

SZCZEGÓŁOWY SPIS TREŚCI

SŁOWO WSTĘPNE XV

WPROWADZENIE XVII

Stosowane podejście XVIII

Dla kogo jest ta książka XVIII

Układ książki XIX

Podstawy XIX

Szyfry symetryczne XIX

Szyfry asymetryczne XIX

Zastosowania XX

Podziękowania XX

SKRÓTY XXI

1. SZYFROWANIE 1

Podstawy 2

Szyfry klasyczne 2

Szyfr Cezara 2

Szyfr Vigenère'a 3

Jak działają szyfry 4

Permutacja 5

Tryb działania 6

Dlaczego szyfry klasyczne nie są bezpieczne 6

Idealne szyfrowanie – klucz jednorazowy 7

Szyfrowanie za pomocą klucza jednorazowego 8

Dlaczego szyfr z kluczem jednorazowym jest bezpieczny? 9

Bezpieczeństwo szyfrowania 10

Modele ataku	11
Cele bezpieczeństwa	13
Kategoria bezpieczeństwa	14
Szyfrowanie asymetryczne	16
Gdy szyfry robią więcej niż szyfrowanie	17
Szyfrowanie z uwierzytelnianiem	17
Szyfrowanie zachowujące format	18
Szyfrowanie w pełni homomorficzne	18
Szyfrowanie przeszukiwalne	19
Szyfrowanie dostrajalne	19
Co może pójść źle	20
Słaby szyfr	20
Niewłaściwy model	20
Inne źródła	21
2. LOSOWOŚĆ	23
Losowy czy nie losowy?	24
Losowość jako rozkład prawdopodobieństwa	24
Entropia – miara niepewności	25
Generatory liczb losowych (RNG) i generatory liczb pseudolosowych (PRNG)	26
Jak działa generator PRNG	28
Kwestie bezpieczeństwa	28
Fortuna PRNG	29
PRNG kryptograficzne i niekryptograficzne	30
Bezużyteczność testów statystycznych	32
Generatory liczb pseudolosowych w praktyce	32
Generowanie bitów losowych w systemach opartych na Uniksie	33

