Ciências ULisboa

Introdução à Criptografia Aplicada

Código: 425233
Ano Letivo: 2015/16
Departamento: Informática
ECTS:
Carga horária:
Área Científica: Informática;

Objetivos da Unidade Curricular

Cryptography is an essential tool in providing information security in today's computer systems and Internet, when in the face of attacks with diversified adversarial goals and capabilities. In this course, which provides a partial introduction to modern cryptography, students will:

· (knowledge) learn about basic principles underlying modern cryptography, including precise definitions of basic cryptographic primitives that can be used, in well-defined adversary models, to protect the confidentiality, integrity and authenticity of digital communications.

· (skills) develop the ability to reason theoretically about correct vs. incorrect usage of primitives and schemes, namely of block ciphers and schemes of encryption, hash and signature.

· (attitude) gain critical insights about how to evaluate and prove the security of proposed cryptographic schemes, when considering the goals and capabilities of different adversaries, thus developing a critical attitude regarding the conditions in which schemes can be used.

Pré-requisitos

Sem pré-requisitos

Conteúdos

Secrecy

· **Blockciphers:** pseudorandom functions (PRFs) and permutations (PRPs), indistinguishability games, “advantage”, switching lemma, asymptotic vs. concrete definitions, negligible functions.

· **Modes of encryption and secrecy properties:** probabilistic encryption modes, IND-CPA, IND-CCA, key-recovery, key-hiding, IND$-CPA

· **Proof methods:** hybrid proofs, tight vs. non-tight reductions, information theoretical lemma, broken schemes and provably secure schemes

Integrity

· **Authenticated encryption:** 1-pass vs. 2-pass schemes, key-separation, insecure schemes, existential forgeries, confusion freedom

· **Hash functions and MACs:** properties and applications, random oracle model, Merkle-Damgard construction, MACs vs. hashes, MACs using PRFs, unconditional security, commitments

Pubic Key Cryptography

· **RSA:** Textbook schemes (encryption & signature), attacks, modes (OAEP, hash-then-sign)

· **Diffie-Hellman (DH):** key-exchange protocol, intractability assumptions, MITM

· **Basic group theory:** axioms, modular arithmetic, Euler’s totient, Euler’s theorem, Chinese Remainder Theorem, generators, quadratic residuosity, etc.

Descrição detalhada dos conteúdos programáticos

Bibliografia

Recomendada

There is no textbook, but the entire course will be based on the following notes, with several recommended readings assigned during the course:

· Introduction to Modern Cryptography (BR), by Mihir Bellare and Phillip Rogaway (available at http://cseweb.ucsd.edu/users/mihir/cse207/classnotes.html).

· Handbook of Applied Cryptography (MOV), by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (available at http://www.cacr.math.uwaterloo.ca/hac/).

· Lecture Notes on Cryptography (GB), by Shafi Goldwasser and Mihir Bellare (available at http://cseweb.ucsd.edu/~mihir/papers/gb.html).

· Other reference papers assigned for reading during the course.

Outros elementos de estudo

Métodos de Avaliação

Língua de ensino