



Guia do Professor



Vídeo


Tempos de guerra

Série Matemática na Escola

Objetivos

1. Mostrar a importância da criptografia na evolução da história e da tecnologia;
2. Apresentar tipos de máquinas e artefatos que possibilitam a criação de cifras e a decodificação das mesmas;
3. Introduzir conceitos de criptografia.

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.

LICENÇA Esta obra está licenciada sob uma licença Creative Commons 

Tempos de guerra

Série

Matemática na Escola

Conteúdos

Criptografia;

Duração

Aprox. 10 minutos.

Objetivos

1. Mostrar a importância da criptografia na evolução da história e da tecnologia;
2. Apresentar tipos de máquinas e artefatos que possibilitam a criação de cifras e a decodificação das mesmas;
3. Introduzir conceitos de criptografia.

Sinopse

Mariana, através da internet, ao desejar feliz aniversário para a sua avó conversa sobre o trabalho dela durante a 2ª guerra mundial, que envolve mensagens, códigos, criptografia e muitas curiosidades sobre máquinas que criavam e decodificavam cifras e os primeiros computadores.

Material relacionado

Áudios: *Números primos*;

Experimentos: *Mensagens secretas com matrizes*;

Vídeos: *Gabarito secreto*, *A loira do banheiro*, *O golpe*, *Daí a César o que é de César*.

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

O programa faz um pequeno histórico sobre o papel da matemática para desvendar códigos criptografados durante a Segunda Guerra Mundial.

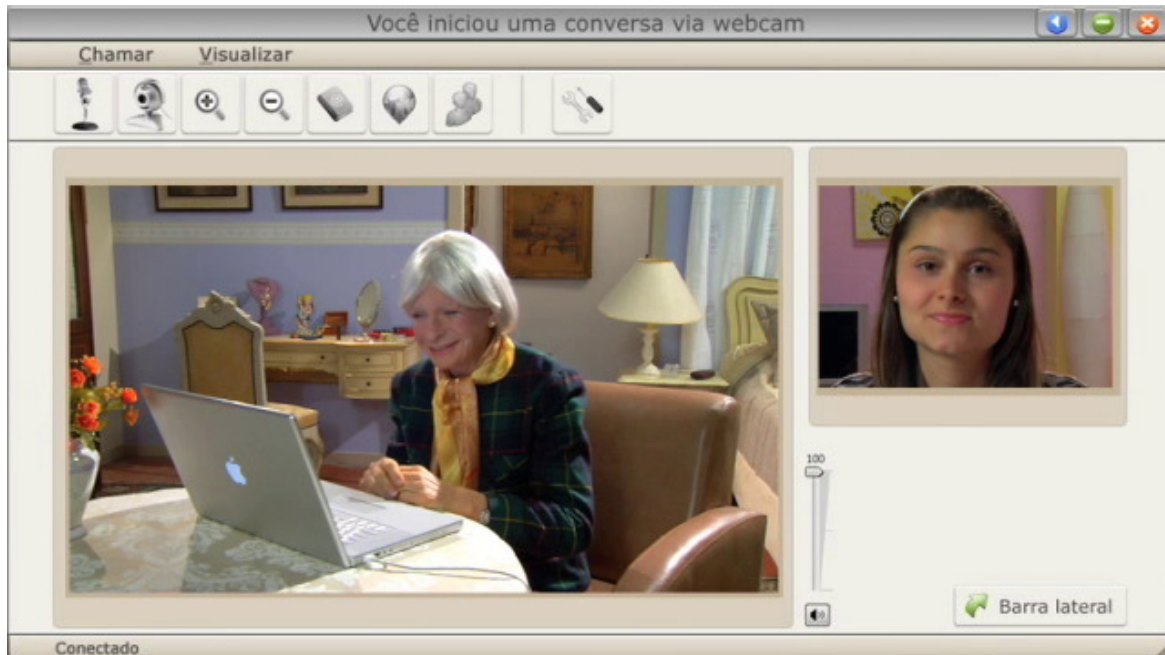


Figura 1 Mariana conversa a a avó pela internet

Na ficção, Mariana conversa com a sua avó que trabalhou durante a guerra na Inglaterra.

