Bibliografia II

Richard Crandall and Carl Pomerance.
Prime Numbers: A computacional Perspective.
Springer, 2ed edition, 2005.

Howard M. Heys.
A tutorial on linear and differential cryptanalysis.
Open access Web, 2015.
URL `https://ioactive.com/wp-content/uploads/2015/07/ldc_tutorial.pdf`.

Gareth A. Jones and J. Mary Jones.
Elementary Number Theory.
Springer London, 1998.
doi: 10.1007/978-1-4471-0613-5.

Brian Kernighan and Dennis Ritchie.
The C Programming Language.
Prentice Hall, 2nd edition, 1988.

Bibliografia III

Mitsuru Matsui.
Linear cryptanalysis method for DES cipher.
In *Advances in Cryptology — EUROCRYPT '93*, pages 386–397. Springer Berlin Heidelberg, 1994.
doi: 10.1007/3-540-48285-7_33.

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.
Handbook of Applied Cryptography.
CRC Press, 5th edition, 2001.

Pedro Quaresma.
Frequency analysis of the portuguese language.
CISUC-TR 2008-003, Centre for Informatics and Systems of the University of Coimbra, 2008.
ISSN 0874-338X.

Bibliografia IV

Pedro Quaresma and Elsa Lopes.
Criptografia.
Gazeta de Matemática, 154:7 – 11, Março 2008.

Pedro Quaresma and Augusto Pinho.
Análise de frequências da língua portuguesa.
In *Livro de Actas da Conferência Ibero-Americana InterTIC 2007*, pages 267–272. IASK, Dezembro 2007.

Pedro Quaresma and Augusto Pinho.
Criptoanálise.
Gazeta de Matemática, 157:22 – 31, 2009.

Hans Riesel.
Prime Numbers and Computer Methods for Factorization, volume 126 of *Progress in Mathematics*.
Birkh user, 2nd edition, 1994.

Bibliografia V

R. Rivest, A. Shamir, and L. Adleman.
A method for obtaining digital signatures and public-key cryptosystems.
Communications of the ACM, 21(2):120–126, 1978.

Pimenta Rodrigues, Pedro Pereira, and Manuela Sousa.
Programação em C++.
FCA, Editora de Informática LDA, 2 edition, 1998.

Richard Spillman.
Classical and Contemporary Cryptology.
Prentice Hall, 2005.

Douglas Stinson.
Cryptography: Theory and Practice.
Chapman & Hall/CRC, 3rd edition, 2006.

Bibliografia VI

Bjarne Stroustrup.
The C++ Programming Language.
Addison Wesley Longman, Inc., 1997.

Bjarne Stroustrup.
Programming: Principles and Practice Using C++.
Addison Wesley Longman, Inc., 2009.

Viktoria Tkotz.
CRIPTOGRAFIA - Segredos Embalados para Viagem.
NOVATEC Editora, São Paulo, Brasil, 2005.