Funkcja CryptGenRandom() w systemie Windows 36

PRNG oparty na sprzęcie – RDRAND w mikroprocesorach Intel 37

Co może pójść źle 38

Słabe źródła entropii 38

Niewystarczająca entropia przy rozruchu 39

PRNG niekryptograficzne 40

Błąd próbkowania z silną losowością 40

Inne źródła 41

3. BEZPIECZEŃSTWO KRYPTOGRAFICZNE 43

Definiowanie niemożliwego 44

Bezpieczeństwo w teorii – bezpieczeństwo informacyjne 44

Bezpieczeństwo w praktyce – bezpieczeństwo obliczeniowe 44

Szacowanie bezpieczeństwa 46

Mierzenie bezpieczeństwa w bitach 46

Koszt pełnego ataku 47

Wybór i ocena poziomu bezpieczeństwa 49

Uzyskiwanie bezpieczeństwa 50

Bezpieczeństwo możliwe do udowodnienia 50

Bezpieczeństwo heurystyczne 53

Generowanie kluczy 54

Generowanie kluczy symetrycznych 54

Generowanie kluczy asymetrycznych 55

Ochrona kluczy 56

Co może pójść źle 57

Niepoprawny dowód bezpieczeństwa 57

Krótkie klucze do obsługi poprzednich wersji 57

Inne źródła 58

4. SZYFRY BLOKOWE 59

Czym jest szyfr blokowy? 60

 Cele bezpieczeństwa 60

 Rozmiar bloku 60

 Ataki książki kodowej 61

Jak budować szyfry blokowe 62

 Rundy szyfru blokowego 62

 Atak ślizgowy i klucze rundowe 62

 Sieci podstawieniowo-permutacyjne 63

 Sieć Feistela 64

Advanced Encryption Standard (AES) 65

 Wnętrze AES 65

 AES w działaniu 68

Implementacja AES 69

 Implementacje oparte na tablicach 69

 Instrukcje natywne 70

 Czy szyfr AES jest bezpieczny? 71

Tryby działania 72

 Tryb elektronicznej książki kodowej (ECB) 72

 Tryb CBC (Cipher Block Chaining) 74

 Jak szyfrować dowolny komunikat w trybie CBC 76

 Tryb licznika (CTR) . 77

Co może pójść źle 79

 Ataki typu meet-in-the-middle 80

 Ataki typu padding oracle 81

Inne źródła 82

5. SZYFRY STRUMIENIOWE 83

Jak działają szyfry strumieniowe 84

Szyfry strumieniowe stanowe i oparte na liczniku 85

Szyfry strumieniowe zorientowane na sprzęt 86

Rejestry przesuwające ze sprzężeniem zwrotnym 87

Grain-128a 93

A5/1 95

Szyfry strumieniowe zorientowane na oprogramowanie 98

RC4 99

Salsa20 103

Co może pójść źle 108

Ponowne użycie wartości jednorazowej 108

Złamana implementacja RC4 109

Słabe szyfry wbudowane w sprzęt 110

Inne źródła 111

6. FUNKCJE SKRÓTU 113

Bezpieczne funkcje skrótu 114

Ponownie nieprzewidywalność 115

Odporność na przeciwobraz 115

Odporność na kolizje 117

Znajdowanie kolizji 118

Budowa funkcji skrótu 120

Funkcje skrótu oparte na kompresji – struktura Merkle'a–Damgåarda 120

Funkcje skrótu oparte na permutacji – funkcje gąbkowe 123

Rodzina funkcji skrótu SHA 125

SHA-1 125

SHA-2 128

Konkurencja ze strony SHA-3 129

Keccak (SHA-3) 130

Funkcja skrótu BLAKE2 132

Co może pójść źle 134

Atak przez zwiększenie długości 134

Oszukiwanie protokołów uwiarygodniania pamięci 135

Inne źródła 135

7. FUNKCJE SKRÓTU Z KLUCZEM 137

MAC (Message Authentication Codes) 138

MAC w bezpiecznej łączności 138

Fałszerstwa i ataki z wybranym tekstem jawnym 138

Ataki powtórzeniowe 139

Funkcje pseudolosowe PRF 139

Bezpieczeństwo PRF 140

Dlaczego funkcje PRF są silniejsze od MAC? 140

Tworzenie skrótów z kluczem na podstawie skrótów bez klucza 141

Konstrukcja z tajnym prefiksem 141

Struktura z tajnym sufiksem 142

Struktura HMAC 142

Ogólny atak na kody MAC oparte na funkcjach skrótu 143

Tworzenie skrótów z kluczem na podstawie szyfrów blokowych – CMAC 144

Łamanie CBC-MAC 145

Naprawa CBC-MAC 145

Dedykowane konstrukcje MAC 146

Poly1305 147

SipHash 150

Co może pójść źle 152

Ataki czasowe na weryfikację MAC 152

Gdy gąbki przeciekają 154

Inne źródła 154

8. SZYFROWANIE UWIERZYTELNIONE 157

Szyfrowanie uwierzytelnione z wykorzystaniem MAC 158

Szyfrowanie i MAC 158

MAC, a potem szyfrowanie 159

Szyfrowanie, a potem MAC 160

Szyfry uwierzytelnione 160

Szyfrowanie uwierzytelnione z powiązanymi danymi 161

Unikanie przewidywalności z wartościami jednorazowymi 162

Co składa się na dobry szyfr uwierzytelniony? 162

AES-GCM – standard szyfru uwierzytelnionego 164

Wnętrze GCM – CTR i GHASH 165

Bezpieczeństwo GCM 166

Skuteczność GCM 167

OCB – uwierzytelniony szyfr szybszy niż GCM 168

Wnętrze OCB 168

Bezpieczeństwo OCB 169

Wydajność OCB 169

SIV – najbezpieczniejszy uwierzytelniany szyfr? 170