Os alemães tinham desenvolvido uma máquina para codificar mensagens entre seus exércitos e comandos. Era chamada de Enigma



Figura 2 Ilustração do vídeo sobre a máquina Enigma dos alemães

O esquema de criptografia automático da Enigma foi entendido pelos Poloneses que inventaram uma máquina para decodificar suas mensagens, mas os alemães de Hitler aprimoraram a Enigma e assim, somente com a cooperação internacional e a ajuda do matemático Alan Turing, foi possível desenvolver a máquina (precursora dos computadores modernos) Colossus que conseguia quebrar uma mensagem codificada em aproximadamente três horas.

A avó da Mariana trabalhou (na ficção) operando essa máquina Colossus. É interessante observar que as mulheres ocuparam postos importantes no desenvolvimento e operação de máquinas automáticas e computadores. Por exemplo, O ENIAC (*Electrical Numerical Integrator and Computer*) foi desenvolvido pelos norte-americanos durante a guerra para calcular tabelas de alcance de projéteis, dentre outras computações. Algumas fotos de época mostram que eram

mulheres quem mais operavam essas máquinas. O ENIAC só ficou de fato operante após o final da guerra e por essa razão a Colossus foi recentemente reconhecida como precursora dos computadores modernos, pois já operava durante a guerra.



Figura 3 Operação do ENIAC feita por mulheres em 1946

De qualquer forma o ENIAC foi o primeiro computador *digital eletrônico*, enquanto a Colossus tinha fortes as partes mecânica e analógica.

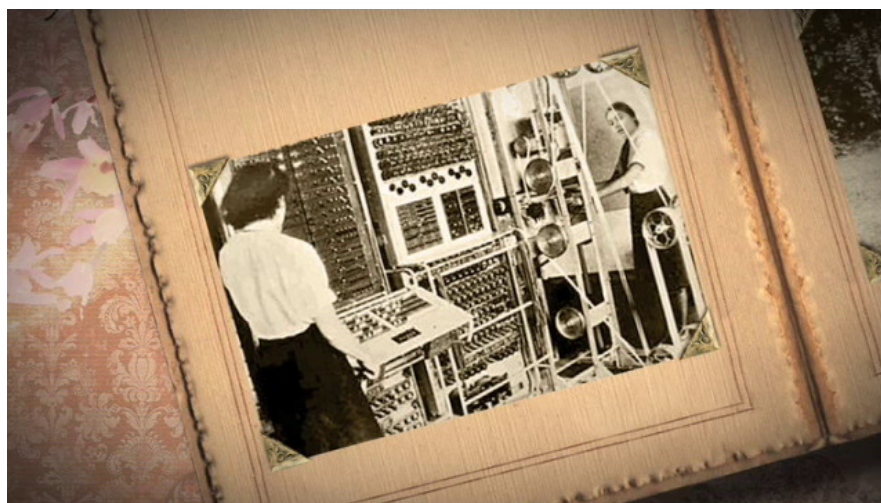


Figura 4 Vó da Mariana operando a Colossus

A máquina Enigma não era apenas uma cifradora de César. A cifra de César mudava as letras do alfabeto por uma operação de “rotação rígida” no alfabeto colocado em um laço. Veja a ilustração abaixo do vídeo *A loira do banheiro*, da coleção M³ Matemática Multimídia.



As mensagens que usam a cifra de César são facilmente descobertas, pois existem apenas 26 cifras possíveis com o alfabeto de 26 letras.

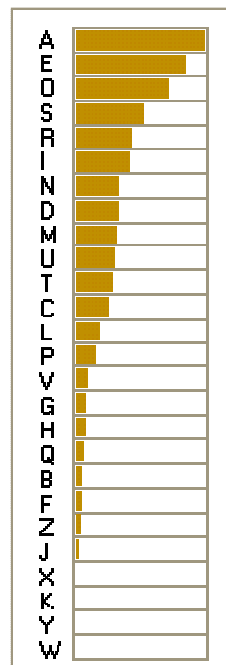
Um método mais elaborado é o da substituição de cada letra por outra diferente. Neste caso podemos permutar todas as letras e existem 26! (26 fatorial) cifras de substituição diferentes. É um número grande de possibilidades, pois $26! = 403.291.461.126.605.635.584.000.000$, isto é, mais de 4×10^{26} .

No entanto, este método de substituição por permutação do alfabeto usualmente é decifrado com o uso de frequência relativa de letras na linguagem que a mensagem foi originalmente escrita. Para isto é preciso observar na mensagem as letras que mais se repetem e estas são provavelmente as letras que mais se repetem na língua em questão. Quanto maior o texto codificado, mais precisa será a frequência relativa das letras em comparação. Essa estratégia é usada nas brincadeiras de força.

