MC932A-MO422 Algoritmos Criptográficos
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/mc938`

Aulas. Curso composto por duas aulas semanais.

Horário das aulas			
Tipo	Dia	Sala	Horário
Teórica	Terça	CC353	10:00 - 12:00
Teórica	Quinta	CC353	10:00 - 12:00

Não haverá aula nos dias 27/08 e 29/08.

Ementa:

- Breve introdução à Criptografia Moderna.
- 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.
- Curvas Elípticas e Geracào de Números Pseudo-aleatórios
- Algoritmos criptográficos: RSA, DSA, ECDSA, EdDSA
- Algoritmos avançados: algoritmos de criptografia pós-quântica.
- Tópicos: implementação em software, padrões de criptografia NIST.

Atendimento. Segunda-feira 16:00-17:00.

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	10/10	10:00-12:00
Prova II– PT_2	26/11	10:00-12:00

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 algoritmos criptográficos. 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): 2 de dezembro de 2019.
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 Frequencia maior ou igual a 75% para aprovação.
Média do Semestre: $M_S = 0.7 \times (2P_1 + 3P_2) + 0.3M_T$
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 $M_S < 5$ e $M_T < 5.0$

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. Existem muitos textos sobre algoritmos criptográficos. Seguem abaixo alguns títulos. Alguns materiais digitais serão divulgados na págino 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, second edition. 2014.
- Cryptography and Network Security (Principles and Practice) seven edition, William Stallings, Pearson, 2017
- Modern Computer Arithmetic, Richard P. Brent and Paul Zimmermann, 2010. http://arxiv.org/pdf/1004.4710v1.pdf
- Implementing SSL/TLS (using cryptography and PKI) Joshua Davies, Wiley Publishing , Inc., 2011
- 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.
- Modern Cryptography Primer, Czesław Kościelny, Mirosław Kurkowski, Marian Srebrny, 2013 http://link.springer.com/b 3-642-41386-5