Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

ZÁZNAM O PRŮBĚHU OBHAJOBY DIPLOMOVÉ PRÁCE

Název práce: Bezpečnost a použitelnost základních hashovacích funkcí, zejména MD-5, SHA-1 a SHA-2

Jazyk práce: český

Jméno studenta/studentky: Bc. Barbora Galaczová

Studijní program: matematika

Studijní obor: matematické metody informační bezpečnosti

Vedoucí práce: doc. RNDr. Jiří Tůma DrSc.

Oponent/oponenti: RNDr. Daniel Joščák
Členové komise:

Předseda:	**Prof. RNDr. Aleš Drápal, DSc. - přítomen**
Místopředseda:	**Doc. RNDr. Jiří Tůma, DrSc. - přítomen**
Členové:	**Mgr. Štěpán Holub, Ph.D. - přítomen**
	RNDr. Přemysl Jedlička, Ph. D. - přítomen
	RNDr. Petr Somberg, Ph. D. - nepřítomen
	Prof. RNDr. Ing. Petr Němec, DrSc. - přítomen

Datum obhajoby: 19. 9. 2011

Průběh obhajoby: Diplomantka pomocí počítačové prezentace podrobně vyložila obsah své práce. Přítomný vedoucí práce přednesl svůj posudek. Poté byl přečten posudek oponenta. Diskuse se soustředila zejména na pomalost doprovodného programového vybavení. Diplomantka vysvětlovala, že přístup po bitech považovala za nejlepší, neboť pak je struktura programu daleko průhlednější. Vedoucí práce naopak zalitoval, že se nepokusila vytvořit program, který by překonal svou rychlostí existující software. Rovněž také vysvětlil praktické důvody, které vedly k zadání tématu.

Výsledek obhajoby: ❑výborně ❑ velmi dobře ☑ dobře ❑ neprospěl/a

Předseda nebo místopředseda komise: Aleš Drápal

Pokyny pro předsedy nebo místopředsedy komisí:

Práce v elektronické podobě musí být studentem vložena do SIS. Formulář vyplňte ve všech bodech v elektronické podobě. V bodě Členové komise se uvedou všichni členové komise a za jejich jména se uvede „(přítomen)“ nebo „(nepřítomen)“. Předseda nebo místopředseda komise je jejím členem. V bodě Průběh obhajoby by měly být uvedeny alespoň čtyři věty vystihující průběh obhajoby. Po vyplnění formuláře ho vytiskněte, dole formulář ještě vlastnoručně podepište a přiložte k zápisu o státní závěrečné zkoušce. Současně vložte formulář v elektronické podobě (bez vlastnoručního podpisu) do SIS.