AS PALAVRAS ATRAVÉS DOS NÚMEROS

Caroline da Cruz Figueiredo[1]
Naiara Beber[2];
Andresa Laurett da Silva[3]

RESUMO: Com o advento da tecnologia, a segurança de transmissão de dados se tornou extremamente importante. Como consequência dessa necessidade, a aplicação da criptografia está cada vez mais presente em nosso cotidiano. A partir desse pressuposto buscou-se investigar a história da criptografia, os fundamentos matemáticos que a sustentam, verificar os sistemas criptográficos mais utilizados e analisar a sua real importância na sociedade atual. Para tanto, utilizou-se de pesquisa em livros, artigos e monografias, além de conversas com profissionais da área. Percebeu-se que a criptografia obteve avanços significativos ao longo dos anos, possibilitando que o algoritmo aplicado ao sistema RSA, embora utilize conceitos simples de números primos, tornou-a tão complexa e segura a ponto de ser utilizada até hoje. No entanto, os sistemas criptográficos por mais avançados que sejam, possuem fragilidades que implicam na necessidade de constante evolução para atender ao seu objetivo de garantir a segurança.

Palavras-chave: Criptografia. Aplicação. RSA.

1 INTRODUÇÃO

O mundo está rodeado por códigos. A população é identificada através do Registro Geral e do Certificado de Pessoa Física, o corpo humano possui códigos presentes no DNA e nas digitais que servem como senhas de acesso a diversos sistemas. Além disso, tudo o que é comprado possui um código. Até nosso próprio sistema de escrita é constituído por um alfabeto formado por 26 letras/códigos. Graças a criptografia, alguns desses códigos podem ser transmitidos de forma segura.

Nos primórdios, a criptografia era uma ferramenta utilizada exclusivamente pelos governos em ações militares onde cifras secretas eram utilizadas para comunicar planos de batalhas. Com os avanços tecnológicos, sua função se expandiu para proteger informações tanto das pessoas comuns, quanto de empresas. Desse modo, passou a ser aplicada em processos eletrônicos, transmissões digitais de informações, transações bancárias *online*, sistemas de compras eletrônicas, entre outros.

Inúmeros são os benefícios gerados com a evolução da tecnologia, porém, a internet nos deixa suscetível às pessoas mal intencionadas que interceptam nossas informações e nos causam danos. Consequentemente, a criptografia passa a ter mais significado e importância para as pessoas leigas. Nesse sentido, buscamos conhecer a origem da criptografia e sua evolução, analisar os sistemas criptográficos utilizados nos primórdios e na sociedade atual,

[1] Estudante do 2º. ano do Ensino Médio do Instituto Maria Auxiliadora;
[2] Estudante do 1º. ano do Ensino Médio do Instituto Maria Auxiliadora;
[3] Professora de Matemática do Instituto Maria Auxiliadora.

compreender os fundamentos matemáticos que garantem o uso da criptografia e analisar sua importância nos dias atuais.

2 MATERIAL E MÉTODOS

O trabalho foi desenvolvido por um grupo de alunos que apresentam interesse pela disciplina de Matemática. Durante os encontros, ocorridos nos meses de fevereiro a julho de 2016, foram realizadas discussões sobre o quanto a tecnologia está presente em nosso dia-a-dia e como a criptografia faz parte desse processo.

Através de leituras em artigos, livros e dissertações investigou-se a história da criptografia. Foram analisados alguns sistemas criptográficos recorrentes nas leituras como a Cifra de César, Cifra de Hill e o sistema RSA. Relacionou-se o uso de diversas funções matemáticas como chaves criptográficas, matrizes e aplicados alguns conceitos da Teoria dos Números, como a aritmética modular, para codificar e decodificar algumas frases e palavras. Foram aplicados e testados os sistemas criptográficos estudados, como também, o algoritmo estendido de Euclides para determinar a chave privada no sistema RSA.

3 RESULTADOS E DISCUSSÃO

A Criptografia é a ciência que estuda as formas de escrever uma mensagem em código. Sua função é proteger uma informação, utilizando-se de técnicas matemáticas para tornar a mensagem incompreensível, salvo o destinatário de direito a mensagem.

Desde os primórdios da civilização a sociedade tem procurado formas de ocultar suas mensagens, seja por motivos diplomáticos, amorosos, defensivos e até mesmo literários. Um dos mais populares códigos já criados foi a cifra de substituição, sendo que o primeiro documento que usou o método foi feito pelo Imperador Júlio César para se comunicar com os generais durante as Guerras Gálicas (LOUREIRO, 2014). A cifra de César, como ficou conhecida, consiste em deslocar as letras do texto claro em 3 casas para direita.

Quadro 1: Cifra de César. Na primeira linha o alfabeto normal, na segunda linha, o alfabeto deslocado em 3 casas.

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

Fonte: As autoras

A cifra de substituição é considerada uma criptografia simétrica, pois, para cifrar e decifrar é utilizado uma mesma chave, ou seja, através de operação matemática cifra-se a mensagem e usa-se a operação inversa para decifrar a mensagem. Pode-se assim, aplicar funções matemáticas como chaves para a encriptação, pois, uma função é a regra matemática que relaciona dois elementos de maneira ordenada. Por exemplo, para criptografar a palavra MILITAR usando a função $f(x) = 2x + 3$ como chave, deve-se atribuir a cada letra do alfabeto um número, como no Quadro 2.

Quadro 2: Código para cifrar e decifrar

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

Fonte: As autoras.

