Instituto de Computação - UNICAMP

MO421 - MC889 - Introdução à Criptografia

Primeiro semestre de 2012

Prof. Julio López
jlopez@ic.unicamp.br

Conteúdo desta página:

Novidades:

- VER LISTA 3
- VER Calendario (temas de Pesquisa) Trabalhos
-
- 27 de junho: Apresentacoes (ver calendario)
- 30 de junho: Apresentacoes (ver calendario) 09-12:00 horas, sala==> IC3-22
- Exame: 10 de julho: 19:00-21:00 horas

Dias, Horários e Local das Aulas:

- Aulas teóricas às 19:00-21:00 (segunda-feira) e às 21:00-23:00 (quarta-feira), na sala CC-16.

Dia, Horário e Local de Atendimento:

- quarta-feira: 19:00-20:00 (sala 34 do IC)

Objetivos da Disciplina:

- O objetivo da disciplina é oferecer uma introdução ao estudo de técnicas criptográficas modernas e suas aplicações.

Ementa:

- Introdução aos sistemas criptográficos
- Técnicas clássicas de criptografia
- Técnicas simétricas (DES, AES, funções de resumo)
- Conceitos básicos de teoria dos números, aritmética modular, grupos e corpos finitos
- Técnicas assimétricas (RSA, DSA, ECC, IBE)
- Protocolos criptográficos
- Tópicos especiais
- Aplicações (projetos)

Bibliografia:

- [1] Criptografia e Segurança de Redes príncipios e práticas, William Stallings, 4a. edição, Pearson Prentice-Hall, 2008.
- [2] Understanding Cryptography, Christof Paar e Jan Pelzl, Springer, 2010
- [3] An introduction to Mathematical Cryptography, Jeffrey Hoffstein, Jill Pipher e Joseph H. Silverman, Springer, 2008
- [4] Introduction to Modern Cryptography (Chapman Hall/CRC Cryptography and Network Security Series) Jonathan Katz e Yehuda Lindell, 2008.
- [5] Cryptography: Theory and Practice, Douglas Stinson, Chapman & Hall/CRC, 2006
-
- [6] Introduction to Modern Cryptography, Mihir Bellare and Phillip Rogaway, 2005, http://www-cse.ucsd.edu/users/mihir/cse207/classnotes.html. [free]
- [7] Handbook of Applied Cryptography, Alfred Menezes, Paul van Oorschot, Scott Vantone, CRC Press, 1996. [free]

Material didático adicional

- Documentary revealing the secret story of how two men hacked into Hitler's personal super-code machine--Bletchley Park
- Intypedia: Information Security Encyclopedia
- Introdução Cap 1 de [4]
- " Capítulo: Técnicas criptográficas modernas: algoritmos e protocolos"
- "Introdução "
- "Algoritmos clássicas"
- Fundamentos
- ** LISTA 1 **
- Cifradores de Bloco
- AES
- AES-como funciona
- Modos
- Resumo
- MACs
- RSA
- ECC
- Protocolos
- **LISTA 3**

Avaliação

- Para os matriculados em MO421: haverá duas provas (P1,P2) e um trabalho de pesquisa TP. Serão atribuídos conceitos (A a D), com base na nota M=(0.35*P1 + 0.40*P2+ 0.25*TP) e na qualidade do trabalho TP.
- Para os matriculados em MC889: haverá duas provas (P1,P3) e um trabalho de pesquisa TP. O aluno Será aprovado se a nota M=(0.35*P1 + 0.40*P3+ 0.25*TP) for maior ou igual a 5.0.
- Não serão ministradas provas substitutivas.
- O aluno será reprovado se a freqüência às aulas for menor do que 75% (regra da Unicamp).

Datas Importantes:

- Prova 1: 23 de abril
- NOTA Prova-I
- Prova 2: 18/06-25/06
- Prova 3: 25 de junho
- Trabalho TP: 27 de junho
- Exame: ***10 de julho*** 19:00 horas

- Projetos:

- Tarefas:
  - Leitura do Cap 1 de [4]; 29/02-05/03 (primeira semana de aula)

- Notas:

- Trabalhos:
  - Trabalho-2012 <
  -

Última atualização em 22/02/2012 por J. López