Z	a	b	C	d	e	f	<u> </u>	g h	11	+	J k	Ť	m	m n	n	_	р	q r	S
Ü	U	v	w	X	÷	z	a	Ъ	С	ă	e	f	_	g h	_	÷	k	Ť	m	n	0	0	р	q r	S	t
V	V	w	X	÷	z	a	b	C	ď	e	f	_	g h	1	÷	k	Ť	m	n		_	р	q r	S	t	u
Ŵ	w	X	÷	z	a	b	C	ਰ	e	f	_	g h	 ''	H	k	Ĥ	m	n	-	_	р	q	S	t	u	V
X	×	Ŷ	z Z	a	b	С	व	e	f	g	g h	 ''	H	k	H	m	n	-	q	p q	q	S	t	u	v	w
Ŷ	V	y Z	a	b	C	ă	e	f	g	h	11	H	k	Ĥ	m	n	0	р	q	ч r	S	t	u u	v	w	X
Ż	y Z	a	b	C	ă	e	f	g	h	+	H	Į,	H	m	n	0	р	q	ч r	S	t	u	V	w	٧٧	Ŷ
	2	а	L		_u	Le		18	111		IJ	_ r		ш	<u> </u>	LO	LΡ	Ч		3	L	u	V	٧V	У	للات

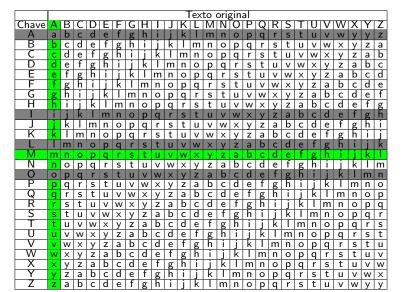
Texto = Abmcocjmssdcx e **Chave** = LIMAO

	П										٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	H		J	K	L	M	N	0	Р	Q	R	S	T	U	V	W	X	Υ	Ζ
A	a	b	С	d	е	f	g	h	i	j	ķ		m	n	0	р	q	r	S	t	u	٧	W	у	у	Z
В	b	c	d	e	f	g	h	i	j	ķ		m	n	0	р	q	r	S	t	u	٧	w	Х	У	Z	a
С	С	d	e	t	g	h	İ	j	ķ	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b
D	d	e	t	g	h.	į.	į	ķ	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С
Ē	e	t	g	h	1	Ļ	ķ	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d
F	†	g	h	ļ.	Į.	k	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e
G	g	h	ļ.	Į.	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f
H	h	1	Ţ	k	П	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	t	g
	Ļ	Ų.	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	Ť	g	h
J	Ļ	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	Ç	d	e	f	g	h	!
K	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	а	b	С	d	e	Ť	g	h	_	J
M	1	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	Ť	g	h	ļ.	J	k
N	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	T	g	h	٠	Ļ	K	
	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	1	J	k	1	m
P	0	р	q	r	t	t	u	V	W	X	У	Z	b	b	d	d	f	T	g	h		k	k	122	m	n
Q	p	q	r	t	<u> </u>	u	V	W	X	y z	z	a b	С	d	e	f		g h		÷	J k	K	<u></u>	m	n	0
R	q	r	t	_	u	V W	W X	V	y z	a	b	C	d	e	f	_	g h	+	-	k	T	m	m n	n o	0	р
S	S	t	u	u	w	X	v	y Z	a	Ъ	С	đ	e	f	g	g h	Ÿ	÷	k	÷	m	n	0	р	p q	q r
 	t	u	v	w	×	÷	Z	a	Ъ	С	ă	e	f	g	h	₩	÷	k	Ť	m	n	0	р	q	r	S
ι	u	V	w	×	÷	z	a	Ъ	С	ă	e	f	g	h	ï	÷	k	Ť	m	'n	0	р	q	r	S	t
V	v	w	X	Ŷ	z	a	Ъ	C	đ	e	f	g	h	٣	÷	k	Ĥ	m	n	0	р	q	r	S	t	u
W	w	×	÷	z	a	Б	C	ă	e	f	g	ĥ	 ;;	H	k	H	m	n	0	р	q	r	S	t	u	V
X	×	Ŷ	z	a	Б	c	ă	e	f	g	h	÷	H	k	Ť	m	n	0	р	q	r	S	t	u	V	w
Ŷ	v	z	a	Б	c	ă	e	f	g	ĥ	ï	÷	k	Η̈́	m	n	0	р	q	r	s	t	u	V	w	X
'	z	a	Б	c	ă	e	f	g	ĥ	÷	÷	k	Η̈́	m	n	''	р	q	r	S	t	u	V	w	V	Ŷ
	12	u			Щ			Ó			J	١,	<u>'</u>	111			Ц	_Ч_			·	u	٧_	**	1	ע

