

Spis treści j

O autorze.....	11
O korektorze merytorycznym.....	12
Wprowadzenie.....	13

CZĘŚĆ 1. Krótka historia i zarys kryptografii

ROZDZIAŁ 1

Pierwsze kroki w kryptografii.....	19
Krótkie wprowadzenie do kryptografii.....	19
Liczby systemu dwójkowego, kod ASCII i notacje.....	23
Wielkie twierdzenie Fermata, liczby pierwsze i arytmetyka modułarna.....	25
Krótka historia kryptografii i ogólne omówienie algorytmów kryptograficznych	30
Kamień z Rosetty.....	30
Szyfr Cezara.....	31
ROT13.....	34
Szyfr Beale'a.....	35
Szyfr Vernama.....	42
Uwagi dotyczące bezpieczeństwa i mocy obliczeniowej.....	44
Podsumowanie.....	48

CZĘŚĆ 2. Kryptografia klasyczna (szyfrowanie symetryczne i asymetryczne)

ROZDZIAŁ 2

Wprowadzenie do szyfrowania symetrycznego.....	51
Notacje i operacje w logice boolowskiej.....	52
Rodzina algorytmów DES.....	56
Simple DES.....	57
DES.....	63
Triple DES.....	73
DESX.....	74

AES Rijndael.....	75
Ogólne omówienie algorytmu AES.....	76
Ataki na AES i luki w zabezpieczeniach tego algorytmu.....	80
Podsumowanie.....	85

ROZDZIAŁ 3

Szyfrowanie asymetryczne.....	86
Wprowadzenie do szyfrowania asymetrycznego.....	86
Pionierzy.....	88
Algorytm Diffiego-Hellmana.....	89
Logarytm dyskretny.....	91
Wyjaśnienie algorytmu D-H.....	93
Analiza algorytmu.....	95
Kryptoanaliza algorytmu D-H i potencjalnych ataków na niego.....	95
RSA.....	95
Omówienie algorytmu RSA.....	98
Analiza RSA.....	99
Konwencjonalne ataki na algorytm RSA.....	101
Zastosowanie algorytmu RSA do weryfikacji przestrzegania umów międzynarodowych.....	101
Ataki niekonwencjonalne.....	105
PGP.....	108
Algorytm ElGamal.....	109
Podsumowanie.....	112

ROZDZIAŁ 4

Wprowadzenie do funkcji skrótu i podpisów cyfrowych.....	113
Ogólne omówienie funkcji skrótu.....	114
Ogólne omówienie najważniejszych algorytmów generowania skrótu.....	117
Logika i notacje używane podczas implementacji funkcji skrótu.....	118
Omówienie algorytmu SHA-1.....	123
Uwagi i przykład SHA-1.....	126
Uwierzytelnianie i podpis cyfrowy.....	129
Podpis cyfrowy w RSA.....	131
Podpis cyfrowy i algorytm ElGamal.....	135
Podpis ślepy.....	138
Podsumowanie.....	142

CZĘŚĆ 3. Protokoły i algorytmy nowej kryptografii

ROZDZIAŁ 5

Wprowadzenie do protokołów z wiedzą zerową	145
Najważniejsze zastosowanie protokołu o wiedzy zerowej: jaskinia cyfrowa	146
Nieinteraktywny protokół o wiedzy zerowej	148
Interaktywny protokół o wiedzy zerowej Schnorra	154
Wprowadzenie do zk-SNARK — upiorna matematyka księżycowa	158
zk-SNARK w kryptowalucie Zcash	163
Jednorundowy protokół o wiedzy zerowej	169
ZK13 — protokół o wiedzy zerowej do uwierzytelniania i przekazywania klucza	172
Podsumowanie	178

