V předložené práci studujeme bezpečnost šifry AES. Zabýváme se možnosti, jak blokovou šífru a její části matematicky reprezentovat a jak tyto reprezentace využít k algebraickým útokům. Uvádíme přehled známých algoritmů, jež lze k útoku použít. Pozornost, věnujeme též možnosti převedení problému řešení soustavy polynomiálních rovnic na SAT problém a vysvětlujeme princip fungování SAT solverů.