Criptografia Aplicada — 2005/2006
Reading Recommendations for Exchange Students

M. B. Barbosa @ di.uminho.pt

January 8, 2007

Terminology

- Following sections from Schneier's "Applied Cryptography"
  - Chapter 1.
  - Chapter 2.
  - Chapter 3, until section 3.3.
  - Chapter 5, until section 5.2.
  - Chapter 7.
  - Chapter 9.
  - Chapter 10, until section 10.2.
  - Chapter 11.
  - Chapter 12.
  - Chapter 17, until section 17.1.
  - Chapter 18.
  - Chapter 19, section 19.3.
  - Chapter 20, section 20.1.
  - Chapter 21, section 21.3.
  - Chapter 22, until section 22.2.
- Description of the Advanced Encryption Standard and IDEA at Wikipedia.

X.509 Certificates and Public Key Infrastructures

- Introductory topics at `http://www.rsasecurity.com/rsalabs/node.asp?id=2267`.
- Introductory topics at Wikipedia (start with `X509`).
- Descriptive part of Internet Dratf *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
- Descriptive part of RFC3647 (Certificate Policies).
- Descriptive part of RFC2560 (OCSP).
- *Trust Models and Management in Public-Key Infrastructures*, John Linn, RSA Laboratories, 2000.
- Complementary reading: *Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations*, W. E. Burr, 1998.

Popular applications of cryptography

- Decriptive part of the Transport Layer Security RFC, the SSL V.3 specification and the Secure Shell (SSH) RFC.
- Kerberos documentation available at `http://web.mit.edu/Kerberos/papers.html`.
- GPG documentation available ar `http://www.gnupg.org`.