Imaginary quadratic fields were first suggested as a setting for public-key cryptography by Buchmann and Williams already in 1988 and more cryptographic schemes followed. Although the resulting protocols are currently not as efficient as those based on elliptic curves, they are comparable to schemes based on RSA and, moreover, their security is believed to be independent of other widely-used protocols including RSA, DSA and elliptic curve cryptography. This work gathers present results in the field of quadratic cryptography. It recapitulates the algebraic theory needed to work with the class group of imaginary quadratic fields. Then it investigates algorithms of class group operations, both asymptotically and practically effective. It also analyses feasible cryptographic schemes and attacks upon them. A library implementing described cryptographic schemes is a part of this work.