Matemática Multimídia

Números e funções

Guia do Professor

Vídeo

A César o que é de César

Série **Matemática na Escola**

Objetivos

1. Apresentar o conceito de criptografia;
2. Dar exemplos da importância da criptografia até os dias de hoje.

ATENÇÃO Este Guia do Professor serve apenas como apoio ao vídeo ao qual este documento se refere e não pretende esgotar o assunto do ponto de vista matemático ou pedagógico.

UNICAMP

FNDE FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO

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

A César o que é de César

Série
Matemática na Escola

Conteúdos
Criptografia; História.

Duração
Aprox. 12 minutos.

Objetivos
1. Ensinar o que é criptografia;
2. Dar exemplos de códigos;
3. Ensinar a importância da criptografia até os dias de hoje.

Sinopse
Na ficção, Pedro, um adolescente *expert* em tecnologias, conversa com o Imperador Romano Júlio César através de um programa de computador. Os dois conversam sobre criptografia e sobre como as mensagens codificadas foram importantes desde a Roma Antiga até os dias de hoje, dando exemplos de códigos e seus usos no decorrer da história.

Material relacionado
Áudios: *Combinação;*
Experimentos: *Mensagens secretas com matrizes, Espelhos e simetrias;*
Vídeos: *O golpe, A loira do banheiro, Gabarito secreto.*

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; além disso, pequenos documentários trazem informações interdisciplinares.

Sobre o programa

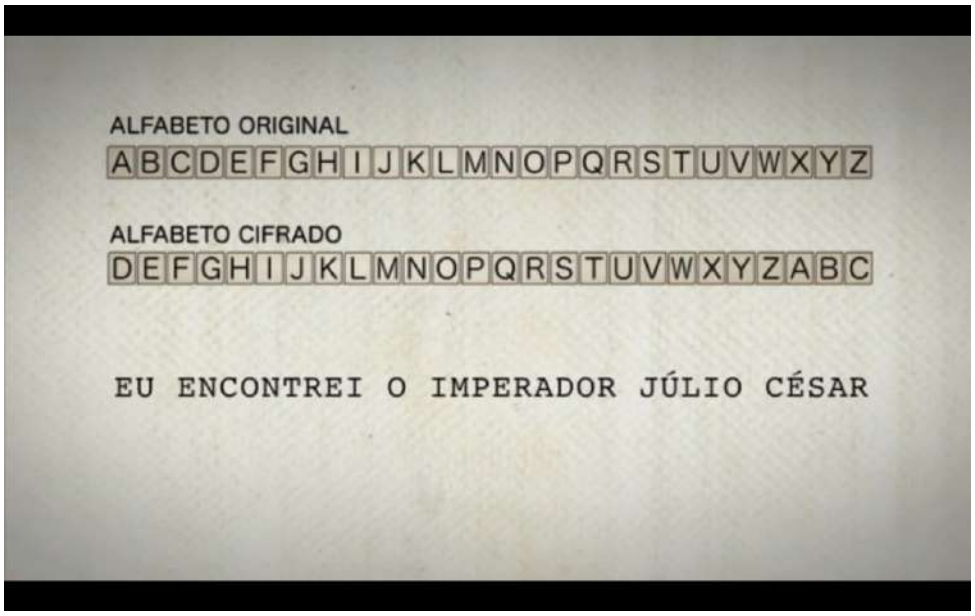
Pedro é um *expert* em computação e consegue, através de seu computador, vencer as barreiras do tempo e entrar em contato com o Imperador Júlio César, na Roma Antiga.

Pedro se apresenta a César e diz estar fazendo uma visita virtual. César pergunta se isso é algum tipo de feitiço e Pedro explica que no futuro existem máquinas que realmente parecem mágicas, como os computadores.

