# Posudek

❑vedoucího ❑**oponenta**
❑**diplomové** ❑bakalářské práce
Autor/Autorka: Bc. Kateřina Štíchová
Název práce: Analýza použití kryptografických funkcí ve formátě PDF
Jméno vedoucího/oponenta: Daniel Joščák

Matematická úroveň:
❑vynikající ❑velmi dobrá ❑průměrná ❑**podprůměrná** ❑nevyhovující

Grafická, jazyková a formální úroveň:
❑vynikající ❑**velmi dobrá** ❑průměrná ❑podprůměrná ❑nevyhovující

Výsledky:
❑originální ❑původní i převzaté ❑netriviální kompilace ❑**citované z literatury** ❑opsané

Použité metody:
❑nestandardní ❑standardní ❑**obojí**

Aplikovatelnost:
❑přínos pro teorii ❑přínos pro praxi ❑přínos pro praxi i teorii ❑bez přínosu ❑**nedovedu posoudit**

Věcné chyby:
❑téměř žádné ❑**vzhledem k rozsahu a pojednávanému tématu přiměřený počet** ❑méně podstatné četné ❑závažné

Tiskové chyby:
❑téměř žádné ❑**vzhledem k rozsahu a pojednávanému tématu přiměřený počet** ❑četné

Celková úroveň práce:
❑vynikající ❑velmi dobrá ❑**průměrná** ❑podprůměrná ❑nevyhovující

Práci
❑**doporučuji** ❑nedoporučuji
uznat jako diplomovou/bakalářskou. Návrh klasifikace přikládám na zvláštním papíru.

**Připomínky a vyjádření oponenta:**

Oponovaná práca sa zaoberá možnosťami využitia kryptografie vo formáte PDF. Po úvodnej kapitole autorka charakterizuje formát PDF jeho štruktúru a základné objekty, z ktorých sa skladá dokument PDF. Tento popis v podkapitolách 2.1 - 2.4 je pomerne výstižný a ukazuje základné princípy PDF formátu. Oponent práce nerozumie zaradeniu podkapitoly 2.5, ktorá je citovaná a prevzatá z [14] a netýka sa predmetu práce. Autorka na deviatich stránkach vysvetľuje nakreslenie tenkej neprerušovanej čiary, hrubej prerušovanej čiary, obdĺžnika s modrou výplňou a červenými okrajmi a kubickej Bézierovej krivky so šedou výplňou a čiernymi okrajmi.

Kapitola 3 sa venuje elektronickému podpisu najprv z pohľadu kryptografie a potom práva. Oponent má výhrady k vágným popisom a definíciám („Elektronický podpis zprávy je datový řetězec (číslo), který se připojuje k dokumentu. Vzniká jistým "spojením" podepisovaného dokumentu a soukromého klíče podepisující osoby", str. 32) a konštatovaniam bez zdôvodnenia alebo odkazu do literatúry („Podpisová schémata s dodatkem jsou v praxi nejpoužívanější. Patří mezi ně např. RSA, DSA, ElGamal. Využívají kryptografické hashovací funkce a obecně jsou méně náchylné k útokům.", str. 33). Podkapitoly 3.3. až 3.5 sú venované RSA a štandardu PKCS #1. Autorka v nich popisuje „datový řetezec", ktorý podpis tvorí. Popis schémy RSASSA-PKCS1-v1.5 aj novšej schémy RSASSA-PSS je presný, čitateľ práce sa však nedozvie, prečo je použitie novšej schémy „bezpečnostně robustnější", či napríklad akú úlohu má maskovacia funkcia MGF. Podkapitoly 3.6 až 3.9. sú natoľko stručné, že ich autorka mohla zhrnúť do jednej kapitoly nazvanej napríklad: „Využitie elektronického podpisu v praxi". Kladne hodnotím podkapitolu 3.9 venovanú biometrickému podpisu ako alternatívnemu elektronickému podpisu podporovanému v PDF formáte.

Kapitola 4 sa venuje konkrétnemu procesu tvorby podpisu v dokumente PDF. Názorný je diagram na obr. 4.4 popisujúci prechod jednotlivými stavmi s ich vysvetlením. Kapitolu hodnotím pozitívne a ukazuje základné pochopenie tvorby podpisu. Oponent sa nazdáva, že táto kapitola poskytovala priestor pre vlastnú tvorbu a analýzu napríklad podpisu uživateľských práv či možností falšovania elektronického podpisu (vnútenie zastaralých šifrovacích schém).

Kapitola 5 pojednáva o šifrovaní v PDF. Popis šifrovania a výpočet šifrovacieho kľúča je pomerne výstižne zachytený. Nechýba spôsob odvodzovania kľúča z hesla aj za pomoci PKI, umiestnenia inicializačního vektora při použiti CBC módu AES, či overovana prístupových práv k súboru. Algoritmu pre výpočet šifrovacieho kľúč sa dá vytknúť jazykový štýl, ktorý je vhodný v populárno náučných článkoch, ale v diplomovej práci je jeho použitie na uváženie („t.j. semele se hashovací funkcí heslo…, přimelou se přistupová oprávnění,…").

Kapitola 6 stručne popisuje formát vhodný pre archiváciu PDF a to PDF/A. K tomuto popisu nemám žiadne výhrady, jedná sa o súhrn štandardu.

Kapitola 7 je analýzou rizík dlhodobého archivovania elektronických faktúr v PDF. Zmysel tejto analýzy je pre autora posudku otázny a je zjavné, že záleží od ohodnotenia zraniteľností, hrozieb a aktív. Toto ohodnotenie autorka nijako nezdôvodňuje a vedie k predpokladanému záveru a návrhu opatrení.
V záverečnej kapitole autorka sumarizuje prácu a vývoj kryptografických funkcií v PDF formáte. Práca obsahuje prehľad možností použitia kryptografie vo formáte PDF a návrhu archivácie, ktorý je výstižný.

**Otázky pre autorku práce k obhajobe:**
Aký bol dôvod zaradenia podkapitoly 2.5 do vašej práce?
Prečo je použitie novšej schémy RSASSA-PSS „bezpečnostně robustnější" oproti RSASSA-PKCS1-v1.5? Viete popísať reálnu slabinu staršej schémy?
Koľkokrát sa aplikuje hashovací algoritmus v algoritme v kap. 5.3.
Na základe čoho ste určovali a potom ohodnocovali aktívá, hrozby a zraniteľnosti v kapitle 7?

V Prahe, 25. 1. 2013