PŘEDMLUVA 3

I. SUBSTITUČNÍ A TRANSPOZIČNÍ ŠIFRY 4

1. Monoalfabetické (substituční) šifry 4

2. Polyalfabetické substituční šifry 12

3. Transpozice (Permutace) 25

4. Dělená morseovka (Fractionated Morse) 32

5. Úkoly pro kryptoanalýzu 35

6. Citovaná a doporučená literatura 39

II. KRYPTOGRAFIE ELIPTICKÝCH KŘIVEK 40

1. Grupa eliptické křivky nad reálnými čísly 40

1.1 Součet bodů eliptické křivky:geometrický přístup 41
1.2 Součet bodů na eliptické křivce: Algebraický přístup 43
1.3 Animace: Modelování eliptické křivky (reálná čísla) 43
1.4 Prvé kontrolní otázky 44

2. Grupy eliptických křivek nad F_P 44

2.1 Příklad grupy eliptické křivky nad F_P 44
2.2 Aritmetika grupy eliptické křivky nad F_P 45
2.3 Animace: Modelování eliptické křivky nad F_P 46
2.4 Druhé kontrolní otázky 46

3. Grupy eliptických křivek nad F_{2m} 46

3.1 Příklad grupy eliptické křivky nad F_{2m} 47
3.2 Aritmetika grupy eliptické křivky nad F_{2m} 47
3.3 Animace: Modelování eliptické křivky F_{24} 48
3.4 Třetí kontrolní otázky 49

4. Grupy eliptických křivek a problém diskrétního logaritmu 49

4.1 Skalární násobení 49
4.2 Problém diskrétního logaritmu eliptické křivky 49
4.3 Příklad problému diskrétního logaritmu eliptické křivky 50

5. Reprezentace polynomiální bází pole F_{2m} 50

5.1 Reprezentace polynomiální bází pole F_{24} 51

6. Reprezentace optimální normální bází pole F_{2m} 52

6.1 Reprezentace optimální normální bází pole F_{24} 52

7. Řešení prvních kontrolních otázek 54

8. Řešení druhých kontrolních otázek 55

9. Řešení třetích kontrolních otázek 55

10. Doporučená literatura 55

III. KRYPTOSYSTÉM SYMETRICKÉHO KLÍČE AES-RIJNDAEL 56

1. Matematický aparát 56

1.1 Grupa, okruh, pole (těleso) 56
1.2 Polynomy 57
1.3 Báze 58
1.4 Polynomiální báze (binární pole) 59
1.5 Normální báze 60
1.6 Operace v GF(2^8) 61

2. Motivace pro návrh Rijndaelu a jeho specifikace 66

2.1 Stav, šifrovací klíč a počet rund 66
2.2 Šifrování 73
2.3 Dešifrování 73

3. Implementační aspekty 75

3.1 8-bitová architektura 75
3.2 32-bitová architektura 76

4. motivace pro návrh struktury 77

5. Bloková schémata šifrovacího a dešifrovacího algoritmu Rijndael 80

6. Citovaná a doporučená literatura 80

OBSAH 81