Tópicos em Sistemas de Computação:
Criptografia e Criptanálise Contemporâneas

profª Denise Goya, denise.goya@ufabc.edu.br

Objetivos:

Ao final da disciplina o(a) estudante deverá ser capaz de: compreender segurança teórica e relacioná-la com requisitos, algoritmos e protocolos para uso em contexto prático; conhecer técnicas de criptanálise e compreender limitações teórica e técnica de abordagens criptográficas.

Ementa (12 créditos):

Algoritmos e protocolos criptográficos para os requisitos de confidencialidade, integridade e autenticidade. Modelos de segurança e Segurança demonstrável. Algoritmos criptográficos pós-quânticos. Encriptação homomórfica. Técnicas de criptanálise para criptografia simétrica e assimétrica.

Metodologia:

Aulas teóricas e expositivas; atividades práticas em laboratório individuais e colaborativas; análise de dissertações e teses para elaboração de artigo de revisão.

Bibliografia Básica:

Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*. 3.ed. Chapman & Hall / CRC Press, 2021. ISBN 9780815354369

Bernstein, D.J.; Buchmann, J.; Dahmen, E. (Ed.) *Post quantum cryptography*. Berlin, DEU: Springer, 2009. ISBN 9783540887010

Swenson, C. *Modern cryptanalysis: techniques for advanced code breaking*. Indianapolis, USA: Wiley Publishing, 2008. ISBN 9780470135938

Bibliografia Complementar:

Catalano, D.; Cramer, R.; Damgård, I.; Di Crescenzo, G.; Pointcheval, D.; Takagi, T. *Contemporary Cryptology*. Berlin: Verlag. 2005. ISBN 3-7643-7294-X

Mao, W. *Modern cryptography: theory and practice*. Upper Saddle River, USA: Prentice Hall, 2004. ISBN 9780130669438

Rothe, J. *Complexity theory and cryptology: an introduction to cryptocomplexity*. Berlin, DEU: Springer, 2005. ISBN 9783540221470

Joux, A. *Algorithmic cryptanalysis*. London, GBR: Chapman & Hall, 2009. ISBN 9781420070026

Acar, A.; Aksu, H.; Uluagac, A.S.; Conti, M. *A Survey on Homomorphic Encryption Schemes: Theory and Implementation*. ACM Comput. Surv. 51, 4, Article 79 (July 2019), 35 pages. https://doi.org/10.1145/3214303