EM CLASSE

CODIFICANDO E DECIFRANDO MENSAGENS

Antonio Carlos Tamarozzi
UFMS, Três Lagoas, MS

Introdução

Operações de serviços disponíveis na Internet, movimentações bancárias e outras transações eletrônicas necessitam da criptografia para comunicação confidencial de dados.

A palavra criptografia tem origem grega (*kripto* = escondido, oculto; *grapho* = grafia) e define a arte ou ciência de escrever mensagens em códigos, de forma que somente pessoas autorizadas possam decifrá-las. A criptografia é tão antiga quanto a própria escrita; já estava presente no sistema de escrita hieroglífica dos egípcios e os romanos utilizavam códigos secretos para comunicar planos de batalha. Contudo, desde aquele tempo, seu princípio básico continua o mesmo: encontrar uma transformação (função) injetiva f entre um conjunto de mensagens escritas em um determinado alfabeto (de letras, números ou outros símbolos) para um conjunto de mensagens codificadas. O fato de f ser inversível é a garantia de o processo ser reversível e as mensagens poderem ser reveladas pelos receptores. O grande desafio de um processo criptográfico, portanto, está em ocultar eficientemente os mecanismos (chaves) para a inversão de f, de modo que estranhos não possam fazê-lo.

Emissor			Receptor	
Mensagem original	$\xrightarrow{f}$	Mensagem codificada	$\xrightarrow{f^{-1}}$	Mensagem original

Descreveremos aqui dois exemplos elementares de processos criptográficos, sendo o primeiro acessível inclusive para alunos do Ensino Funfamental. Acreditamos que possam constituir material útil para exercícios, como também para atividades e jogos de codificação. O professor pode dispor deles para fixação de conteúdos matemáticos associados, como nos exemplos: funções e matrizes.

Inicialmente, relacionamos números ao alfabeto (o símbolo # representa um espaço em branco) que vamos utilizar nos modelos. Assim:

#	A	B	...	J	K	L	...	V	W	X	Y	Z
0	1	2	...	10	11	12	...	22	23	24	25	26

Portanto, cifrar uma mensagem recai no problema de permutar números por meio de uma regra f. Pode-se fazer isso, de forma muito prática, por exemplo, através das funções afins $f(x) = ax + b$ com a, b inteiros, $a \neq 0$, definidas no conjunto $\{0,1,\ldots,26\}$. Suponhamos que Ana e Ivo desejem trocar mensagens sigilosas utilizando o alfabeto escolhido. O primeiro passo a tomarem é definirem a função cifradora, digamos $f(x) = 2x - 3$. Assim, por exemplo,

à mensagem	**R**	**E**	**V**	**I**	**S**	**T**	**A**		**R**	**P**	**M**
Ana associa a seqüência numérica	18	5	22	9	19	20	1	0	18	16	13

mas transmite a Ivo a seqüência numérica obtida pelas imagens de f, isto é,

$$33 \quad 7 \quad 41 \quad 15 \quad 35 \quad 37 \quad -1 \quad -3 \quad 33 \quad 29 \quad 23.$$

Ao recebê-la, Ivo, calculando a imagem de $f^{-1}(x) = \dfrac{x+3}{2}$ nessa seqüência e utilizando a correspondência alfabeto-numérica, obtém a mensagem original.

Depois de os alunos dominarem o processo, seria oportuno que o professor propusesse situações em que um intruso tente decifrar mensagens apoderando-se das seqüências numéricas codificadas. Como estamos utilizando funções afins, para tanto é suficiente apenas duas associações corretas entre números das seqüências original e codificada. Admitindo conhecidas essas associações, é um exercício interessante para os alunos determinarem f.

O segundo método criptográfico que apresentaremos utiliza matrizes invertíveis como chaves, o que dificulta um pouco mais sua violação.

Suponhamos que Ana e Ivo combinem previamente utilizar a matriz $A = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$ e sua inversa $A^{-1} = \begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix}$ como chaves. Para transmitir a mesma mensagem acima, Ana inicialmente monta uma matriz mensagem M dispondo a seqüência numérica associada em colunas e completa a posição restante com 0, ou seja, obtém $M = \begin{pmatrix} 18 & 22 & 19 & 1 & 18 & 13 \\ 5 & 9 & 20 & 0 & 16 & 0 \end{pmatrix}$. Em seguida, codifica-a calculando,

$$AM = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 18 & 22 & 19 & 1 & 18 & 13 \\ 5 & 9 & 20 & 0 & 16 & 0 \end{pmatrix} = \begin{pmatrix} 64 & 84 & 97 & 3 & 86 & 39 \\ 23 & 31 & 39 & 1 & 34 & 13 \end{pmatrix},$$

e transmite a seqüência $64\ 23\ 84\ 31\ 97\ 39\ 3\ 1\ 86\ 34\ 39\ 13$. Para ler a mensagem recebida, Ivo, da mesma forma, restaura a forma matricial AM, e em seguida,

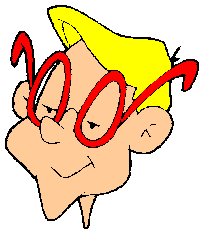
com sua chave A^{-1}, pode recuperar M através da identidade matricial, $M = A^{-1}(AM)$.

Como já frisamos, os métodos tratados neste trabalho tem apenas caráter instrutivo. Na prática atual são pouco utilizados pela inconveniência de exigirem trocas prévias de chaves entre os usuários. São, portanto, inviáveis na descrição de transações eletrônicas nas quais um único receptor recebe dados de milhares de emissores, como ocorre em vendas pela Internet, transações bancárias e outras. Mesmo nesses casos mais complexos, a Matemática resolveu a trama, e desta vez, quem diria, o ramo da Teoria dos Números. Ao leitor interessado em mais detalhes deste envolvente tema, sugerimos o excelente livro [1] ou o artigo [2].

Referências bibliográficas:

[1] COUTINHO, S. *Números inteiros e criptografia RSA*. Sociedade Brasileira de Matemática, 2000.

[2] Terada, R. *Criptografia e a importância das suas aplicações*. **RPM** 12. SBM, 1988.



VOCÊ SABIA?

Que o quadrado de um número inteiro não pode terminar em mais de três algarismos iguais a 4 ?

RPM: O primeiro número inteiro positivo cujo quadrado termina em três algarismos iguais a 4 é o 38, cujo quadrado é igual a 1444. O inteiro seguinte é 462, cujo quadrado é igual a 213 444. Entre os 1000 primeiros inteiros positivos, existem apenas mais dois, que são 538 e 962. De um modo geral, pode-se mostrar que o quadrado de um inteiro x termina em três algarismos iguais a 4 se e só se x puder ser colocado na forma $500k \pm 38$, onde k é um inteiro. Usando esse fato, pode-se mostrar que se o quadrado de um número inteiro termina em três algarismos iguais a 4, o algarismo da unidade de milhar desse quadrado é necessariamente ímpar, o que mostra que o quadrado de um inteiro não pode terminar em mais de três algarismos iguais a 4.