

# Sumário

|   |           |
|---|-----------|
| <b>Agradecimentos</b> .....   | <b>7</b>  |
| <b>Sobre os Autores</b> .....   | <b>9</b>  |
| <b>Prefácio</b> .....   | <b>17</b> |
| <br>  |           |
| <b>Parte I – Conceitos Básicos de Criptografia, Software e Hardware</b> ..... | <b>19</b> |
| <b>Capítulo 1 – Conceitos de Segurança de Dados e Criptografia</b> .....      | <b>21</b> |
| 1.1 Criptografia .....  | 21        |
| 1.1.1 Breve História da Criptografia .....                                    | 22        |
| 1.1.2 A Importância da Criptografia .....                                     | 24        |
| 1.1.3 Alguns Termos Utilizados na Criptografia .....                          | 27        |
| 1.1.4 Algoritmos de Bloco e Fluxo .....                                       | 28        |
| 1.1.5 Vírus ou Informação Cifrada .....                                       | 29        |
| 1.2 Importância da Chave ou “Senha” .....                                     | 30        |
| 1.2.1 Como Gerar a Chave .....  | 33        |
| 1.2.2 Importância do Tamanho da Chave .....                                   | 33        |
| 1.3 Criptografia de Chaves Simétrica e Assimétrica .....                      | 37        |
| 1.4 Assinatura Digital .....  | 39        |
| 1.5 Considerações Finais .....  | 41        |
| <b>Capítulo 2 – Conceitos de Circuitos Programáveis FPGAs e VHDL</b> .....    | <b>43</b> |
| 2.1 Estrutura Interna de FPGA .....   | 43        |
| 2.2 Roteamento e Configuração de FPGA .....                                   | 45        |
| 2.3 VHDL – Descrição Estrutural e Comportamental.....                         | 46        |
| 2.4 Exemplo dos Estilos de Descrições em VHDL.....                            | 46        |
| 2.4.1 Descrição Algorítmica .....   | 47        |
| 2.4.2 Descrição de Fluxo de Dados .....                                       | 48        |
| 2.4.3 Descrição Estrutural .....  | 48        |
| 2.5 Elementos Sintáticos de VHDL .....  | 48        |
| 2.6 Operadores em VHDL .....  | 50        |
| 2.6.1 Operador de Concatenação .....  | 50        |
| 2.6.2 Operadores Aritméticos.....   | 50        |
| 2.6.3 Operadores Relacionais.....   | 50        |
| 2.6.4 Operadores Lógicos.....   | 50        |
| 2.7 Tipos de Dados em VHDL .....  | 50        |
| 2.7.1 Tipos Escalares.....  | 51        |
| 2.7.2 Tipos Compostos.....  | 51        |
| 2.8 Atributos em VHDL.....  | 52        |
| 2.9 Constantes, Variáveis e Sinais.....                                       | 53        |
| 2.9.1 Constantes .....  | 53        |
| 2.9.2 Variáveis .....   | 53        |
| 2.9.3 Sinais.....   | 53        |
| 2.10 Entidade e Arquitetura .....   | 54        |
| 2.10.1 Entidade (ENTITY).....   | 54        |

|  |            |
|--|------------|
| 2.10.2 Arquitetura (ARCHITECTURE).....                                 | 54         |
| 2.11 Componentes em VHDL.....  | 55         |
| 2.12 Pacotes em VHDL (Package).....                                    | 55         |
| 2.13 Configuração em VHDL (CONFIGURATION).....                         | 56         |
| 2.14 Procedimentos e Funções em VHDL.....                              | 57         |
| 2.15 Execução Concorrente em VHDL.....                                 | 57         |
| 2.16 Execução Seqüencial.....  | 58         |
| 2.16.1 Processo (PROCESS).....   | 58         |
| <b>Capítulo 3 – Exemplos de Circuitos em VHDL .....</b>                | <b>61</b>  |
| 3.1 Circuitos Combinacionais.....                                      | 61         |
| 3.2 Portas Lógicas Básicas.....  | 62         |
| 3.2.1 Porta AND.....   | 62         |
| 3.2.2 Porta OR.....  | 63         |
| 3.2.3 Porta NOT.....   | 64         |
| 3.2.4 Porta NAND.....  | 64         |