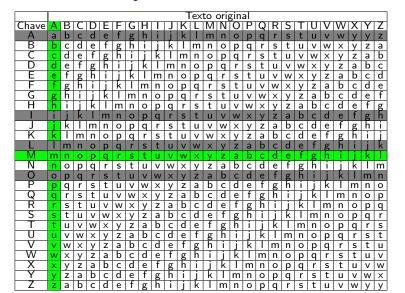
Texto = ATmcocjmssdcx e **Chave** = LIMAO

											٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н	П	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	Χ	Y	Ζ
Α	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	Ь	С	d	е	f	g	h	-	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а
C	C	d	е	f	g	h	-	j	k	_	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	Х	у	z	а	b	С
E	е	f	g	h	i	j	k	_	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	Ь	С	d
F	f	g	h	i	j	k	_	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	U	d	е
G	g	h	i	j	k		m	n	0	р	q	r	s	t	u	٧	W	Х	У	Z	а	b	С	d	е	f
Н	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g
	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	С	d	е	f	g	h
J	j	k		m	n	0	р	q	r	S	t	u	V	w	Х	У	Z	а	b	С	d	e	f	g	h	i
K	k		m	n	0	р	q	r	S	t	u	٧	w	Х	У	z	а	b	С	d	е	f	g	h	i	j
L		m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	f	g	h	i	j	k
M	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	i	j	k	Ш
N	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	е	f	g	h	<u>i</u>	j	k	Ш	m
0	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	į	j	k		m	n
Р	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	C	d	e	f	g	h	1	j	k		m	n	0
Q	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	е	f	g	h	İ	j	k		m	n	0	р
R	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	İ	j	ķ	П	m	n	0	р	q
S	S	t	u	٧	w	Х	У	Z	a	b	С	d	e	f	g	h	i	j	k	<u> </u>	m	n	0	р	q	r
_ !	t	u	٧	W	Х	У	z	a	b	С	d	e	f	g	h	į	į	ķ	ı	m	n	0	р	q	r	S
U	u	٧	w	Х	У	Z	a	b	С	d	е	f	g	h	İ	Ĺ	k	1	m	n	0	р	q	r	S	t
V	٧	W	Х	У	z	a	b	c	d	e	f	g	h	Ļ	į	ķ	1	m	n	0	р	q	r	S	t	u
W	W	Х	У	z	a	b	Ç	d	e	t	g	h	ļ.	Į,	ķ	Ш	m	n	0	р	q	r	S	t	u	٧
X	Х	У	z	a	b	С	d	e	t	g	h	Ţ	لٰہا	ķ	1	m	n	0	р	q	r	S	t	u	٧	W
<u>Y</u>	У	Z	a	b	Ç	d	e	t	g	h	ļ	Ĺ	ķ	Ш	m	n	0	р	q	r	S	t	u	٧	W	Х
L	Z	а	b	С	d	е	†	g	h	ı	J	k		m	n	0	р	q	r	S	t	u	V	W	У	У

Texto = ATmcocjmssdcx e Chave = LIMAO



Texto = ATAcocjmssdcx e Chave = LIMAO



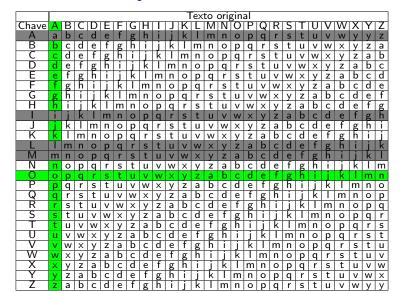
Texto = ATAcocjmssdcx e Chave = LIMAO

	Г										٦	ex	to	orig	gin	al										\neg
Chave	Α	В	C	D	E	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Τ	U	V	W	Χ	Y	Ζ
A	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	X	У	Z	а
С	c	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	u	٧	w	Х	У	Z	a	b
D	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	у	Z	a	b	С
E	e	f	g	h	į	Ĺ	k	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d
F	t	g	h	į.	Ĺ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	c	d	e
G	g	h	+	Ļ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f
H	h	ı.	1	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d	e	t	g
	ļ	J	k	1	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	f	g	h
J	Ļ	K		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	
K	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	а	b	С	d	e	Ť	g	h		
L	1	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	C-	d	e	Ť	g	h	ŀ	┦	k
M	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	Ť	g	h	!	J	K	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	1	J	k		m
P	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	d	d	f	T	g	h	÷	Ļ	k	ina	m	n
Q	p	q	r	S	t	u	V	W	X	У	z	a b	b	C	_	f		g	h	!	J	k	<u>n</u>	m	n	0
R	q	r	s t	t	u	V	W	X	У	Z	a	C	d	d	e	_	g h	h	-	J k	k	l m	m	n	0	p
S	r	t	u u	u v	W W	W X	V	y z	z a	a b	b	đ	e	f	g	g h	"	+	J k	T	m	m n	n o	0	р	q r
	t	u	V	w	X	÷	y Z	a	b	C	ď	e	f	-	h	+	÷	J k	Ť	m	n	0	р	p q	q r	S
ι	u	V	w	×	÷	z	a	Ъ	С	ă	e	f	g	g h	Η̈́	÷	k	Ť	m	n	0	р	_	r	s	t
V	v	w	X	÷	z	a	b	C	đ	e	f	g	h	٣	H	k	Ĥ	m	n		р	q	q r	S	t	u
W	w	×	Ŷ	z	a	Б	c	ă	e	f	g	ĥ	+-	H	k	H	m	n	0	р	q	r	S	t	u	v
X	×	Ŷ	z	a	Б	c	ă	e	f	g	h	+	H	k	H	m	n	0	р	q	r	S	t	u	V	w
Ŷ	Ŷ	z	a	Б	c	ă	e	f	g	h	''	÷	k	H	m	n	0	р	q	r	S	t	u	V	w	X
 	z	a	Ь	c	ă	e	f	g	ĥ	÷	÷	k	Η̈́	m	n	''	р	q	r	S	t	u	V	w	V	Ŷ
	12	u			<u> </u>		<u>'</u>	Ó			J	١,	<u>'</u>	111	<u> </u>		Ц	_Ч_		,	٠,	u	٧_	vv	y	

