

Introdução aos Protocolos Criptográficos

Carlos Caleiro

Resumo

Os protocolos criptográficos, potenciados pelos desenvolvimentos matemáticos da criptografia moderna, são uma das ferramentas essenciais da revolução das telecomunicações nas últimas décadas. Destinados a atingir uma miríade de fins, os protocolos criptográficos tornam possível, por exemplo, a implementação dos modernos sistemas de comércio electrónico, ou a identificação de agentes e o acesso remoto a informação confidencial. No entanto, levantam um sem número de problemas teóricos e práticos a quem os desenvolve e analisa, bem como a quem procura as suas vulnerabilidades. Neste mini-curso pretende dar-se uma perspectiva dos fundamentos e potencialidades dos protocolos criptográficos, bem como dos desafios que nos colocam.

Plano

- 1) Introdução aos protocolos criptográficos. Criptografia clássica, cifras simétricas, segurança incondicional e teorema de Shannon. Esquemas de partilha de segredos de Blom e Shamir.
- 2) Criptografia moderna, cifras assimétricas, complexidade, segurança computacional contra atacantes passivos. Protocolos de acordo de chaves de Diffie-Hellman e Massey-Omura.
- 3) Autenticação e segurança computacional contra atacantes activos. Protocolo de Needham-Schroeder e ataque de Lowe. Assinaturas digitais e certificados. Kerberos.
- 4) Anonimidade e computação segura: o jantar dos criptógrafos. Protocolos de identificação: das passwords aos protocolos de desafio-resposta, provas de conhecimento nulo, Fiat-Shamir.

Bibliografia

- D. Stinson. *Cryptography: Theory and Practice*, 3rd edition. Chapman&Hall, 2005.
- 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/>