Posudek vedoucího na bakalářskou práci

Miroslava Prater, **Protokoly pro dohodu na klíči**

Práce Miroslavy Prater se zabývá protokoly používanými pro vytvoření klíče pro komunikaci mezi dvěma a více partnery, kteří chtějí k utajení obsahu komunikace použít nějakou symetrickou šifru. Jde o velmi důležitou skupinu protokolů, která je základem prakticky veškeré šifrované elektronické komunikace v současnosti.

Autorka práci rozdělila do čtyř kapitol v závislosti na tom, jde-li o protokoly pro dohodu na klíči nebo protokoly pro transport klíče, a dále využívají-li symetrické šifrování nebo šifrování s veřejným klíčem. V každé z těchto čtyř skupin protokolů je pak uveden jeden nebo více příkladů konkrétních protokolů a zmíněny některé bezpečnostní aspekty těchto protokolů. Celá práce je pak ještě uvedena kapitolou, ve které jsou vysvětleny základní pojmy.

Práce je napsána velmi pečlivě a přehledně, autorka vycházela z různých zdrojů, které vhodně propojila de jednolitého textu. Pokusila se vytvořit českou terminologii, která povětšinou v této oblasti schází tak, aby odpovídala obsahu jednotlivých pojmů.

Jde o práci velmi kvalitní, které nemám příliš co vytknout. Nepochybně bude možné využít ji při výuce této problematiky v následujících létech. Pouze bude potřeba doplnit ji o podrobnější zkoumání bezpečnostních aspektů této problematiky. O pojetí pojmu „dokazatelné bezpečnosti" těchto protokolů se v současné době vedou rozsáhlé diskuse mezi vedoucími osobnostmi světové akademické kryptologie.

Práci navrhuji uznat jako práci bakalářskou a hodnotit ji známkou **výborně.**

V Praze 31.8.2007

Doc. RNDr. Jiří Tůma, DrSc.