Matemática Multimídia

Números e funções

Guia do Professor

Vídeo

O Golpe

Série **Matemática na Escola**

Objetivos

1. Apresentar o conceito de criptografia;
2. Contextualizar o assunto através de exemplos práticos.

UNICAMP

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.

FNDE FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO

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

O Golpe

Série
Matemática na Escola

Conteúdos
Criptografia, o futuro da criptografia.

Duração
Aprox. 10 minutos.

Objetivos
1. Apresentar o conceito de criptografia.
2. Contextualizar o assunto através de exemplos práticos.

Sinopse
Um possível golpe milionário aos cofres públicos está sendo planejado supostamente por bandidos, que trocam mensagens via e-mail. Guto investiga o caso, porém encontra dificuldades em obter informações dos suspeitos, pois suas mensagens são criptografadas e, portanto, difíceis de desvendar. A única saída está no futuro dos computadores.

Material relacionado
Vídeos: *Venda segura; Gabarito secreto, Loira do banheiro; A Cesar o que é de Cesar.*
Experimentos: *Mensagem secreta com matrizes;*

Introdução

Sobre a série

A série Matemática na Escola aborda conteúdos de matemática do ensino médio através de aplicações em situações do cotidiano. Os programas desta série usualmente são informativos e podem servir como introdução a um assunto ou fechamento de um tema já desenvolvido pelo professor. Os programas são ricos em representações gráficas, para dar suporte ao conteúdo matemático, e pequenos documentários, que trazem informações interdisciplinares relacionadas ao assunto principal.

Sobre o programa

Guto, um "cyber-investigador" que trabalha para o governo, e seu chefe conversam sobre um possível golpe milionário que será aplicado nos cofres públicos. Apesar de ter descoberto os nomes dos suspeitos e o endereço de um deles, através de uma escuta telefônica, um dos problemas para Guto é que os supostos criminosos agora só se comunicam pela internet, via e-mail, o que dificulta a interceptação das mensagens. Guto explica a seu chefe que consegue interceptar os e-mails, mas o fato deles serem criptografados impede a descoberta de seus conteúdos. Isso os obriga a investigar os suspeitos através de outros métodos.

Embora esse vídeo retrate um cenário fictício, seu conteúdo é atual e ajuda a entendermos o que é, de onde veio e para onde vai a criptografia, além das implicações desse assunto em nosso cotidiano em geral.

Juntando a palavra grega *cryptos*, que significa secreto, oculto, com o sufixo *grafia*, oriundo do verbo grafar, escrever, *criptografia* significa então escrever de forma oculta, isto é, a arte de escrever uma mensagem mantendo seu conteúdo real em segredo. Os primeiros

indícios de criptografia datam do império romano, quando o imperador Júlio César (100 – 44 a.C.) trocava mensagens sigilosas com os militares romanos que estavam espalhados na Europa.

Para falar de criptografia é importante entendermos o conceito de cifra (ou chave). Em geral, é a complexidade da cifra que determina a força do sigilo. Uma cifra é uma regra segundo a qual uma mensagem será criptografada. Por exemplo, a cifra de César, utilizada pelo imperador romano, era uma regra simples que associava a cada letra do alfabeto uma outra letra, univocamente, através de um deslocamento do alfabeto original. Assim, partindo do nosso alfabeto

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

a cifra de César consistia em criar uma chave a partir de um deslocamento qualquer desse alfabeto. Se deslocarmos o alfabeto em quatro letras para a esquerda, por exemplo, obteremos:

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

que é a chave em questão. Então uma mensagem qualquer, por exemplo

Matematica multimidia

era reescrita como **Qewiqewmge qypwmqmhme**, através da correspondência das letras na chave, isto é, troca-se o A por E, o B por F, o C por G e assim por diante.

Como foi dito, o poder da cifra está em sua complexidade. A cifra de César é simples e fraca, pois há uma correspondência direta entre as letras do alfabeto e da mensagem cifrada, de modo que **a estrutura geral das palavras se mantém**. Mesmo se a cifra fosse construída sobre um conjunto de 26 símbolos quaisquer, seria possível para um interceptador determinar a mensagem enviada através de uma contagem de frequências de aparição das letras/símbolos na oração. Utilizando outras deduções, como supor que em geral as palavras sempre são formadas juntando-se vogal-consoante-vogal-consoante, determinar-se-iam as associações de símbolos com vogais, e com um

pouco mais de análise o restante do alfabeto. Com a chave em mãos, bastaria inverter o processo para descobrir a mensagem interceptada.

No decorrer da história, a necessidade de troca de informações com segurança foi a força motriz do desenvolvimento de novas maneiras de se criptografar informações, isto é, de criptossistemas mais seguros. Além disso, cada novo criptossistema buscava erradicar as falhas dos sistemas anteriores, de maneira que os métodos já conhecidos para desvendar as chaves, até então, não fossem úteis para quebrar as novas cifras. Inicialmente, todo esforço foi baseado em adaptações da cifra de César, isto é, na substituição das letras segundo uma regra fixa. Outro criptossistema, por exemplo, utilizava várias vezes a cifra de César numa mesma mensagem. Isto é, utilizando-se cinco alfabetos-chaves diferentes, A1, A2, A3, A4 e A5, a primeira letra a ser criptografada era feita utilizando-se a chave A1 a maneira da cifra de César, a segunda letra com a chave A2, e assim por diante. Depois de utilizada a chave A5, voltava-se para a chave A1 e o ciclo se repetia até terminar a mensagem.

Mesmo essa mescla elaborada de cifra de César com utilização de várias chaves não resistiu aos ataques de investigadores, curiosos, e logo foi descoberta. Até a invenção dos computadores, pode-se dizer que praticamente todas as cifras e criptossistemas foram, cedo ou tarde, descobertas e quebrados. Essa aparente vulnerabilidade se explicava por dois motivos principais, que estão interligados:

1. Para que houvesse a compreensão da mensagem pelo receptor, era preciso que a chave de criptografia fosse previamente combinada entre o emissor e o receptor.

2. A regra combinada pelo emissor e pelo receptor é simétrica, no sentido de que as operações realizadas pelo emissor para cifrar uma mensagem são feitas de maneira inversa pelo receptor para decifrá-la.

Estes problemas tornavam qualquer tipo de criptografia muito difícil de ser utilizado em grande escala, pois demandava uma grande operação logística de distribuição das chaves de criptografia em diferentes locais onde os receptores estariam e, cada vez que essa

chave fosse eventualmente descoberta, uma nova distribuição de chaves deveria ser feita. Ambas dificuldades só foram vencidas com a criação dos chamados criptossistemas de chave pública, na segunda metade do século XX.

Estudiosos da ciência da computação notaram que, desde então, todos os criptossistemas baseados em transposição de alfabetos e trocas de letras, por mais seguros que parecessem ser, pecavam no seguinte sentido: se a chave fosse de alguma maneira descoberta, todo o sistema falhava, pois automaticamente o interceptador decifrava as mensagens utilizando os passos inversos àqueles utilizados para cifrar, ou criptografar, a mensagem original. Na busca por um criptossistema que resistisse a esse problema, os pesquisadores criaram, depois de muito esforço, os chamados criptossistemas de chave pública. Nestes criptossistemas, a chave para criptografia de uma mensagem é tornada pública, mas a maneira cuja qual ela é criptografada não permite, a princípio, que façamos o processo inverso para decifrá-la. Desse modo, a implementação computacional de um criptossistema de chave pública foi o passo seguinte para garantir mais segurança na troca de mensagens.

Atualmente a confiabilidade desses criptossistemas é tamanha que considera-se praticamente impossível, decifrar uma mensagem criptografada sem possuir outras informações além da chave pública. É por isso que, no vídeo, Guto relata os problemas em decifrar os e-mails interceptados, uma vez que as mensagens são criptografadas por um método de criptografia moderno.

