Předložené práce studuje využití Grobnerových bází v kryptografii, a to speciálně při kryptoanalýze blokový šifer. Nejprve seznamujeme se základními pojmy teorie Grobnerových bází a metodou pro jejich nalezení, kterou je Buchbergerův algoritmus. Je vysvětlen princip řešení soustav polynomiálních rovnic pomocí vhodných Grobrenových bází. Následně je věnována pozornost moderním algoritmům pro nalezení Grobnerovy báze, jež Buchbergerův algoritmus vylepšují. V poslední části jsou shrnuty dosavadní výsledky dosažené v kryptografii pomocí metod založených na Grobnerových bázích a je představen pojem algebraické kryptoanalýzy. Ta převádí problém prolomení kryptosystému na problém nalezení řešení soustavy polynomiálních rovnic nad konečným tělesem. Na příkladech je vysvětleno jak konstruovat soustavy polynomů více proměnných popisující blokové šifry a jsou prezentovány výsledky praktických pokusů s takovými soustavami.