Posudek bakalářské práce

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze

Autor práce	Martin Dvořák		
Název práce	Využití celulárních automatů pro šifrování dat		
Rok odevzdání	2017		
Studijní program	Informatika	**Studijní obor**	Obecná informatika

Autor posudku	RNDr. František Mráz, CSc.	**Role**	Oponent
Pracoviště	KSVI 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*.

K celé práci	lepší	OK	horší	nevyhovuje
Obtížnost zadání	☐	☒	☐	☐
Splnění zadání	☐	☒	☒	☐
Rozsah práce *... textová i implementační část, zohlednění náročnosti*	☐	☒	☐	☐

Komentář Práca diskutuje možnosti využitia celulárnych automatov na šifrovanie súborov. Autor vybral metódu založenú na predlžovaní kľúča, ktorá z krátkeho vloženého kľúča pomocou celulárneho automatu generuje kľúč ľubovoľnej dĺžky potrebnej na šifrovanie zadaného súboru. Toto je možné robiť mnohými spôsobmi a autor rozoberá, ktoré z nich sú vhodné, a hlavne meria kvalitu šifrovania podľa niekoľkých kritérií.

Textová část práce	lepší	OK	horší	nevyhovuje
Formální úprava *... jazyková úroveň, typografická úroveň, citace*	☐	☒	☐	☐
Struktura textu *... kontext, cíle, analýza, návrh, vyhodnocení, úroveň detailu*	☐	☒	☐	☐
Analýza	☐	☒	☒	☐
Vývojová dokumentace	☐	☒	☒	☐
Uživatelská dokumentace	☐	☐	☐	☒

Komentář Práca je napísaná prehľadne na dobrej jazykovej úrovni. Občas sa vyskytujú preklepy. Napr. "staganografie" namiesto "steganografie" (niekoľkokrát na s. 10), "přijehorším" (s. 19, r. 3), apod. Do analýzy by bolo vhodné zahrnúť aj to, ako testovať kvalitu šifry. Nemyslím tým len voľbu vhodných kritérií, ktorá je v práci dobre zdôvodnená, ale to ako tieto testy vykonávať – na akých sekvenciách (akej dĺžky?, je treba skúšať všetky sekvencie danej dĺžky alebo iba vybrané?, atď.). To sa totiž potom ukázalo ako hlavný problém pri hľadaní celulárnych automatov vhodných na šifrovanie.

Vývojovú dokumentáciu považujem za dostatočnú, ale užívateľská dokumentácia je nevyhovujúca. Užívateľský popis toho, čo robia priložené programy je nedostatočný. Priložené programy robia testy, ale užívateľ takmer nemá možnosť ovplyvniť čo sa bude testovať a ako. Napr. program MartinDvorak umožňuje načítať aspoň číslo elementárneho celulárneho automatu zo súboru, ale to sa dá zistiť iba v zdrojovom kóde, nie v dokumentácii.

Implementační část práce	lepší	OK	horší	nevyhovuje
Kvalita návrhu *... architektura, struktury a algoritmy, použité technologie*	☐	☒	☒	☐
Kvalita zpracování *... jmenné konvence, formátování, komentáře, testování*	☐	☒	☐	☐
Stabilita implementace	☐	☒	☐	☐

Komentář Autor si dal záležať na všeobecnosti návrhu implementácie celulárnych automatov, metód šifrovania i testov šifier. Taktiež sa zaoberal vhodnou voľbou dátových štruktúr s ohľadom na časovú zložitosť. Aj keď je charakter práce experimentálny, tak by implementácia mala byť navrhnutá tak, aby užívateľ mohol robiť testy jednotlivo, aby sa nestávalo, že program čaká na stlačenie klávesy, ale užívateľa o tom neinformuje a ani sa o tom nepíše v texte práce (program Interactive).

Celkové hodnocení Velmi dobře (spíše lepší)
Práci navrhuji na zvláštní ocenění Ne

Datum 23. ledna 2017 **Podpis**