ROZDZIAŁ 6

Nowe algorytmy w kryptografii klucza prywatnego i publicznego	179
Geneza algorytmu MB09	180
Wprowadzenie do algorytmu MB09	184
Omówienie systemu MB09	187
Wprowadzenie do algorytmu MBX1	194
Przykład liczbowy zastosowania algorytmu MBX1	197
Niekonwencjonalne ataki na RSA	200
Podpisy cyfrowe w MBX1	207
Metoda bezpośredniego podpisu cyfrowego w MBX1	209
Metoda podpisu cyfrowego z załącznikiem w MBX1	211
Matematyczne aspekty podpisu cyfrowego w algorytmie MBX1	212
Ewolucja algorytmów MB09 i MBX1 — wprowadzenie do MBXX	215
Omówienie protokołu MBXX	218
Podsumowanie	224

ROZDZIAŁ 7

Krzywe eliptyczne	226
Ogólne omówienie krzywych eliptycznych	227
Operacje na krzywych eliptycznych	227
Mnożenie skalarne	232
Implementacja algorytmu Diffiego-Hellmana w krzywych eliptycznych	235

Krzywa eliptyczna secp256k1 — podpis cyfrowy bitcoina.....	240
Krok 1. Generowanie kluczy.....	242
Krok 2. Podpis cyfrowy w secp256k1.....	242
Krok 3. Weryfikacja podpisu cyfrowego.....	243
Przykład liczbowy dotyczący podpisu cyfrowego i krzywej secp256k1.....	244
Ataki na ECDSA i bezpieczeństwo krzywych eliptycznych.....	248
Krok 1. Odkrycie losowo wybranego klucza, [k].....	248
Krok 2. Odtworzenie klucza prywatnego, [d].....	249
Rozważania o przyszłości kryptografii krzywych eliptycznych.....	251
Podsumowanie.....	252

ROZDZIAŁ 8

Kryptografia kwantowa.....	253
Wprowadzenie do mechaniki kwantowej i kryptografii kwantowej.....	253
Eksperyment myślowy pomocny w zrozumieniu elementów	
mechaniki kwantowej.....	256
Krok 1. Superpozycja.....	256
Krok 2. Nieoznaczoność.....	258
Krok 3. Spin i splątanie.....	259
Kryptografia kwantowa.....	262
Przekazywanie klucza kwantowego — BB84.....	266
Krok 1. Inicjalizacja kanału kwantowego.....	267
Krok 2. Przekazywanie fotonów.....	268
Krok 3. Określenie klucza współdzielonego.....	268
Potencjalne ataki i problemy techniczne.....	270
Obliczenia kwantowe.....	274
Algorytm faktoryzacji Shora.....	277
Krok 1. Inicjalizacja kubitów.....	279
Krok 2. Losowy wybór liczby — a	279
Krok 3. Pomiar kwantowy.....	280
Krok 4. Znalezienie właściwego kandydata — (r)	281
Kwantowa transformacja Fouriera.....	282
Krok 5. Rozkład na czynniki (n)	286
Uwagi dotyczące algorytmu faktoryzacji Shora.....	287
Kryptografia postkwantowa.....	287
Podsumowanie.....	288

CZĘŚĆ 4. Szyfrowanie homomorficzne i silnik CSE

ROZDZIAŁ 9

Silnik Crypto Search Engine.....	293
Wprowadzenie do CSE — homomorfizm.....	294
Częściowy homomorfizm w algorytmie RSA.....	296
Analiza szyfrowania homomorficznego i jego implikacje.....	299
Matematyka i logika kryjące się za silnikami wyszukiwania.....	301
Wprowadzenie do drzew w teorii grafów.....	306
Kod Huffmana.....	308
Skrót i logika boolowska.....	310
Omówienie silnika CSE.....	312
Innowacje w silniku CSE.....	313
Analiza mocy obliczeniowej w silniku CSE.....	317
Przykład złamania szyfrowania za pomocą techniki brute force.....	319
Zastosowania silnika CSE.....	321
Podsumowanie.....	324