| 3.2.5 Porta NOR.....   | 65         |
| 3.2.6 Porta XOR.....   | 66         |
| 3.2.7 Porta XNOR.....  | 66         |
| 3.2.8 Estatísticas de Recursos Usados em FPGAs.....                    | 67         |
| 3.3 Multiplexadores e Demultiplexadores .....                          | 68         |
| 3.3.1 Multiplexador 2x1 – Códigos em VHDL.....                         | 69         |
| 3.3.2 Multiplexador 2x1 – Estatísticas em FPGAs.....                   | 70         |
| 3.4 Decodificadores.....   | 71         |
| 3.4.1 Decodificador 3x8 – Códigos em VHDL.....                         | 72         |
| 3.4.2 Decodificador 3x8 – Estatísticas em FPGAs.....                   | 74         |
| 3.5 Codificadores em VHDL e FPGAs.....                                 | 75         |
| 3.5.1 Codificador 8x3 – Códigos em VHDL.....                           | 76         |
| 3.5.2 Codificador 8x3 – Estatísticas em FPGAs.....                     | 77         |
| 3.6 Circuitos Combinacionais Aritméticos em VHDL.....                  | 78         |
| 3.6.1 Comparadores.....  | 78         |
| 3.6.2 Somadores e Subtratores.....                                     | 80         |
| 3.6.3 Multiplicadores.....   | 83         |
| 3.6.4 Divisores.....   | 85         |
| 3.6.5 Estatísticas de Circuitos Aritméticos em FPGAs.....              | 87         |
| <b>Capítulo 4 – ALPOS: Um Algoritmo Didático de Criptografia .....</b> | <b>89</b>  |
| 4.1 Conceitos e Exemplos.....  | 89         |
| 4.2 Descrição do Algoritmo.....  | 91         |
| 4.3 Implementação em C do ALPOS.....                                   | 93         |
| 4.4 Implementação em Hardware (VHDL).....                              | 94         |
| 4.5 Análise de Desempenho do ALPOS.....                                | 96         |
| 4.5.1 Desempenho em Software.....                                      | 96         |
| 4.5.2 Desempenho em Hardware.....                                      | 98         |
| 4.6 Criptoanálise.....   | 100        |
| 4.7 Considerações Finais.....  | 101        |
| <b>Capítulo 5 – Otimizações no ALPOS.....</b>                          | <b>103</b> |
| 5.1 Motivação.....   | 103        |
| 5.2 Criptografia Posicional Usando Blocos.....                         | 103        |

|  |            |
|--|------------|
| 5.3 Inclusão de Bits Aleatórios.....                                 | 104        |
| 5.4 Desempenho das Otimizações.....                                  | 106        |
| 5.4.1 Desempenho da Otimização em Blocos.....                        | 106        |
| 5.4.2 Desempenho da Otimização com Bits Aleatórios.....              | 107        |
| 5.5 Considerações Finais.....  | 108        |
| <b>Parte II – Algoritmos Clássicos de Criptografia.....</b>          | <b>111</b> |
| <b>Capítulo 6 – Algoritmo DES em Software e Hardware .....</b>       | <b>113</b> |
| 6.1 Breve Histórico do DES.....                                      | 113        |
| 6.2 Algoritmo DES.....   | 114        |
| 6.2.1 Chaves e Subchaves do DES.....                                 | 115        |
| 6.2.2 Processamento Principal.....                                   | 116        |
| 6.3 Exemplo Preliminar de Funcionamento do DES.....                  | 121        |
| 6.4 Segurança do DES.....  | 122        |
| 6.5 Implementação em C e VHDL.....                                   | 123        |
| 6.6 Estatísticas de Desempenho das Implementações do DES.....        | 127        |
| <b>Capítulo 7 – Algoritmo IDEA .....</b>                             | <b>131</b> |
| 7.1 Descrição do Algoritmo IDEA.....                                 | 131        |
| 7.2 Operações no IDEA.....   | 131        |
| 7.2.1 Geração das Subchaves.....                                     | 132        |
