Desvendando os mistérios do criptossistema RSA

Dra. Grasiele Cristiane Jorge – Pós-Doc. Unicamp

Data: 13/11/2013

Resumo

Encaminhar uma mensagem de forma segura é uma preocupação que persegue os estrategistas desde a Grécia Antiga. Com o passar dos anos, a evolução da Matemática e a criatividade humana em desenvolver novos mecanismos fizeram com que a arte cifrar mensagens ganhasse destaque nas decisões políticas, com influência direta nos acontecimentos históricos.

A partir da década de 70 a criptografia assumiu um papel essencial na garantia da segurança de informações trocadas pela internet. Isso não seria possível sem a utilização da Teoria dos Números, uma área tida por muitos como meramente abstrata.

A proposta deste minicurso é abordar a Matemática envolvida no criptossistema RSA. Veremos que a segurança de tal criptossistema está relacionada ao fato de até o momento não existirem algoritmos que funcionem em tempo polinomial capazes de fatorar um número inteiro como um produto de números primos. Veremos também que se os pesquisadores chegarem ao tão sonhado computador quântico, tal fatoração será realizada rapidamente e a segurança do RSA estará quebrada.