MO422-MC938 - Algoritmos Criptográficos

2º Semestre de 2016 (aulas iniciam-se em 23/8/2016)

Prof. Ricardo Dahab

Instituto de Computação - UNICAMP

Novidades

Professor (menu principal)

- Prof. Ricardo Dahab, IC1 - Sala 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 IC-3, sala 351, 14-16h.
- Local e horário de atendimento do professor: IC-1, sala 28, em horário a ser definido.

Programa da disciplina (menu principal)

O programa desta disciplina cobre os algoritmos necessários à implementação da maioria dos sistemas criptográficos modernos. Tais algoritmos estão presentes nas funções de encriptação/decriptação, acordos de chaves, resumos (hash), geração de sequências pseudo-aleatórias de bits, entre outras. Duas vertentes de algoritmos serão explorados: (i) os não-resistentes a ataques (por algoritmos) quânticos, baseados predominantemente na Teoria dos Números e (ii) os resistentes a ataques quânticos, baseados na Teoria dos Reticulados, Teoria dos Códigos, e técnicas ad-hoc como é o caso dos algoritmos simétricos e de resumo. Algoritmos básicos, intermediários e avançados serão estudados, de forma que muito poucas noções de Criptografia serão necessárias, sendo mais desejável que o aluno tenha bons conhecimentos de Álgebra Linear e Análise de Algoritmos e Estatística e Probabilidade. É necessário que o aluno tenha também alguma prática de programação em Linguagem C, que será usada na confecção dos trabalhos práticos que serão parte da avaliação.

Ementa resumida (menu principal)

1. Breve introdução à Criptografia moderna.
2. Algoritmos e criptossistemas baseados em Teoria dos Números
    a. Algoritmos básicos: aritmética básica de precisão arbitrária, aritmética modular, máximo

divisor comum, resolução de congruências.
    b. Algoritmos intermediários: testes de primalidade, fatoração, logaritmo discreto, aritmética de corpos finitos, aritmética em curvas elípticas.
    c. Algoritmos avançados: emparelhamentos bilineares, teste de primalidade.
3. Algoritmos baseados em Teoria dos Reticulados
    a. Amostragem de vetores
    b. Algoritmos para redução de base - LLL
    c. Algoritmos para operações da Álgebra Linear
4. Algoritmos baseados em Teoria dos Códigos
5. Algoritmos baseados em técnicas adhoc para encriptação simétrica
6. Algoritmos baseados em técnicas adhoc para resumo (hash) criptográfico

Diário de aulas (menu principal)

- **(23/8)** Breve introdução ao curso e à Criptografia moderna.

Material didático (menu principal)

Usaremos uma variedade de materiais, incluindo transparências, artigos, trechos de livros, etc. Todos serão colocados nesta seção à medida que se fizerem necessários.

Referências (menu principal)

Algumas referências importantes para o material discutido nesta disciplina são:

1. *An Introduction to Mathematical Cryptography. Series: Undergraduate Texts in Mathematics*. J. Hoffstein, J. Pipher, J.H. Silverman. Springer.
2. *Introduction to Cryptography with Coding Theory*. W. Trappe, L. Washington. Pearson.
3. *Understanding Cryptography*. C. Paar, J. Pelzl, Springer.
4. *Introduction to Cryptography*. J.A. Buchmann, Springer.
5. *Handbook of Applied Cryptography*. A. Menezes, P. v. Oorschot, S. Vanstone. Disponível em http://www.cacr.math.uwaterloo.ca/hac/
6. *A Computational Introduction to Number Theory and Algebra*. V. Shoup. Disponível em http://shoup.net/ntb/
7. *Cryptography: Theory and Practice*. D. Stinson. Ed. Chapman & Hall/CRC, 3a. edição.
8. *Guide to Elliptic Curve Cryptography*. D. Hankerson, A. Menezes, S. Vanstone. Springer.
9. *Post-Quantum Cryptography*. D.J. Bernstein; J.A. Buchmann; E. Dahmen (Eds.).

Critério de avaliação (menu principal)

A avaliação será baseada em duas provas e três trabalhos de implementação. Detalhes e datas de entrega dos trabalhos serão divulgados no início das aulas.
O critério de avaliação será o seguinte:

1. As notas das provas P1 e P2 terão pesos iguais. Seja a média das provas P= (P1+P2)/2.
2. As notas dos trabalhos T1, T2 e T3 terão pesos iguais. Seja a média dos trabalhos T= (T1+T2+T3)/3.
3. Se as notas dos trabalhos forem todas maiores ou iguais a 3.0,
    a. então MA= 0.6×P + 0.4×T;
    b. senão, se a menor nota dos trabalhos estiver no intervalo [2.0, 2.9],

    i. então MA= 0.6×P + 0.4×min{T1, T2, T3};
    ii. senão MA= min{T1, T2, T3}.
4. Se MA >= 5.0, então o aluno estará aprovado; caso contrário, estará reprovado. Em ambos os casos, a média final será MA.

Todas as notas de provas e trabalhos estarão no intervalo [0, 10]. Todas as notas serão arredondadas para uma casa decimal.

Os intervalos de notas que serão usados na conversão para conceitos, no caso de alunos de pós-graduação, são:

- A: [8.5, 10.0]; B: [7, 8.4]; C: [5.0, 6.9]; D: [0, 4.9].

Datas importantes (menu principal)

- Prova 1: 18 de outubro
- Prova 2: 6 de dezembro