

Criptografia e Criptanálise

Rodrigo Girão Serrão

Criptografia..?

Técnicas para codificar informação.

Criptografia..?

Técnicas para codificar (?) informação.

Criptografia..?

Técnicas para esconder informação dos outros.

Criptanálise..?

Técnicas para aceder à informação dos outros.

Cifra de César

Criptografia

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

Criptografia

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

Criptografia

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

Criptografia

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

Criptografia

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

Criptografia

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

Criptografia

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
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

Criptografia

0

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
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

Criptografia

0	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
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

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

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

Criptografia

0 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

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

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

0

Criptografia

0	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
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
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
						0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

Criptografia


0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

Criptografia

0	1	2	3	4	5	6	7	8
A	B	C	D	E	F	G	H	I
U	V	W	X	Y	Z	A	B	C
20	21	22	23	24	25	0	1	2

Criptografia


0	1	2	3	4	5	6	7	8
A	B	C	D	E	F	G	H	I
U	V	W	X	Y	Z	A	B	C
20	21	22	23	24	25	0	1	2



The diagram illustrates a modular addition operation in a 26-letter alphabet. A curved arrow starts at index 2 (C) and points to index 20 (U), with the label $+20$ indicating the shift.

Criptografia

0	1	2	3	4	5	6	7	8
A	B	C	D	E	F	G	H	I
U	V	W	X	Y	Z	A	B	C
20	21	22	23	24	25	0	1	2



The diagram illustrates a Caesar cipher shift of +20. A curved arrow points from index 1 (B) to index 21 (V), with the label "+20" next to it.


Criptografia

0	1	2	3	4	5	6	7	8
A	B	C	D	E	F	G	H	I
U	V	W	X	Y	Z	A	B	C
20	21	22	23	24	25	0	1	2

The diagram illustrates a modular addition operation on a 26-letter alphabet. A curved arrow starts at the index '2' (corresponding to letter 'C') in the top row and points to the index '22' in the bottom row. The label '+20' is placed near the arrow, indicating the shift value. The bottom row shows the resulting indices: 20, 21, 22, 23, 24, 25, 0, 1, 2.

Criptografia

0	1	2	3	4	5	6	7	8
A	B	C	D	E	F	G	H	I
U	V	W	X	Y	Z	A	B	C
20	21	22	23	24	25	0	1	2



+20 ???

Criptografia



mod 12

Criptografia



mod 60

Criptografia

0	1	2	3	4	5	6	7	8
A	B	C	D	E	F	G	H	I
U	V	W	X	Y	Z	A	B	C
20	21	22	23	24	25	0	1	2

+20 mod 26

Cifra de César – encriptar

Criptografia

14 11 0 0 19 14 3 14 18

O L A A T O D O S

Criptografia

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

14	11	0		0		19	14	3	14	18
O	L	A		A		T	O	D	O	S
I							I		I	
8							8		8	

Criptografia

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

14	11	0		0		19	14	3	14	18
O	L	A		A		T	O	D	O	S
I	F					I		I		
8	5					8		8		

Criptografia

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

14	11	0		0		19	14	3	14	18
O	L	A		A		T	O	D	O	S
I	F	U		U		I		I		
8	5	20		20		8		8		

Criptografia

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

14	11	0		0		19	14	3	14	18
O	L	A		A		T	O	D	O	S
I	F	U		U		N	I		I	
8	5	20		20		13	8		8	

Criptografia

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

14	11	0		0		19	14	3	14	18
O	L	A		A		T	O	D	O	S
I	F	U		U		N	I	X	I	
8	5	20		20		13	8	23	8	

Criptografia

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

14	11	0		0		19	14	3	14	18
O	L	A		A		T	O	D	O	S
I	F	U		U		N	I	X	I	M
8	5	20		20		13	8	23	8	12

Criptografia

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

“Jogo”

Cifra de César – desencriptar

Criptanálise

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

													?		
W	I	G	I		P	U	C		U		P	C	X	U	?
22	8	6	8		15	20	2		20		15	2	23	20	

Criptanálise

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

2															
C													?		
W	I	G	I		P	U	C		U		P	C	X	U	?
22	8	6	8		15	20	2		20		15	2	23	20	

Criptanálise

2	14		14												
C	O		O										?		
W	I	G	I		P	U	C		U		P	C	X	U	?
22	8	6	8		15	20	2		20		15	2	23	20	

Criptanálise

[illegible]

Criptanálise

2	14	12	14	21				21					
C	O	M	O	V				V				?	
W	I	G	I	P	U	C		U	P	C	X	U	?
22	8	6	8	15	20	2		20	15	2	23	20	

Criptanálise

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

2	14	12	14		21	0		0	21		0
C	O	M	O		V	A		A	V		A ?
W	I	G	I		P	U	C	U	P	C	X U ?
22	8	6	8		15	20	2	20	15	2	23 20

Criptanálise

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

2	14	12	14		21	0	8		0		21	8		0
C	O	M	O		V	A	I		A		V	I		A ?
W	I	G	I		P	U	C		U		P	C	X	U ?
22	8	6	8		15	20	2		20		15	2	23	20

Criptanálise

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

2	14	12	14		21	0	8		0		21	8	3	0	
C	O	M	O		V	A	I		A		V	I	D	A	?
W	I	G	I		P	U	C		U		P	C	X	U	?
22	8	6	8		15	20	2		20		15	2	23	20	

Criptanálise

0	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
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
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
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

“Jogo”

Ataque “plaintext”

Criptanálise

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
0	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

<

Criptanálise

14				17				0												12					
O				R				A												M					
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
0	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

17 14 12 0

R O M A

E B Z N A N B F R P B A F G E H V H R Z H Z Q V N

4 1 25 13 0 13 1 5 17 15 1 0 5 6 4 7 21 7 17 25 7 25 16 21 13

Criptanálise

14	17												0												12
O	R												A												M
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
0	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

+13 mod 26

17 14 12 0

R O M A

E B Z N A N B F R P B A F G E H V H R Z H Z Q V N

4 1 25 13 0 13 1 5 17 15 1 0 5 6 4 7 21 7 17 25 7 25 16 21 13

Criptanálise

13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	<div>+13 mod 26</div>	
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		
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		
0	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		

17	14	12	0	13	0	14	18	4	2	14	13	18	19	17	20	8	20	4	12	20	12	3	8	0
R	O	M	A	N	A	O	S	E	C	O	N	S	T	R	U	I	U	E	M	U	M	D	I	A
E	B	Z	N	A	N	B	F	R	P	B	A	F	G	E	H	V	H	R	Z	H	Z	Q	V	N
4	1	25	13	0	13	1	5	17	15	1	0	5	6	4	7	21	7	17	25	7	25	16	21	13

Ataque “plaintext” – nível 2

Criptanálise

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
0	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

L X K H N G T H L X K , X B L T J N X L M T H

11 23 10 7 13 6 19 7 11 23 10 23 1 11 19 9 13 23 11 12 19 7

Criptanálise

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
0	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

18 4 17

S E R

LXKHNGTHLXK,XBLTJNXLMTH

11231071361971123102311119913231112197

Criptanálise

L	X	K		H	N		G	T	H		L	X	K	,		X	B	L		T		J	N	X	L	M	T	H
11	23	10		7	13		6	19	7		11	23	10			23	1	11		19		9	13	23	11	12	19	7

18	4	17
S	E	R
L	X	K
11	23	10

18	4	17
S	E	R
G	T	H
6	19	7

18	4	17
S	E	R
X	B	L
23	1	11

Criptanálise

S E R S E R ,
L X K H N G T H L X K , X B L T J N X L M T H

Criptanálise

7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6
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
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
0	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

18	4	17	14	20	13	0	14	18	4	17	4	8	18	0	16	20	4	18	19	0	14	
S	E	R	O	U	N	A	O	S	E	R	,	E	I	S	A	Q	U	E	S	T	A	O
L	X	K	H	N	G	T	H	L	X	K	,	X	B	L	T	J	N	X	L	M	T	H
11	23	10	7	13	6	19	7	11	23	10	23	1	11	19	9	13	23	11	12	19	7	

Cifra afim

Criptografia

$$f(x) = ax + b$$

0	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
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

Criptografia

$$f(x) = 11x + 3$$

0	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
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

Criptografia

$$f(0) = 11 \times 0 + 3 = 3$$

0	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
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

D

3

Criptografia

$$f(1) = 11 \times 1 + 3 = 14$$

0	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
---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

