The threat of large-scale quantum computers motivates cryptographers to base cryptosystems on problems believed to be resistant against quantum computers. In this thesis, we focus on the LWE problem which is believed to be resistant against quantum computers. First, we describe lattices which are closely related to the LWE problem. We introduce basic notions, describe lattice problems and solve exercises related to the covering radius of lattice. After that, we introduce the LWE problem and its variants. We prove reductions from two lattice problems to certain variant of the LWE problem. We define the notion of statistical distance and prove some lemmata about it which we need within reductions. Moreover, we show concrete application of the LWE problem. We describe a scheme for key exchange and briefly prove its security under the assumption that the LWE problem is hard.