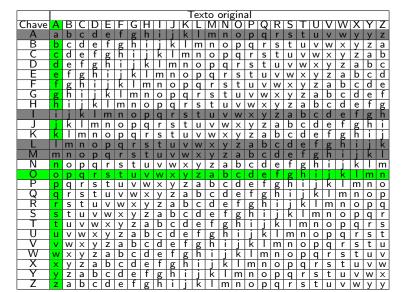
Texto = ATACocjmssdcx e **Chave** = LIMAO

	Г										٦	ex	to	orig	gin	al										\neg
Chave	Α	В	C	D	E	F	G	Н		J	K	L	M	N	0	Р	Q	R	S	Τ	U	V	W	Χ	Y	Ζ
A	a	b	С	d	е	f	g	h	i	j	k		m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	С	d	e	f	g	h	i	j	k		m	n	0	р	q	r	S	t	и	٧	W	X	У	Z	а
С	c	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	u	٧	w	Х	У	Z	a	b
D	d	e	f	g	h	i	j	ķ	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	у	Z	a	b	С
E	e	f	g	h	į	Ĺ	k	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b	С	d
F	t	g	h	į.	Ĺ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	c	d	e
G	g	h	+	Ļ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f
H	h	ı.	1	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	а	b	С	d	е	t	g
	ļ	J	k	1	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	f	g	h
J	Ļ	K		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	f	g	h	
K	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	а	b	С	d	e	Ť	g	h		
L	1	m	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	C-	d	e	Ť	g	h	ŀ	┦	k
M	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	е	Ť	g	h	!	J	K	
N	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f	g	h	1	J	k		m
P	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	d	d	f	T	g	h	÷	Ļ	k	ina	m	n
Q	p	q	r	S	t	u	V	W	X	У	z	a b	b	C	_	f		g	h	!	J	k	<u>n</u>	m	n	0
R	q	r	s t	t	u	V	W	X	У	Z	a	C	d	d	e	_	g h	h	-	J k	k	l m	m	n	0	p
S	r	t	u u	u v	W W	W X	V	y z	z a	a b	b	đ	e	f	g	g h	"	+	J k	T	m	m n	n o	0	р	q r
	t	u	V	w	X	÷	y Z	a	b	C	ď	e	f	-	h	+	÷	J k	Ť	m	n	0	р	p q	q r	S
ι	u	V	w	×	÷	z	a	Ъ	С	ă	e	f	g	g h	Η̈́	÷	k	Ť	m	n	0	р	_	r	s	t
V	v	w	X	÷	z	a	b	C	đ	e	f	g	h	٣	H	k	Ĥ	m	n		р	q	q r	S	t	u
W	w	×	Ŷ	z	a	Б	c	ă	e	f	g	ĥ	 ; 	H	k	H	m	n	0	р	q	r	S	t	u	v
X	×	Ŷ	z	a	Б	c	ă	e	f	g	h	+	H	k	H	m	n	0	р	q	r	S	t	u	V	w
Ŷ	Ŷ	z	a	Б	c	ă	e	f	g	h	''	÷	k	H	m	n	0	р	q	r	S	t	u	V	w	X
 	z	a	Ь	c	ă	e	f	g	ĥ	÷	÷	k	Η̈́	m	n	''	р	q	r	S	t	u	V	w	V	Ŷ
	12	u			<u> </u>		<u>'</u>	Ó			J	١,	<u>'</u>	111	<u> </u>		Ц	_Ч_		,	٠,	u	٧_	vv	y	

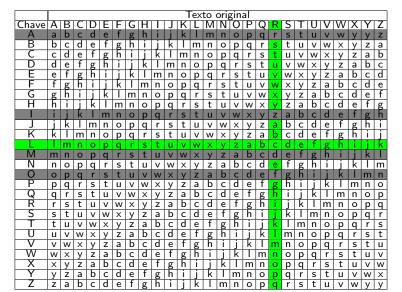
Texto = ATACocjmssdcx e **Chave** = LIMA**O**



Texto = ATACAcjmssdcx e Chave = LIMAO



Texto = ATACAcjmssdcx e **Chave** = LIMAO



Texto = ATACARjmssdcx e **Chave** = **L**IMAO

	П										٦	ex	to	ori	gin	al										
Chave	Α	В	C	D	E	F	G	Н		J	K	Ļ	M	N	0	Р	Q	R	S	Т	U	V	W	X	Y	Ζ
A	a	b	С	d	е	f	g	h	i	j	ķ	П	m	n	0	р	q	r	S	t	u	٧	W	У	У	Z
В	b	c	d	e	f	g	h	i	j	ķ		m	n	0	р	q	r	S	t	и	٧	w	Х	У	Z	a
С	С	d	e	t	g	h	İ	j	ķ	ı	m	n	0	р	q	r	S	t	и	٧	W	Х	У	Z	a	b
D	d	e	t	g	h.	į.	į	ķ	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	а	b	c
E	e	t	g	h	1	Į.	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d
F	t	g	h	ļ.	Į.	k	ı	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e
G	g	h	ļ.	Į.	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	f
H	h	ı.	Ų.	k	1	m	n	0	р	q	r	S	t	и	٧	W	Х	У	z	а	b	С	d	e	Ť	g
	ļ	Į	k	ı	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	f	g	h
J	Ļ	K		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	c	d	e	Ť	g	h	
K	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	Ť	g	h		
M	<u> </u>	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	T	g	h		1	K
N	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	T	g	h	٠	Ļ	K	
	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	e	f	g	h	1	J	k		m
P	0	р	q	r	t	t	u	V	W	X	У	Z	b	b	d	d	f	T	g	h		k	k	122	m	n
Q	p	q	r	t	<u> </u>	u	V	W	X	y z	z	a b	С	d	e	f		g h	h	÷	k	K	<u></u>	m	n	0
R	q	S	t	_	u	V W	W X	V	y z	a	b	C	d	e	f	_	g h	+	+	J k	Ť	m	m n	n	0	р
S	S	t	u	u	w	X	v	y Z	a	Ъ	С	ă	e	f	g	g h	Ÿ	÷	k	Ť	m	n	0	o p	p q	q r
 	t	u	V	w	×	÷	Z	a	b	С	ă	e	f	g	h	₩	÷	k	Ť	m	n	0	р	q	r	S
ι	u	V	w	×	÷	z	a	Ъ	С	ਰ	e	f	g	h	ï	÷	k	Ť	m	n	0	р	q	r	s	t
V	V	w	X	Ŷ	z	a	Ъ	С	ă	e	f	g	h	٣	÷	k	Ĥ	m	n	"	р	q	r	S	t	u
W	w	×	÷	z	a	Б	C	ਰ	e	f	g	ĥ	 ;;	H	k	H	m	n	0	р	q	r	S	t	u	v
X	×	Ŷ	z	a	Б	c	ă	e	f	g	h	÷	H	k	Ť	m	n	0	р	q	r	S	t	u	v	w
Ϋ́	v	z	a	Б	c	ă	e	f	g	ĥ	ï	÷	k	Η̈́	m	n	0	р	q	r	s	t	u	V	w	X
	z	a	Ь	c	ă	e	f	g	h	÷	÷	k	Η̈́	m	n	''	р	a	r	s	t	u	V	w	V	Ŷ
	_							0	٠.,	<u> </u>	ı J	٠.	Ļ.		٠.,		ᅩ						_	- •		

Cifra de Vigenère

A ideia da cifra de Vigenère era ser invulnerável à análise de frequência, além de permitir um número enorme de chaves. A natureza polialfabética da cifra era a responsável por sua força, mas também tornou o seu uso mais complicado. E o esforço adicional necessário para usar a cifra desestimulou o seu uso pelos dois séculos seguintes.

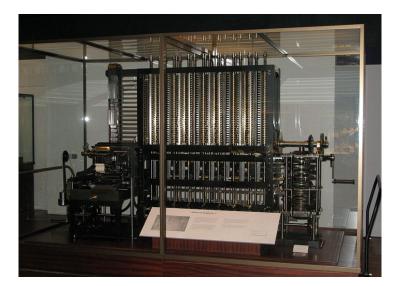
Sumário

- Introdução
- 2 Cifrando com Vigenère
- 3 Decifrando com Vigenère
- 4 Criptoanálise da Cifra de Vigenère

Charle Babbage, um excêntrico gênio britânico, mostrou que embora a criptoanálise da cifra de Vigenère fosse difícil, ela não era impossível, esse foi o primeiro avanço em 300 anos. Babbage é mais conhecido por ter desenvolvido o precursor dos computadores modernos (Motor de Subtração - N1). A calculadora, com mais de 25 mil peças, foi projetada para computar tabelas marítimas (que causavam muitos acidentes na época devido a grande quantidade de erros — mais de 1000 em apenas uma constatou Babbage).

Babbage, infelizmente não terminou o Motor N1, causando um prejuízo de quase 18 mil libras ao governo britânico, que financiou o projeto na época. Dinheiro suficiente para construir um par de navios. O motivo foi que Babbage, após 10 anos de desenvolvimento da máquina, começou o Motor N2, que incluía um "depósito" (memória) e um "triturador" (processador) que permitia que ela tomasse decisões e repetisse instruções. Sem o financiamento do governo essa nova máquina também não foi concluída.

Museu de ciência de Londres



Em 1854, John H. B. Thwaites escreveu uma carta para o Journal of the Society of Arts afirmando ter inventado uma nova cifra com a intenção de patentear a ideia, aparentemente sem saber que estava chegando vários séculos atrasado. Babbage escreveu para a sociedade "... a cifra é muito antiga e pode ser encontrada na maioria dos livros". Thwaites não aceitou e desafiou Babbage a decifrá-la.

Considere o seguinte exemplo, com o uso da palavra 'KING':

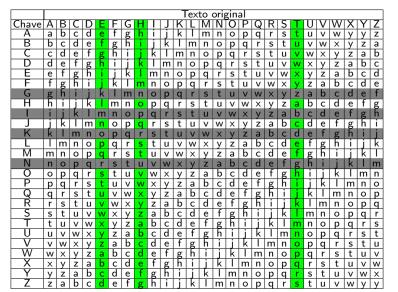
Considere o seguinte exemplo, com o uso da palavra 'KING':

```
Chav. K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I | N | G | K | I |
```

Chave = KING Texto = the

											٦	ex	to	ori	gin	al										\neg
Chave	Α	В	C	D	Е	F	G	Н		J	ΙK	L	M	N,	0	Р	Q	R	S	Т	U	V	W	X	Y	Ζ
Α	а	b	С	d	е	f	g	h	í	j	k	Г	m	n	0	р	q	r	S	t	и	٧	W	У	у	z
В	b	c	d	e	f	g	h	i	j	ķ		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a
C	С	d	e	f	g	<u>h</u>	i	j	ķ	1	m	n	0	p	q	r	S	t	u	٧	W	Х	У	Z	a	b
D	d	e	f	g	h	Ĺ	j	k		m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С
E	e	f	g	h	į	Ĺ	ķ	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d
F	f	g	h	<u>i</u>	j	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	z	a	b	С	d	e
G	g	h	ļ	J	k	1	m	n	0	р	q	r	S	t	u	٧	W	X	У	Z	a	b	С	d	e	f
H	h	1	J	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	t	g
	ļ	J	k	1	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	а	b	С	d	е	f	g	h
J	J	k	1	m	n	0	р	q	r	S	t	u	٧	W	Х	У	Z	a	b	Ç	d	e	Ť	g	h	
K	k	1	m	n	0	р	q	r	S	t	u	V	W	X	У	Z	a	b	С	d	e	t	g	h	ļ	Į
L	ı	m	n	0	р	q	r	S	t	u	٧	W	X	У	z	a	b	c	d	e	f	g	ḥ	-	Į.	k
M	m	n	0	p	q	r	S	t	u	٧	W	Х	У	Z	a	b	С	d	e	_	g	h	ļ.	J	k	ш
N	n	0	р	q	r	S	t	u	V	W	Х	У	Z	a	b	С	d	е	f	g	h	Ļ	J	k		m
P	0	p	q	r	S	t	u	٧	W	X	У	z	a	b	C	d	e	f	g	<u>h</u>	!	Į,	k	1	m	n
	p	q	r	S	t	u	V	W	X	У	z	a	b	C	d	e	f	g	h	÷	Į.	k	1	m	n	0
Q R	q	r	S	t	u	V	W	X	У	Z	a	b	C	d	e	T	g	h	+	1	k	1	m	n	0	p
S	r	t	t	u	V	W	X	y	Z	a	b	d	d e	f	1	g	h :	+	Ţ	k T	m	m	n	0	p	q
	s t	u	u	V	W	v	<u>y</u>	Z	a b	b	d	e	f	-	g	h	+	J k	k	<u> </u>	m	n	0	р	q	r
U	-	v	w	W	X	y Z	z a	a b	C	d	e	f		g h	h :	÷	k	K T	m	m	n	0	р	q	S	t
V	u	w		V	y Z	a	b	D C	d	e	f	_	g h	1	H	k	K T	m	m n	n	0	p	q	r	t	-
W	w	X	X	z	a	b	C	q	e	f	_	g h	1	H	k	Ť	m	m	_	0	p	q	S	t	u	u
X	X	\	z z	a	b	С	q	e e	f	4	g h	;;	H	k	∺	m	n	n	0	p	q	S	t	ι u	v	w
Ŷ	V	z	a	b	C	d	e	f	_	g h	111	H	k	∺	m	n	0	0	р	q	S	t	u u	u V	W	X
	y Z	a	b	С	d	e	f	ρ	g h	+	H	k	1	m	n	0	р	р	q	S	t	11	v	W	VV	V
		a	ט		u		' '	8	11	1	IJ	_ N	<u> </u>	1111		U	רא_	q	-	3	L	u	V	٧V	У	У

Possibilidades: **DPR**, **BUK**, **GNO** e **ZRM**.



O primeiro passo na criptoanálise de Babbage é procurar por **sequências de letras** que apareçam mais de uma vez no texto cifrado. Nesse caso, o mais provável é que a mesma sequência de letras no texto original tenha sido cifrada usando-se a mesma parte da chave.

Exemplo:

```
k | m | f |
                                 vah f
        v s
                              t
                                 |\mathbf{t}|\mathbf{f}|\mathbf{x}|\mathbf{w}|\mathbf{c}|\mathbf{h}
                              g
                ģ
                          e
                                     cm
                                             Χ
                                 s|k|m
                     S
                                             Χ
                                                              S
                                                                 p
                                 ko f
                                             t
W
```

Identificando sequências repetidas com quatro ou mais caracteres:

```
b|v|s|k|m|f|t|v|a|h|f|f|m|k|w|
              gtfxwch
fokmmb
     wg
             e
                  cm
                      X
                 skm
          S
                      Χ
                lklol f
W
```

Distância entre "x-g-r-h": 50 caracteres.

```
| r | h | s | J | b | g | m | 1 | 0 | b | c | V | I | b | z | 0 | K | x | b | v | s | k | m | f | t | v | a | h | f | f | m | k | w | c |
          r h t o h g t f x w c h f w g k I f o k m m h g
           f w g k l
m h i l e
                                 e |j|g|c|m|i
                     u f t b h p
                                      r z h r
                                       c i q h e n
                g
h
                                 |\mathbf{x}|\mathbf{h}|\mathbf{h}|\mathbf{u}|\mathbf{r}|\mathbf{x}|\mathbf{q}|
                     h|s|r|
                                           skm x i
                v \mid c \mid u \mid v \mid f \mid k \mid o \mid f \mid t
```

Distância entre "f-i-q-t-r-x-h": 25 caracteres.

```
g | r | h | s | J | b | g | m | 1 | o | b | c | v | I | b | z | o | k | b | x | b | v | s | k | m | f | t | v | a | h | f | f | m | k | w | c
           f w g k I m h i I e
                            e |j|g|c|m|i
                   u f t b h p
                                r z h r
               g
h
                                              e n
                            x |h|h|u|r|x|q|
                   h|s|r|
                                   skm x i
               v \mid c \mid u \mid v \mid f \mid k \mid o \mid f \mid t
```

Distância entre "r-h-t-o": 120 caracteres.

```
b|v|s|k|m|f|t|v|a|h|f|f|m|k|w|c
     r h t o h g t f x w c h f w g k l f o k m m h g
     f w g
                  e
                         cm
                               Χ
                       s|k|m|
               S
                               Χ
                 v | f | k | o | f |
                               t
W
              u l
```

Tamanho provável da chave = 5 (múltiplo de 25, 50 e 120).

```
| b | g | m | 1 | 0 | b | c | V | 1 | b | z | 0 | k 
| k | m | f | t | v | a | h | f | f | m | k | w | c
x b v s
         htohgtfxwch
wgklfokmmhg
      fwgkl
mhile
                          |o|k|m|m|h|g|
                          |g|c|m| i |u|m|
                    e
                          |z|h| r |
                        c i q h e n
             b|h|p|
      Χ
          g
h
                0
                    x |h|h|u|r|x|q|t
                          skm x i
         |h|h|s|r|
          v c |u| v |f| k |o| f |t|
```

Se a suposição for correta, então as letras em verde foram codificadas com a mesma posição da chave.

```
v s k m f
                t |v|a| h
             h
                g t
f o
                         x |w|c
         0
             е
                                u|m|
                   g
                   zh
e
      b
   g
             \times |h| h |u|
                         r
         0
                             x | q
                   s|\mathbf{k}|\mathbf{m}|
          S
                 f|k|o|f
         u
             ٧
```

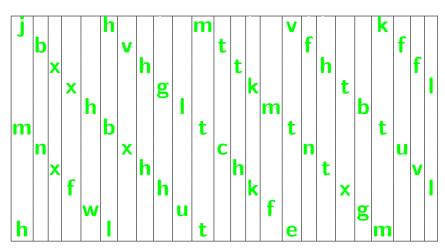
Nesse caso nosso problema se reduz a criptoanálise de cinco cifras monoalfabéticas.

```
x b v s k m f t va h f f m k w
                h g t f x w c h y l f o k m m h g t
             0
                е
                      g
                t
                      zh r
        g
                p
                \mathbf{x}
                          r
             0
                             x | q
                      s k m
                   f|k|o|f
                ٧
```

Solução: análise de frequência em cada cifra monoalfabética.

```
b v s k m f t va h
             gtfxwch
fokmmh
           h
         0
                g
                z|h|
    g
           p
                    r
         0
                      x | q
                s k m
              f|k|o|f
```

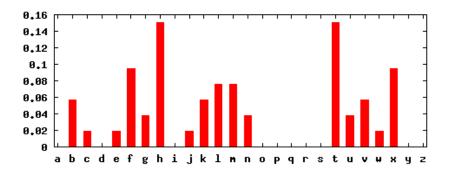
Solução: análise de frequência em cada cifra monoalfabética.



