Tato práce se zabývá triangulačním algoritmem a jeho využitím v kryptoanalýze. Uvedeme si definici soustavy nelineárních rovnic, na kterou můžeme aplikovat trian. alg., a objasníme si co je výstupem trian. alg. Ukážeme si použití tohoto algoritmu v kryptoanalýze, konkrétně při útoku na šifru Rijndael. Tento útok si ilustrujeme při hledání kolize pro námi vytvořenou hashovací funkci v Davies-Mayerově módu za použití šifry Rijndael. Součástí této práce je implementační část, ve které si ukážeme reálné využití trian. alg. při hledání kolize pro výše zmíněnou hashovací funkci.