Abstract

The thesis is focused on the theory of special lattices that are important in cryptography, namely ideal, cyclic and NTRU lattices. Specifically, we expand and generalise the work of Ding and Lindner on Identifying Ideal Lattices. The algorithm for identifying ideal lattices is included, along with illustrative examples and more detailed proofs of propositions on which the algorithm is based. In the section about Lattice Isomorphism there is also included a generalised theorem from the paper. We extend the result of identifying the NTRU lattices and supplement it with several examples. The thesis also contains Chapter Applications in Cryptography where we describe a cryptographic hash function based on ideal lattices. And finally, we provide a brief overview of the cryptographic algorithms using NTRU lattices.