

MO421/MC889A - Introdução à Criptografia

1º Semestre de 2019

Prof. Ricardo Dahab

Instituto de Computação - UNICAMP

Novidades	Professor	Locais e horários	Objetivos e programa	Diário de aulas	Referências bibliográficas e material didático	Avaliação	Datas importantes
---------------------------	---------------------------	-----------------------------------	--------------------------------------	---------------------------------	--	---------------------------	-----------------------------------

Novidades

- [25/02] Critério de aprovação ligeiramente ajustado: não haverá mais a possibilidade de exame final para alunos de graduação. Os critérios agora são idênticos para alunos de graduação e de pós. [Veja aqui](#).
- [18/02] **Início das aulas será no dia 28/2, quinta-feira.**

Professor [\(menu principal\)](#)

- Prof. Ricardo Dahab - Sala IC-9, <http://www.ic.unicamp.br/~rdahab>, (19) 3521-5874, rdahab@ic.unicamp.br

Locais e horários [\(menu principal\)](#)

- Aulas na sala 352 (IC-3) às terças e quintas, das 16 às 18h.
- Atendimento do professor: sala 28 do IC-1, horário a ser divulgado.

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. Até a década de 1970, a Criptografia foi uma técnica de interesse limitado aos meios diplomáticos e militares. Com o advento das redes de computadores, evoluiu e expandiu-se rapidamente, abarcando várias áreas teóricas e aplicadas, com intensa atividade de pesquisa e desenvolvimento. Hoje está presente na base de quase todas as 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 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

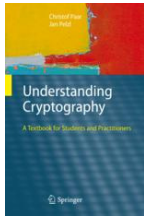
1. Introdução à Criptografia: requisitos da Segurança da Informação, métodos clássicos de encriptação.
2. Cifras de fluxo: vantagens e desvantagens. Exemplos teóricos e reais.
3. Cifras de bloco: DES, AES. Modos de encriptação.
4. Encriptação com sistemas de chave pública: RSA, ElGamal, Curvas Elípticas.
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 [\(menu principal\)](#)

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 baseada no seguinte livro:



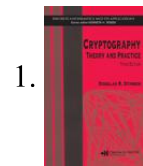
Understanding Cryptography - A Textbook for Students and Practitioners. Christof Paar e Jan Pelzl. Springer, 2010. [Disponível aqui para](#)

[download](#) a partir do domínio unicamp.br.

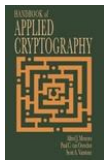
[Veja errata no site do livro aqui.](#) ou [arquivo pdf diretamente aqui.](#)

[Veja errata que estamos construindo aqui.](#)

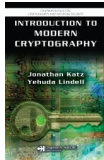
Outros livros técnicos



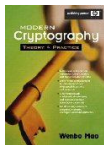
1. *Cryptography - Theory and Practice.* Douglas R. Stinson. Chapman & Hall/CRC, 2005.



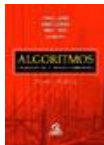
2. [Handbook of Applied Cryptography.](#) A. Menezes, P. van Oorschot and S. Vanstone. CRC Press, 1997.



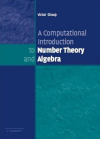
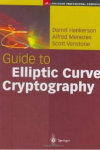
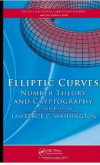
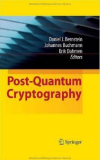
3. *Introduction to Modern Cryptography.* J. Katz and Y. Lindell. Chapman & Hall/CRC, 2007.





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.
7.  [*Guide to Elliptic Curve Cryptography*](#), Hankerson, Menezes, Vanstone, Springer, 2004.
8.  [*Elliptic Curves: Number Theory and Cryptography*](#), 2nd. Edition (Discrete Math and Its Applications), L. C. Washington
9.  [*Post-Quantum Cryptography*](#). Bernstein, Buchmann, Dahmen (editores). 2009, Springer.

Livros sobre a História da Criptografia ao longo 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 produzido 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.
- Outros materiais didáticos adicionais 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 ao nível das provas e à qualidade e profundidade do trabalho serão maiores para os alunos de pós. O prazo para feitura do trabalho ainda será divulgado.
- **Critério de notas**
 - Sejam P1, P2, as notas das provas e T a nota do trabalho, todas entre 0 e 10.
 - A média de provas, MP, será igual a $(P1 + P2)/2$.
 - A média de aproveitamento, MA, será igual a $(6MP + 4T)/10$.
 - Se $MA \geq 5$, o aluno estará aprovado; caso contrário, estará reprovado. No caso de alunos de pós-graduação, o conceito atribuído à disciplina seguirá a seguinte convenção:
 - Conceito A: Se $MA \geq 8,5$

- Conceito B: Se $7,0 \leq MA \leq 8,4$
- Conceito C: Se $5,0 \leq MA \leq 6,9$
- Conceito D: Se $MA < 5,0$
- *Observações:*
 - *Somente será possível a um aluno fazer a prova substitutiva por motivo de saúde, com apresentação de atestado médico. Além disso, a nota de apenas uma das provas poderá ser substituída. Isto é, se um aluno não fizer as duas provas principais, a nota de uma delas será zero.*

Datas importantes ([menu principal](#))

- Prova 1: terça-feira, 30/4
- Prova 2: terça-feira, 18/6
- Prova substitutiva: terça-feira, 25/6
- Data da entrega dos enunciados dos trabalhos pelo professor: a ser definido.
- Data para entrega dos trabalhos pelos alunos: a ser definido.

Esta página é mantida pelo Prof. R. Dahab.