The thesis focuses on the use of GrÄobner bases in cryptography and especially on applications in cryptanalysis of block ciphers. Some elementary concepts from the theory of GrÄobner bases are introduced together with Buchberger's algorithm, a method for constructing such bases. The principle of solving of poly nomial systems using suitable GrÄobner bases is explained. This is followed by pre sentation of modern algorithms that improve the Buchberger's algorithm. In the last part of the thesis present results achieved by GrÄobner bases are summarised and the notion of algebraic cryptanalysis is introduced. In algebraic cryptanalysis we transform breaking of given cryptosystem into a problem of solving polynomial equations over some nite eld. Examples of polynomial descriptions of block ciphers are provided together with some experimental result on arising polynomial systems.