The main goal of this thesis is to articulate and to prove security properties of the key exchange protocol IKE, through which the IPSec protocol establishes agreement on keys used for securing internet traffic. It also covers the description of differences between asymptotic and concrete security treatments and the notions of key exchange security and the security of underlying primitives used by key exchange protocols, in the context of concrete security. A general description of IPSec and its main functionalities follows, accompanied by detailed descriptions of both versions of IKE (IKEv1, IKEv2). A general introduction to key exchange is also included and a representative of signature-based version of IKE is introduced and its security is analysed.