CRIPTOGRAFIA: FUNDAMENTOS, EVOLUÇÃO E IMPORTÂNCIA NA SEGURANÇA DA INFORMAÇÃO

Silva, Elias Lopes da[1]
Brito, Sérgio Kunrath[2]
Freitas, Walter Luiz Barbosa[3]
Souza, Fernando Pereira de[4]

Resumo: Este trabalho apresenta um estudo sobre a aplicação da Matemática à criptografia, com ênfase no sistema RSA, um dos métodos mais conhecidos de criptografia de chave pública. A pesquisa teve como objetivo compreender os principais conceitos da Teoria dos Números utilizados no funcionamento desse sistema e analisar como esses conceitos contribuem para a segurança das informações digitais. Inicialmente, foram estudados conteúdos como máximo divisor comum, fatoração, critérios de divisibilidade, números primos, aritmética modular e o Teorema Chinês do Resto. Em seguida, esses conhecimentos foram aplicados ao estudo do algoritmo RSA, permitindo compreender as etapas de geração das chaves, criptografia e descriptografia de mensagens.

Palavras-chave: Codificar, Segurança, Algoritmo.

INTRODUÇÃO

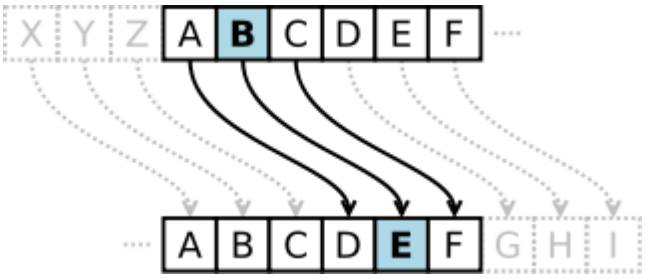
A criptografia surgiu com a necessidade de proteger informações e impedir que mensagens importantes fossem compreendidas por pessoas não autorizadas, no Egito Antigo, já existiam formas diferenciadas de representação na escrita hieroglífica. Outros povos também desenvolveram métodos para ocultar informações, como as cifras hebraicas utilizadas na Palestina. Um dos exemplos mais antigos e conhecidos é a Cifra de César, atribuída ao ditador romano Júlio César (100–44 a.C.). Segundo relatos históricos, César utilizava esse método para transmitir informações relacionadas às suas estratégias militares, dificultando

[1] Universidade Federal do Mato Grosso do Sul (UFMS); licenciatura em Matemática; elias.lopes@ufms.br .
[2] Universidade Federal do Mato Grosso do Sul (UFMS); licenciatura em Matemática; sergio_brito@ufms.br .
[3] Universidade Federal do Mato Grosso do Sul (UFMS); licenciatura em Matemática; walter.freitas@ufms.br .
[4]Universidade Federal do Mato Grosso do Sul (UFMS); licenciatura em Matemática; fernando.pereira@ufms.br .

que seus inimigos compreendessem suas mensagens. Dessa forma, a cifra funcionava como um mecanismo simples de substituição de letras.

O escritor romano Suetônio (c. 69–c. 122 d.C.), em sua obra Vida dos Doze Césares, relata que César utilizava, em sua correspondência, um sistema de substituição no qual cada letra do alfabeto era deslocada três posições adiante, conforme mostra a Figura 1.

Figura 1 – Estratégia usada por César



Fonte: setesys.com.br

Por exemplo, a mensagem INICIE A GUERRA seria codificada em:

LQLFLH D XHUUD

Um código como o de César pode não ser tão eficaz, tornando fácil de ser compreendido, principalmente nos dias de hoje, com avanço tecnológico e da ciência, dotado de hackers e de investigadores em potencial.

Esse tipo de codificação ficaria comprometido mediante uma simples análise da frequência da utilização das letras na língua portuguesa, conforme mostra a tabela 1:

Tabela 1 – Frequência das letras usadas no português

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Fonte: Coutinho, 2015

A criptografia moderna e usada nas transações eletrônicas via internet, nas quais um receptor recebe dados de milhares de emissores, e assim criar uma ferramenta segura e eficaz na troca de informações, que fique praticamente impossível de ser quebrada por terceiros.

O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1977 por Ronald Linn Rivest, Adi Shamire e Leonard Max Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.), uma das melhores universidades americanas. As letras RSA correspondem às iniciais dos sobrenomes dos inventores do código. Há vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais (Coutinho, 2015). Com isso, a criptografia é fundamental para a segurança da informação, ela protege dados contra acessos e alterações não autorizadas, ajuda a manter a confidencialidade, integridade e autenticidade das informações, sendo utilizada em bancos, aplicativos de mensagens, compras on-line, sistemas empresariais e serviços digitais.

METODOLOGIAS

Descreveremos abaixo como se proceder matematicamente para codificar e decodificar uma determinada mensagem pelo método em questão. Utilizaremos a palavra ‘’MATEMÁTICA’’ para nosso exemplo.

Etapa 1 – Conversão das letras da mensagem criptografada em números de dois dígitos para evitar ambiguidades, feita por meio da tabela mostrada abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
23	24	25	26	27	28	29	30	31	32	33	34	35

Etapa 2 – Escolha dos primos p e q que serão usados. Sejam, p= 11 e q= 13, os números escolhidos, sendo assim teremos:

$$n = p \cdot q = 11 \cdot 13 = 143.$$

Etapa 3 – Quebra da sequência numérica, obtida na etapa 1, em blocos que devem respeitar as seguintes restrições: serem formados por números menores que n e não podem começar com 0.

