

# Posudek bakalářské práce

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze

**Autor práce** Miroslav Kratochvíl  
**Název práce** Implementation of cryptosystem based on error-correcting codes  
**Rok odevzdání** 2013  
**Studijní program** Informatika **Studijní obor** Programování

**Autor posudku** RNDr. Jakub Yaghob, Ph.D. **Role** Vedoucí  
**Pracoviště** KSI MFF UK

Prosím vyplňte hodnocení křížkem u každého kritéria. Hodnocení *OK* označuje práci, která kritérium vhodným způsobem splňuje. Hodnocení *lepší* a *horší* označují splnění nad a pod rámec obvyklý pro bakalářskou práci, hodnocení *nevyhovuje* označuje práci, která by neměla být obhájena. Hodnocení v případě potřeby doplňte komentářem. Komentář prosím doplňte všude, kde je hodnocení jiné než *OK*.

<b>K celé práci</b>	lepší	OK	horší	nevyhovuje
Obtížnost zadání	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Splnění zadání	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rozsah práce ... <i>textová i implementační část, zohlednění náročnosti</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Komentář K vypracování práce byly nezbytné netriviální kryptografické znalosti. Práce je dotažená do konce, nabízené nástroje jsou plně funkční.				

<b>Textová část práce</b>	lepší	OK	horší	nevyhovuje
Formální úprava ... <i>jazyková úroveň, typografická úroveň, citace</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Struktura textu ... <i>kontext, cíle, analýza, návrh, vyhodnocení, úroveň detailu</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Analýza	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vývojová dokumentace	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Uživatelská dokumentace	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Komentář Kapitoly 1 a 2 se zabývají kryptografickou teorií nezbytnou pro zhotovení zadané práce. Je nutné ale poznamenat, že se nejedná o teoretickou práci z oboru kryptografie, je to jen potřebný úvod do problematiky. Práce je v čitelné angličtině.				

<b>Implementační část práce</b>	lepší	OK	horší	nevyhovuje
Kvalita návrhu ... <i>architektura, struktury a algoritmy, použité technologie</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kvalita zpracování ... <i>jmenné konvence, formátování, komentáře, testování</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Stabilita implementace	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Komentář Nástroje fungují, jak bylo zadáno, jsou stabilní. V práci jsou provedeny i experimenty porovnávající rychlost nabízeného řešení s volně dostupným GnuPG, který je přímým ekvivalentem, aspoň co do funkčnosti, nabízeného řešení				

**Celkové hodnocení** Výborně  
**Práci navrhuji na zvláštní ocenění** Ano

**Datum** 11. června 2013

**Podpis**