Braid groups involve certain problems that enable the construction of trapdoor functions for the purposes of asymmetric cryptography. Specifically, the conjugacy problem has shown potential in this direction, leading to the development of several schemes. However, it was soon revealed that instances of this problem used in designed schemes are vulnerable to attacks. The aim of this thesis is to formally describe braid groups and construct a theoretical framework to study this problem, selected derived cryptosystems, and attacks on these cryptosystems. In the conclusion, we will explore further potential problems that could be utilized to construct a new asymmetric cryptosystem.