D	O
---	---

3	14
---	----

Criptografia

$$f(2) = 11 \times 2 + 3 = 25$$

0 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

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

D O Z

3 14 25

Criptografia

$$f(3) = 11 \times 3 + 3 = 36 = 10 \pmod{26}$$

[illegible]

Criptografia

$f(x) = 11x + 3$

0	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
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
D	O	Z	K	V	G	R	C	N	Y	J	U	F	Q	B	M	X	I	T	E	P	A	L	W	H	S
3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15	0	11	22	7	18

Cryptografia

zf zwdzf j vf izwvjf zfftmzuzavf
nxj az vrtajmozu ewztz uxftozmz
evw dzwjf mxmrz aj zmojf mzgjbzavf
ezffzwzd ztmaz zujd az ozewvizmz,
jd ejwtbvf j bxjwwzf jfsvwrzavf
dztf av nxj ewvdjotz z svwrz kxdzmz,
j jmowj bjmoj wjdvoz jatstrzwzd
mvgv wjtmv nxj ozmov fxiutdzwzd;

Cryptografia

zf zwdzf j vf izwvjf zfftmzuzavf
nxj az vrtajmozu ewztz uxftozmz
eww dzwjf mxmrz aj zmojf mzgjbzavf
ezffzwzd ztmaz zujd az ozewvizmz,
jd ejwtbvf j bxjwwzf jfsvwrzavf
dztf av nxj ewvdjotz z svwrz kxdzmz,
j jmowj bjmoj wjdvoz jatstrzwzd
mvgv wjtmv nxj ozmov fxiutdzwzd;

Cryptografia

zf zwdzf j vf izwvjf zfftmzuzavf
nxj az vrtajmozu ewztz uxftozmz
eww dzwjf mxmrz aj zmojf mzgjbzavf
ezffzwzd ztmaz zujd az ozewvizmz,
jd ejwtbvf j bxjwwzf jfsvwrzavf
dztf av nxj ewvdjotz z svwrz kxdzmz,
j jmowj bjmoj wjdvoz jatstrzwzd
mvgv wjtmv nxj ozmov fxiutdzwzd;

Cryptografia

zf zwdzf j vf izwvjf zfftmzuzavf
nxj az vrtajmozu ewztz uxftozmz
eww dzwjf mxmrz aj zmojf mzgjbzavf
ezffzwzd ztmaz zujd az ozewvizmz,
jd ejwtbvf j bxjwwzf jfsvwrzavf
dztf av nxj ewvdjotz z svwrz kxdzmz,
j jmowj bjmoj wjdvoz jatstrzwzd
mvgv wjtmv nxj ozmov fxiutdzwzd;

Criptografia

zf zwdzf j vf izwvjf zfftmzuzavf
nxj az vrtajmozu ewztz uxftozmz
eww dzwjf mxmrz aj zmojf mzgjbzavf
ezffzwzd ztmaz zujd az ozewvizmz,
jd ejwtbvf j bxjwwzf jfsvwrzavf
dztf av nxj ewvdjotz z svwrz kxdzmz,
j jmowj bjmoj wjdvoz jatstrzwzd
mvgv wjtmv nxj ozmov fxiutdzwzd;

Análise frequencista

Criptanálise

Letras mais frequentes em português
A
E
O
S
R
I
N
D
M
T

Criptanálise

zf zwdzf j vf izwvjf zfftmzuzavf
nxj az vrtajmozu ewztz uxftozmz
evw dzwjf mxmrz aj zmojf mzgjbzavf
ezffzwzd ztmaz zujd az ozewvizmz,
jd ejwtbvf j bxjwwzf jfsvwrzavf
dztf av nxj ewvdjotz z svwrz kxdzmz,
j jmowj bjmoj wjdvoz jatstrzwzd
mvgv wjtmv nxj ozmov fxiutdzwzd;

