TEORIA DOS NÚMEROS E CRIPTOGRAFIA

Amanda Viana Braga, João Victor de Souza Monteiro, Irene Naomi Nakaoka (Orientadora). E-mail: amandavianabra60@gmail.com

Universidade Estadual de Maringá, Centro de Ciências Exatas, Maringá, PR.

Matemática, Álgebra/Teoria dos Números.

Palavras-chave: ElGamal; Criptografia da Mochila; Tecnologias.

RESUMO

Historicamente, a troca de informações foi essencial para práticas diplomáticas e militares. Com o passar do tempo foi necessária a criação de métodos seguros para que, caso a informação fosse interceptada por pessoas não autorizadas, quem estivesse lendo não conseguisse interpretá-la. Neste sentido, sistemas de criptografia foram criados para proteger o envio e o armazenamento de dados. Com o crescente desenvolvimento de tecnologias, muitos desses métodos vão se tornando obsoletos, então surge uma nova necessidade de criar criptografias mais seguras. Neste trabalho, abordaremos sobre a criptografia ElGamal e a criptografia da Mochila, como uma forma de aplicação da Teoria dos Números.

INTRODUÇÃO

A Teoria dos Números, juntamente com a Geometria, é um dos campos de estudo mais antigos da Matemática, sendo altamente desenvolvida desde a Grécia Antiga; inclusive, muitos dos resultados que conhecemos hoje estão presentes nos Elementos de Euclides. Apesar disso, a Teoria dos Números não era desenvolvida pensando em resolver problemas reais e não havia tantas aplicações práticas para as teorias desenvolvidas. Porém, isso muda com a chegada da criptografia como uma área de estudos.

A criptografia surgiu a partir de práticas militares romanas quando Júlio César, cerca de 50 A.C, escreveu para Marcus Cícero usando um código de substituição rudimentar, em que cada letra do alfabeto é substituída por outra que se apresenta três posições abaixo dela no alfabeto. Por exemplo, $A \to D$; $B \to E$; $C \to F$, e assim sucessivamente (BURTON, 2016).

Assim, com a evolução das tecnologias, a criptografia tem se tornado cada vez mais essencial para a proteção de dados. Nesse sentido, no decorrer das últimas décadas surgiram inúmeros sistemas que fornecem métodos para codificar mensagens e que utilizam a matemática como alicerce.

Nesse contexto, o presente trabalho tem como objetivo definir e exemplificar dois desses métodos: a criptografia da mochila que foi baseada em um problema clássico da combinatória, conhecido como o problema da mochila, e a criptografia ElGamal,

introduzido por Taher ElGamal que utilizou como base uma versão do chamado problema do logaritmo discreto.

REVISÃO DE LITERATURA

A pesquisa foi feita por meio da leitura dos livros: *Introdução à Teoria dos Números*, de J. P. O. Santos, *Criptografia para Iniciantes*, de S. Shokranian, e *Elementary number theory*, de D. M. Burton. A partir dessa leitura, foram realizados seminários para a discussão sobre os temas.

RESULTADOS E DISCUSSÃO

Na criptografia usada por César, se uma pessoa sabe criptografar, então também sabe descriptografar. Muitas criptografias que se seguiram a essa também tinham essa característica. Entretanto, com o crescente uso da comunicação e de transações comerciais e financeiras pela internet, surgiu a necessidade de sistemas que possibilitem que uma pessoa A possa disponibilizar publicamente a forma de enviar mensagens codificadas para ela sem que, com isso, as pessoas saibam a forma de decodificar as mensagens que a pessoa A recebe. Neste contexto, surgem os sistemas de criptografia de chave pública, na qual uma pessoa irá possuir uma chave pública, visível a todos para ser feita a codificação, e uma chave privada, onde somente ela terá acesso para fazer a decodificação. O remetente criptografa a mensagem que deseja enviar usando a chave pública do destinatário e, este, ao receber, decodifica usando a sua chave privada, a qual somente ele conhece.
Os sistemas de criptografia da Mochila e o ElGamal são sistemas de criptografia de chave pública.

Criptografia da Mochila

O sistema de criptografia é um sistema de chave pública baseado no *problema da mochila* ou problema da soma dos conjuntos. Este problema pode ser expresso da seguinte forma: Dada uma mochila de volume □ e n itens de vários volumes a□, a□, ⋯, a□, podemos encontrar um subconjunto desses itens que preencha completamente a mochila? Descrevendo esse problema em termos matemáticos a partir de uma formulação alternativa, temos: Para inteiros positivos $□_1, □_2, \ldots, □_□$ e uma soma □, resolva a equação

