MC938-MO422 Algoritmos Criptográficos:
https://sites.google.com/site/unicampjlopez/mc938

Programa:

-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.
-Aritmética de Curvas Elípticas
-Algoritmos criptográficos: RSA, DSA, ECDSA
-Algoritmos avançados: emparelhamentos bilineares, bibliotecas criptográficas, algoritmos de criptografiapos-quântica.
-Tópicos: geração de números pseudoaleatórios, implementação em software, algoritmos novos.
-Projetos--aspectos práticos e teóricos de algoritmos criptográficos

Aulas terças e quintas: 10:00-12:00

Provas:
Prova 1: 23 de Outubro 2014
Prova 2: 16 de Dezembro 2014
Exame: 13 de Janeiro de 2015

Referências:

[1] Modern Cryptography Primer, Czesław Kościelny, Mirosław Kurkowski, Marian Srebrny, 2013 http://link.springer.com/book/10.1007/978-3-642-41386-5
[2] Cryptography and Network Security (Principles and Practice) sixth edition, William Stallings, Pearson, 2013
[3 ] Modern Computer Arithmetic Richard P. Brent and Paul Zimmermann, 2010. http://arxiv.org/pdf/1004.4710v1.pdf
[4] Implementing SSL/TLS (using cryptography and PKI) Joshua Davies, Wiley Publishing , Inc., 2011
[5] Understanding Cryptography, Paar-Pelzl, 2010: http://link.springer.com/book/10.1007/978-3-642-04101-3/page/1
[6] Introduction to Modern Cryptography, Jonathan Katz e Yehuda Lindell, Chapman and Hall/CRC, 2014.

Outros Materiais:
CriptoRED: http://www.criptored.upm.es