

GUIA PRÁTICO DE CIFRAGEM MANUAL

APRENDA A ESCREVER MENSAGENS SECRETAS

Fred Ribeiro

Novatec

Copyright © 2017 da Novatec Editora Ltda.

Todos os direitos reservados e protegidos pela Lei 9.610 de 19/02/1998. É proibida a reprodução desta obra, mesmo parcial, por qualquer processo, sem prévia autorização, por escrito, do autor e da Editora.

Editor: Rubens Prates

Editoração eletrônica: Carolina Kuwabata

Capa: Carolina Kuwabata

ISBN: 978-85-7522-622-3

Histórico de impressões:

Novembro/2017 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110

02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

E-mail: novatec@novatec.com.br

Site: www.novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

Sumário

| | |
|---|-----------|
| Capítulo 1 ■ Introdução | 11 |
| Conceitos gerais | 11 |
| Segurança estratégica x segurança tática | 12 |
| Classificação de documentos | 13 |
| Dicas gerais de cifragem | 13 |
| Conversão de letras em números | 14 |
| Operação em módulo..... | 17 |
| Geração de números | 18 |
| Capítulo 2 ■ Esteganografia | 23 |
| Cifra nula | 23 |
| Cifra de Bacon | 24 |
| Grade de Cardano..... | 26 |
| Cifra de Fleissner | 28 |
| Capítulo 3 ■ Cifragem por transposição | 31 |
| Cifra da rota | 32 |
| Cifra do tabuleiro..... | 32 |
| Rasterschlüssel 44 (RS44) | 35 |
| Adaptação da RS44, a grade de sudoku | 39 |
| Dupla transposição | 40 |
| Capítulo 4 ■ Cifragem por substituição | 45 |
| Alfabeto Congo..... | 45 |
| Cifras hebraicas | 45 |
| Atbash..... | 45 |
| Albam (Rot13) | 46 |
| Atabah | 47 |
| Cifra de César..... | 47 |
| Cifra da palavra-chave | 48 |

| | |
|--|------------|
| Cifra de Vigenère | 49 |
| Cifra de Beaufort..... | 50 |
| Cifra da autochave | 51 |
| Cifra diagonal..... | 52 |
| Cifra Snake..... | 57 |
| Cifra do livro | 61 |
| Cifra de Playfair | 64 |
| Cifra dos quatro quadrados..... | 66 |
| Cifra dos dois quadrados..... | 67 |
| Cifra bífida | 69 |
| Cifra trífida..... | 71 |
| Cifra nihilista | 73 |
| Versão inicial | 73 |
| Versão avançada | 74 |
| Cifra de Vernam ou OTP..... | 75 |
| OTP de letras com Vigenère | 76 |
| OTP de letras com Nihilista | 77 |
| OTP de números..... | 78 |
| Capítulo 5 ■ Cifragem por substituição e transposição | 79 |
| Cifra ADFGVX..... | 79 |
| Cifra de Vic | 81 |
| Geração de números pseudoaleatórios | 81 |
| Substituição..... | 83 |
| Transposição | 84 |
| Cifra SECOM | 88 |
| Cifra prática..... | 88 |
| Cifra Peraí | 92 |
| Considerações finais | 98 |
| Bibliografia..... | 99 |
| Anexo | 101 |
| Apêndice..... | 102 |
| Entropia da chave | 102 |