Kivonat

A dolgozat célja egy kód-alapú kriptorendszer, a McEliece-féle kriptotlrendszer bemutatása.

Az első fejezetben ismertetem a rendszerhez tartozó titkos és nyilvános kulcsok felépítését, valamint előállítását.

A második fejezetben egy példán keresztül szemléltetem a működését.

A harmadik fejezetben néhány lehetséges támadást ismertetek, amely veszélyeztetheti a rendszer biztonságát. Megvizsgálom, mi történik, ha a titkos kulcs egy mátrixa a támadó tudomására jut, valamint bemutatok három támadóalgoritmust, a Stern támadást, a Bit cserélést és a Leon algoritmust.