

Guia do Professor



Vídeo


Venda segura

Série Matemática na Escola

Objetivos

1. Apresentar alguns conceitos de criptografia de chave pública;
2. Contextualizar o assunto através de exemplos práticos.
3. Motivar o estudo de operações matemáticas envolvendo números inteiros.

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 

Venda Segura

Série

Matemática na Escola

Conteúdos

Criptografia, chave pública e privada.

Duração

Aprox. 10 minutos.

Objetivos

1. Apresentar alguns conceitos de criptografia de chave pública;
2. Contextualizar o assunto através de exemplos práticos.
3. Motivar o estudo de operações matemáticas envolvendo números inteiros.

Sinopse

Um empresário que acaba de inaugurar suas vendas por internet está preocupado com a segurança das transações na rede e liga para um especialista para tirar suas dúvidas. Durante a conversa, vários conceitos fundamentais e exemplos de criptografia moderna são abordados de forma simples.

Material relacionado

Vídeos: *O golpe*, *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

Na ficção, Lucio é um empresário que acaba de inaugurar suas vendas por internet e está preocupado com a segurança das transações comerciais pela rede. Ele conversa com um consultor em segurança e vários conceitos fundamentais da criptografia moderna são abordados.

Embora esse vídeo retrate um cenário fictício, seu conteúdo é atual e ajuda a entendermos um pouco sobre criptografia e suas aplicações 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.

Um dos pilares fundamentais da criptografia é o conceito de cifra (ou chave). Em geral, é a complexidade de se obter a cifra que determina a força do sigilo criptografado. Uma cifra é uma regra segundo a qual uma mensagem será codificada, ou 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.

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.

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. No entanto, 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 se considera praticamente impossível, decifrar uma mensagem criptografada sem possuir outras informações além da chave pública. Isto se deve a utilização de operações matemáticas que são difíceis de serem invertidas, como a operação MÓDULO, ilustrada no vídeo e explorada a seguir.

Aritmética modular

Dados dois números inteiros a e n , denota-se por $a \pmod{n}$ o resto da divisão euclidiana de a por n . Assim, por exemplo, $5 \pmod{4}$ vale 1 , pois $5 = 4 \times 1 + 1$, ou seja, quando divide-se 5 por 4 obtém-se resto 1 . Esta representação para o resto de uma divisão é bastante convenientemente no caso em que temos um outro inteiro b e queremos dizer que tanto a como b têm o mesmo resto quando divididos por n . Neste caso escrevemos, simplesmente, $b = a \pmod{n}$. Como um exemplo, veja que $9 = 5 \pmod{4}$, pois $9 = 4 \times 2 + 1$.

O interessante na aritmética modular é que, para uma escolha apropriada do número n , podemos evitar trabalhar com números muito grandes. Isto acontece porque, se estivermos interessados em determinar o resto da divisão euclidiana de um produto de números inteiros por um dado inteiro n , então não precisamos nos preocupar com números maiores do que n^2 . De fato, consideremos primeiramente o caso em que temos um produto de apenas dois números inteiros. Sejam x e y estes números e

$$a = x \pmod{n} \quad \text{e} \quad b = y \pmod{n}$$

seus restos pela divisão por n . Então a e b são ambos números menores do que n e, necessariamente, o produto ab é menor do que n^2 , o qual também pode ser reduzido a um número menor do que n tomando-se o resto da divisão dele por n . Logo, em um produto qualquer, basta procedermos desta forma, tomando quaisquer pares de números.

Exemplo: Calcule $a = 41 \times 67 \times 29 \pmod{3}$.

Solução: A primeira coisa que devemos fazer é notar que

$$41 = 2 \pmod{3}, \quad 67 = 1 \pmod{3} \quad \text{e} \quad 29 = 2 \pmod{3},$$

de onde fica claro que $41 \times 67 = 2 \times 1 \pmod{3} = 2 \pmod{3}$ e

$$2 \times 29 = 2 \times 2 \pmod{3} = 4 \pmod{3} = 1 \pmod{3}.$$

Portanto, $a = 1 \pmod{3}$. Observe que, realmente, em nenhum momento trabalhamos com um número maior ou igual a $9 = 3^2$. \square

Pode-se trabalhar com a soma de restos da divisão de números inteiros de maneira análoga a descrita acima para a multiplicação. Em Coutinho (2007) o leitor poderá encontrar mais informações sobre aritmética de números inteiros e criptografia. Em particular, sobre o problema da fatoração de números inteiros, que é a base de um sistema de criptografia muito utilizado conhecido como RSA.

O sistema RSA, cuja sigla é formada pelas iniciais dos sobrenomes de seus inventores, Rivest, Shamir e Adelman, é um tipo de criptografia de chave-pública, assim denominada por distribuir abertamente a chave (pública) usada na cifra de codificação de informações. A seguir, apresentamos um exemplo prático de como uma versão simplificada deste algoritmo pode ser utilizada para criptografar uma palavra.

Exemplo: Vamos criptografar e posteriormente descriptografar a palavra CURIOSO.

O primeiro passo para se encriptar esta palavra é escolher uma chave para a cifra de encriptação. No algoritmo RSA, as chaves públicas

consistem de dois números inteiros, n e r , sendo o primeiro deles o produto de dois números primos quaisquer p e q e o segundo, qualquer número no intervalo $(1, (p-1)(q-1))$ que seja coprimo com $(p-1)(q-1)$. No nosso caso, tomamos $n = 5 \times 7 = 35$ e $r = 5$.

