V předložené práci se věnujeme různým pohledům na využití mřížek v kryptografii. Poté, co píšeme mřížky obecně a problémy s nimi spojené, se věnujeme kryptosystémům založených na mřížích. Popisujeme jejich matematické pozadí i formulaci algoritmů na šifrování a dešifrování. V další části popisujeme využití mřížek v kryptoanalýze. Jedná se především o útoky na knapsack systém a řešení hidden number problému. Významnou součástí práce je také srovnání dvou kryptosystémů RSA a NTRU pro srovnatelnou úroveň bezpečnosti a to z hlediska rychlosti šifrování, dešifrování a generování klíčů.