MO421/MC889A - Introdução à Criptografia

1º Semestre de 2013

Instituto de Computação - UNICAMP

Novidades

- (19/3) Página atualizada, com datas, etc.

Professor (menu principal)

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

Locais e horários (menu principal)

- Aulas na sala CC-22 às segundas (21-23h) e quartas (19-21h).
- Atendimento do professor: a combinar

Objetivos, pré-requisitos e programa (menu principal)

Objetivos

O objetivo principal desta disciplina é o de explorar o amplo espectro de fundamentos, técnicas e aplicações da Criptografia moderna. De uma técnica obscura e limitada aos meios diplomáticos e militares (e até como atividade lúdica) até a década de 1970, a Criptografia evoluiu rapidamente para a se tornar a confluência de várias áreas teóricas e aplicadas, de intensa pesquisa e desenvolvimento agora de domínio público, onde repousam a grande maioria das técnicas para provimento de requisitos de segurança da informação e de sistemas computacionais.
A abordagem do curso é em largura, sem descuido do rigor na apresentação das teorias subjacentes às diversas técnicas criptográficas. Exemplos de algoritmos e protocolos serão discutidos e implementados, na medida do possível.

Pré-requisitos

A disciplina é auto-contida: serão cobertos todos os conceitos não-elementares de Matemática, Estatística e Ciência da Computação necessários ao entendimento das técnicas criptográficas estudadas. De qualquer maneira, são desejáveis conhecimentos básicos de Álgebra, Álgebra Linear, Estatística e Probabilidade, e Análise de Algoritmos, comumente cobertos em disciplinas dos primeiros anos de graduação.

Programa

1. Introdução à Criptografia: requisitos da Segurança da Informação, métodos clássicos de encriptação.
2. Cifras de fluxo: vantagens e desvantagens. Exemplos teóricos e reais.
3. Cifras de bloco: DES, AES. Modos de encriptação.
4. Encriptação com sistemas de chave pública: RSA, ElGamal, Curvas Elípticas.
5. Assinaturas digitais: RSA, DSA, ECDSA.
6. Resumos criptográficos (Hash): motivação, exemplos e aplicações.
7. Códigos para autenticação: MDC, MACs.
8. Estabelecimento de chaves: técnicas simétricas e assimétricas, PKIs.
9. Tópicos avançados: emparelhamentos bilineares, acordo de chaves quântico; métodos pós-quânticos; encriptação homomórfica.

Diário de aulas (menu principal)

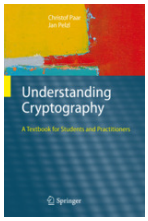
- (27/2) Introdução geral à disciplina.
- (4/3) Introdução aos sistemas criptográficos. Criptografia simétrica e assimétrica.
    - Provisoriamente foi usado material do texto "Técnicas criptográficas e aplicações", que pode ser encontrado aqui.
- (6/3) Iniciamos o uso do material do livro-texto, cobrindo praticamente todo capítulo 1: Introdução à Criptografia clássica: cifras simétricas e artimética modular.
    - Slides: Capítulo 1.
    - Leitura recomendada: Todo o Capítulo 1.
    - Exercícios do livro-texto recomendados: 1.1, 1.3, 1.4, 1.5, 1.6, 1.7, 1.9, 1.13, 1.14.
- (11/3) Cobrimos o final do Capítulo 1 e as seções Capítulo 2: Cifras de fluxo (stream ciphers).
    - Slides: Capítulo 2.
    - Leitura recomendada: Seções 2.1 e 2.2.
    - Exercícios do livro-texto recomendados: 2.1 a 2.6
- (13/3) Não houve aula.
- (18/3) Não houve aula.
- (20/3) ~~Iniciaremos o capítulo 3 (DES).~~ Cobrimos parcialmente o Capítulo 3, até o início da decriptação.
    - Slides: Capítulo 3.
    - Leitura recomendada: Todo Capítulo 3.
    - Exercícios do livro-texto recomendados: 3.1 a 3.12
- (25/3) Terminaremos o estudo do DES, concluindo o Capítulo 3. Iniciaremos Capítulo 5: modos de encriptação em bloco.
    - Slides: Capítulo 3 e Capítulo 5.
    - Leitura recomendada: Capitulo 5 até Cipher Block Chaining Mode.
    - Exercícios do livro-texto recomendados:
- (27/3) Continuaremos Capítulo 5: modos de encriptação em bloco.
    - Slides: Capítulo 5.

- Leitura recomendada: Capitulo 5 a partir de Cipher Block Chaining Mode.
- Exercícios do livro-texto recomendados:

Referências e material didático (menu principal)

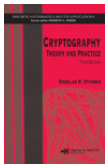
Livro-texto

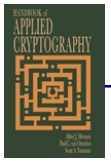
Exceto por alguns tópicos mais avançados, cobertos nas últimas aulas do semestre, a disciplina será quase que totalmente baseado no seguinte livro:

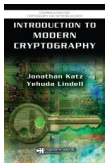


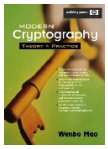
Understanding Cryptography - A Textbook for Students and Practitioners. Christof Paar e Jan Pelzl. Springer, 2010. Disponível aqui para download a partir do domínio unicamp.br.

