Název práce: Aplikace Gröbnerových bází v kryptografii

Autor: Aleš Fuchs

Katedra: Katedra algebry

Vedoucí diplomové práce: Mgr. Jan Šťovíček Ph.D., Katedra algebry

Abstrakt: V této práci studujeme přípustná uspořádání a postupy redukce polynomu množinou jiných polynomů v prostředí polynomiálních okruhů nad konečnými tělesy. Zde hrají významnou roli Gröbnerovy báze nějakého ideálu, které díky svým vlastnostem umožňují řešit problém náležení do daného ideálu. Zkoumáme také vlastnosti takzvaných redukovaných Gröbnerových bází, které jsou pro daný ideál jednoznačně určené a v jistém ohledu minimální. Dále se zabýváme rozšířením této teorie do prostředí volných algeber nad konečnými tělesy, kde proměnné nekomutují. Na rozdíl od prvního případu zde Gröbnerovy báze mohou být nekonečné i pro konečně generované oboustranné ideály. V poslední kapitole uvádíme asymetrický kryptosystém Polly Cracker založený právě na problému náležení do ideálu jak v komutativní, tak v nekomutativní teorii. Zkoumáme známé metody kryptoanalýzy aplikované na tyto systémy a v několika případech i opatření, která útokům předchází. Souhrn opatření aplikujeme v poslední části věnované návrhům bezpečných konstrukcí Polly Crackeru.

Klíčová slova: nekomutativní Gröbnerovy báze, Polly Cracker, bezpečnost, kryptoanalýza