| 7.2.2 Processamento das Iterações.....                               | 132        |
| 7.3 Decriptografia.....  | 134        |
| 7.4 Implementação em C.....  | 134        |
| 7.5 Implementação de Otimizações.....                                | 138        |
| 7.6 Desempenho.....  | 138        |
| 7.7 Considerações Finais.....  | 139        |
| <b>Capítulo 8 – Algoritmo Assimétrico – RSA .....</b>                | <b>141</b> |
| 8.1 Introdução ao RSA.....   | 141        |
| 8.2 Exemplos de Funcionamento.....                                   | 142        |
| 8.3 Descrição do Algoritmo.....                                      | 144        |
| 8.4 Implementação em C.....  | 145        |
| 8.5 Exemplos de Funcionamento do Algoritmo Implementado em C.....    | 149        |
| 8.6 Implementação em Hardware (VHDL).....                            | 149        |
| 8.7 Desempenho do RSA.....   | 153        |
| 8.7.1 Desempenho em Software.....                                    | 153        |
| 8.7.2 Desempenho em Hardware.....                                    | 154        |
| 8.8. Considerações Finais.....                                       | 154        |
| <b>Capítulo 9 – Algoritmos Baseados em Hashing (MD5, SHA-1).....</b> | <b>157</b> |
| 9.1 Definição de MAC – Código de Autenticação de Mensagens.....      | 157        |
| 9.2 Algoritmo MD5.....   | 157        |
| 9.2.1 Implementação em C.....  | 160        |
| 9.2.2 Desempenho em Software.....                                    | 163        |
| 9.3 Algoritmo SHA-1.....   | 164        |
| 9.3.1 Implementação em C.....  | 166        |
| 9.3.2 Desempenho em Software.....                                    | 168        |

|  |            |
|--|------------|
| <b>Parte III – Algoritmos Modernos de Criptografia.....</b>              | <b>171</b> |
| <b>Capítulo 10 – Algoritmo AES (Rijndael) .....</b>                      | <b>173</b> |
| 10.1 Breve Histórico do Projeto AES.....                                 | 173        |
| 10.2 Funcionamento do AES/Rijndael.....                                  | 174        |
| 10.2.1 Corpo $GF(2^8)$ .....   | 174        |
| 10.2.2 Estrutura do Algoritmo AES.....                                   | 176        |
| 10.2.3 Operações por Iteração.....                                       | 177        |
| 10.2.4 Geração de Subchaves.....   | 181        |
| 10.3 Algoritmo de Cifragem do AES.....                                   | 182        |
| 10.4 Algoritmo de Decifragem do AES.....                                 | 183        |
| 10.5 Estatísticas de Desempenho das Implementações.....                  | 186        |
| 10.6 Considerações Finais.....   | 188        |
| <b>Capítulo 11 – Algoritmo RC5 em Software e Hardware .....</b>          | <b>189</b> |
| 11.1 Introdução.....   | 189        |
| 11.2 Parâmetros do RC5.....  | 190        |
| 11.3 Operações Básicas do RC5.....                                       | 190        |
| 11.4 Geração de Subchaves do RC5.....                                    | 191        |
| 11.4.1 Algoritmo de Subchaves RC5.....                                   | 191        |
| 11.5 Algoritmos de Cifragem e Decifragem do RC5.....                     | 192        |
| 11.5.1 Algoritmo de Cifragem RC5.....                                    | 192        |
| 11.5.2 Algoritmo de Decifragem RC5.....                                  | 193        |
| 11.6 Algoritmo RC5-64.....   | 193        |
| 11.7 Estatísticas de Desempenho do RC5.....                              | 193        |
| <b>Capítulo 12 – AES – Outros Candidatos.....</b>                        | <b>195</b> |
| 12.1 Motivação para um Novo Padrão de Criptografia Simétrica.....        | 195        |
