Kryptosystémy s veřejným klíčem, které v dnešní době využíváme (jako např. RSA), budou v budoucnu prolomitelné kvantovými počítači. Z toho důvodu byl institucí NIST v roce 2017 zahájen proces standardizace postkvantové kryptografie. K dnešnímu datu bylo několik kryptosystémů vybráno pro standardizaci, u několika dalších kryptosystémů zatím není jasné, zda budou standardizovány. Jedním z takových kryptosystému je i Classic McEliece – kryptosystém založený na samoopravných kódech. Tato práce se zabývá McEliecovým a Niederreiterovým kryptosystémem, stejně jako jejich variantami využívajícími kódy s rank metrikou. Detailně je v práci popsán Sidelnikův-Shestakovův útok spolu s konkrétním příkladem útoku. Práce se dále zabývá Sternovým a Overbeckovým útokem. Je v ní také představen nový polynomiální útok proti GGPT kryptosystému bez maskující matice X.