Outros livros técnicos

1. 

Cryptography - Theory and Practice. Douglas R. Stinson. Chapman & Hall/CRC, 2005.
2. 

Handbook of Applied Cryptography. A. Menezes, P. van Oorschot and S. Vanstone. CRC Press, 1997.
3. 

Introduction to Modern Cryptography. J. Katz and Y. Lindell. Chapman & Hall/CRC, 2007.
4. 

Modern Cryptography - Theory and practice. Wenbo Mao. Pearson Education, 2004.
5. 

Algoritmos - Teoria e Prática. Cormen, Leiserson, Rivest and Stein. Editora Campus, 2002.
Errata (do Prof. Zanoni)
6. 

A Computational Introduction to Number Theory and Algebra, Victor Shoup. Cambridge University Press, 2005.

Livros sobre a História da Criptografia através dos séculos

1.  *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Simon Singh. Anchor, 2000.
2.  *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. David Khan. Scribner, 1996.

Referências sobre Bletchley Park

Bletchley Park (1, 2) foi um centro de criptoanálise montado na Segunda Guerra Mundial pelo governo inglês, com o objetivo de quebrar (decriptar) as transmissões encriptadas de países do Eixo, especialmente as oriundas das tropas e comando alemães. Bletchley Park fica na pequena cidade de Bletchley no interior da Inglaterra. Entre vários feitos formidáveis, nasceu em Bletchley Park o primeiro computador, batizado de Colossus, cujo objetivo específico era acelerar a criptoanálise de um tipo de cifra especialmente difícil, produzida pelas máquinas Lorenz, mais sofisticadas e complexas que as bem conhecidas máquinas Enigma. Entre outros, Alan Turing estava lá. As referências abaixo descrevem e discutem esses feitos.

1.  *Codebreakers: The Inside Story of Bletchley Park*. F. H. Hinsley and Alan Stripp (Editors). Oxford University Press, USA, 2001.
2.  *Bletchley Park's Lost Heroes*. Fascinante vídeo produzindo pela BBC, contando a história de W. T. Tutte, e outros heróis da Segunda Guerra desconhecidos do grande público. Tutte foi um matemático conhecidíssimo na área de Teoria dos Grafos, mas que em Bletchley Park realizou o feito de quebrar a cifra produzida pela máquina Lorenz sem jamais ter visto uma descrição dela. Para esse fim, o computador moderno (Colossus) teve que ser inventado, por Tommy Flowers, também do nada. Em inglês.
3.  Colossus: The secrets of Bletchley Park's code-breaking computers. B. Jack Copeland. Oxford University Press, USA, 2010.

Material didático

- Usaremos como material principal as transparências produzidas pelos próprios autores. Estão disponíveis na Internet mas serão colocadas no diário de aulas, junto à descrição do material coberto em aula. Estamos trabalhando numa versão em português das transparências. Se você quer ser um voluntário nessa atividade, por favor, escreva para o professor.
- Outros materiais didáticos, como lista de exercícios, serão colocados também no diário de aulas.

Avaliação (menu principal)

- **Forma de avaliação**
  - A avaliação se dará na forma de duas provas teóricas e um trabalho final, que poderá ser feito em grupos de 2 estudantes no caso de alunos de graduação, e individualmente no caso de alunos de pós-graduação. Além disso, as exigências quanto à qualidade e profundidade do trabalho serão maiores para os alunos de pós. O prazo para feitura do trabalho será de duas semanas.
- **Critério de notas**
  - Dadas notas de provas P1, P2, a média de provas MP será igual a (P1 + P2)/2.
  - A média de aproveitamento MA será igual a (6MP + 4T)/10, onde T é a nota do trabalho.
  - Se MA >= 5, então o aluno não precisará fazer o exame e sua média final MF será igual a MA; caso contrário o aluno terá que fazer o exame e MF= (MA+E)/2, onde E é a nota do exame.
  - Se MF >=5, o aluno estará aprovado, caso contrário estará reprovado.
- *Obs: Somente haverá a possibilidade de substituição de uma das notas de provas pela nota do exame por motivo de saúde, com apresentação de atestado médico.*

Datas importantes (menu principal)

- Prova 1: quarta-feira, 17/4
- Prova 2: quarta-feira, 29/5
- Data da entrega dos enunciados dos trabalhos pelo professor: segunda-feira, 3/6
- Data para entrega dos trabalhos pelos alunos: segunda-feira, 17/6
- Exame Final: quarta-feira, 10/7

Esta página é mantida pelo Prof. R. Dahab.
Última atualização em 20/3/2013.