Em português podemos apresentar a Tabela 1 (xenográfica) de frequência relativa das letras do nosso alfabeto. Nos textos analisados as vogais acentuadas (á, ã, ô,...) foram transformadas em vogais normais e o C cedilha em C. Esse trabalho foi feito por vovó Vicki do site www.numaboa.com sob Licença Creative Commons.

Tabela 1

Letra	Freq. %	Letra	Freq. %
A	14.63	N	5.05
B	1.04	O	10.73
C	3.88	P	2.52
D	4.99	Q	1.20
E	12.57	R	6.53
F	1.02	S	7.81
G	1.30	T	4.34
H	1.28	U	4.63
I	6.18	V	1.67
J	0.40	W	0.01
K	0.02	X	0.21
L	2.78	Y	0.01
M	4.74	Z	0.47



Histograma por
Ordem de
Frequência

É fácil perceber porque as vogais *a*, *e*, *o* são as 3 letras de maior frequência em português (em espanhol também, mas não nessa ordem). Todos os substantivos femininos terminam com *a* e exigem a letra para fazer referência. Por exemplo, *a porta*. Idem para a letra *o*. O fato da letra *s* ser a quarta letra na ordem decrescente de frequência vem principalmente por causa do plural. E a quinta letra, *r*, aparece em função dos nossos verbos regulares.

Assim, a cifra de substituição, se for mantida por algum tempo e as mensagens interceptadas, para que o texto fique maior para a análise de frequência, será decifrada mais cedo ou mais tarde.

Para evitar a análise de frequência relativa das letras, a equipe que desenvolveu a Enigma alemã inventou um procedimento de “rotação individual” da seguinte forma. Cada letra recebe um número de 0 a 25.

Se a r -ésima letra da mensagem é associada ao número i_r do alfabeto, então ele é trocado pelo número

$$R(r, i_r) = r - 1 + i_r - 26j_r,$$

onde j_r é o inteiro necessário para fazer com que o número $r - 1 + i_r - 26j_r$ esteja entre 0 e 25, isto é, corresponda a uma letra do alfabeto.

Exemplo de rotação individual

Aplicar a rotação descrita acima à palavra MATEMATICA. A substituição das letras pelos correspondentes números iniciais associa

MATEMATICA \rightarrow 12001904120019080200

Sendo que cada número associado às letras tem dois dígitos de 00 a 25. Agora a aplicação da rotação transforma aquele número da seguinte maneira:

$$R(1, 12) = 12, \quad R(2, 00) = 01, \quad R(3, 19) = 21, \quad R(4, 04) = 07, \quad R(5, 12) = 16, \\ R(6, 00) = 05, \quad R(7, 19) = 25, \quad R(8, 08) = 15, \quad R(9, 02) = 10, \quad R(10, 00) = 09$$

Assim o número composto é 12012107160525151009, que por sua vez se traduz nas seguintes letras: MBVHQFZPKJ. Confira com a sua turma.

Se o interceptador souber que a mensagem codificada é resultado de uma rotação como essa, é fácil obter a inversa e decifrar a mensagem.

Exemplo de mensagem decifrada

Digamos que RPVD foi cifrada pela rotação individual das letras, pela descrição acima. Assim temos:

- $R(1, i) = 17 = 1 - 1 + i, \Rightarrow i = 17,$
- $R(2, i) = 15 = 2 - 1 + i, \Rightarrow i = 14,$
- $R(3, i) = 21 = 3 - 1 + i, \Rightarrow i = 19,$
- $R(4, i) = 03 = 4 - 1 + i, \Rightarrow i = 00.$



Portanto a palavra original é ROTA. Verifique com os seus alunos.

A máquina ENIGMA dos alemães combinava permutação de múltiplos alfabetos (originalmente três e depois quatro) além do esquema de rotação individual para evitar análise de frequência. A chave de decodificação era trocada até duas vezes ao dia. O procedimento de codificar era feito pela máquina e a mesma máquina com a “corrente” no sentido oposto decodificava automaticamente a mensagem criptografada.

