



Matemática
Multimídia

Números
e funções



Guia do Professor



Vídeo


A loira do banheiro

Série Matemática na Escola

Objetivos

1. Apresentar os princípios básicos da criptografia.
2. Mostrar o funcionamento de algumas cifras de substituição.
3. Apresentar alguns esquemas de criptoanálise.

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 



UNICAMP

A loira do banheiro

Série

Matemática na Escola

Conteúdos

Criptografia.

Duração

Aprox. 10 minutos.

Objetivos

1. Apresentar os princípios básicos da criptografia.
2. Mostrar o funcionamento de algumas cifras de substituição.
3. Apresentar alguns esquemas de criptoanálise.

Sinopse

Um detetive particular recebe estranhas mensagens no seu celular assinadas pela misteriosa “Loira do banheiro”. Com a ajuda do seu amigo especialista em segurança de sistemas, ele tentará decifrar o conteúdo das mensagens.

Material relacionado

Experimentos: *Mensagem secreta 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 introdutórios de um assunto a ser estudado em sala de aula 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 vídeo trata de princípios básicos de criptografia e criptoanálise. De maneira mais específica, são introduzidas as técnicas de criptografia de substituição monoalfabética e análise de frequência para a decifragem de mensagens.

O assunto, apesar de não ser tradicional em currículos do ensino médio, ilustra muito bem como a intuição adquirida com o estudo de matemática pode ser aplicada para resolver problemas importantes, como de transmitir mensagens de maneira segura.

A criptografia é um processo tão antigo quanto a necessidade de manter a segurança de informação sigilosa e, dentre as cifras utilizadas, a de substituição monoalfabética, descrita no vídeo, é uma das mais antigas e amplamente utilizadas até o século XIX. Ela trata de substituir um alfabeto por outro e escrever os símbolos trocados, conforme mostrado neste trecho do vídeo:



Fig.1 Substituição monoalfabética do texto

A etimologia de “monoalfabética”, significa que para o texto só foi utilizado um alfabeto cifrado. Existem cifras polialfabéticas, que utilizam mais que um alfabeto para cifrar o texto, como por exemplo, a Cifra de Vigenère.

Do ponto de vista matemático, é possível para o professor formalizar um pouco mais o processo de cifragem e decifragem através do conceito de função. Uma cifra é, em suma, uma função (bijetiva) que leva o alfabeto real no alfabeto cifrado, ou seja, no caso do vídeo: $f(A) = Z$, $f(B) = Y$, etc. *Cifrar uma mensagem* é exatamente aplicar a função a cada uma de suas letras. Para *decifrar uma mensagem*, é necessário aplicar a inversa da função na mensagem cifrada. *Quebrar uma mensagem* é conseguir inferir o valor do texto original sem possuir, a priori, a função. Este formalismo pode ser usado pelo professor para ilustrar os conceitos de função, funções injetoras e sobrejetoras e função inversa.

Por fim, o vídeo mostra uma maneira de *quebrar mensagens*. Existe um dilema ético em relação à quebra de mensagens. Entretanto é preciso ter em mente que o estudo da criptoanálise se sustenta pelo fato de, a partir da descoberta da fragilidade de sistemas criptográficos, construir sistemas melhores.

A cifra apresentada ao detetive, no vídeo, bem como a Cifra de César, possui a fragilidade de ser decifrada facilmente pela análise de

freqüência, que constitui, a partir do conhecimento de em qual língua o texto foi cifrado, comparar as tabelas de freqüência das letras com a tabela de freqüência dos textos da língua. A tabela de freqüências (em porcentagem) do português do Brasil é a seguinte:

