

# **Chybová analýza v kryptografii**

TOMÁŠ TVRDÝ

*MU, Brno, Fakulta informatiky*

Cieľom práce je zoznámenie sa s tzv. chybovou analýzou a s metódami ochrany proti nej. V prvej časti práce sa venujeme stručnému popisu základných aspektov kryptológie a úvodu do problematiky kryptoanalýzy postrannými kanálmi. V hlavnej časti práce sa potom zameriavame na preštudovanie techník chybovej analýzy, predstavíme si základné modely útokov tohto typu a na demonštrovanom príklade útoku na CRT-RSA si popíšeme základné protopatrenia. Posledná kapitola sa zaobrá samotným popisom funkčnosti a implementácie vytvoreného programu.