Sendo assim, o domínio da função assumirá valores de 1 a 26. Ao aplicar a função chave na palavra MILITAR obtém-se os valores 29-21-27-21-43-5-41, produzindo um conjunto imagem com números naturais no intervalo de 5 a 55. Porém, para identificar as letras equivalentes, necessita-se aplicar a aritmética modular, com isso o número $29 \equiv 3 \pmod{26}$, $27 \equiv 1 \pmod{26}$, $43 \equiv 17 \pmod{26}$, $41 \equiv 15 \pmod{26}$, obtendo a cifragem CUAUQEO.

Quem recebe a mensagem cifrada, deve conhecer a chave de cifração para decifra-la. Como foi utilizada uma função como chave cifradora, a mesma deve possuir inversa, o que implica na obrigatoriedade de que a função chave seja bijetora. No exemplo dado, a função $f^{-1}(x) = \frac{x-3}{2}$ deverá ser empregada para decifrar a mensagem, voltando assim, a mensagem original. Qualquer função matemática pode-se aplicar como chave, desde que a mesma possua uma função inversa.

A cifra de Hill, inventada em 1929, é uma cifra de substituição que torna difícil um ataque de análise de frequência. O algoritmo utiliza blocos de *n* letras. Cada bloco forma uma matriz coluna *P* com *n* elementos. Uma matriz invertível, *K* será utilizada como chave e a cifragem consiste na multiplicação da matriz *K* pelo vetor *P*. Assim, a mensagem cifrada C será: C = K.P; a inversa K^{-1} da matriz *K* será utilizada para decifrar a mensagem, para isso, multiplicamos por K^{-1} pela mensagem cifrada C.

A criptografia continuou evoluindo a cada passo que um sistema era quebrado. A famosa máquina Enigma, construída por alemães a fim de substituir os sistemas criptográficos inadequados usados na Primeira Guerra Mundial, parecia indecifrável, até que o Colossus, computador inglês, foi criado para decodificar os códigos criados por ela, iniciando a era moderna da criptografia.

Em 1977, Ron Rivest, Adi Shamir e Len Adleman criaram o sistema RSA, que é atualmente, o sistema criptográfico assimétrico mais usado em aplicações comerciais. Para cifrar uma mensagem usando o sistema RSA, é necessário escolher dois números primos, p e q (muito grandes). Calcula-se n que é o produto de p e q, em seguida, é determinado a função totiente $\varphi(n) = (p-1)(q-1)$, que determina a quantidade de números co-primos a n, então, escolhe-se ao acaso um número d, tal que MDC(d, $\varphi(n)$) = 1 e, encontra-se e de forma que $e.d \equiv 1(mod \varphi(n))$. Com esses passos, determina-se que a chave pública é formada pelo par (e,n) e a chave privada pelo par (d,n). Sendo assim, para cifrar uma mensagem M, é calculado: $C \equiv M^e (mod\ n)$, onde C é a cifra. Para decifrar, é calculado $M \equiv C^d (mod\ n)$.

O sistema é seguro quando utilizado números relativamente grandes para p e q, tornando a fatoração um trabalho árduo até mesmo para supercomputadores.

4 CONCLUSÕES

É comum associar a criptografia como forma de ocultar as informações para nossa segurança, sem compreender como é realizada essa operação e quais conceitos matemáticos estão envolvidos. As cifras de substituição podem ser relacionadas à funções matemáticas, no qual é possível aplicar o conhecimento sobre o conjunto domínio e imagem, além da determinação de sua função inversa. Com as cifras de Hill, tem-se um amplo conhecimento sobre matrizes, desde o seu conceito, até as operações de multiplicação de matrizes e o cálculo da matriz inversa que podemos obter associando a um sistema de equações ou pode-se ainda utilizar-se do cálculo do determinante para obter a inversa. O sistema RSA permite verificar a utilidade dos números primos que parecem não ser importantes no nosso cotidiano, quando os aprendemos no sexto ano do ensino fundamental. O sistema parece brilhante ao usar conceito tão simples ao ponto de deixa-lo complexo e extremamente difícil de quebrar.

Por meio dos avanços obtidos na Matemática, consequentemente na Criptografia, estamos diante de um mundo onde a tecnologia evolui cada vez mais rápido, obtendo assim, cada vez mais comodidade e segurança ao realizar compras em lojas virtuais e transições bancárias através de nossos computadores ou smartphones. Com isso, as pessoas estão sobrecarregadas com senhas de acesso, e há milhares de informações sigilosas que podem ser facilmente interceptadas caso não haja um sistema criptográfico seguro para nos resguardar de invasores mal intencionados.

Durante a pesquisa, foi possível perceber que a Criptografia vive um momento em que é totalmente indispensável, além de ser uma área promissora para campo de trabalho devido a necessidade de estar sendo aprimorada a cada momento em que um sistema é quebrado ou suas fragilidades identificadas. Por mais avançado que o sistema seja, com o avanço da matemática, criam-se sistemas cada vez mais complexos.

5 REFERÊNCIAS

CAVALCANTE, André L.B. **Teoria dos números e Criptografia.** Disponível em: <http://www.ebah.com.br/content/ABAAAAayYAA/teoria-dos-numeros-criptografia>. Acesso em: 08 mar. 2016.

FREIRE, P. B.; CASTILHO, J. E. **A matemática dos códigos criptográficos.** Disponível em: < https://www.ucb.br/sites/100/103/TCC/12007/PalomaBarbosaFreire.pdf >. Acesso em: 15 mar. 2016.

LOUREIRO, F. O. **Tópicos de criptografia para o ensino médio**. 2014. 43 p. Dissertação – Universidade Estadual do Norte Fluminense Darcy Ribeiro – Campos dos Goytacazes, Rio de Janeiro, 2014.

SAUTOY, Marcus du. **Os mistérios dos números**. 1. ed. Rio de Janeiro: Zahar, 2013.