The thesis deals with a subfield of cryptography called secure multi-party computation which is a technique that allows multiple parties to work together to compute a single function while preserving the privacy of it's inputs. More specifically, the thesis deals with secure multi-party computation over the ring of integers modulo p^k. The thesis begins with an introduction of the general principle of secure multi-party protocols, followed by the construction of the necessary theoretical groundwork over commutative rings, wich will be needed to describe and understand a specific protocol in the last section of the thesis.