

## MATEMÁTICA E A TECNOLOGIA: A IMPORTÂNCIA DA CRIPTOGRAFIA NO MUNDO MODERNO

Heitor Ferraz Cornélio<sup>1</sup> ; Leon Cavalcante Lima<sup>3</sup>

1 Instituto Federal do Sertão Pernambucano – Campus Floresta, [heitorfcornelio@hotmail.com](mailto:heitorfcornelio@hotmail.com).

Neste projeto, trabalhamos com uma aplicação da matemática à criptografia. É muito comum as pessoas associarem mensagens codificadas a 007 ou outros agentes secretos, mas há mais de uma década que esta não é a aplicação mais importante da criptografia. Nos dias atuais, grande variedade de transações que envolvem dinheiro é feita de maneira eletrônica, desde compras por cartão de crédito via internet a saques em caixas eletrônicos. As informações a respeito dessas transações são encaminhadas por linha telefônica ou redes de alta-velocidade e, em qualquer um dos casos, estão facilmente sujeitas a escutas. Para nossa felicidade, estas informações não caminham por esses mecanismos em aberto, elas são codificadas, de tal forma que só o banco, empresa de cartão de crédito ou loja que você está utilizando consegue ler a informação. Ainda que alguma pessoa intercepte as informações visando esvaziar sua conta, ele não será capaz de decifrar as informações, que continuarão em segurança. O procedimento para codificar as mensagens que serão enviadas eletronicamente depende, fortemente, do uso da matemática. Um fato muito curioso é que até 1960, a teoria dos números, que é a parte da matemática mais utilizada nas aplicações à criptografia, era considerada quase que completamente separada de utilidade prática. Assim, nós trabalhamos com os métodos da teoria dos números necessários às aplicações em um sistema de criptografia específico, o chamado RSA. Existem duas razões fortes para esta escolha. A primeira é que, como este sistema engloba diversos algoritmos importantes da teoria dos números, os resultados matemáticos utilizados neste sistema são relativamente elementares; a segunda é que se trata do mais utilizado dos métodos de criptografia atualmente pelas grandes empresas. Além de estudos bibliográficos, utilizamos um software chamado Octave para trabalhar na prática, programando algoritmos necessários para o desenvolvimento da criptografia RSA e seu estudo.

**Palavras-chave:** Teoria dos números; criptografia; programação.

**Agradecimentos:** Agradeço ao meu orientador Leon Lima e ao IF Sertão por fazerem do projeto possível.