Posudek na bakalářskou práci:

Marie Švarcová: **Důkazy bezpečnosti schémat symetrické kryptografie**

Téma bakalářské práce bylo s mým souhlasem zúženo na oblast důkazů bezpečnosti schémat symetrického šifrování s ochranou integrity. To autorce umožnilo zabývat se nejen technikou jednotlivých důkazů ale i představit oblast, které se důkazy týkaly, ve značně uceleném tvaru včetně souvislostí.

Práce vycházela z trojice základních článků této oblasti. První z nich se zabývá zejména generickými kombinacemi šifrování a MAC do schémat symetrického šifrování s ochranou integrity, druhý zejména konstrukcí a bezpečností schémat NMAC a HMAC a třetí přechodem ke schématům s připojenými daty, které se sice nešifrují, ale jejichž integritu je nutné rovněž chránit.

Obsažené důkazy a souvislosti jsou v bakalářské práci zpracovány pečlivě a srozumitelně vysvětleny. Celkově je práce přehledná a dobře se v ní orientuje. V závěru práce jsou zhrnuty závěry autorky o metodách důkazů bezpečnosti schémat prostudované oblasti.

Navrhuji práci hodnotit známkou výborně.

V Praze 8. 6. 2010
RNDr. Bohuslav RUDOLF