# Criptografia RSA: uma abordagem para o ensino médio

**Fabricia Auxiliadora Queiroz (Seduc/MT)**
**Professora da Educação Básica do Estado de Mato Grosso**
**fabriciaqueirozcba@gmail.com**

## INTRODUÇÃO

A comunicação pela internet necessita de segurança para que as informações que circulam pela rede, como *e-mails*, operações bancárias e compras *online*, não sejam acessadas por pessoas não autorizadas. A criptografia tem a função de proteger essas informações. É uma ciência que estuda métodos para codificar uma mensagem de maneira segura, de modo que apenas seu destinatário consiga interpretá-la. Há vários tipos de criptografia e um dos mais usados é o sistema RSA, que iremos apresentar aqui.

A sigla RSA é composta pelas iniciais dos nomes de seus inventores: Rivest, Shamir e Adleman.

Para o desenvolvimento da criptografia RSA foram fundamentais assuntos relacionados à teoria dos números, uma parte da matemática para a qual por muito tempo nenhuma aplicação prática era conhecida. Especificamente, são necessários dois conteúdos matemáticos que ainda aprendemos no Ensino Fundamental: os números primos e a decomposição em fatores primos (fatoração). Terada (2008) afirma que o sistema é seguro pelo fato de não existir um algoritmo eficiente para fatoração e fabricação de primos, pois o que existem são algoritmos que testam se $n$ é um primo com uma probabilidade alta.