Julio López

Search this site

MC938-MO422 Algoritmos Criptográficos

Novidades: Aulas

terças: (19:00-21:00) CC51

quintas: (21:00-23:00) CC51

Programa:

1. Breve introdução à Criptografia Moderna.
2. Algoritmos computacionais básicos: aritmética modular, máximo divisor comum, aritmética de números grandes.
3. Aritmética de corpos finitos, testes de primalidade, fatoração, logaritmo discreto.
4. Algoritmos simétricos: DES, AES, modos de operação.
5. Algoritmos de funções de resumo: Família SHA (SHA-1, SHA-2, SHA-3), outros.
6. Curvas Elípticas
7. Algoritmos criptográficos: RSA, DSA, ECDSA, EdDSA
8. Algoritmos avançados: algoritmos de criptografia pos-quântica.
9. Tópicos: geração de números pseudoaleatórios, implementação em software, algoritmos novos.

Aulas:

- Tema-01
- Tema-02
- Tema-03
- Tema-04
- Tema-05
- GCM

Traduzir

- SHA3
- Tema-06
- Projetos
- ECC
- ENISA
- LISTA

Provas:

- Prova 1: (P1) 28 de Setembro 2017
- Prova 2: (P2) 28 de Novembro 2017
- Exame: (E) 12 de Dezembro de 2017
- Projeto da Disciplina (PD): 5 de Dezembro de 2017

Avaliação:

- Média do Semestre MS=(3*P1 + 4*P2 + 3*PD)/10
- Mádia Final: (MO422) : A,B,C,D; aprovado se MS>=5.0 e PD>=5.0
- Conceitos: **A** : MS>= 8.5; **B:** 7.0<=MS< 8.5; **C:** 5.0<=MS< 7; **D**: MS<5.0 ou PD<5.0
- Média Final: (MC938); aprovado se MS>=5.0 e PD>=5.0 , caso contrário MF= (min{4.9,MS} + E)/2

Referências:

- **[**1**]** Cryptography and Network Security (Principles and Practice) seven edition, William Stallings, Pearson, 2017
- [2] Modern Computer Arithmetic
  Richard P. Brent and Paul Zimmermann, 2010.
  http://arxiv.org/pdf/1004.4710v1.pdf
- [3] Implementing SSL/TLS (using cryptography and PKI) Joshua Davies, Wiley Publishing , Inc., 2011
- [4] Understanding Cryptography, Paar-Pelzl, 2010:
  http://link.springer.com/book/10.1007

/978-3-642-04101-3/page/1

- [5] Introduction to Modern Cryptography, Jonathan Katz e Yehuda Lindell, Chapman and Hall/CRC, 2011.
- [6] Modern Cryptography Primer, Czesław Kościelny, Mirosław Kurkowski, Marian Srebrny, 2013 **http://link.springer.com/book/10.1007/978-3-642-41386-5**

Outros Materiais:

- CriptoRED: http://www.criptored.upm.es

AC-ModosOperação…	Julio López, …	v.1	
AC-cifradorAES.pdf …	Julio López, …	v.2	
AC-cifradores-2013.…	Julio López, …	v.1	
AC-macs.pdf (356k)	Julio López, …	v.1	
AC-projeto-2014.pdf…	Julio López, …	v.1	
ENISA-2014.pdf …	Julio López, …	v.1	
FHE-overview.pdf …	Julio López, …	v.1	
GCM-counter-mode.…	Julio López, …	v.1	
NotaFinal-AC-2015.…	Julio López, …	v.1	
SHA3.pdf (160k)	Julio López, …	v.1	
cpublica.pdf (424k)	Julio López, …	v.2	
ecc.pdf (817k)	Julio López, …	v.1	
fips-197.pdf (1157k)	Julio López, …	v.1	
fm-MO422.pdf (294k)	Julio López, …	v.1	

introducao-AC-422....	Julio López, ...	v.2	
listaIC3.pdf (31k)	Julio López, ...	v.1	

Comentários

Você não tem permissão para adicionar comentários.