POSUDEK

Autorka diplomové práce: Jana Zimmermannová, BBus.
Název diplomové práce: Vývoj a využití hašovacích funkcí při zpracování informací
Vedoucí práce: Doc. Jiří Ivánek, CSc.
Oponent práce: Ing. Martin Souček, Ph.D.
Hodnocení: velmi dobře

Posudek: 18. 5. 2012

Cíl práce:
Cílem práce bylo podat celkový přehled o problematice hašovacích funkcí, jak z teoretického, tak z praktického hlediska.

Shoda se zadáním diplomového úkolu:
Cíl i struktura práce dobře sleduje zadání diplomového úkolu.

Hodnocení práce:
Předložená diplomová práce se věnuje zajímavé problematice hašovacích funkcí. S porozuměním komplikovaným matematickým a kryptografickým postupům autorka vymezuje smysl a význam používání hašovacích funkcí, popisuje způsob jejich konstrukce, uvádí v současnosti používané funkce a popisuje vývoj hašovacího standardu v posledních letech. Ke všem těmto tématům přistupuje pečlivě a s velkou erudicí. Z hlediska našeho oboru bych však uvítal větší akcent na popis použití těchto hašovacích funkcí, popis toho jakým způsobem nástup hašovacích funkcí ovlivnil informační společnost, jakým způsobem mění používání těchto funkcí jak stroji tak běžnými uživateli náš způsob práce s informacemi. V této podobě má práce těžiště spíše v oblasti „comupter science“ než „information science“. Velmi zajímavá je z tohoto hlediska kapitola 2.5, kterou by bylo dobré detailněji rozebrat. Práci uzavírá dobře a čtivě zpracovaná kapitola popisující veřejnou soutěž, pořádanou National Institute of Standards and Technology, která výrazně posunula vývoj v oblasti hašovacích funkcí.

Volba informačních zdrojů:
Autorka pracuje s rozsáhlým množstvím kvalitních, ve většině případů zahraničních informačních zdrojů, citace v textu jsou systematicky uváděny.

Stylistická úroveň práce:
Po této stránce nemám k práci výhrady, práce je dobře napsaná.

Formální úprava práce:
Po pravopisné stránce nemám žádné výtky, překlepy jsou výjimkou, grafická úroveň práce je velmi dobrá. Na titulním listě by mělo být uvedeno přesné jméno univerzity (Univerzita Karlova v Praze), jméno ústavu by se mělo psát s pouze velkým počátečním písmenem, ostatní písmena by měla být malá. Je dobře, že je práce vybavena seznamem symbolů a zkratek.

Doplňující otázky:

1. Vidíte významnější možnost uplatnění hašovacích funkcí v oblasti čistě strojových algoritmů, nebo v oblasti aplikací pro běžné uživatele?
2. Jsou nějaké nové informace soutěži NIST o vytvoření nového hašovacího algoritmu?

Závěr

Celkově mohu říci, že práci považuji díky úrovni pochopení složité problematiky hašovacích funkcí za velmi dobrou, pečlivě zpracovanou. Doporučuji hodnocení velmi dobře.

Martin Souček