AEAD oparty na permutacjach 170

Co może pójść źle 172

AES-GCM i słabe klucze mieszające 172

AES+GCM i małe znaczniki 174

Inne źródła 175

9. TRUDNE PROBLEMY 177

Trudność obliczeniowa 178

Pomiar czasu wykonania 178

Czas wielomianowy a superwielomianowy 180

Klasy złożoności 182

Niedeterministyczny czas wielomianowy 183

Problemy NP-zupełne 183

Problem P kontra NP 185

Problem rozkładu na czynniki 186

Rozkład dużej liczby na czynniki w praktyce 187

Czy rozkład na czynniki jest NP-zupełny? 188

Problem logarytmu dyskretnego 189

Czym jest grupa? 189

Trudność 190

Co może się pójść źle 191

Gdy rozkład na czynniki jest łatwy 191

Małe trudne problemy nie są trudne 192

Inne źródła 194

10. RSA 195

Matematyka kryjąca się za RSA 196

Permutacja z zapadką w RSA 197

Generowanie klucza RSA a bezpieczeństwo 198

Szyfrowanie za pomocą RSA 199

 łamanie złamania podręcznikowego szyfrowania RSA 200

 Silne szyfrowanie RSA – OAEP 200

Podpisywanie za pomocą RSA 202

 łamanie podpisów podręcznikowego RSA 203

 Standard podpisu PSS 203

 Podpisy ze skrótem pełnodomenowym 205

Implementacje RSA 206

 Szybki algorytm potęgowania – podnoszenie do kwadratu i mnożenie 206

 Małe wykładniki w celu szybszego działania klucza publicznego 208

 Chińskie twierdzenie o resztach 210

Co może pójść źle 211

 Atak Bellcore na RSA-CRT 212

 Współdzielenie prywatnych wykładników lub modulo 212

Inne źródła 214

11. DIFFIE–HELLMAN 217

Funkcja Diffiego–Hellmana 218

Problemy z protokołami Diffiego–Hellmana 220

 Problem obliczeniowy Diffiego–Hellmana 220

 Problem decyzyjny Diffiego–Hellmana 221

 Więcej problemów z Diffiem–Hellmanem 221

Protokoły uzgadniania klucza 222

 Przykład uzgadniania kluczy różny od DH 222

 Modele ataku dla protokołów uzgadniania klucza 223

 Wydajność 225

Protokoły Diffiego–Hellmana 225

Anonimowy Diffie–Hellman 225

Uwierzytelniony Diffie–Hellman 227

Protokół MQV (Menezes–Qu–Vanstone) 229

Co może pójść źle 231

Brak skrótu współdzielonego klucza 231

Przestarzały Diffie–Hellman w TLS 232

Parametry grupy, które nie są bezpieczne 232

Inne źródła 232

12. KRZYWE ELIPTYCZNE 235

Czym jest krzywa eliptyczna? 236

Krzywe eliptyczne na liczbach całkowitych 237

Dodawanie i mnożenie punktów 239

Grupy krzywych eliptycznych 242

Problem ECDLP 243

Uzgadnianie klucza Diffiego–Hellmana na krzywych eliptycznych 244

Generowanie podpisu ECDSA 245

Szyfrowanie z wykorzystaniem krzywych eliptycznych 247

Wybór krzywej 248

Krzywe NIST 249

Curve25519 249

Inne krzywe 250

Co może pójść źle 250

ECDSA z nieodpowiednią losowością 250

Złamanie ECDSA za pomocą innej krzywej 251

Inne źródła 252

13. TLS 253

Docelowe aplikacje i wymagania 254

Zestaw protokołów TLS 255

Rodzina protokołów TLS i SSL – krótka historia 255

TLS w pigułce 256

Certyfikaty i centra certyfikacji 256

Protokół rekordu 259

Protokół TLS Handshake 260

Algorytmy kryptograficzne w TLS 1.3 262

Ulepszenia w TLS 1.3 w porównaniu z TLS 1.2 263

Ochrona przed aktualizacją wsteczną 263

Pojedyncze obustronne uzgadnianie 264

Wznowienie sesji 264

Siła bezpieczeństwa TLS 265

Uwierzytelnienie 265

Poufność w przód 265

Co może pójść źle 266

Naruszenie bezpieczeństwa centrum certyfikacji 266

Naruszenie bezpieczeństwa serwera 267

Naruszenie bezpieczeństwa klienta 267

Błędy w implementacji 268

Inne źródła 268

14. KRYPTOGRAFIA KWANTOWA I POSTKWANTOWA 271

Jak działają komputery kwantowe 272

Bity kwantowe 273

Bramki kwantowe	275
Przyspieszenie kwantowe	278
Przyspieszenie wykładnicze i algorytm Simona	278
Zagrożenie ze strony algorytmu faktoryzacji Shora	279
Algorytm Shora rozwiązuje problem rozkładu na czynniki	280
Algorytm Shora i problem logarytmu dyskretnego	280
Algorytm Grovera	281
Dlaczego tak trudno jest zbudować komputer kwantowy?	282
Postkwantowe algorytmy szyfrowania	283
Kryptografia oparta na kodach korekcyjnych	284
Kryptografia oparta na kratkach	285
Kryptografia wielu zmiennych	286
Kryptografia oparta na funkcjach skrótów	287
Co może pójść źle	288
Niejasny poziom bezpieczeństwa	288
Szybko do przodu – co się stanie, jeśli będzie za późno?	289
Problemy implementacji	290
Inne źródła	290
SKOROWIDZ	293