

Obsah

Úvod	5
1. Abychom si rozuměli...	9
Základní pojmy	11
Opakování definic a základních pojmů	22
Základní rozdělení klasických šifrových systémů	24
Rozdělení substitučních šifer	25
2. Přehled klasických šifrových systémů	29
Polyalfabetické šifry	43
Jednoduchá transpozice	57
Úhlopříčkově-sloupcová transpozice	63
Další transpoziční systémy	67
Zlomkový šifrovací systém	70
Kombinované klasické šifry	80
Steganografické metody	85
Neviditelné inkousty	89
3. Šifry, které nikdy skutečnými šiframi nebyly	95
Transpoziční systémy	96
Jednoduchá záměna	100
Jednoduché steganografické textové metody	118
4. Klíče a hesla	123
Klíče	125
Hesla	127
5. Důležitá data a mezníky v dějinách kryptologie	133
6. Příklady	197
7. Literatura	213
8. Rejstřík	219
Jmenný rejstřík	220
Věcný rejstřík	224