

SPIS TREŚCI

Słowo wstępne	xv
Wprowadzenie	xvii
Skróty	xxi
Rozdział 1: Szyfrowanie	1
Rozdział 2: Losowość	23
Rozdział 3: Bezpieczeństwo kryptograficzne	43
Rozdział 4: Szyfry blokowe	59
Rozdział 5: Szyfry strumieniowe	83
Rozdział 6: Funkcje skrótu	113
Rozdział 7: Funkcje skrótu z kluczem	137
Rozdział 8: Szyfrowanie uwierzytelnione	157
Rozdział 9: Trudne problemy	177
Rozdział 10: RSA	195
Rozdział 11: Diffie–Hellman	217
Rozdział 12: Krzywe eliptyczne	235
Rozdział 13: TLS	253
Rozdział 14: Kryptografia kwantowa i postkwantowa	271
Skorowidz	293