

## Kapitola 1

# Obsah

## Úvod do problematiky bezpečnosti informačních technologií

1	Úvod do problematiky bezpečnosti informačních technologií	4
2	Matematický background	6
3	Úvod do kryptografie	8
4	Symetrická kryptografie	10
5	Asymetrická kryptografie	12
6	Kryptografické hashovací funkce	14
7	Kryptografie na bázi eliptických křivek	16
8	Náhodné a pseudonáhodné generátory	18
9	Autentizace	20
10	Digitální podpis a certifikáty	22
11	Počítačové viry	24
12	Principy firewallů	26