POSUDEK OPONENTA NA BAKALÁŘSKOU PRÁCI MIROSLAVY PRATER *PROTOKOLY PRO DOHODU NA KLIČI*

Práce nabízí přehled protokolů pro nejrůznější zacházení se šifrovacím klíčem. Protokoly jsou rozděleny do čtyř kapitol (kap. 2–5) a předchází jim úvod do základních pojmů a technik.

Práce je psána přehledně a srozumitelně. Nakolik jsem mohl posoudit srovnáním s použitou literaturou, nejedná se o pouhý doslovný přenos z předlohy, práce obsahuje jednotný komentář a sjednocenou terminologii.

Z tohoto hodnocení existuje několik výjimek:

- Pro porozumění struktuře kapitol chybí vysvětlení, co znamenají „asymetrické techniky" v nadpisu páté kapitoly a jak se liší od technik s veřejným klíčem, což je jinak v práci protipól k „symetrickému šifrování".
- Při popisu RSA na str. 9 je dešifrování popsáno s odvoláním na Čínskou větu o zbytcích, přičemž z matematického hlediska je přirozenějším popisem práce v multiplikativní grupě $\mathbb{Z}_n^*$, která má právě ϕ prvků. Tento přirozený matematický popis je ostatně v práci dále používán.
- Na str. 10 by bylo vhodné naznačit, proč má e čtyři odmocniny.
- Definice pojmu „kryptoanalýza" na str. 13 je kruhem a i jinak podivná.
- Na str. 15 je řečeno, že R je „bijekce do" $\mathcal{M}_{\mathcal{S}}$, správně má být asi „prosté zobrazení do".
- Inkluze $\mathcal{M}_R \subseteq \mathcal{M}_{\mathcal{S}}$ na str. 15 pak platí prostě proto, že $\mathcal{M}_R = \mathrm{Im}(R)$.
- Na straně 16, ř. 12 má být $[0, 2n-1]$, namísto $[0, n-1]$.
- Pojem „obnova klíče" není v práci definován, zřejmě mu odpovídá v úvodu definované „dynamické vytvoření klíče".
- Na str. 40 je chybné pořadí kroků strany B v popisu protokolu.

Práci doporučuji přijmout jako bakalářskou. Při volbě hodnocení kolísám mezi výborně a velmi dobře, z pozice oponenta a vzhledem k ryze kompilačnímu charakteru práce navrhuji *velmi dobře*.

Praha 5. září 2007 Štěpán Holub