Atualmente, diante da presumida dificuldade computacional de se quebrar as cifras que são utilizadas nas comunicações modernas, as táticas de espionagem se difersificaram para explorar outras fraquezas, em geral do usuário. Vírus, câmeras escondidas, pessoas infiltradas, hardwares falsos e ligações telefonicas falsas estão entre as principais técnicas utilizadas, para as quais devemos estar sempre alertas.

No filme, Guto, o agente do governo utiliza várias delas. O chefe de Guto se pergunta como será possível realizar investigações policiais que dependam de informações de e-mails sendo que é impossível

determinar o conteúdo das mensagens, dada a segurança garantida pela criptografia?

De fato, essa é uma questão importante, que pode ser debatida em sala – ao criar um criptossistema forte, capaz de resguardar as informações de uma mensagem sigilosa sem permitir a descoberta de seu conteúdo, a mesma segurança também pode ser utilizada por bandidos que queiram trocar informações com sigilo. Será que existe uma solução de compromisso nesse sentido?

Sabe-se que os criptossistemas utilizados atualmente nos sistemas de e-mails, e na internet de modo geral, são seguros pois baseiam-se na dificuldade de resolver certos **problemas matemáticos** computacionalmente. Acredita-se que a única maneira de quebrá-los seria construir um supercomputador capaz de realizar inúmeras operações num curto espaço de tempo. Portanto, o dilema está posto: Quebrar um criptossistema, para obter conteúdo de mensagens de bandidos e terroristas, implica na perda de privacidade para quem o utiliza idoneamente, assim como criar um criptossistema à prova de quebra garante não só a segurança dos usuários idôneos, mas pode encobrir ações criminosas.

Embora haja uma divisão de opiniões nas esferas públicas e acadêmicas, alguns pesquisadores acreditam que será possível, num futuro não muito distante, construir um supercomputador capaz de quebrar a melhor criptografia que conhecemos atualmente. Esse supercomputador funcionará segundo as leis da mecânica quântica e terá uma capacidade computacional incomparável em relação aos computadores atuais.

Algumas universidades e centros de pesquisas internacionais já conseguiram desenvolver protótipos de computadores quânticos, mas sua capacidade ainda é limitada, frente ao potencial teórico que possuí. Resta esperar para ver se os computadores quânticos vão, de fato, atingir a capacidade requerida para que os atuais criptossistemas sejam decifráveis – enquanto isso, os investigadores tentam a sorte em métodos alternativos para colher informações.

Sugestões de atividades

Antes da execução

É importante que o professor apresente o conceito de criptografia estabelecendo paralelos com nosso cotidiano, principalmente no que se refere à internet e à troca de informações. Deve-se ressaltar a questão da segurança virtual e como ela é feita a partir da criptografia.

Além disso, criar nos alunos o sentimento de importância da matemática, fazê-los reconhecer que mesmo nas ações mais triviais existe a fundamentação dos números e mostrá-los que a disciplina ultrapassa a "decoreba" é dever do professor e pode ser auxiliado através do vídeo.

Depois da execução

Sugerimos que o professor discuta com os alunos se eles sentem-se seguros ao utilizar os recursos computacionais, ao trocar mensagens com os colegas, etc.

Para exemplificar o processo de criptografia, o professor pode propor exercícios para decifrar uma mensagem criptografada pela cifra de César, como também ensinar criptografia através de matrizes e assim ligar o estudo de matrizes e suas propriedades com criptografia, ou mesmo explicar rudimentos da teoria dos números e criptografia RSA (há outros vídeos e guias sobre esses assuntos).

Sugestões de leitura

S. Singh. O livro dos códigos. Editora Record, 2001.

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

Autores *Alan Bondesan De Maria e Cristiano Torezzan*
Revisão *Cristiano Torezzan*
Coordenação de Mídias Audiovisuais *Prof. Dr. Eduardo Paiva*
Coordenação Geral *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*