MO422-MC938 - Algoritmos Criptográficos

2º Semestre de 2011

Prof. Ricardo Dahab

Instituto de Computação - UNICAMP

Novidades - leia frequentemente	Professor	Locais e horários	Programa da disciplina	Diário de aulas	Material didático	Critério de avaliação	Datas importantes

Novidades

Professor (menu principal)

- Prof. Ricardo Dahab (turma B) - Sala IC-28, http://www.ic.unicamp.br/~rdahab, (19) 3521-5874, rdahab @ ic . unicamp . br

Locais e horários (menu principal)

- Aulas às terças e quintas, sala CC-51 (IC-3), 14-16sh.
- Local e horário de atendimento do professor: IC, sala 28, em horário previamente combinado.

Programa da disciplina

Resumidamente, o programa desta disciplina inclui os seguintes tópicos. Outros podem ser adicionados durante o desenvolvimento das aulas.

1. Breve introdução à Criptografia moderna.
2. Algoritmos básicos: aritmética básica de precisão arbitrária, aritmética modular, máximo divisor comum, resolução de congruências.
3. Algoritmos intermediários: testes de primalidade, fatoração, logaritmo discreto, aritmética de corpos finitos, aritmética em curvas elípticas.
4. Algoritmos avançados: emparelhamentos bilineares, teste de primalidade.

Diário de aulas (menu principal)

- **(2/8)** Introdução geral ao curso.
- **(4/8)** Introdução à Criptografia. Veja slides aqui.

Material didático (menu principal)

Aqui serão relacionados os materias didáticos de apoio como transparências, textos avulsos, artigos, etc, não relacionados nas aulas acima nem nas referências abaixo.

- **Leituras introdutórias recomendadas:**
  - **Capítulo 1 da referência 2 abaixo. Esse capítulo é uma introdução a várias técnicas da Criptografia moderna, ainda que um pouco desatualizada. Não se trata, portanto, de uma introdução muito suave à Criptografia de forma geral, mas é uma introdução suave às técnicas que usaremos neste curso.**
  - **Capítulo 1 da referência 3 abaixo. Esse capítulo é uma introdução à matemática que será necessária ao estudo dos algoritmos deste curso. É bem mais didática que a parte matemática da referência anterior, com exercícios muito úteis. O texto da referência 3 pode ser encontrado aqui (disponivel por pouco tempo).**

Referências

Algumas referências importantes para o material discutido nesta disciplina são:

1. *Técnicas Criptográficas Modernas - Algoritmos e Protocolos.* R. Dahab, J. C. López-Hernández. Em: Tomasz Kowaltowski; Karin Breitman. (Org.). Atualizações em Informática 2007. Rio de Janeiro: Editora PUC-Rio, 2007, v. , p. 115-170. Veja aqui uma versão disponível na Internet.
2. *Handbook of Applied Cryptography*. A. Menezes, P. v. Oorschot, S. Vanstone. Disponível em http://www.cacr.math.uwaterloo.ca/hac/
3. An Introduction to Mathematical Cryptography. Series: Undergraduate Texts in Mathematics. Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H. 2008, XVI, 524 p. 29 illus.. Springer. ISBN: 978-0-387-77993-5.
4. *A Computational Introduction to Number Theory and Algebra*. V. Shoup. Disponível em http://shoup.net/ntb/
5. *Cryptography: Theory and Practice*. D. Stinson. Ed. Chapman&Hall/CRC, 3a. edição, 2005. ISBN-10: 1584885084.
6. *Guide to Elliptic Curve Cryptogaphy*. D. Hankerson, A. Menezes, S. Vanstone. Springer, 2004. ISBN 0-387-95273-X.
7. *Post-Quantum Cryptography*. Bernstein, Daniel J.; Buchmann, Johannes; Dahmen, Erik (Eds.) 2009, IX, 245 p. 25 illus.. Springer. Hardcover. ISBN: 978-3-540-88701-0
8. ... em construção

Critério de avaliação (menu principal)

A avaliação será baseada em provas, trabalho final e projetos simples de implementação. Detalhes serão colocados aqui em breve.

Datas importantes (menu principal)

A serem divulgadas em breve.