Jana Divišová: Kryptografie založená na mřížkách

posudek vedoucího práce

Předmětem práce je přehled užití teorie mřížek v kryptografii a kryptoanalýze. V teoretické části práce je uvedeno několik kryptosystémů, které jsou založeny na problému nalezení nejbližšího vektoru k dané mřížce (Ajtai-Dwork, GGH, a především NTRU, který je v současné době považován za smysluplnou alternativu k RSA) a dva útoky pomocí algoritmu LLL (knapsack, hidden number problem). Poslední kapitola je pak věnována srovnání kryptosystémů RSA a NTRU z hlediska časové náročnosti šifrování a dešifrování na vlastní implementaci v jazyce C++.

Jde o slušnou kompilační práci s nemalou přidanou hodnotou. Studentka zpracovala řadu článků a vybrala podstatné informace. Výsledný text může být použit jako výukový materiál pro studenty, které zajímá využití mřížek v kryptografii. Po stránce jazykové a stylové práce nijak nevybočuje ze slušného průměru, na svůj rozsah obsahuje poměrně málo nepřesností. Vlastní implementace plní své účely, testy jsou zpracovány kvalitně a mají dobrou vypovídací hodnotu. Práce prokazuje, že studentka zvládla několik oblastí spojených s matematikou v informační bezpečnosti (teorie mřížek, teorie složitosti, použití výpočetních nástrojů atd.) a je důstojným zakončením studia.

Závěr:
Předloženou práci doporučuji uznat jako diplomovou a navrhuji hodnocení stupněm **výborně.**

V Praze, 18.5.2010
David Stanovský