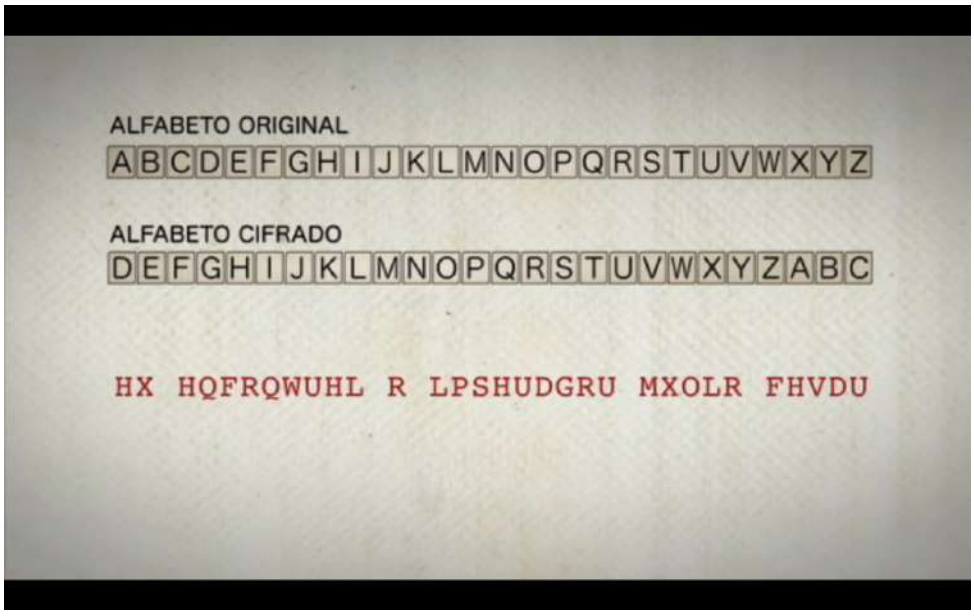
Em seguida, Pedro explica a César que os computadores são máquinas capazes de processar dados, realizar cálculos matemáticos, armazenar informações e que também permitem a comunicação entre pessoas de quaisquer lugares do mundo em tempo real. Assim, através do computador, Pedro conseguiu se conectar com o passado.

César fica curioso para saber como o homem criou o computador e Pedro conta que tudo começou nos tempos antigos, através da criptografia, que é a técnica de transformar uma mensagem da sua forma original para uma forma codificada, de modo que pessoas que não saibam como foi feita a transformação não consigam ler.

César então diz que utiliza esse método para se comunicar com suas tropas, através de um código secreto desconhecido por seus inimigos. Pedro informa que o método de César foi muito importante para a humanidade e César quer saber se Pedro sabe a sua cifra secreta. Pedro então explica como funciona o código.

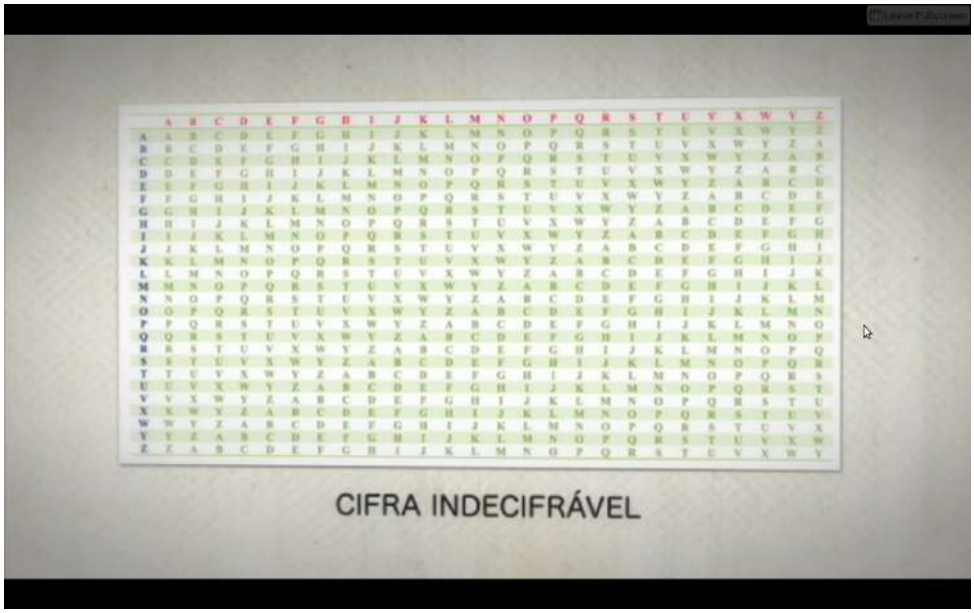


César fica preocupado em saber como Pedro conhece seu código secreto, e Pedro conta que quem decifrou o código foi os árabes, aproximadamente mil anos depois do governo de César, através da análise de frequência das letras.

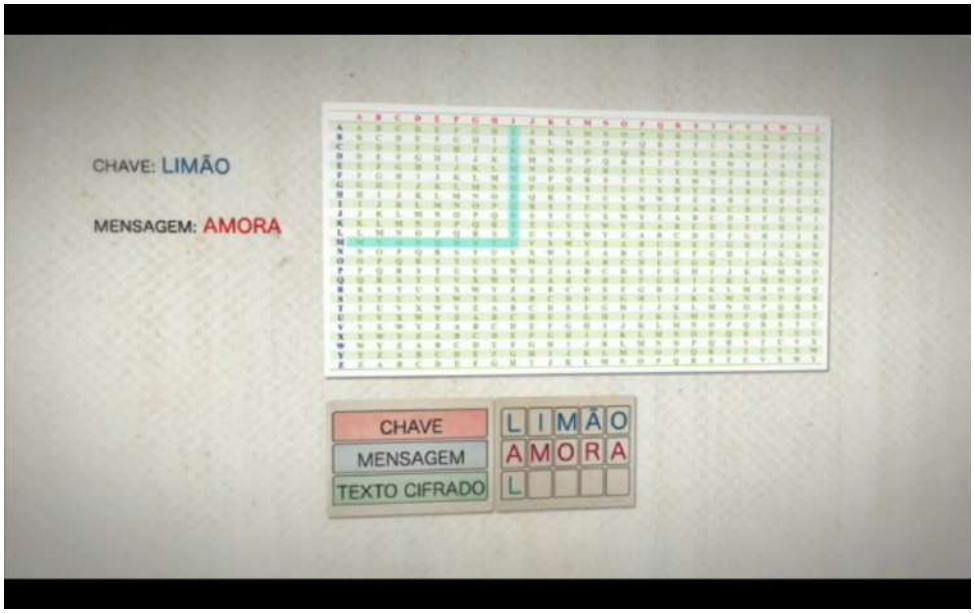


A análise de frequência dos árabes buscava as letras mais usadas nas palavras dos romanos e, com essa informação, era possível descobrir as letras correspondentes na mensagem codificada. Através disso era possível descobrir a chave do código.

César se revolta ao saber que os árabes decifraram seu código, mas Pedro explica que isso foi positivo, pois se iniciou uma competição entre criadores e decifradores de códigos, fazendo com que mais códigos fossem criados, cada vez mais elaborados, como uma cifra que ficou conhecida como “a cifra indecifrável”.



A cifra indecifrável é uma tabela com 25 combinações diferentes do código de César. Através de uma palavra-chave codifica-se a mensagem. Cada letra da mensagem é codificada pelo encontro da coluna onde está a letra da mensagem com a linha onde está a letra da chave.



Pedro conta em seguida que a cifra indecifrável também é quebrada e que outras cifras foram criadas, cada vez mais fortes.

Na Segunda Guerra Mundial, os alemães criam uma máquina de criptografia chamada Enigma, com um sextilhão de possibilidades de senhas. No esforço de decifrar os códigos dos alemães, o britânico Alan Turing e sua equipe criam uma máquina chamada Colossus, capaz de ler as mensagens alemãs. A Colossus é considerada a precursora dos computadores modernos.

Através dos computadores, a criptografia passou por uma nova revolução, o que demandou muitas inovações nesta área. Dentre elas, a descoberta de um método de criptografia de chave pública, que permite a troca de segredos sem a necessidade de um encontro prévio para combinar uma senha. Os criptossistemas de chave pública são fundamentais para as trocas de mensagens por *e-mail* e para o comércio eletrônico que existe hoje.

Pedro explica por fim que a evolução dos computadores ainda continua num ritmo muito acelerado e que computadores mais rápidos surgem todos os anos. Um dos grandes desafios é a fabricação do computador quântico, que, se vier a existir, será bilhões de vezes mais rápido do que os computadores já existentes. Com isso, a criptografia poderá dar um novo grande salto.

Sugestões de atividades

Antes da execução

Pergunte aos alunos exemplos que eles conheçam de códigos secretos para troca de informação, mesmo que seja troca de bilhetes. Para servir de estímulo, pode lembrá-los de livros e filmes, de ação e suspense, que envolvem a decifração de algum código, como, por exemplo: *O código de da Vinci (2003)*, a trilogia *Matrix (1999)*, a trilogia do *Senhor dos anéis (1937-1943 e 2001-2003)* ou a série do *Harry Potter*. O que está em jogo é uma mensagem ou informação que deve ser mantida secreta para alguns, mas que pode ser desvendada eventualmente. Pode lembrá-los de uma forma bem simples de codificações utilizadas nas escolas antigamente, a linguagem do p: “p-eu p-vou p-con p-tar p-um p-se p-gre p-do p-pa p-ra p-vo p-ces”.

