21ª SEMANA NACIONAL DE CIÊNCIA E TECNOLOGIA
Criar - Polo de Inovação do IFG
17° sict SEMINÁRIO DE INICIAÇÃO CIENTÍFICA E TECNOLÓGICA DO IFG 2024

TEORIA DOS NÚMEROS E CRIPTOGRAFIA

LOPES, Heitor Curado Maciel[1]; SANTOS, Laredo Rennan Pereira[1]*

[1]Instituto Federal de Goiás, Câmpus Formosa.
*laredo.santos@ifg.edu.br.

O avanço tecnológico e a crescente dependência de comunicações digitais levantam preocupações significativas sobre a segurança dos dados transmitidos. A criptografia é uma das principais medidas para proteger a confidencialidade e a integridade das informações. Embora se possa associar mensagens codificadas a 007 ou a outros agentes igualmente secretos, há mais de duas décadas que esta não é a aplicação mais importante da criptografia. Isto porque, hoje em dia, uma grande variedade de transações que envolvem dinheiro são feitas de maneira eletrônica, desde compras por cartão de crédito via internet a saques em caixas eletrônicos. A informação referente a estas transações segue por linha telefônica ou redes de alta-velocidade e, em ambos os casos, está facilmente sujeita a escutas. Felizmente, estas informações não trafegam em aberto pela rede telefônica. Elas são codificadas, de modo que só o banco, empresa de cartão de crédito ou loja que está sendo utilizada consegue ler a informação. Assim, mesmo que alguém intercepte a informação com a intenção de esvaziar uma conta, ele não conseguirá interpretar as informações, que continuarão seguras. Os processos pelos quais informações enviadas eletronicamente são codificadas depende, de maneira crucial, do uso da matemática. O mais curioso é que até os anos 1960, a teoria dos números, que é a parte da matemática mais utilizada nas aplicações à criptografia, era considerada quase que destituída de utilidade prática. O objetivo deste projeto foi estudar aplicações da matemática à criptografia. Desenvolvemos os métodos da Teoria dos Números necessários às aplicações em um sistema de criptografia específico, o chamado RSA. Há duas razões para isto. A primeira é que os resultados matemáticos utilizados neste sistema são relativamente elementares; a segunda é que se trata do mais utilizado dos métodos de criptografia atualmente em uso. Para isso consideramos em nosso trabalho os principais conceitos e resultados da Teoria dos Números envolvendo a Aritmética Modular. Iniciamos desenvolvendo ideias como o da fatoração única de inteiros, congruência modular, inversos modulares, Algoritmo Chinês do Resto e o Teorema de Fermat. Com esse aporte teórico demonstramos o funcionamento e a segurança do sistema de criptografia conhecido como RSA. Além disso, exibimos alguns exemplos de como esse processo funciona na prática, exibindo os cálculos para a codificação e consequente decodificação da palavra PIBIC pelo método RSA.

Palavras-chave: números primos; aritmética modular; criptografia RSA.

Agradecimentos: O presente trabalho foi realizado com apoio do Instituto Federal de Goiás (n° 18/2023). Lopes, Heitor Curado Maciel agradece ao CNPq pela bolsa concedida.