Matemática Multimídia

Números e funções

Guia do Professor

Vídeo

A Carta

Série **Matemática na Escola**

Objetivos

1. Introduzir noções de criptografia

UNICAMP

FNDE FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO

Secretaria de Educação a Distância | Ministério da Ciência e Tecnologia | Ministério da Educação | Governo Federal

A Carta

Série
Matemática na Escola

Conteúdos
Criptografia

Duração
Aprox. 11 minutos.

Objetivos
1. Introduzir noções de criptografia

Sinopse
Andréa tem em mãos uma carta criptografada cujo conteúdo deseja conhecer.

Material relacionado
Vídeos: *A César o que é de César, A loira do banheiro, Em tempos de guerra, Gabarito secreto*;
Experimento: Mensagens secretas com matrizes,

Introdução

Sobre a série

A série Matemática na Escola aborda o conteúdo de matemática do ensino médio através de situações, ficções e contextualizações. Os programas desta série usualmente são informativos e podem ser introdutórios de um assunto a ser estudado em sala de aula ou fechamentos de um tema ou problema desenvolvidos pelo professor. Os programas são ricos em representações gráficas para dar suporte ao conteúdo mais matemático e pequenos documentários trazem informações interdisciplinares.

Sobre o programa

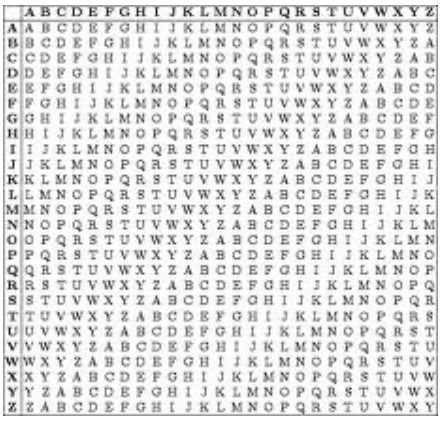
No vídeo, Andréa deseja desvendar o que tem numa cartada cifrada de sua avó que fora enviada por um amigo. Ela pede ajuda a um senhor, que diz se tratar de uma **cifra indecifrável**, também conhecida como **cifra de Vigenère**.

Trata-se de um tipo de criptografia conhecida como **criptografia de chave privada**, na qual uma senha é escolhida entre as partes.

Mais detalhadamente, na cifra de Vigenère, a tabela com as letras do alfabeto funciona como um plano cartesiano em que a palavra-chave serve de referência para a primeira linha vertical e a mensagem a ser cifrada serve como referência para a primeira linha horizontal. A partir do cruzamento das letras da mensagem com as letras da chave, é possível fazer a codificação da mensagem.

No exemplo a seguir, a mensagem é “ATACARBASE” e a chave é “LIMAO”:

Texto: **ATACARBASE**
Chave: **LIMAOLIMAO**
Texto cifrado: **LBMCOCJMSS**



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

Um método para decifrar a chave é associar cada letra do alfabeto a outra letra qualquer aleatoriamente. O problema é que o número de possibilidades de chaves é imenso, mais precisamente, 26!. Esse método é conhecido como **ataque de força bruta**.

Em muitos casos, utilizar a **análise de freqüência** no texto pode levar à mensagem mais rapidamente. A análise de frequência é um método empregado para decifrar criptografias por meio da análise de padrões que se repetem constantemente, que podem indicar a ocorrência de letras ou de palavras de uso comum.

Sugestões de atividades

Antes da execução

Sugerimos a revisão de Inversão de Matrizes.

Depois da execução

Após a execução do vídeo, o professor poderia discorrer um pouco sobre o tema criptografia e na sequência apresentar um problema de codificação usando matrizes.

Um dos métodos usados para criptografar mensagens é por meio de matrizes. Para isso, podemos relacionar as letras do alfabeto às

sequências dos números primos ímpares, e o espaço entre palavras por 2. Em seguida, dispomos esses dados numéricos em uma matriz (X) cujo número de linhas deverá ser igual a ordem da matriz chave (C). A matriz codificada (Y) é a matriz produto CX.

Para decodificar a mensagem é necessário obter a matriz de criptografia, que é a inversa da matriz C, pois de CX=Y, tem-se as seguintes implicações:

$$C^{-1}(CX) = C^{-1}Y \Rightarrow (C^{-1}C)X = C^{-1}Y \Rightarrow IX = C^{-1}Y \Rightarrow X = C^{-1}Y\,.$$

Como exemplo, consideremos que a matriz chave (senha) do receptor seja $C = \begin{bmatrix} 5 & 2 \\ 3 & 1 \end{bmatrix}$, e a matriz codificada Y, recebida por ele seja, $\begin{bmatrix} 39 & 109 & 441 & 501 & 371 \\ 23 & 56 & 254 & 284 & 212 \end{bmatrix}$.

Para obter a matriz X e decodificar a mensagem, o receptor deverá então multiplicar a matriz C^{-1} pela matriz Y.

$$X = \begin{bmatrix} -1 & 2 \\ 3 & -5 \end{bmatrix}\begin{bmatrix} 39 & 109 & 441 & 501 & 371 \\ 23 & 56 & 254 & 284 & 212 \end{bmatrix}$$

$$X = \begin{bmatrix} 7 & 3 & 67 & 67 & 53 \\ 2 & 47 & 53 & 83 & 53 \end{bmatrix}$$

Colocando as linhas 1 e 2 da matriz X (nesta ordem) em uma linha textual, obtém-se a sequência numérica: 7,3,67,67,53,2,47,53,83,53

Em seguida, utilizando a tabela de associação entre letras e números primos, o receptor determina a mensagem CARRO NOVO.

Tabela de Associação entre letras e números primos

	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
2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	101	103

Sugestões de leitura

IEZZI, G. *Fundamentos de Matemática Elementar*, vol. 2, Atual Editora, 1977.
MACHADO, A.S. *Temas e Metas* – vol. 2. Atual Editora,
SOUZA, J. *Matemática – Novos olhares*, vol. 2. FTD
COUTINHO, S.C. *Números Inteiros e Criptografia RSA*. IMPA.

Ficha técnica

Autor *Luiz Antonio Mesquiari*
Revisor *José Plínio de Oliveira Santos*
Coordenador de audiovisual *Prof. Dr. José Eduardo Ribeiro de Paiva*
Coordenador acadêmico *Prof. Dr. Samuel Rocha de Oliveira*

Universidade Estadual de Campinas
Reitor *Fernando Ferreira Costa*
Vice-reitor *Edgar Salvadori de Decca*
Pró-Reitor de Pós-Graduação *Euclides de Mesquita Neto*

Instituto de Matemática, Estatística e Computação Científica
Diretor *Caio José Colletti Negreiros*
Vice-diretor *Verónica Andrea González-López*