Letras mais frequentes em português

A

E

O

S

R

I

N

D

M

T

Criptanálise

zf zwdzf j vf izwvjf zfftmzuzavf
nxj az vrtajmozu ewztz uxftozmz
evw dzwjf mxmrz aj zmojf mzgjbzavf
ezffzwzd ztmaz zujd az ozewvizmz,
jd ejwtbvf j bxjwwzf jfsvwrzavf
dztf av nxj ewvdjotz z swrz kxdzmz,
j jmowj bjmoj wjdvoz jatstrzwzd
mvgv wjtmv nxj ozmov fxiutdzwzd;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

zf zwdzf j vf izwvjf zfftmzuzavf
nxj az vrtajmozu ewztz uxftozmz
evw dzwjf mxmrz aj zmojf mzgjbzavf
ezffzwzd ztmaz zujd az ozewvizmz,
jd ejwtbvf j bxjwwzf jfsvwrzavf
dztf av nxj ewvdjotz z svwrz kxdzmz,
j jmowj bjmoj wjdvoz jatstrzwzd
mvgv wjtmv nxj ozmov fxiutdzwzd;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

af awdaf j vf iawvjf afftmauaavf
nxj aa vrtajmoau ewata uxftoama
evw dawjf mxmra aj amojf magjbaavf
eaffawad atmaa aujd aa oaewviamas,
jd ejwtbvf j bxjwwaf jfsvwraavf
datf av nxj ewvdjota a svwra kxdama,
j jmowj bjmoj wjdvoa jatstrawad
mvgv wjtmv nxj oamov fxiutdawad;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

af awdaf e vf iawvef afftmauaavf
nxe aa vrtaemoau ewata uxftoama
evw dawef mxmra ae amoef magebaavf
eaffawad atmaa aued aa oaewviamas,
ed eewtbvf e bxewwaf efsvwraavf
datf av nxe ewvdeota a svwra kxdama,
e emowe bemoe wedvoa eatstrawad
mvgv wetmv nxe oamov fxiutdawad;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

ao awdao e vo iawveo aootmauaavo
nxe aa vrtaemoau ewata uxotoama
evw daweo mxmra ae amceo magebaavo
eaooawad atmaa aued aa oaewviamas,
ed eewtbvo e bxewwao eosvwraavo
dato av nxe ewvdeota a svwra kxdama,
e emowe bemoe wedvoa eatstrawad
mvgv wetmv nxe oamov oxiutdawad;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

ao awdao e vo iawveo aootmauaavo
nxe aa vrtaemoau ewata uxotoama
evw daweo mxmra ae amoeo magebaavo
eaooawad atmaa aued aa oaewviamas,
ed eewtbvo e bxewwao eosvwraavo
dato av nxe ewvdeota a svwra kxdama,
e emowe bemoe wedvoa eatstrawad
mvgv wetmv nxe oamov oxiutdawad;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

as awdas e vs iawves asstmauaavs
nxe aa vrtaemoau ewata uxstoama
evw dawes mxmra ae amoes magebaavs
eassawad atmaa aued aa oaewviamas,
ed eewtbvs e bxewwas essvwraavs
dats av nxe ewvdeota a svwra kxdama,
e emowe bemoe wedvoa eatstrawad
mvgv wetmv nxe oamov sxiutdawad;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

as awdas e vs iawves asstmauaavs
nxe aa vrtaemoau ewata uxstoama
evw dawes mxmra ae amoes magebaavs
eassawad atmaa aued aa oaewviamas,
ed eewtbvs e bxewwas essvwraavs
dats av nxe ewvdeota a svwra kxdama,
e emowe bemoe wedvoa eatstrawad
mvgv wetmv nxe oamov sxiutdawad;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

as awdas e os iawoes asstmauaaos
nxe aa ortaemoau ewata uxstoama
eow dawes mxmra ae amoes magebaaos
eassawad atmaa aued aa oaewoiama,
ed eewtbos e bxewwas essowraaos
dats ao nxe ewodeota a sowra kxdama,
e emowe bemoe wedooa eatstrawad
mogo wetmo nxe oamoo sxiutdawad;

Texto	Português
Z (42)	A
J (25)	E
F (19)	O
W/V (18)	S
W/V (18)	R
D/T (12)	I
D/T (12)	N
A/O (10)	D
A/O (10)	M
X (8)	T

Criptanálise

as armas e os barões assinalados
que da ocidental praia lusitana
por mares nunca de antes navegados
passaram ainda além da taprobana,
em perigos e guerras esforçados
mais do que prometia a força humana,
e entre gente remota edificaram
novo reino que tanto sublimaram;

Texto	Português
A (42)	A
E (25)	E
S (19)	O
O/R (18)	S
O/R (18)	R
I/M (12)	I
I/M (12)	N
D/T (10)	D
D/T (10)	M
U (8)	T

Perguntas?