Posudek

☐vedoucího ☑oponenta
☐diplomové ☑bakalářské práce
Autorka: Veronika Čadová
Název práce: O DSA
Jméno oponenta: RNDr. Přemysl Jedlička, Ph.D.

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

Místo, datum, podpis oponenta:

Hodnocení oponenta:

Úkolem bakalářské práce bylo popsat:

1. Okolnosti vzniku DSA a jeho normativní doporučení;
2. Vztah DSA a RSA – výhody a nevýhody, porovnání rychlostí;
3. Důsledky krácení prvního parametru modulo q pro nepopiratelnost podpisu;
4. Některé útoky na DSA.

Bod 1. je popisován na začátku kapitoly 2. Je tam i citován český zákon 227/2000 Sb., bohužel ale pouze jeho název a je vysvětleno, které pojmy zákon vymezuje. Není uvedeno, jestli se zákon zabývá i technickými kritérii a jakými.
Bod 2. není v práci rozpracován vůbec.
Bod 3. není v práci rozpracován vůbec.
Bodu 4. je v práci věnována celá kapitola čtvrtá.
Největší prostor je v práci, kromě popisu DSA, věnován popisu Schnorrova algoritmu a srovnávání těchto dvou algoritmů. Studentka by měla při obhajobě řádně zdůvodnit, proč došlo ke změně témat.
První kapitola je věnována základním kryptografickým pojmům a cyklickým grupám. Nerozumím tomu, proč jsou v práci dokazována tvrzení známá ze základního kursu algebry, zvláště tedy, proč je dokazováno, že řád prvku grupy je nejmenší n takové, že $a^n=1$. Neobstojí ani argument, že počítáme se čtenářem, který není s teorií grup obeznámen, neboť se v práci odkazuje na Lagrangeovu větu. Perličkou je totožný příklad zopakovaný dvakrát na straně 6.
Na konci první kapitoly je přehled nejzákladnějších algoritmů na řešení problému diskrétního logaritmu. Jejich popis je ale příliš neurčitý na to, aby se podle něj daly naprogramovat a na druhou stranu zase příliš podrobný, uvážíme-li, že je vlastně v práci nepotřebujeme mít; stačilo by se o nich zmínit a říci, jakou mají složitost.
V kapitole druhé se na začátku vysvětluje, proč byl DSA vyvinut a algoritmus je stručně popsán.
Třetí kapitola popisuje podobný algoritmus Schnorrův.
Čtvrtá kapitola přináší nejjednodušší typy útoků na DSA a příbuzné algoritmy.
Pátá kapitola je vlastním přínosem, bohužel ten přínos není velký (1,5 stránky). Autorka se zaměřila na jeden typ hashovací kolize, která by mohla být vést k nějakému útoku. K jakému, není ani vysvětleno ani naznačeno. Následně se provádí měření na souboru 15 dat, ze kterého studentka usoudí, že pravděpodobnost, že nastane kolize, klesá s narůstajícím klíčem. Toto pozorování není nijak teoreticky zdůvodněno. Jedna drobnost: slovo „najití“ ve spisovné češtině neexistuje, říká se „nalezení“.
Šestá kapitola přichází s krátkým historickým exkurzem do problematiky asymetrického šifrování a digitálního podpisu.
Sedmá kapitola vysvětluje, co nalezneme na přiloženém CD. Program se mi nepodařilo přeložit, ale vypadá věrohodně, že ve vývojovém prostředí, které použila autorka a které já nemám, program funguje. Předvádí DSA, tj. nabízí možnost vytvoření klíčů, šifrování a dešifrování. Kromě toho předvádí prolomení klíče při opakovaném použití stejné jednorázové hodnoty a měření doby běhu programu.

Práce není natolik hluboká, jak bylo zamýšleno při vypisování tématu. Téměř všechen obsah práce je v osnovách povinných přednášek pro bakalářské studium MIB.