Hrozba silného kvantového počítače vede ke snaze založit kryptosystémy na problémech, které budou těžké i pro kvantový počítač. V této práci si představíme problém LWE, o kterém se předpokládá, že by takovým problémem mohl být. Nejprve si představíme mříže, které s problémem LWE úzce souvisí. Zavedeme základní pojmy, popíšeme mřížové problémy a vyřešíme cvičení týkající se pokrývajícího poloměru mříže. Poté definujeme problém LWE, představíme jeho varianty a ukážeme redukce dvou mřížových problémů na vhodnou variantu problému LWE. K tomuto účelu definujeme pojem statistické vzdálenosti a dokážeme o něm tvrzení, která potřebujeme pro redukci. Nakonec ukážeme konkrétní využití problému LWE. Popíšeme schéma na výměnu klíče a naznačíme, jak dokázat jeho bezpečnost za předpokladu, že problém LWE je těžký.