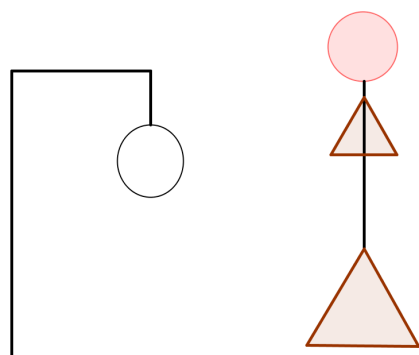
Para conseguir decifrar as mensagens dos alemães, foi necessária a construção da máquina COLOSSUS com a liderança do matemático britânico Alan Turing.

Sugestões de atividades

Antes da execução

O professor pode pedir aos seus alunos, revisar ou estudar a história de segunda guerra mundial e como o serviço de inteligência dos aliados desvendou as manobras dos países do eixo, liderados pela Alemanha. Se for apropriado, pode conversar com o professor de História e fazer um trabalho conjunto.

É recomendável uma revisão sobre fatoriais e permutações e se for apropriado, permitir uma brincadeira de Forca em duplas. Cada aluno da dupla propõe uma palavra que o outro deve desvendar.



Estabeleça as regras mais simples possíveis. O objetivo é criar a idéia de decifrar a palavra do colega e assim prepará-lo para o vídeo sobre criptografia. Por exemplo, o bonequinho deve conter apenas a cabeça, o tronco, o par de braços

e o par de pernas.

Depois da execução

Atividade 1

Quantas cifras de substituição nós podemos construir?

Uma maneira de fazer uma cifra é associar cada letra a outra letra diferente. Considere apenas as vogais a, e, i, o, u. Quantas cifras diferentes podem ser feitas apenas trocando as vogais? Nesse caso são 5! Verifique se todos os alunos entendem que há $5 \times 4 \times 3 \times 2 \times 1$ maneiras de associar uma vogal a outra diferente.

Atividade 2

Mostrar que a cifra de César é um caso particular de permutação das letras – uma rotação.

Vamos considerar apenas as vogais AEIOU \rightarrow 01234 e codificar interjeição dos mineiros UAI, por uma translação de 3 letras, isto é,

A,E,I,O,U \rightarrow O,U,A,E,I

Assim UAI \rightarrow IOA.

Agora considere o procedimento de rotação. $R(r, i) = r - 1 + i_r + 5 i_j$, onde o último termo faz com que o número volte a ser entre 0 e 4.

Aplicar a rotação ao IOA \rightarrow 230. Então temos

$R(1, 2) = 2$, $R(2, 3) = 4$, $R(3, 0) = 2$. Assim IOA \rightarrow IUI.

Considere atividade similar para a ênfase dos gaúchos, TCHE, mas agora com as 26 letras.



Desafio

Desafie os seus alunos a escreverem palavras cifradas com o procedimento de rotação. Por exemplo, uma dupla cifra uma palavra (não deixe os alunos usarem palavras longas, caso contrário eles vão demorar muito para fazer a atividade e podem perder o interesse) e outra dupla decifra a palavra.

Discussão

Com base na Tabela 1, promova uma rápida discussão sobre a estratégia de usá-la nos jogos de Forca. Observem que uma palavra pequena pode ter letras que não são as mais freqüentes em geral. Igualmente uma mensagem típica de guerra deve ter particularidades que fogem do padrão dos textos comuns de uma linguagem. Por exemplo, as mensagens dos exércitos americanos tinham muito freqüente a sigla *USA* e a palavra *América* - um erro básico de mensagem secreta.

Sugestões de leitura

S. Singh (2001). **O livro dos códigos**. Editora Record. Veja também o site mantido por este autor, em inglês (página visitada em 12/04/2011): <http://www.simonsingh.net/cryptography/>.

S. Coutinho (2007). **Números inteiros e criptografia RSA**. IMPA.

Aplicativo para a Cifra de César, página visitada em 12/04/2011:

<http://www.sccs.swarthmore.edu/users/03/julieg/hw14cipher.html>

Vicki, *Frequência de ocorrência de letras no Português*, **Criptografia numaboa**, página visitada em 12/04/2011:

<http://www.numaboa.com/criptografia/criptoanalise/310-Frequencia-no-Portugues>.

Ficha técnica

Autor: *Samuel Rocha de Oliveira*

Revisão: *Cristiano Torezzan*

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 *Caio José Colletti Negreiros*

Vice-diretor *Verónica Andrea González-López*



Matemática Multimídia

VÍDEO

Tempos de guerra 12/12