Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

ZÁZNAM O PRŮBĚHU OBHAJOBY

DIPLOMOVÉ PRÁCE

Název práce: Gröbnerovy báze v kryptografii
Jazyk práce: anglicky

Jméno studenta/studentky: Pavel Hubáček

Studijní program: matematika

Studijní obor: matematické metody informační bezpečnosti

Vedoucí práce: David Stanovský

Oponent/oponenti: Jan Šťovíček

Členové komise:

Aleš Drápal (přítomen)
Jiří Tůma (přítomen)
Štěpán Holub (přítomen)
Přemysl Jedlička (přítomen)
Petr Somberg (přítomen)
Petr Němec (přítomen)

Datum obhajoby: 16. září 2010

Průběh obhajoby: Uchazeč vyložil základy teorie Gröbnerových bází. Poté se věnoval sestavování polynomiálních rovnic pro symetrické šifry a útokům odvozeným od řešení takových rovnic pomoci Gröbnerových bází. Dobře ukázal limity této metody. Po přečetní posudků následovala rozprava, ve které byly dotazy doc. Tůmy zodpovězeny způsobem, který nebyl zcela přesvědčivý.

Výsledek obhajoby: ❑ neprospěl/a

Předseda nebo místopředseda komise: