Hlavním cílem této práce je formulace a důkaz bezpečnostních vlastností protokolu IKE, jehož prostřednictvím dochází k dohodě na klíčích používaných protokolem IPSec k zabezpečení síťové komunikace. Věnujeme se také popisu rozdílů konkrétní a asymptotické bezpečnosti a přinášíme definice pojmu bezpečnosti výměny klíče a základních kryptografických primitivů používaných protokoly výměny klíče právě v kontextu konkrétní bezpečnosti. Dále přinášíme obecný popis protokolu IPSec a jeho hlavních funkcionalit následovaný podrobným popisem obou verzí protokolu IKE. Součástí práce je úvod do problematiky protokolů výměny klíče a popis a analýza protokolu Sigma0, který tvoří jádro verze protokolu IKE používající k ochraně autentičnosti a integrity digitální podpis.