

This thesis is focused on the RSA algorithm in number fields and on lattices. Specifically, we extend the work the authors Zheng and Liu in their article High Dimensional RSA. In the thesis we precisely describe all the theory required theory with theorems and examples using mostly Algebraic number theory and lattice theory. In the second chapter, we create the RSA only in number fields, we discuss its problems and the necessity of lattices. In the third chapter, we precisely describe and prove properties of ideal matrices, we define the vector multiplication in R^n and at the end we prove the ring isomorphism $K \simeq Q^n \simeq M_Q^*$. In the fourth chapter, we prove the ring isomorphism $Z[x]/(m_\theta(x)) \simeq \mathcal{O}_K \simeq Z^n \simeq M_Z^*$, we define ideal lattices and we create all the required theory over lattices for RSA. The last chapter consists of the complete RSA algorithm in number fields and on lattices and example.