MC938-MO422 Algoritmos Criptográficos

Novidades:

- **Aulas:** sala 85 às quartas (19:00 horas) e sextas (21:00 horas)
- Leitura Capítulo 1, 6: Understanding Cryptography, Paar-Pelzl, 2010: http://link.springer.com/book/10.1007/978-3-642-04101-3/page/1

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-2), outros.
6. Aritmética de Curvas Elípticas
7. Algoritmos criptográficos: RSA, DSA, ECDSA
8. Algoritmos avançados: emparelhamentos bilineares, bibliotecas criptográficas, algoritmos de criptografia pos-quântica.
9. Tópicos: geração de números pseudoaleatórios,

implementação em softwate

Aulas:

- Aula-01
- Aula-02
- Aula-03

Referências:

- Cryptography and Network Security (Principles and Practice) sixth edition, William Stallings, Pearson, 2013
- 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

Google Tradutor

AC-cifradores-20…	Julio López, Aug 29	v.2	⬇
fips-197.pdf (1157k)	Julio López, Aug 29	v.1	⬇
fm-MO422.pdf (307k	Julio López, Aug 7,	v.1	⬇
introducao-AC-42…	Julio López, Aug 7,	v.1	⬇

Comentários

Você não tem permissão para adicionar comentários.