$$□ = □_1□_1 + □_2□_2 + \ldots + □_□□_□,$$

onde $□_□$ é 0 ou 1, para $□ = 1, 2, \ldots, □$.
Esse problema pode não apresentar solução, ou apresentar uma única solução ou, ainda, apresentar mais de uma solução. Isso depende da escolha da sequência $□_1, □_2, \ldots, □_□$, e do número inteiro V. Encontrar a solução para um problema da mochila escolhido de forma aleatória é difícil. Uma classe particular do problema da mochila que é muito útil é quando a sequência de inteiros $□_1, □_2, \ldots, □_□$ possui

uma característica especial: cada $\square_{\square}$ é maior do que a soma de todos os seus anteriores.
A partir do algoritmo para resolver esse tipo de problema, R. Merkle e M. Hellman em 1978 criaram um sistema de criptografia de chave pública. A ideia é escolher uma sequência aumentada, ou seja, com cada termo maior que a soma dos anteriores, formando a chave privada. Em seguida, essa sequência é transformada por meio de uma multiplicação modular e permutação, gerando a chave pública. Para criptografar, converte-se a mensagem em um vetor binário e calcula-se a soma ponderada dos termos correspondentes da chave pública. A descriptografia utiliza o inverso modular para recuperar a sequência original e, então, aplica um algoritmo guloso para obter a mensagem. Apesar da simplicidade e da elegância matemática, esse método foi quebrado em 1984 por Adi Shamir e, por isso, não é mais considerado seguro.

Criptografia ElGamal

Para desenvolver o algoritmo de Criptografia ElGamal, é necessário o estudo sobre Raíz Primitiva, definida como segue: “Dados inteiros positivos $\square$ e $\square$, relativamente primos, $\square$ será uma raiz primitiva módulo $\square$ se $\phi(\square)$ for o menor inteiro positivo tal que $\underline{\square}^{\square(\square)} = \underline{1}$ ocorre em $\blacksquare_{\square}$”. A partir desse conceito, obtém-se vários resultados, sendo os dois fundamentais para o sistema ElGamal estabelecidos como segue: “Todos os números primos admitem raiz primitiva” e “Se $\square$ é uma raiz primitiva módulo $\square$, então as potências $\square, \square^2, \ldots, \square^{\square(\square)}$ formam um sistema reduzido de resíduos módulo $\square$”.
O sistema ElGamal inicia-se escolhendo um número primo $\square$ e uma de suas raízes primitivas $\square$, bem como um inteiro $\square$ de modo que $1 < \square < \square(\square)$. Assim, calculemos o valor de $\square$ pela fórmula $\underline{\square} = \underline{\square}^{\square}$ em $\blacksquare_{\square}$.
Feito isso, teremos que a terna $(\square, \square, \square)$ é a chave pública, enquanto que $\square$ é a chave privada. A criptografia é feita separando a mensagem em blocos $\square_1, \ldots, \square_{\square}$ de um mesmo tamanho menor que $\square$, escolhendo inteiros $\square_{\square}$, com $1 < \square_{\square} < \square(\square)$ para cada bloco $\square_{\square}$, e calculando, em $\blacksquare_{\square}$,

$$\underline{\square_{\square 1}} = \underline{\square}^{\square_{\square}} \text{ e } \underline{\square_{\square 2}} = \underline{\square_{\square}} \cdot \underline{\square}^{\square_{\square}}.$$

A mensagem criptografada será o par $(\square_{\square 1}, \square_{\square 2})$ para cada um dos blocos $\square_{\square}$.
Já a descriptografia será dado pelo cálculo

$$\underline{\square_{\square 1}}^{\square(\square)-\square} \cdot \underline{\square_{\square 2}}$$

em $\blacksquare_{\square}$. Desta forma, apenas quem conhecer o valor de $\square$ será capaz de descriptografar a mensagem.

CONCLUSÕES

A pesquisa desenvolvida mostra como a Teoria dos Números tem um papel essencial na construção dos sistemas criptográficos modernos, especialmente nos de chave pública. Ao estudar os métodos da mochila e do ElGamal, foi possível

perceber não apenas os conceitos matemáticos que garantem a segurança desses sistemas, mas também as dificuldades que surgem quando eles são aplicados na prática. A criptografia da mochila exemplifica como um problema matemático simples, porém de difícil resolução, pode ser usado para proteger informações, enquanto o sistema de ElGamal destaca a importância dos grupos cíclicos e do desafio do logaritmo discreto nesse mesmo contexto.

REFERÊNCIAS

BURTON, D. M. **Elementary number theory**. 7.ed. New York ; Boston: Mcgraw-Hill, 2011.

SANTOS, J. P. O. **Introdução à Teoria dos Números.** 3. ed. Rio de Janeiro: IMPA, 2009.

SHOKRANIAN, S. **Criptografia para Iniciantes.** 2. ed. Rio de Janeiro: Editora Ciência Moderna Ltda. 2012.