## MCZB015-13 Introdução à Criptografia

**TPI 4-0-4**

**RECOMENDAÇÃO**: Matemática Discreta; Teoria Aritmética dos Números

**OBJETIVOS**:

**EMENTA**: Geradores pseudoaleatóreos. Cifras de fluxo. Cifras de bloco simétricas e modos de operação. Resumos criptográficos. Teoria dos Números e criptografia assimétrica. Autenticação de mensagens. Assinaturas digitais. Protocolos criptográficos.

**BIBLIOGRAFIA BÁSICA:**


KATZ, J.; LINDELL, Y. Introduction to Modern Cryptography. Boca Raton: Chapman&Hall/CRC, 2008.

MAO, W. Modern Cryptography: theory and practice. Upper Saddle River: Prentice Hall, 2004.

SANTOS, P. Introdução à Teoria dos Números. Rio de Janeiro: IMPA, 2010.

STINSON, D. Cryptography: theory and practice. Boca Raton: Chapman&Hall/CRC, 2006.

TALBOT, J.; WELSH, D. Complexity and Cryptography: an introduction. Cambridge: Cambridge University Press, 2006.

TRAPPE, W.; WASHINGTON, L. Introduction to Cryptography with coding theory. Upper Saddle River: Prentice Hall, 2006.


**BIBLIOGRAFIA COMPLEMENTAR:**


ANDREWS, G. Number Theory. New York: Dover Publications, 1994.

BALDONI, M.; CILIBERTO, C.; CATTANEO, G. Elementary Number Theory, Cryptography and Codes. Berlin-Heidelberg: Springer-Verlag, 2009.

BERNSTEIN, D.; BUCHMANN, J.; DAHMEN, E. Post-Quantum Cryptography. Berlin-Heidelberg: Springer-Verlag, 2009.

CATALANO, D. et al. Contemporary Cryptology. Basel: Birkhäuser, 2005.

CORMEN, L.; RIVEST, S. Algoritmos - Teoria e Prática. Rio de Janeiro: Campus, 2002.

DASGUPTA, S.; PAPADIMITRIOU, C. H.; VAZIRANI, U. V. Algoritmos. Porto Alegre: McGraw-Hill/Artmed, 2009.

GOLDREICH, O. Fundamentals of Cryptography, v. I: Basic Tools. Cambridge: Cambridge University Press, 2001.

GOLDREICH, O. Fundamentals of Cryptography, v. II: Basic Applications. Cambridge: Cambridge University Press, 2004.

HOFFSTEIN, J.; PIPHER, J.; SILVERMAN, J. H. An Introduction to Mathematical Cryptography. New York: Springer-Verlag, 2008.

SHOUP, V. A. Computational Introduction to Number Theory and Algebra. Cambridge: Cambridge University Press, 2005.

SIPSER, M. Introdução à Teoria da Computação. São Paulo: Thomson Learning, 2007.