Spis rozdziałów

Przedmowa 6

Spis oznaczeń 8

1. Podstawowe pojęcia kryptograficzne i szyfry klasyczne 11

2. Podzielność i kongruencje 36

3. Liczby pierwsze, pseudopierwsze i testowanie pierwszości 95

4. Grupy skończone 117

5. Pierścienie przemienne z jedynką 152

6. Ciała skończone 161

7. Wielomiany o współczynnikach w ciele skończonym 171

8. Szyfry z kluczem publicznym 177

9. Szyfry z kluczem prywatnym 195

10. Uwierzytelnianie 217

11. Funkcje skrótu 222

12. Dzielenie tajemnic 230

13. Efektywna implementacja algorytmów kryptograficznych 233

14. Zagadnienia probabilistyczne w kryptografii 249

Literatura 264