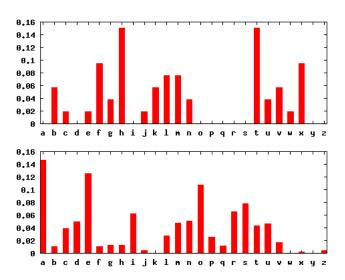
Suponha que $L_1L_2L_3L_4L_5$ represente a palavra chave, de modo que L_1 represente a primeira letra da palavra e assim por diante:

L_1 L_1 L_1	L_1	L_1	$\begin{vmatrix} L_1 \\ L_1 \end{vmatrix} L_1$	$\begin{bmatrix} L_1 \\ L_2 \end{bmatrix}$	L_1	-1
L_1	$\begin{vmatrix} L_1 \\ L_2 \end{vmatrix} L_1$	$egin{bmatrix} L_1 \\ L_1 \end{bmatrix}$	L_1 L_1	$\begin{vmatrix} L_1 \\ L_1 \\ L_1 \end{vmatrix}$	$\begin{vmatrix} L_1 \\ L_1 \\ L_1 \end{vmatrix}$	<i>L</i> 1
L_1	$\begin{vmatrix} L_1 \\ L_1 \end{vmatrix}_{L_1}$		L_1	$\begin{vmatrix} L_1 \\ L_1 \\ L_1 \end{vmatrix} = \begin{vmatrix} L_1 \\ L_1 \end{vmatrix}$	$\begin{vmatrix} L_1 \\ L_1 \\ L_1 \end{vmatrix}$	L_1

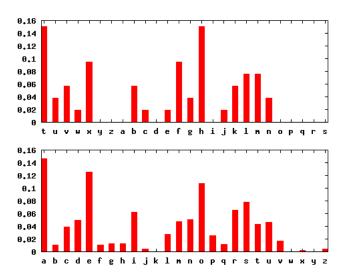
Distribuição de frequências (cifrado): L_1 .



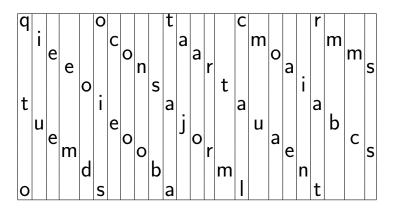
Comparação de frequências: L_1 e português.



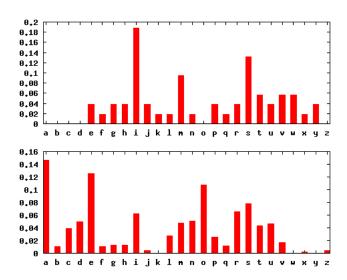
Matching: L_1 e português (deslocamento).



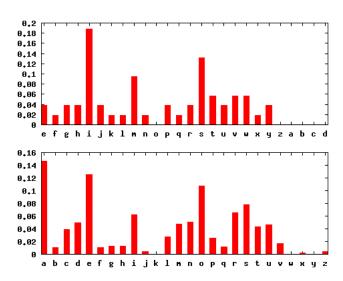
Substituindo "t" por "a", "x" por "e", ...



Comparação de frequências: L_2 e português.



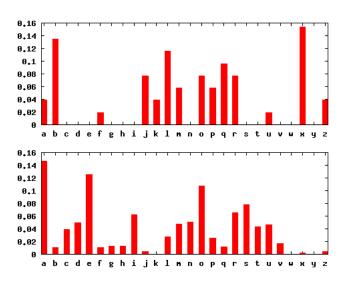
Matching entre L_2 e português.



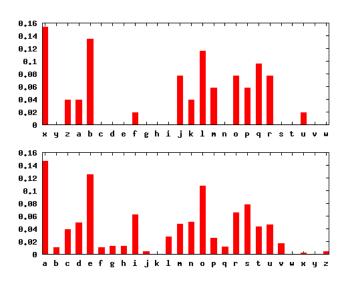
Substituindo "e" por "a", "i" por "e", ...

q	u				0	0				t	e				С	h				r	j		
	i	m				С	0				a	r	_			m	i				m	е	
		e	d				0	p				a	b				0	0				m	e
			е	d					g				r	i				a	S				S
				0	S				<u></u> Ծ	a				t	e	_			i	n			
t	O				i	a				a	ņ				a	f				a	ļ		
	u					e					j					u		_			b		
		e	i				0	p				0	q				a	i				С	0
			m	ŗ				0	0				r	Ì				e	0				S
e				d	e				b	r				m	þ	_			n	t			
0	С				S					a	S					f				t	0		

Comparação de frequências: L_3 e português.