Seguem, abaixo, os blocos obtidos separados apenas por espaçamentos:

22 102 91 42 2 102 91 81 2 10

Etapa 4 – Calculamos ϕ (143) com o intuito de obter um número k de maneira que $mdc(k,\phi(143)) = 1$. Assim, temos:

$$\phi(143) = \phi(11 \cdot 13) = (11-1) \cdot (13-1) = 10 \cdot 12 = 120.$$

Tomaremos $k = 7$, visto que $mdc(7,120) = 1$.

Etapa 5 – Tomaremos cada bloco codificado como $C(b)$ onde $b^k \equiv C(b)\ mod\ n$, sendo $0 \leq C(b) \leq n$, dessa maneira podemos dizer que o bloco codificado $C(b)$ corresponde ao resto da divisão de b^k por n, ou seja, de b^7 por 187, onde b representamos blocos obtidos na etapa 3.

Faremos os detalhes apenas para o primeiro bloco.

$22^7 \equiv 22^2 \cdot 22^2 \cdot 22^2 \cdot 22 \equiv 55 \cdot 55 \cdot 55 \cdot 22 \equiv 22 \cdot 66 \equiv 1452227 \equiv 22\ mod\ 143$.

Procedendo da maneira descrita acima, teremos:

$102^7 \equiv 119\ mod\ 143$ $\quad$ $2^7 \equiv 128\ mod\ 143$ $\quad$ $81^7 \equiv 16\ mod\ 143$

$91^7 \equiv 130\ mod\ 143$ $\quad$ $102^7 \equiv 119\ mod\ 143$ $\quad$ $2^7 \equiv 128\ mod\ 143$

$42^7 \equiv 134\ mod\ 143$ $\quad$ $91^7 \equiv 130\ mod\ 143$ $\quad$ $10^7 \equiv 10\ mod\ 143$

Após a realização de todos os cálculos acima, obtemos os seguintes blocos codificados:

22 119 130 134 128 119 130 16 128 10

Etapa 6 – Nesta etapa tem-se o início do processo de decodificação da mensagem. Para isso é necessário a posse de dois números: n e d, onde d é o inverso de $k$módulo $\phi(n)$, ou seja, d deverá ser obtido pela relação: $d \cdot k \equiv 1\ mod$

$\phi(n)$. Para k = 7 e $\phi(n)$ = 120, temos: d = 103. Assim, obtemos a chave privada, composta por n = 143 e d = 103.

Etapa 7 – De posse da chave privada, seja a a denominação de cada um dos blocos codificados na etapa 5, que queremos decodificar, e $D(a)$ o resultado de cada um dos blocos decodificados, o cálculo de $D(a)$ será feito da seguinte maneira: $a^d \equiv D\ a\ mod\ n$, sendo 0 ≤ $D(a)$ ≤ n. Como n = 187, d = 23 e sabemos, um por um, os blocos codificados (valores de a), procedendo da maneira descrita acima, devemos encontrar o resto da divisão de 22^{103} por 143.

Fatorando 143 obtemos 143 = 11 · 13, assim calcularemos o resto da divisão de 22^{103} por 11 e por 13.

Fatorando 143 obtemos 143 = 11 · 13, assim calcularemos o resto da divisão de 22^{103} por 11 e por 13.

$$22^{103} \equiv 0^{103} \equiv 0\ mod\ 11$$

$$22^{103} \equiv 9^{103} \equiv (9^{12})^{8} \cdot 9^{7} \equiv 3^{4} \equiv 3^{12} \cdot 3^{2} \equiv 9\ mod\ 13.$$

Desta forma, 22^{103} satisfaz o seguinte sistema:

$$\begin{cases} x \equiv 0\ mod\ 11 \quad (I) \\ x \equiv 9\ mod\ 13 \quad (II) \end{cases}$$

De (I) temos que x = 11k. Substituindo em (II), teremos:

$$11k \equiv 9\ mod\ 13 \Rightarrow 6 \cdot 11\ k \equiv 6 \cdot 9\ mod\ 13 \Rightarrow k \equiv 2\ mod\ 13.$$

Assim, temos k = 13q + 2. Substituindo em x, obtemos:

$$x = 143q + 22$$

Dessa forma, conclui-se que o valor do bloco decodificado é 22. Realizando este procedimento para os demais blocos, obtém-se os seguintes valores:

$119^{103} \equiv 102\ mod\ 143$ $\quad$ $128^{103} \equiv 2\ mod\ 143$ $\quad$ $16^{103} \equiv 81\ mod\ 143$

$130^{103} \equiv 91\ mod\ 143$ $\quad$ $119^{103} \equiv 102\ mod\ 143$ $\quad$ $128^{103} \equiv 2\ mod\ 143$

$134^{103} \equiv 42\ mod\ 143$ $130^{103} \equiv 91\ mod\ 143$ $10^{103} \equiv 10\ mod\ 143$

Etapa 8 - Para que seja concluída a última etapa devemos juntar os blocos formados na etapa anterior. Sequência numérica formada:

22102914221029181210

Usando a correspondência alfabeto-numérica da tabela, formada por associações de números de dois algarismos a letras, obtemos a palavra

"MATEMÁTICA".

CONSIDERAÇÕES FINAIS

O estudo permitiu compreender a importância da Teoria dos Números em uma aplicação prática da Matemática e mostrou como conceitos estudados de forma abstrata podem ser utilizados na proteção de informações em sistemas digitais. Além disso, a pesquisa possibilitou o contato com conteúdo que, em geral, não são abordados de maneira aprofundada no ensino médio, ampliando a compreensão e o interesse pela Matemática.

REFERÊNCIAS

ALENCAR FILHO, Edgard de. **Teoria elementar dos números**. São Paulo: Nobel, 1988

COUTINHO, S. C. **Criptografia**. Rio de Janeiro: Programa de Iniciação Científica, 2008.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2011.