Título: Sistemas de Assinatura Digital

Ana Sofia Teixeira, Bárbara Silva, Carlos Freitas, Mariana Cristino, Tiago Rodrigues
(bolseiros do CMAT – Programa FCT "Verão com Ciência")

Resumo: Grande parte dos sistemas criptográficos usados nas comunicações modernas tem uma componente matemática.

Na atualidade, sistemas baseados em curvas elípticas estão altamente disseminados não só na cifração de mensagens, mas também em protocolos de trocas de chave e de assinatura digital. Ao invés da segurança se basear na dificuldade da factorização de um número natural nos seus primos, como sucede com o RSA, é o Problema do Logaritmo Discreto que sustenta a segurança da generalidade dos sistemas definidos no grupo aditivo dado por uma curva elíptica sobre um corpo. Assim, iremos mostrar alguns dos sistemas de assinatura digital mais conhecidos baseados no anel dos inteiros, tais como o RSA, El Gamal e o DSA. Além disso, há sistemas comparáveis definidos em curvas elípticas definidas sobre corpos primos, nomeadamente o sistema de assinatura digital ECDSA.