

# MO421/MC889A - Introdução à Criptografia

1º Semestre de 2020

Prof. Ricardo Dahab

Instituto de Computação - UNICAMP

<a href="#">Novidades</a>	<a href="#">Professor</a>	<a href="#">Locais e horários</a>	<a href="#">Objetivos e programa</a>	<a href="#">Diário de aulas</a>	<a href="#">Referências bibliográficas e material didático</a>	<a href="#">Avaliação</a>	<a href="#">Datas importantes</a>
---------------------------	---------------------------	-----------------------------------	--------------------------------------	---------------------------------	--	---------------------------	-----------------------------------

## Novidades

- [20/3] Obviamente, a grande novidade é a suspensão das aulas presenciais na Unicamp, devido à pandemia do coronavírus. Veja as modificações na página, com trechos novos **em laranja**.
- [12/3] Divulgação de troca do livro-texto, de Smart para Stinson-Paterson. Veja a seção de [referências](#).
- [9/3] Esta página entra no ar

## 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 14 às 16h. **As aulas presenciais não ocorrerão. Em vez disso, serão indicadas leituras do livro texto, acompanhadas de listas de exercícios semanais que serão corrigidas, e cujas notas farão parte da avaliação.**
- Atendimento do professor: ~~sala 28 do IC-1, em horário combinado por email.~~ **O atendimento ocorrerá por email e em sessões remotas de atendimento coletivo, no horário original das aulas. O meio de comunicação será Google Meets ou outro canal, caso seja considerado mais adequado. Essa informação será divulgada oprotunamente.**

## 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, abrangendo 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. Criptografia clássica
2. Teoria da informação, segurança incondicional
3. Cifras de blocos e de fluxo.
4. Funções de hash, códigos de autenticação de mensagens, funções de derivação de chaves
5. O RSA de métodos baseados em fatoração de inteiros
6. Outros métodos para encriptação de chave pública
7. Assinaturas digitais
8. Criptografia baseada em problemas muito difíceis (PQC)
9. Certificados, métodos de estabelecimento e transporte de chaves

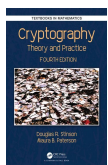
## Diário de aulas [\(menu principal\)](#)

Manterei o diário de aulas [neste link](#), com observações feitas durante as aulas, recomendações diversas, etc.

## Referências e material didático [\(menu principal\)](#)

### Livro-texto

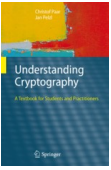
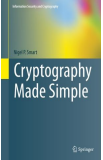
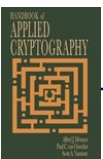
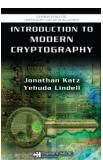
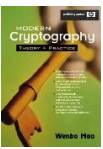
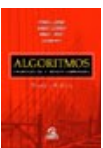

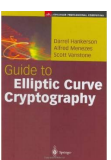
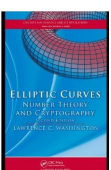
O livro texto será o seguinte, do qual serão utilizados partes dos capítulos. Está disponível [aqui](#).

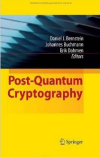


*Cryptography - Theory and Practice, 4th ed.*, Douglas R. Stinson and Maura B. Paterson. CRC



Press, 2019.

### Outros bons livros para referência

1.  *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](#).
2.  *Cryptography Made Simple*. Nigel P. Smart. Springer, 2016. (disponível para [download gratuito aqui](#) com IP da Unicamp).
3.  *Handbook of Applied Cryptography*. A. Menezes, P. van Oorschot and S. Vanstone. CRC Press, 1997.
4.  *Introduction to Modern Cryptography*. J. Katz and Y. Lindell. Chapman & Hall/CRC, 2007.
5.  *Modern Cryptography - Theory and practice*. Wenbo Mao. Pearson Education, 2004.
6.  *Algoritmos - Teoria e Prática*. Cormen, Leiserson, Rivest and Stein. Editora Campus, 2002.  
[Errata \(do Prof. Zanoni\)](#)
7.  *A Computational Introduction to Number Theory and Algebra*, Victor Shoup. Cambridge University Press, 2005.
8.  *Guide to Elliptic Curve Cryptography*, Hankerson, Menezes, Vanstone, Springer, 2004.
9.  *Elliptic Curves: Number Theory and Cryptography*, 2nd. Edition (Discrete Math and Its Applications), L. C. Washington




10.  [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 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

- O livro-texto é o material didático principal, a partir de onde produziremos notas de 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 listas de exercícios semanais ou quinzenais, que serão usadas como parte da avaliação. A outra parte da avaliação será feita sobre um trabalho final.** ~~duas provas teóricas e um trabalho final, que deverá ser feito individualmente.~~ Além disso, as exigências quanto ao nível das ~~provas~~ **listas de exercícios** e à qualidade e profundidade do trabalho serão maiores para os alunos de pós. O prazo para feitura do trabalho ainda será divulgado. **O canal de disponibilização das listas e de comunicação, em geral, deverá ser email ou Google Classroom. Esse fato será divulgado em breve, na próxima semana.**
- **Critério de notas**
  - Sejam  $P_1, P_2$ , ~~as notas das provas~~  **$L_1, L_2, \dots$  as notas das listas de exercícios e  $T$  a nota do trabalho, todas entre 0 e 10.**
  - A média de ~~provas~~,  $MP$ , será igual a  $(P_1 + P_2)/2$ . **listas,  $ML$ , será a média aritmética das listas.**
  - A média de aproveitamento,  $MA$ , será igual a  ~~$(6MP + 4T)/10$ .~~  **$(6ML + 4T)/10$ .**
  - 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, ou por razões acadêmicas como eventos com apresentação de trabalho ou participação em competições acadêmicas. 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.~~ **Qualquer tentativa de fraude acarretará nota zero no curso a todos os envolvidos.**

## Datas importantes [\(menu principal\)](#)

- **As datas de todas as atividades são dependentes da progressão da pandemia e as resoluções da reitoria da Unicamp. As datas de entrega das listas de exercícios dependerão da data da sua disponibilização, adicionadas de uma ou duas semanas, a depender da dificuldade da lista. A data de entrega do trabalho será definida oportunamente.**
- Prova 1: terça-feira, 14/4
- Prova 2: terça-feira, 16/6
- Prova substitutiva: quinta-feira, 2/7
- Data da entrega dos enunciados dos trabalhos pelo professor: a ser definido.
- Data para entrega dos trabalhos pelos alunos: a ser definido.
- ~~Não haverá aula nos dias 9/4, 21/4, 11/6, devido aos feriados.~~