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



ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

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

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

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

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

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

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 D E F G H I J K L M N O P Q R S T

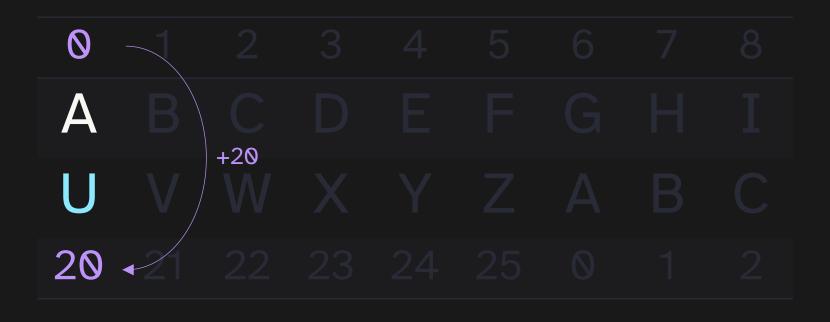




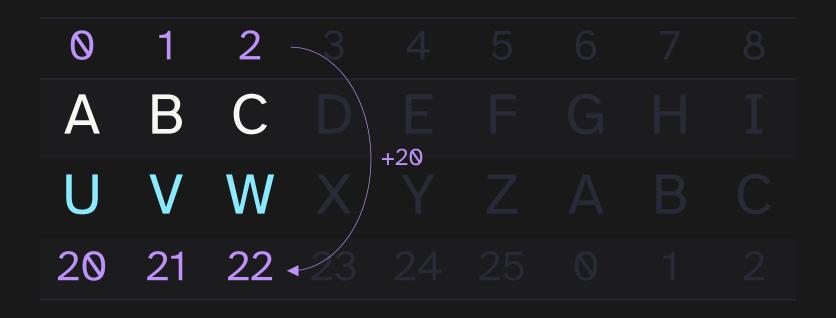


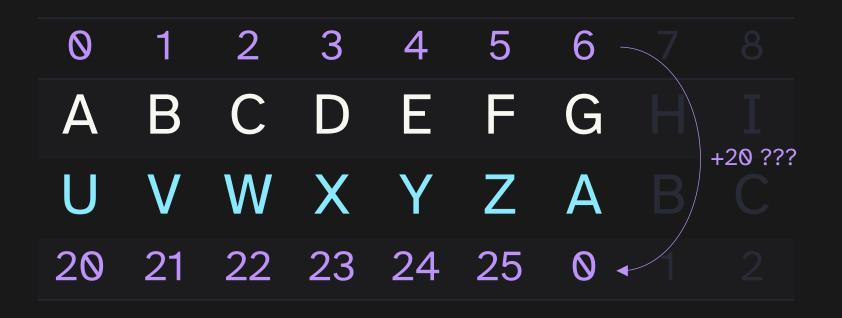


0	1	2	3	4	5	6	7	8
A	В	C	D	Ε	F	G	Н	Ι
U	V	W	X	Y	Z	A	В	C
20	21	22	23	24	25	0	1	2















Cifra de César - encriptar

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
Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	X	Υ	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т
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

O L A A T O D O S	14	11	0	0	19	14	3	14	18
	O	L	A	Α	Т	O	D	O	S

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	X	Y	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т
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	Α	А	Т	O	D	O	S
Ι					Ι		Ι	
8					8		8	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	Ν	O	Р	Q	R	S	Т	U	V	W	X	Υ	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т
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	Α	А	Т	O	D	O	S
Ι	F				Ι		Ι	
8	5				8		8	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	X	Y	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т
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	Α	Α	Т	O	D	O	S
Ι	F	U	U		Ι		Ι	
8	5	20	20		8		8	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	X	Υ	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т
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
0	L	Α	Α	Т	O	D	O	S
Ι	F	U	U	N	Ι		Ι	
8	5	20	20	13	8		8	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	X	Υ	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т
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	Α	Α	Т	O	D	O	S
Ι	F	U	U	N	Ι	X	Ι	
8	5	20	20	13	8	23	8	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	Ν	O	Р	Q	R	S	Т	U	V	W	X	Υ	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т
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
0	L	Α	А	Т	O	D	O	S
Ι	F	U	U	Ν	Ι	X	Ι	M
8	5	20	20	13	8	23	8	12

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

20 21 22 23 24 25 6 7 8 6 7 8 6 7 8 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 12 22 23 24 25

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

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	Ν	O	Р	Q	R	S	Т	U	V	W	X	Υ	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т
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	Ι	G	I	Р	U	С	U	Р	C	X	U	?
22	8	6	8	15	20	2	20	15	2	23	20	

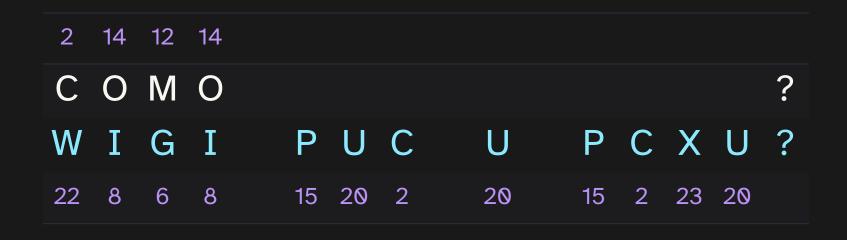
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	Χ	Y	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т
20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

2												
C												?
W	Ι	G	Ι	Р	U	С	U	P	С	X	U	?
22	8	6	8	15	20	2	20	15	2	23	20	

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
А	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	Χ	Υ	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т
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		14									
C	O		O									?
W	Ι	G	Ι	Р	U	С	U	Р	C	X	U	?
22	8	6	8	15	20	2	20	15	2	23	20	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	Ν	O	Р	Q	R	S	Т	U	V	W	X	Υ	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т
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



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
Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	Χ	Y	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т
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				21				
C	O	M	O	V				V				?
W	Ι	G	Ι	Р	U	С	U	Р	С	X	U	?
22	8	6	8	15	20	2	20	15	2	23	20	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	X	Y	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т
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	
С	O	M	O	V	А		А	V			А	?
W	Ι	G	Ι	Р	U	C	U	Р	С	X	U	?
22	8	6	8	15	20	2	20	15	2	23	20	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	X	Y	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т
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	
С	O	M	O	V	Α	Ι	А	V	Ι		Α	?
W	Ι	G	Ι	Р	U	С	U	Р	С	X	U	?
22	8	6	8	15	20	2	20	15	2	23	20	

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
Α	В	С	D	Ε	F	G	Н	Ι	J	K	L	M	N	O	Р	Q	R	S	Т	U	V	W	X	Y	Z
U	V	W	X	Υ	Z	Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	O	Р	Q	R	S	Т
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	
С	O	M	O	V	Α	Ι	А	V	Ι	D	Α	?
W	Ι	G	Ι	Р	U	C	U	Р	С	X	U	?
22	8	6	8	15	20	2	20	15	2	23	20	

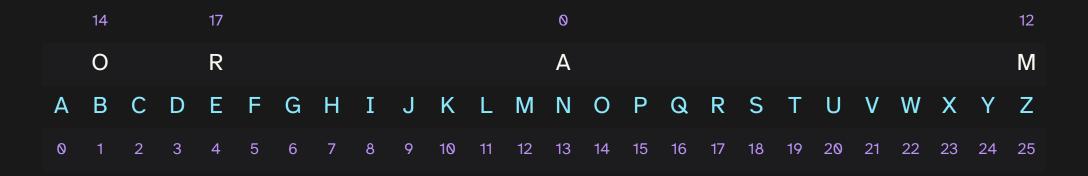
8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 E F G H I J K L M N O P Q R S U V W X Y Z AG H I BCDEF J K L M N O P Q R S T 23 24 25 0 2 8 10 11 12 13 14 15 16 17 18 19

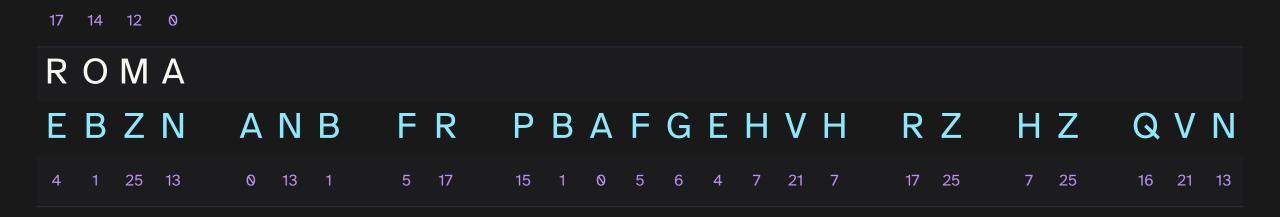
"Jogo"

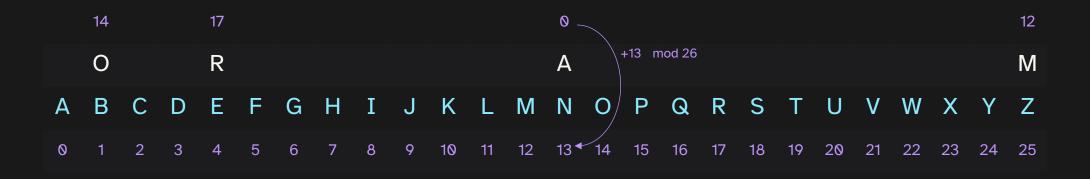
Ataque "plaintext"

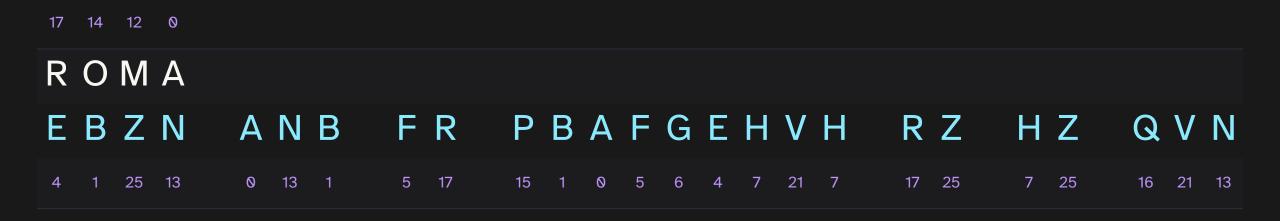
Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	X	Υ	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

E B Z N	ANB	FR	ΡВ	A F	G E	HV	H R	Z H	Z QVN
4 1 25 13	0 13 1	5 17	15 1	0 5	6 4	7 21	7 17 2	25 7	25 16 21 13









20 21 22 23 24 25 0 2 10 +13 mod 26 W X ZA В C D Ε F G H K M Ν O Р Q R 10 12 13 15 17



Ataque "plaintext" - nível 2

Α	В	С	D	Ε	F	G	Н	I	J	K	L	M	N	0	Р	Q	R	S	Т	U	V	W	X	Υ	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

LXK	ΗN	GTH	LXK,	XBL	Т	JNXLMTH
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

SER

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

L	X	K	Н	N	G	Т	Н	L	X	K	,	X	В	L	Т	J	Ν	X	L	M	Т	Н
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

SER

LXK

11 23 10

18 4 17

SER

G T H

6 19 7

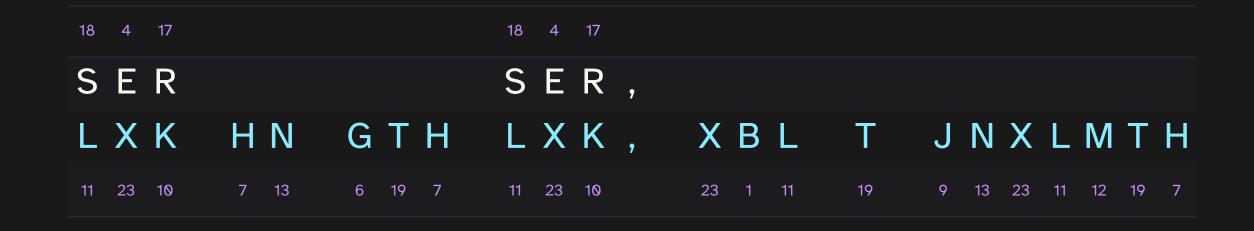
18 4 17

S E R

X B L

23 1 11





 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
 H
 I
 J
 K
 L
 M
 N
 O
 P
 Q
 N
 Y
 Z
 A
 B
 C
 D
 E
 F
 G

 A
 B
 C
 D
 F
 G
 H
 I
 J
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I
 I

18 4 17	14 20	13 0 14	18 4 17	4 8 18	0	16 20	4 18 19	0 14
SER	O U	NAO	SER,	E I S	Α	QU	E S T	АО
LXK	ΗN	GTH	LXK,	XBL	Т	JN	X L M	ТН
11 23 10	7 13	6 19 7	11 23 10	23 1 11	19	9 13	23 11 12	19 7

Cifra afim

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

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

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

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

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

 6
 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

3 14

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

 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
 -

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

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

$$f(3) = 11 \times 3 + 3 = 36 = 10 \mod 26$$

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

3 14 25 10

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



Análise frequencista

Letras mais frequentes em português Α Ε 0 S R Ν D M

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

Letras mais frequentes em português Ε O S R Ν D M

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

Texto	Português
Z (42)	Α
J (25)	Ε
F (19)	Ο
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)	Т

Texto	Português

awdaf j vf iawvjf afftmauaavf a nxj aa vrtajmoau ewata uxftoama evw dawjf mxmra aj amojf magjbaavf eaffawad atmaa aujd aa oaewviama jd ejwtbvf j bxjwwaf jfsvwraavf atf av nxj ewydjota a sywra kxdama j jmowj bjmoj wjdvoa jatstrawad mvgv wjtmv nxj oamov fxiutdawa

Texto	Português
Z (42)	А

awdaf e vf iawvef afftmauaavf a na vrtaemoau ewata uxftoama (e ew davef mxmra ae amoef magebaa eafavad atmaa aued aa oaewiama d eewtbyf e bxewwaf efsywraayf latf av nxe ewydeota a sywra kxdama nowe ber moe wedvoa eatstrawad e e mvgv wetmv nxe oamov fxiutdawad

Texto	Português
Z (42)	Α
J (25)	Ε

ao avdao e vo la veo aoo na la vo ia vrtaemoau ewata uxotoama nxe evw daweo mxmra ae amoeo magebaavo aooa ad almaa aled aa aewlana ewtovo e bxevv ao eosywr aavo av nxe ewydeota a sywra kxdama ao e wedvoa eatstrawad nowe ber e e mvgv wetmv nxe oamov oxiutdawa

Texto	Português
Z (42)	Α
J (25)	Е
F (19)	Ο

ao avdao e o aveo aoo aua o ia vrtaemoau ewata uxotoama nxe evw daweo mxmra ae amoeo magebaavo eaooa vad atmaa aued aa oae viama ewtovo e bxevv ao eosywr aavo av nxe ewydeota a sywra kxdama ao e wedvoa eatstrawad nowe ber e e mvgv wetmv nxe oamov oxiutdawa

Texto	Português
Z (42)	А
J (25)	Ε
F (19)	Ο

as awdas e vs iavves asstrauaavs nxe aa vrtaemoau ewata uxstoama evw dawes mxmra ae amoes magebaavs eassa vad almaa alled aa oaewiama d eewtovs e bxevvas ess sywraays lats av nxe ewydeota a sywra kxdama. nowe bemoe wedvoa eatstrawa e e mvgv wetmv nxe oamov sxiutdawa

Texto	Português
Z (42)	Α
J (25)	Ε
F (19)	
	S

as awdas e vs iavves asstrauaavs nxe aa vrtaemoau ewata uxstoama evw dawes mxmra ae amoes magebaavs eassa vad almaa alled aa oaewiama d <u>eewtovs</u> e <u>bxewwas</u> ess sywraays lats av nxe ewydeota a sywra kxdama. nowe bemoe wedvoa eatstrawa e e mvgv wetmv nxe oamov sxiutdawa

Texto	Português
Z (42)	Α
J (25)	Ε
F (19)	Ο
W/ V (18)	S

as avolas e os a oes assinala os ewata uxstoama (e a o rtaer noal ov daves mxmra ae amoes magebaaos assa ad almaa aled aa oae olana os e bxe as eso aos ev las o xe e o e a a o a ka a a noe wedooa eatstrawad e bei е no nxe cambo s dutdawa 000 wet

Texto	Português
Z (42)	Α
J (25)	Е
F (19)	Ο
W/ V (18)	S

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

Texto	Português
A (42)	Α
E (25)	Ε
S (19)	Ο
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)	Т

Perguntas?