| 12.2 Critérios para o Projeto AES.....                                   | 196        |
| 12.2.1 Áreas de Aplicação.....   | 196        |
| 12.2.2 Plataformas.....  | 196        |
| 12.2.3 Exigências Adicionais.....  | 197        |
| 12.2.4 Decisões de Projeto.....  | 197        |
| 12.2.5 Processamento de Blocos.....                                      | 198        |
| 12.3 Comparação dos Candidatos ao AES.....                               | 199        |
| <b>Parte IV – Ferramentas e Dispositivos Modernos de Segurança .....</b> | <b>203</b> |
| <b>Capítulo 13 – Bibliotecas Criptográficas em Software .....</b>        | <b>205</b> |
| 13.1 Motivação.....  | 205        |
| 13.2 Bibliotecas Modernas de Criptografia.....                           | 206        |
| 13.2.1 Biblioteca OpenSSL.....   | 206        |
| 13.2.2 Biblioteca CryptoAPI.....   | 208        |
| 13.2.3 Biblioteca JCA.....   | 209        |
| 13.3 Alguns Dados de Desempenho.....                                     | 214        |
| 13.3.1 Ambiente de Teste.....  | 214        |
| 13.3.2 Testes Preliminares.....  | 215        |
| 13.4 Considerações Finais.....   | 220        |

|  |            |
|--|------------|
| <b>Capítulo 14 – Hardware Especializado em Segurança .....</b>                               | <b>221</b> |
| 14.1 Criptoprocessadores.....  | 221        |
| 14.1.1 Criptoprocessador DSRCP .....   | 222        |
| 14.1.2 Processadores de Segurança da Motorola .....  | 224        |
| 14.1.3 Características das Arquiteturas e Desempenho.....                                    | 226        |
| 14.2 Processadores de Rede com Segurança .....   | 227        |
| 14.2.1 Conceitos de NPs .....  | 227        |
| 14.2.2 Arquitetura dos Sistemas de Segurança com NPs .....                                   | 231        |
| 14.2.3 Processador IXP 2800 .....  | 233        |
| 14.3 Co-processador IBM 4758 .....   | 236        |
| 14.4 Smart Cards .....   | 237        |
| 14.5 HSM .....   | 238        |
| 14.6 Considerações Finais.....   | 238        |
| <b>Capítulo 15 – Arquitetura e Implementação de um Criptoprocessador VLIW em FPGAs .....</b> | <b>239</b> |
| 15.1 Introdução .....  | 239        |
| 15.2 Arquitetura do Criptoprocessador VLIW .....   | 242        |
| 15.3 Conjunto de Instruções.....   | 245        |
| 15.3.1 Formato das Instruções.....   | 246        |
| 15.3.2 Instruções Exclusivas.....  | 247        |
| 15.3.3 Instruções de Propósito Geral .....   | 249        |
| 15.3.4 Instruções Especiais .....  | 249        |
| 15.4 Pipeline do Criptoprocessador VLIW.....   | 256        |
| 15.5 Estatísticas de Desempenho do Criptoprocessador VLIW .....                              | 258        |
| <b>Capítulo 16 – Desempenho do Criptoprocessador .....</b>                                   | <b>261</b> |
| 16.1 Implementação do Algoritmo DES .....  | 261        |
| 16.2 Minimização do Impacto da Dependência de Dados do DES – Loop Pipelining .....           | 264        |
| 16.3 Implementação do Algoritmo RC5.....   | 268        |
| 16.4 Implementação da S-BOX do AES.....  | 269        |
| 16.5 Interface em Hardware para Teste do Criptoprocessador VLIW .....                        | 270        |
| <b>Capítulo 17 – WebCry – Uma Ferramenta Didática de Criptografia na WEB.....</b>            | <b>273</b> |
| 17.1 Motivação.....  | 273        |
| 17.2 Apresentação da Ferramenta .....  | 273        |
| 17.3 Guia para Usuários e Leitores.....  | 274        |
| 17.4 Exemplo de Funcionamento .....  | 275        |
| 17.5 Considerações Finais .....  | 278        |
| <b>Apêndice A – Referências Bibliográficas .....</b>   | <b>279</b> |
| Bibliografia Recomendada.....  | 284        |
| <b>Índice Remissivo .....</b>  | <b>287</b> |