



Atividade: Decodificando a mensagem

Habilidades

LA11 Compreender função como uma relação de dependência entre duas variáveis, as ideias de domínio, contradomínio e imagem, e suas representações algébricas e gráficas e utilizá-las para analisar, interpretar e resolver problemas em contextos diversos, inclusive fenômenos naturais, sociais e de outras áreas.

Para o professor

Objetivos específicos

OE1 Estabelecer modelo matemático a partir de funções, mais especificamente, em uma situação que envolve codificação de mensagens.

OE2 Compreender intuitivamente as condições necessárias para a existência da inversa de uma função. (injetividade e sobrejetividade)

Observações e recomendações

■ Na solução do item (d) estimule seus estudantes a descrever com palavras de maneira precisa o que acontece com os números maiores que 26 caso ele use a expressão $f(x) = x + 14$.

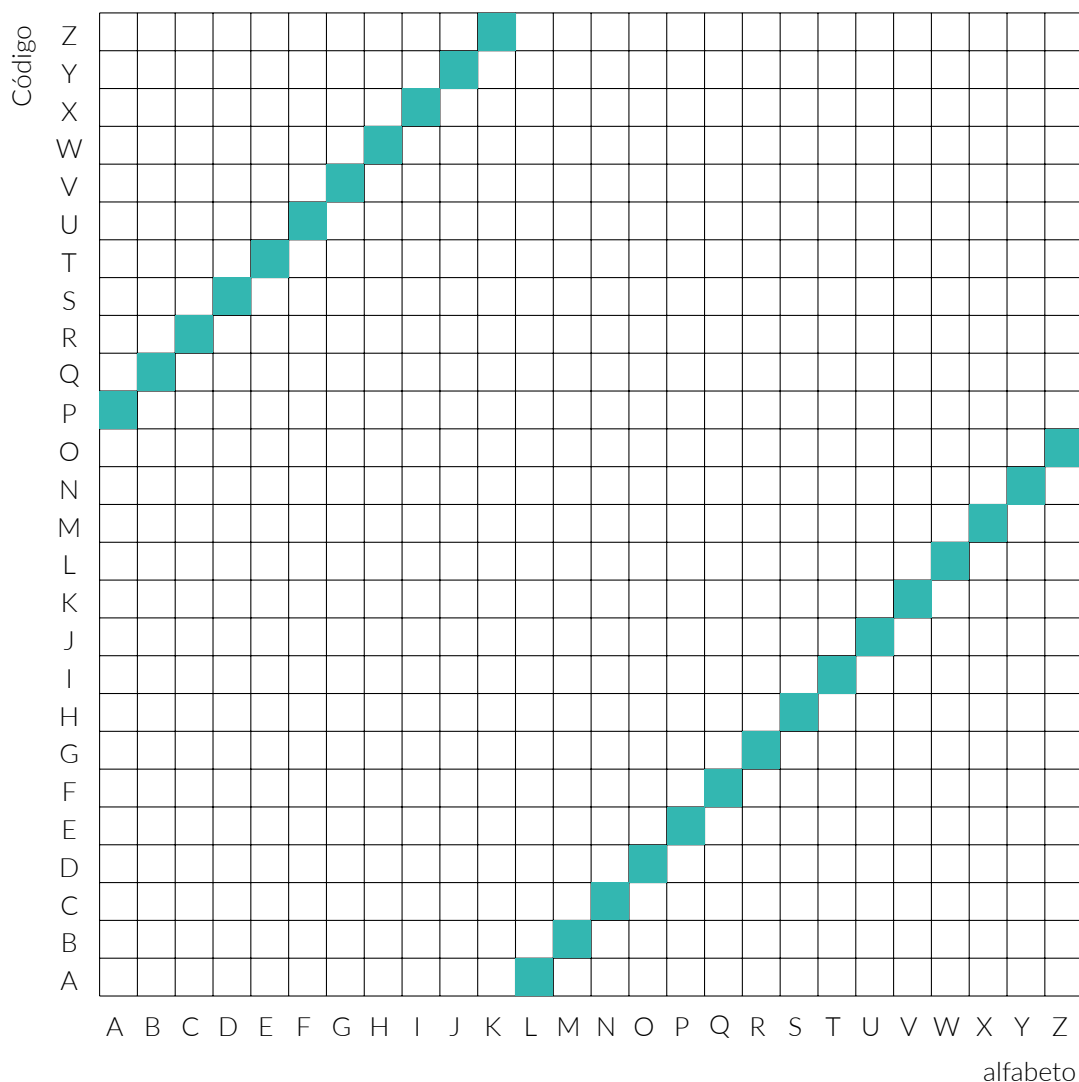
Atividade

Um dos conceitos mais importantes para a segurança na *internet* nos dias de hoje é o que chamamos de **criptografia** (do grego *criptos* = escondido, *grafia* = escrita). Segundo o site *wikipedia* ela é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra codificada, de forma que possa ser conhecida apenas por seu destinatário (detentor da “chave secreta”), o que a torna difícil de ser decifrada por alguém não autorizado. Em outras palavras, cria-se um código que pode ser facilmente desfeito (decodificado) mas apenas por aqueles que conhecem a codificação.

