Posudek bakalářské práce

předložené na Matematicko-fyzikální fakultě
Univerzity Karlovy v Praze

☐ posudek vedoucího ■ posudek oponenta

Autor/ka:	**Martin Franců**
Název práce:	**Test Rabina-Millera a volba báze**
Studijní program a obor:	**Obecná informatika**
Rok odevzdání:	**2011**
Jméno a tituly vedoucího/oponenta:	**Mgr. Vladimír Čunát**
Pracoviště:	**KTIML MFF UK**

	excelentní	**odpovídající**	**slabší**	**nevyhovující**
Náročnost zadaného tématu	X			
Míra splnění zadání		X		
Rozsah práce		X		
Struktura textové části práce	X			
Analýza		X	X	
Vývojová dokumentace		X		
Uživatelská dokumentace		X	X	
Jazyková a typografická úroveň			X	
Návrh a design implementace		X		
Kvalita zpracování softwarové části		X		
Stabilita aplikace	X			

Nejvýznamnější klady:

- náročné téma vyžadující znalosti z teorie čísel a pravděpodobnostních algoritmů
- dobrá modularita a rozšiřitelnost implementace

Nejzávažnější nedostatky:

- volba hlavní testovací množiny z malých čísel do 2*10^8. V článku [7] je uvedena množina 4 bází, které odhalí všechna složená čísla do 10^12. Takto malá čísla lze tedy snadno testovat přesně. Navíc v praxi jsou pro RSA potřeba prvočísla o velikosti stovek dekadických cifer.
- text obsahuje velké množství překlepů, typografických a pravopisných chyb. Na některých místech jsou slovní formulace nejednoznačné nebo nesrozumitelné.
- uživatelská dokumentace je zaměřena na to, kde se nachází jak nazvané prvky v GUI, místo zaměření na vlastní způsob práce s programem

Další poznámky:

	výborně	**velmi dobře**	**dobře**	**neprospěl/a**
Návrh známky		**X**		

Datum: 30. 8. 2011

Podpis: