



ZADANIE DIPLOMOVEJ PRÁCE

Študent: **Bc. Pavol Dobročka**
ID študenta: **8739**
Študijný program: **Aplikovaná informatika**
Študijný odbor: **9.2.9. aplikovaná informatika**
Vedúci práce: **doc. Ing. Pavol Zajac, PhD.**
Miesto vypracovania: **Ústav informatiky a matematiky**

Názov práce: **Podpisové schémy v postkvantovej kryptografii**

Špecifikácia zadania:

Cieľom práce je implementovať podpisovú schému pomocou prostriedkov postkvantovej kryptografie. Zameriame sa prioritne na schémy využívajúce dekodovací problém.

Úlohy:

1. Naštudujte problematiku podpisových schém pomocou postkvantovej kryptografie založenej na dekodovacom probléme.
2. Analyzujte knižnicu BitPunch a navrhňte potenciálne rozšírenie knižnice o podpisové schémy.
3. Implementujte vybranú podpisovú schému.
4. Otestujte a vyhodnoťte riešenie.


Zoznam odbornej literatúry:

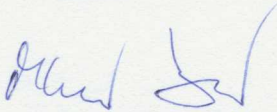
1. F. Uhrecký: Implementácia kryptografickej knižnice s McEliece kryptosystémom. Diplomová práca, 2015.
2. M. Repka, P. Zajac: "Overview of the McEliece Cryptosystem and its Security." Tatra Mountains Mathematical Publications 60.1 (2014): 57-83.
3. N. Courtois, M. Finiasz, and N. Sendrier. "How to achieve a McEliece-based digital signature scheme." Advances in Cryptology—ASIACRYPT 2001. Springer Berlin Heidelberg, 2001. 157-174.

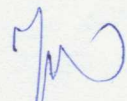
Riešenie zadania práce od: 21. 09. 2015

Dátum odovzdania práce: 20. 05. 2016




Bc. Pavol Dobročka
študent


prof. RNDr. Otokar Grošek, PhD.
vedúci pracoviska


prof. RNDr. Gabriel Juhás, PhD.
garant študijného programu