Considere a seguinte maneira de codificar o alfabeto

Original	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
Código	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

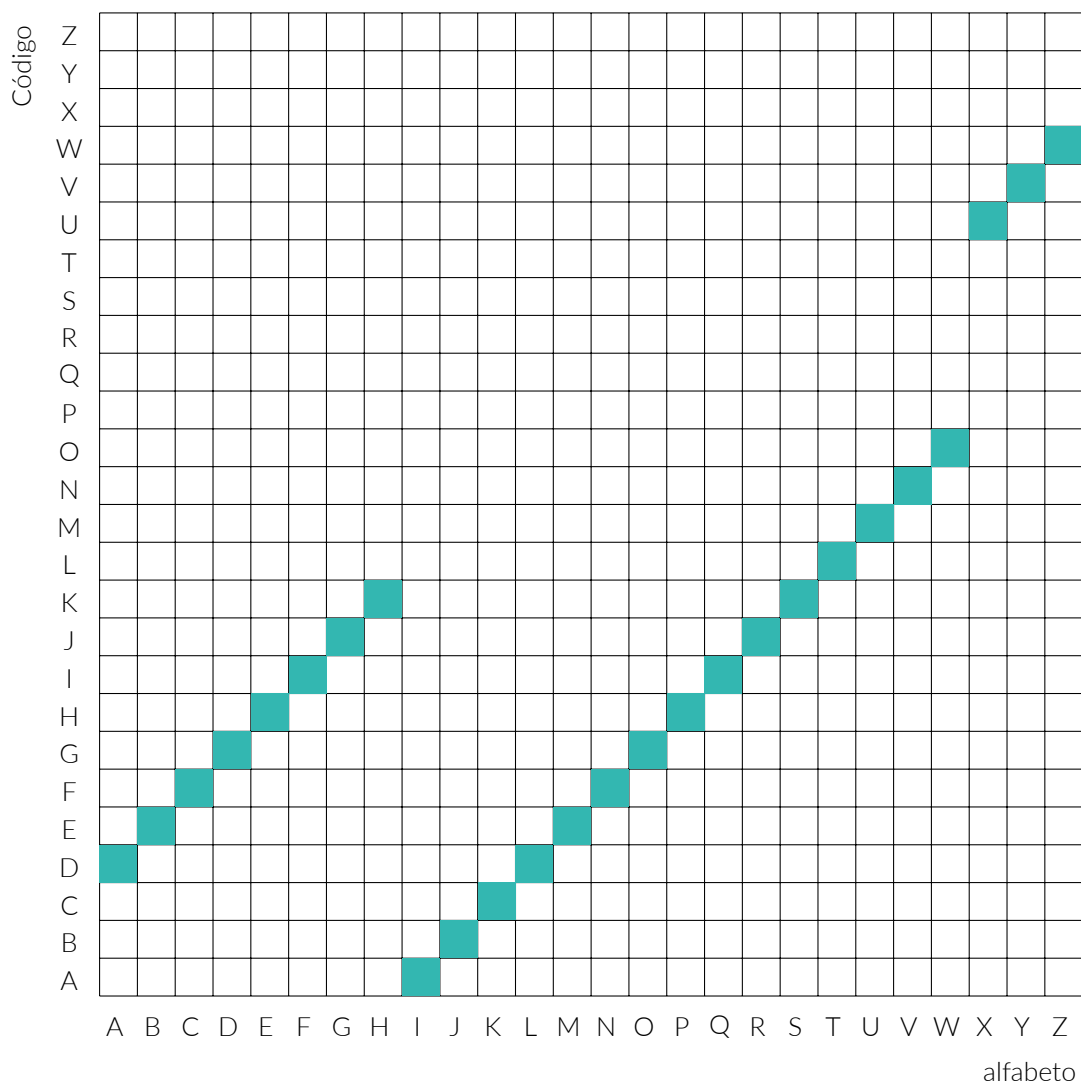
- Use o código acima para codificar a palavra IMAGEM.
 - Se você recebesse uma mensagem com a expressão RGXEIDVGPUPG, como faria para decodificá-la?
- A codificação acima pode também ser representada em um gráfico em que no eixo horizontal estão as letras originais e no vertical os seus respectivos códigos.



- c) Usando ainda o código acima escreva uma mensagem codificada com duas ou três palavras e troque com algum colega seu de classe. Decodifique a mensagem que recebeu.

Você deve ter percebido que a codificação é uma função do conjunto das letras do alfabeto em si mesmo: todas as letras precisam ter um código e uma mesma letra não pode ter mais de um código associada a si.

- d) Seja X o conjunto dos números naturais de 1 a 26. Fazendo a correspondência, $A \mapsto 1, B \mapsto 2, C \mapsto 3$, e assim por diante até $Z \mapsto 26$, determine uma função $f : X \rightarrow X$ que corresponda ao código acima. Observe que por exemplo, $f(1) = 16$.
- e) Usando a expressão $f(x) = x^2$ crie um novo código entre as letras, representando-o no gráfico. O que devemos fazer quando os valores são maiores que 26?
- f) Considerando o código do gráfico abaixo, tente decodificar a palavra APQGJXV.



g) Quais letras do código acima são impossíveis de decodificar e por quê?

h) Que propriedades deve ter um código para que seja possível decodificá-lo?

Solução:

a) XBPVTB

b) Usaria a linha de baixo para descobrir a letra original correspondente: CRIPTOGRAFAR.

c) Resposta pessoal

d) Uma resposta possível seria:

Original	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	26
Código	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Outra possibilidade é escrever $f(x) = x + 15$, subtraindo 26 se $f(x)$ for maior que 26.

The grid shows the following teal squares (row, column) pairs:

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

Para valores maiores que 26 devemos subtrair 26 sucessivamente até encontrar um valor positivo menor que ou igual a 26 e então encontrar a letra correspondente. Isso equivale a tomar o resto da divisão por 26.

- e) Impossível decodificar, pois os códigos P, Q e X não têm correspondente no alfabeto e os códigos G e J têm mais de uma opção de escolha.
- f) Códigos de D a K têm duas letras do alfabeto associadas a cada um. Códigos de P a T e de X a Z não têm correspondente no alfabeto.
- g) Todo código deve possuir um único correspondente no alfabeto. Ou seja, a relação (código, alfabeto) deve ser uma função.