MO422/MC938A Algoritmos Criptográficos
Instituto de Computação — UNICAMP

Julio López
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	Terça	CC85	19:00 - 21:00
Teórica	Quinta	CC85	19:00 - 21:00

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 (AES, ASCON) e modos de operação.
- Algoritmos de funções de resumo: Família SHA (SHA-1, SHA-2, SHA-3), outros.
- Criptografia assimétrica: conceitos, encriptação, mecanismos de encapsulamento de chaves, assinatura digital.
- Algoritmos de chave pública: RSA, DSA, ECDSA, EdDSA.
- Geração de números pseudo-aleatórios.
- Introdução à algoritmos pós-quânticos.
- Tópicos: padrões industriais de criptografia, implementação em software e bibliotecas.

Atendimento. Terça-feira 18:00-19:00 (ou horário agendado).

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	26/09	19:00-21:00
Prova II– PT_2	28/11	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 dezembro de 2024.
Média Final (MC938A): 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: $M_S = 0.7 \times \frac{2PT_1+3PT_2}{5} + 0.3M_T$
Média Final (MO422): aprovado se $M_T \geq 5.0$ 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 $M_S < 5$ ou $M_T < 5.0$

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

Bibliografia. Segue abaixo alguns títulos de livros. Alguns materiais adicionais serão divulgados na página do curso.

- Introduction to Modern Cryptography, Jonathan Katz e Yehuda Lindell, Chapman and Hall/CRC, third edition, 2020.
- Cryptography Theory and Practice, Fourth Edition, Douglas Stinson and Maura Paterson, Chapman and Hall/CRC, 2018.
- Cryptography and Network Security (Principles and Practice) eight edition, William Stallings, Pearson, 2023.
- Understanding Cryptography, Christof Paar , Jan Pelzl , Tim Güneysu: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms. Springer, 2024.
- Implementing Cryptography, using Python, Sahnnon W Bray, Wiley, 2020.