Durante a execução

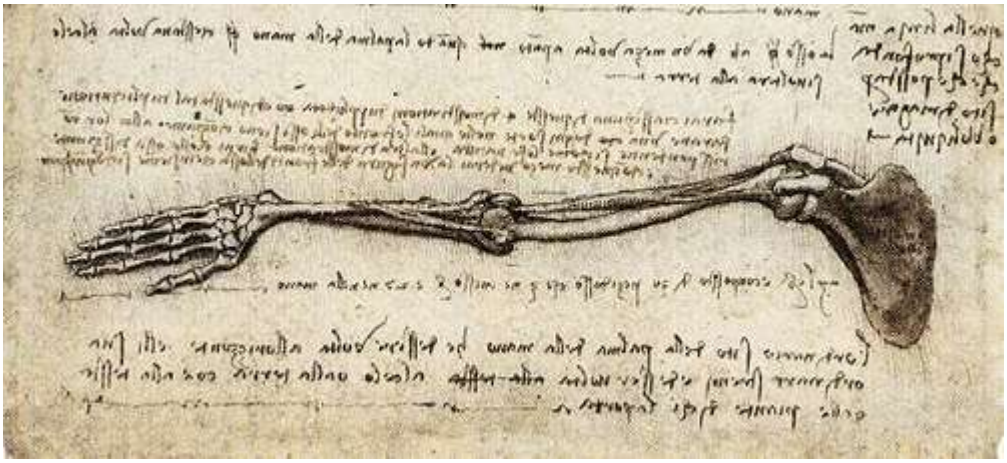
É interessante chamar a atenção de algumas palavras ou dados que aparecem no vídeo, escrevendo no quadro negro para discussão posterior.

Depois da execução

Faça uma breve discussão dos novos termos, nomes e dados anotados durante o programa.

Veja os guias do professor dos seguintes recursos educacionais da coleção M³: Áudios: *Combinação*; Experimentos: *Mensagens secretas com matrizes*; Vídeos: *O golpe, A loira do banheiro, Gabarito secreto.*

O código de da Vinci



Alguns manuscritos de da Vinci foram feitos pela cópia da imagem no espelho. Em uma época que poucos tinham costume de leitura, podemos dizer que era uma estratégia simples de codificar suas informações. Neste caso, para decifrar a mensagem, basta ler por um espelho. O professor pode aproveitar algumas ideias que envolvem o espelho no experimento *Espelhos e simetrias*.

Uma transcodificação

Considere a seguinte tabela: cada número da primeira coluna é transformado por uma função linear (proporcionalidade ou

porcentagem). O resultado está em códigos na segunda coluna. Deve-se entender que cada letra representa um dígito. Assim, a letra C, por exemplo, sempre vai representar o mesmo dígito. Obtenha a proporcionalidade. Permita tempo aos alunos para encontrarem a função transformadora.

20	G C
15	I J
45	A C
35	C G
70	J C
80	H F
25	E B
60	D G

Vamos escrever a função $f(x)=k\,x$. O objetivo é obter k.

A primeira observação a ser feita é que todos os números naturais da tabela, de dois dígitos, são transformados em números naturais de dois dígitos.

Assim, concluímos que $k>9/15$ e $k<100/80$, pois, ao aplicarmos a função a 15 e a 80, obteríamos 9 e 100 respectivamente ao invés de números com dois dígitos. Em outras palavras, $3/5<k<5/4$, isto é, $0,6<k<1,25$.

Talvez não por acaso todos os números da primeira coluna são múltiplos de 5. Já os números da segunda coluna exibem C, J, G, F e B como dígito final, portanto não são múltiplos de cinco, que devem ter apenas 0 e 5 no dígito final. Com isso, já podemos concluir que $k=4/5$.

Assim, f(x)=4x/5 e, desta forma, devemos ter na segunda coluna múltiplos de 4, que sabemos ter 0, 2, 4, 6 e 8 como dígito final.

Veja outras possibilidades deste problema no portal NRICH (em inglês).

Sugestões de leitura

J. R. Giovanni e J. R. Bonjorno (2000). **Matemática – Uma nova abordagem**. Editora FTD.
S. Singh. **O livro dos códigos**. Editora Record, 2001.
S. Coutinho (2007). Números inteiros e criptografia RSA. IMPA.
I. Stewart (2010). **Incríveis Passatempos Matemáticos**: Tradução D. Alfaro. Editora Zahar
NRICH. *A change in code*. Disponível em http://nrich.maths.org/4799 . Acesso em 08 mar. 2011.

Ficha técnica

Autora *Beatriz Castro Dias Cuyabano*
Revisão *Cristiano Torezan*
Coordenação de Mídias Audiovisuais *Prof. Dr. Eduardo 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 *Jayme Vaz Jr.*
Vice-diretor *Edmundo Capelas de Oliveira*