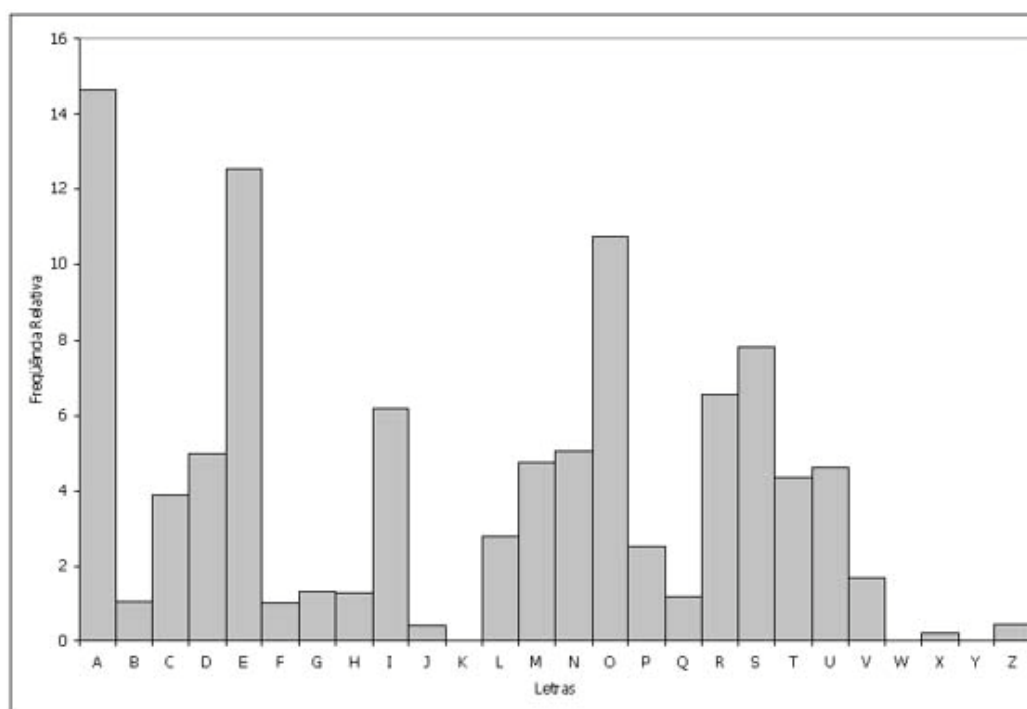


Fig.2 Tabela de freqüência relativa das letras do português

Portanto, ao pegar um texto criptografado, é razoável supor que a letra mais freqüente deverá ser o “A”, a segunda deverá ser o “E” e assim por diante, podendo fazer algumas correções no processo de decifragem, eventualmente. Também é possível fazer uma análise “de segunda ordem”, em que se analisa quais são as letras que ocorrem com mais freqüência próximas de outras. Por exemplo, se duas letras formarem uma palavra, as possibilidades que fazem sentido restringem-se a algumas poucas (no português: ao, ou, de, da, em, na, etc.).

Essa fragilidade no sistema mostra que, para aplicações importantes (como seguranças de informações de bancos), são necessários sistemas mais seguros. Estes sistemas utilizam propriedades aritméticas dos números (por exemplo, a dificuldade de fatorar um número que seja produto de dois primos), entretanto este assunto foge ao escopo da introdução da criptografia através do vídeo.

Sugestões de atividades

Antes da execução

É possível, antes da execução, propor aos alunos que troquem mensagens entre si de uma maneira que ninguém consiga descobrir. Aqui, uma sugestão de experimento:

Experimento 1: Dois alunos são escolhidos entre a turma. É dito a eles que eles terão algum tempo (um ou dois minutos) para combinar uma maneira de trocar mensagens, fora da sala. A mensagem será constituída de algum número de 0 até 9 e este número será dito aos alunos escolhidos após eles combinarem a chave secreta. Depois do retorno dos dois alunos, o professor fala no ouvido de algum deles três desses números e o aluno, publicamente, tem que transmitir esse número ao outro de maneira que a sala não descubra. Este experimento leva aproximadamente 10 minutos e motiva os outros alunos a tentarem quebrar a cifra dos dois escolhidos.

Depois da execução

Depois da execução, é interessante comparar as cifras apresentadas com o experimento realizado. A cifra utilizada pelos alunos é mais fácil ou mais difícil que a do detetive? A maneira dos alunos de tentar quebrar é parecida? Quais as diferenças? (No experimento proposto foram utilizados números, o que não permite a criptoanálise por análise de frequência, entretanto são possíveis outros métodos de dedução). Para pensar: E se a troca de cifras não fosse segura, ou seja, os alunos tivessem que trocar a cifra com os outros ouvindo, ainda seria possível? (A resposta é sim, e a cifra é a conhecida “criptografia de chave pública”, que utiliza propriedades de números primos para divulgação de cifras).

Podem ser propostos também experimentos em que os alunos são divididos em dupla e combinam uma cifra e transmitem mensagens

uns para os outros, enquanto, num segundo momento, as duplas tentam quebrar as mensagens da outra com a análise de frequência.

É possível também propor problemas individuais com o objetivo de fixar os conceitos. Seguem algumas sugestões:

Problema 1 (Quando a análise de frequência falha): Suponha que se queira cifrar a seguinte mensagem: “De Zanzibar ao zénite, feliz!”. Com a seguinte cifra:

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
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

Como ficaria o alfabeto cifrado? Para decifrar, como você o faria por análise de frequência?

Resposta: O aluno deverá conseguir facilmente cifrar a mensagem (“kl ghugpihy hv glupal, mlspg!”), não modificando as pontuações.

Se o problema fosse decifrar a mensagem (“kl ghugpihy hv glupal, mlspg!”), a análise de frequência não seria tão apropriada, pois no texto original, há mais letras “z”, do que “a”.

Problema 2 (Cifra de Vigenère): Suponha que se quer *cifrar* a mensagem “EUTEAMO”, com o seguinte processo:

Para as letras ímpares (a primeira, a terceira, etc...) utiliza-se a chave:

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
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

Para as pares, utiliza-se:

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
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

Como ficaria a mensagem? Se você tivesse que *decifrar* uma mensagem com esta cifra, como faria?

Resposta: A mensagem ficaria: “lgaqhyv”. A maneira “tradicional” de quebrar é aplicando duas vezes a análise de frequência, uma para as pares e outra para as ímpares.

Sugestões de leitura

S. Singh (2001). O livro dos códigos. Editora Record

Sugestão de aprofundamento: S. Coutinho (2007). Números inteiros e criptografia RSA. IMPA

Sites recomendados: Aplicativo para a Cifra de César:

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

História dos códigos e muitas curiosidades (inglês):

http://www.simonsingh.com/Crypto_Corner.html

Ficha técnica

Autor *Antonio Carlos de Andrade Campello Junior*

Revisor *Samuel Rocha de Oliveira*

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 *Jayme Vaz Jr.*

Vice-diretor *Edmundo Capelas de Oliveira*