

Spis treści

Rozdział 1. Wprowadzenie	1
Jak korzystać z tej książki	5
Rozdział 2. Zrozumieć kryptografię	9
Wprowadzenie	9
Podstawowe koncepcje	9
Rozdział 3. Historyczne algorytmy: proste przykłady	21
Wprowadzenie	21
Szyfr Cezara	22
Proste szyfry podstawieniowe	28
Statystyki języka angielskiego	33
Szyfr Playfaira	37
Szyfrowanie homofoniczne	40
Szyfry polialfabetyczne	43
Szyfr Vigenère'a	44
Szyfry transpozycyjne	52
Superszyfrowanie	54
Kilka wniosków	55
Dodatek	56

Rozdział 4. Szyfry nie do złamania?	61
Wprowadzenie	61
Poufność doskonała	63
Szyfr z kluczem jednorazowym	66
Rozdział 5. Współczesne algorytmy	71
Wprowadzenie	71
Ciągi bitów	71
Szyfry strumieniowe	74
Szyfry blokowe (tryb ECB)	78
Funkcje skrótu	82
Systemy z kluczem publicznym	84
Rozdział 6. Bezpieczeństwo w praktyce	89
Wprowadzenie	89
Realistyczne bezpieczeństwo	91
Wyczerpujące poszukiwania klucza w praktyce	93
Ataki na systemy z kluczem publicznym	97
Rozdział 7. Zastosowania kryptografii	101
Wprowadzenie	101
Zastosowanie algorytmów symetrycznych	
dla zapewnienia poufności	104
Uwierzytelnienie	109
Zastosowanie algorytmów symetrycznych	
w celu uwierzytelnienia i zapewnienia	
integralności danych	110
Podpisy cyfrowe	113
Urzędy certyfikacji	117
Infrastruktura Klucza Publicznego	121
Potrzeba zaufania	123

Rozdział 8. Zarządzanie kluczami	127
Wprowadzenie	127
Cykl życia klucza	128
Generowanie klucza	129
Dystrybucja i przechowywanie klucza	130
Ustalanie klucza	133
Zastosowania klucza	134
Zmiana kluczy	137
Niszczenie klucza	137
Hierarchie kluczy	138
Zarządzanie kluczami w sieciach	140
Wykorzystanie zaufanego centrum zarządzania	141
Odzyskiwanie klucza i jego kopie zapasowe	143
Rozdział 9. Kryptografia w życiu codziennym	147
Wprowadzenie	147
Wyplacanie gotówki z bankomatu	147
Płatna telewizja	149
PGP – całkiem niezła prywatność	150
PGP keys	152
Encrypt	153
Sign	153
Encrypt and Sign	153
Bezpieczne przeglądanie sieci	153
Wykorzystanie telefonu komórkowego GSM	155
Bibliografia i dalsze lektury	159
Skorowidz	163