

OBSAH

Předmluva	6
Úvod	9
Teoretická část	11
1. Algebraické struktury	13
1.1 Definice základních pojmů	13
1.2 Algebraické struktury s jednou binární operací	18
1.3 Algebraické struktury se dvěma binárními operacemi	22
2. Konečné pole	28
2.1 Základy modulární aritmetiky	28
2.2 Modulární sčítání	40
2.3 Modulární násobení	49
2.4 Výpočet modulární multiplikační inverze	56
2.5 Konečné pole	81
Praktická část	115
3. Šifra Advanced Encryption Standard	116
3.1 Historie AES	116
3.2 Základní popis šifry AES	116
3.3 Matematika	117
3.4 Vnitřní struktura šifry AES	117
3.5 Postup šifrování	118
3.6 Postup dešifrování	121
3.7 Příklad na šifrování pomocí AES	123
4. Šifra RSA	126
4.1 Historie RSA	126
4.2 Rozdíly mezi symetrickou a asymetrickou kryptografií	126
4.3 Matematika, kameny bezpečnosti a délky klíčů	126
4.4 Šifrování a dešifrování	127
4.5 Odvození klíčů	128
4.6 Příklad šifrování	128
5. Aritmetika eliptických křivek	131
5.1 Rovnice eliptické křivky	131
5.2 Konstrukce eliptických křivek	133
5.3 Negace bodu na eliptické křivce	141
5.4 Operace sčítání na eliptické křivce $P + Q = R$	141
5.5 Operace sčítání na eliptické křivce $P + P = 2P = R$	148
5.6 Operace násobení bodu skalárem	152
5.7 Ukázka použití aritmetiky eliptických křivek	154
5.8 Problematika aritmetiky eliptických křivek nad \mathbb{R}	160
6. Eliptické křivky nad konečnými poli	163
6.1 Rovnice eliptické křivky	163
6.2 Eliptická křivka nad $GF(p)$ jako grupa	164
6.3 Konstrukce eliptických křivek nad $GF(p)$	174
6.4 Násobení bodu skalárem	182
6.5 Ukázka použití eliptických křivek nad konečnými poli $GF(p)$	185