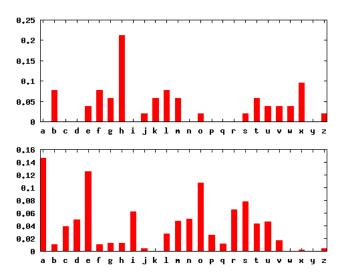
Matching entre L_3 e português.



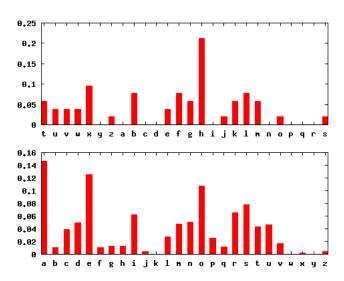
Substituindo "x" por "a", "b" por "e", ...

q	u	a			0	0	m			t	е	r			С	h	e			r	j	a	
	i	m	e			С	0	n			a	r	d			m	i	n			m	е	t
		e	d	a			0	p	r			a	b	a			0	u	t			m	e
t			е	d	0			n	g	0			r	i	p			a	S	e			s
q	u			0	S	p			S	a	m			t	e	X			i	n	С		
t	O	S			i	a	0			a	n	C			a	f	O			a		u	
	u	e	ģ			e	С	e			j	e	t			u	e	m			b	e	O
		e	i	r			0	p	r			0	q	u			a	i	a			С	0
m			m	r	e			0	0				r	i	a			е	0	S			S
е	t			d	e	S			b	r	i			m	p	a			n	t	е		
0	С	0			S		е			a	S	d				f	a			t	0		

Comparação de frequências: L_4 e português.



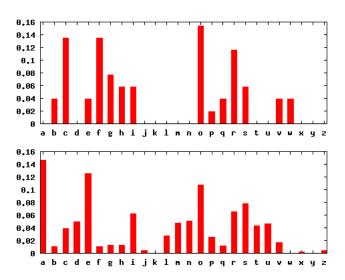
Matching entre L_4 e português.



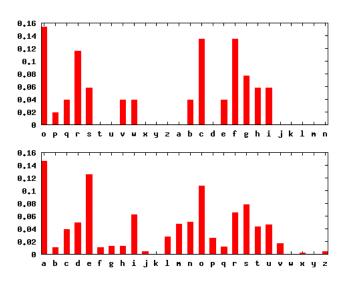
Substituindo "t" por "a", "x" por "e", ...

o ntra rdormi ndom oprosabadooutra e |d|o|m| i |n|g|o|m|a|r| ip | o | s |a semos o u samno te x t o b r a n c o d a f o I h a |e|t|o|q|u|e|m|s|a| e c e o b j e i rod o pre toqu e c t oou seri mo u m r e s a q u e o s o s de s c obr i ramp a

Comparação de frequências: L_5 e português.



Matching entre L_5 e português.



Substituindo "o" por "a", "s" por "e", ...

```
|m| e |e|n| c | o |n| t | r | a | r |d| o | r |m| i | n |d|o|m| e | t
        d | a | n | d | o | p | r | o | s | a | b | a | d | o | o | u | t | r | a
     d \mid e \mid d \mid o \mid m \mid i \mid n \mid g \mid o \mid m \mid a \mid r \mid i
                                                 a sem
                                         p \mid o \mid s \mid
                    o u samno text
                p
                   o b r a n c o d a f o I h a
                                etoquemsa
                e
                   c e o b j
     e i rod
                   o pre toqu
                                        e c
                    t o o u s e r i
mo u m r e s
                                        a q u
                                                 e o s
     o s de s c obr i ramp
                                           a
```

Chave utilizada para ciframento: texto!

(letras emparelhadas com a letra "a").

 $m \mid e \mid e \mid n \mid c \mid o \mid n \mid t \mid r \mid a \mid r \mid d \mid o \mid r \mid m \mid i \mid$ oprosabadooutra d a n d $d \mid e \mid d \mid o \mid m \mid i \mid n \mid g \mid o \mid m \mid a \mid r \mid i$ a sem $p \mid o \mid s \mid$ o u s a m n o t e x t o |b| r |a| n |c|o| d |a| f c e o b i |e|t|o|q|u|e|m|s|a| е i irod o pre toqu e c t oou s e r i S a q u m r e |u| e os o | s | d | e | s | c | o | b | r | i | r | a | m | p |a

Quando o mistério chegar, já vai me encontrar dormindo, metade dando pro sábado, outra metade, domingo. Mariposas e mosquitos pousam no texto incerto. Seria o branco da folha, luz que parece objeto? Quem sabe o cheiro do preto, que cai ali como um resto? Ou seria que os insetos descobriram parentesco com as letras do alfabeto?

Paulo Leminski.