Em uma segunda etapa, há a necessidade de se trocar os caracteres da mensagem original por números segundo alguma correspondência previamente estabelecida. Neste exemplo, optemos por substituir a letra A ou a por 1 , a letra B ou b por 2 e assim por diante, até a letra Z ou z ser substituída por 26 :

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tome cuidado para não identificar nenhuma letra com o número zero ou um valor maior ou igual a n . Para a palavra CURIOSO este procedimento fornece

$3\ 21\ 18\ 9\ 15\ 19\ 15.$

Por fim, para encerrar o processo de encriptação, nós substituímos cada número b desta seqüência por um número a tal que $a = b^r \pmod{n}$, ou seja, pelo resto da divisão de b^r por n . Fazendo as devidas substituições obtemos

$33\ 21\ 23\ 4\ 15\ 24\ 15.$

O processo de descriptação, por sua vez, funciona de maneira análoga ao de encriptação: precisamos determinar um número s para o qual $x = y^s \pmod{n}$ e depois substituir cada x pela respectiva letra que ele representa. Este s é tal que $rs = 1 \pmod{(p-1)(q-1)}$. No nosso caso, $s = r = 5$, pois o resto da divisão de $rs = 25$ por 24 é 1 . □

É possível justificar porque o processo descrito no exemplo anterior funciona (Coutinho (2007), usando-se o pequeno teorema de Fermat, mas não isto foge muito do escopo desse guia.

Do que foi apresentado, podemos perceber que basta determinarmos o valor do número s para decodificarmos uma mensagem encriptada pelo algoritmo RSA. A primeira vista isto pode parecer uma tarefa fácil, afinal já conhecemos os valores de n e r , por estes compõem a chave pública do algoritmo, e s está intrinsecamente relacionado a eles. No entanto, s é na verdade determinado pela equação

$$rs = 1 \pmod{(p-1)(q-1)},$$

o que mostra que não é suficiente somente conhecer o valor de n para determiná-lo, mas sim precisaríamos conhecer a sua fatoração em números primos: $n = p \times q$. O problema é que ainda hoje não conhecemos uma maneira eficiente de se fazer uma tal fatoração e a criptografia RSA explora justamente esta deficiência, sendo por isso considerada uma das criptografias mais seguras existentes atualmente.

Os criptosistemas utilizados atualmente nos sistemas de e-mails, e na internet de modo geral, são presumidamente seguros, pois baseiam-se na dificuldade de resolver, de forma eficiente, os dois problemas matemáticos citados anteriormente: a fatoração de um número inteiro, que é produto de dois primos grandes e o problema do logaritmo discreto, proveniente da aritmética modular.

Comenta-se atualmente que, com o eventual surgimento de um computador quântico (cujas operações são baseadas na mecânica quântica), estes problemas tornariam-se vulneráveis a um ataque de tentativa e erro. Por isso, já se estuda novos sistemas de criptografia que se baseiam em outros problemas matemáticos. Esses sistemas são conhecidos como sistemas de criptografia pós-quânticos.

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 é feita a partir da criptografia.

O professor pode alertar que o vídeo mostrará um exemplo prático de utilização da matemática numa atividade prática do cotidiano e que, assim como inúmeras outras, a matemática desempenha um importante papel, sem que o usuário perceba.

Depois da execução

Sugerimos que o professor discuta com seus alunos os conceitos apresentados no vídeo, sobretudo a fundamental importância dos sistemas de chave pública.

Além disso, esta é uma boa oportunidade para reforçar alguns conteúdos matemáticos que são tratados no vídeo, como funções inversas e, até mesmo, alguns rudimentos da aritmética modular, como descrito no começo deste guia, enfatizando que esta é uma teoria utilizada em criptografia.

Uma maneira de motivar os alunos é, logo após o vídeo, desafiá-los em alguma atividade recreativa e simples, como, por exemplo, pedindo para que descriptassem o código

FULSWRJUDILD

usando a cifra de César (que consiste no simples deslocamento do alfabeto). A dica para fazer isso com sucesso na sala de aula é pedir que cada aluno tente decifrar a palavra com um deslocamento específico. O primeiro aluno desloca uma casa, o segundo duas e assim por diante. Se feito corretamente, algum aluno encontrará a palavra *CRIPTOGRAFIA*.

Se você achar pertinente e ainda desejar mostrar a eles como a aritmética modular pode realmente ser aplicada a criptografia, você pode trabalhar na lousa o exemplo em que encriptamos e descriptamos a palavra *CURIOSO* usando o algoritmo RSA. Se isto for

feito, então seria bastante proveitoso deixá-los descriptarem em casa o código

11 1 23 1 32 10 14 24,

também usando o algoritmo RSA com a mesma correspondência entre letras e números empregada no exemplo anterior. Não se esqueça de fornecer a eles a chave pública, que neste caso também será $n = 35$ e $r = 5$. A mensagem decodificada é *PARABENS*

Sugestões de leitura

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

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 *Douglas Mendes*

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 *Caio José Colletti Negreiros*

Vice-diretor *Verónica Andrea González-López*

