

Introdução à Criptografia

Paulo Mateus

Sumário

Apesar de ter sido movida inicialmente por aplicações militares e diplomáticas, a Criptografia encontra-se hoje presente em quase todo o lado, em grande parte devido à omnipresença das aplicações informáticas na sociedade moderna – comércio electrónico, banca electrónica, acesso remoto a serviços do estado. Por outro lado, a criptografia motiva a investigação em Matemática ao mais alto nível pois está intrinsecamente ligada a conjecturas fundamentais da Complexidade Computacional (eg, $P \neq NP$), à Teoria dos Números, bem como à Computação e Informação Quânticas. Neste curso introdutório pretende-se dar uma perspectiva dos problemas centrais da criptografia moderna, das suas limitações e do seu futuro.

Plano

1. Sistemas criptográficos simétricos. Sistemas clássicos. Teorema de Shannon. Sistemas modernos. Problemas em aberto.
2. Sistemas criptográficos assimétricos. Implicações na Complexidade Computacional. Candidatos baseados em Teoria dos Números. O problema da factorização e do logaritmo discreto. Problemas em aberto.
3. Novos problemas da criptografia. Provas de conhecimento nulo. Partilha de segredos. Assinaturas digitais. Funções de dispersão. Problemas em aberto.
4. Criptografia e análise quânticas. Algoritmo de Shor. Protocolos quânticos de acordo de chave. Problemas em aberto.

Bibliografia

- A.J. Menezes, P. C. van Oorschot and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press. 1996. <http://www.cacr.math.uwaterloo.ca/hac/>
- W. Trappe and L. C. Washington. Introduction to Cryptography with Coding Theory, 2nd edition. Prentice Hall. 2005.
- D. Stinson. Cryptography: Theory and Practice, 3rd edition. Chapman & Hall. 2005