MO421/MC889 Introdução à Criptografia
Instituto de Computação — UNICAMP

Julio Lopez
jlopez@ic.unicamp.br

Página do curso. As informações específicas do curso estarão disponíveis em:

`https://sites.google.com/site/unicampjlopez/`

Aulas. Curso composto por duas aulas semanais.

Horário das aulas			
Tipo	Dia	Sala	Horário
Teórica	Segundas	CC52	19:00 - 21:00
Teórica	Quartas	CC52	19:00 - 21:00

Não haverá aula nos dias 01/05, 12/06.

Ementa:

- Breve introdução à Criptografia.
- Algoritmos computacionais básicos: aritmética modular, máximo divisor comum, aritmética de números grandes.
- Aritmética de corpos finitos, testes de primalidade, fatoração, logaritmo discreto.
- Algoritmos simétricos: DES, AES, modos de operação.
- Algoritmos de funções de resumo: Família SHA (SHA-1, SHA-2, SHA-3), outros.
- Criptografia Assimétrica: conceitos, encriptação, assinatura digital
- Algoritmos criptográficos: RSA, DSA, ECDSA, EdDSA
- Protocolos Criptográficos
- Tópicos: geração de números pseudo-aleatórios, padrões de criptografia, algoritmos avançados: algoritmos de criptografia pós-quântica, implementação em software e bibliotecas.

Atendimento. Segunda-feira 18:00-19:00.

Provas. Haverá duas provas teóricas durante o semestre, PT_1 e PT_2, com pesos 2 e 3. Não haverá exame. As data das provas:

Prova	Data	Horário
Prova I – PT_1	03/05	19:00-21:00
Prova II– PT_2	28/06	19:00-21:00

A média das provas teóricas, M_P, é calculada da seguinte forma:

$$M_P := \frac{2PT_1 + 3PT_2}{5}$$

Projeto. Será proposto um trabalho teórico- prático sobre o estudo de técnicas criptográficas. O aluno fará uma apresentação e entregará um relatório. M_T será a nota do trabalho. A data de entrega do relatório (formato de artigo): 3 de julho de 2023.
Média Final: A média final M_F e a situação do(a) aluno(a) serão definidas de acordo com as regras a seguir. Note que, de acordo com o Regimento Geral de Graduação/Pós-Graduação os(as) alunos(as) devem ter frequência maior ou igual a 75% para aprovação.
Média do Semestre: $M_S = 0.7 \times (2P_1 + 3P_2) + 0.3M_T$
Média Final (MO421): aprovado se $M_P \geq 5.0$ e $M_T \geq 5.0$. O conceito final é calculado da seguinte forma:

- A se $M_S \geq 8.5$
- B se $7.0 \leq MS < 8.5$
- C se $5.0 \leq MS < 7.0$
- D se $M_S < 5$ e $M_T < 5.0$

Média Final (Graduação): aprovado se $M_P \geq 5.0$ e $M_T \geq 5.0$ com $M_F = M_S$. Caso contrário, $M_F = min(M_P, M_T)$.

Bibliografia. Existem muitos bons livros sobre criptografia. Seguem abaixo alguns títulos. Outros materiais digitais serão divulgados na página do curso.

- Cryptography Theory and Practice, Fourth Edition, 2018 Douglas Stinson and Maura Paterson, Chapman and Hall/CRC.
- Introduction to Modern Cryptography, Jonathan Katz e Yehuda Lindell, Chapman and Hall/CRC, third edition. 2020.
- Cryptography and Network Security (Principles and Practice) seven edition, William Stallings, Pearson, 2017
- Understanding Cryptography, Paar-Pelzl, 2010: http://link.springer.com/book/10.1007/978-3-642-04101-3/page/1
- Introduction to Modern Cryptography, Jonathan Katz e Yehuda Lindell, Chapman and Hall/CRC, 2011.
- Implementing Cryptography, using Python, Sahnnon W Bray, Wiley, 2020.
- An Introduction to Mathematical Cryptography, Jeffrey Hoffstein, Jill Pipher e Joseph H. Silverman, Springer, 2001.
- Design and Analysis of Cryptographic Algorithms in Blockchain, Ke Huang, CRC Press, 2021.