Posudek vedoucího na diplomovou práci

Michal Botka, Kryptoanalýza AES

Cílem práce bylo vytvořit přehled algebraických metod, které jsou v současné době vyvíjeny a používány k pokusům o prolomení šifry AES, nového standardu blokových šifer vzešlého z celosvětové soutěže pořádané americkým NIST (National Institute of Standards and Technology).

Po úvodu následuje ve druhé kapitole popis šifry a ve třetí kapitole je zkoumán algebraický popis S-boxů. Ty tvoří v moderních blokových šifrách jedinou nelineární část a bezpečnost těchto šifer plně závisí na bezpečnosti S-boxů. Výzkum je soustředěn na hledání algebraických rovnic, které (úplně) popisují S-boxy. Na tyto rovnice jsou pak používány standardní nebo různě upravené metody řešení soustav algebraických rovnic. Vzhledem ke složitosti a velkému řádu S-boxu používaného v AES jsou tyto soustavy současnými prostředky neřešitelné. Metody jsou proto testovány na jednodušších S-boxech nižších řádů. Vlastní přínos práce měl být v důkazech správnosti algoritmů používaných v případě S-boxů malých řádů. Zde je třeba říci, že tento přínos je poměrně malý. Jde hlavně o dimenzi prostoru všech řešení u algoritmu, který navrhli N.T. Courtois aj. Pieprzyk pro hledání soustav kvadratických rovnic popisujících S-boxy. Vysvětlit důvod, proč tento algoritmus dává tak velký počet rovnic u S-boxu použitého v AES, zatímco u náhodně zvoleného S-boxu nenajde ani jednu rovnici, se bohužel nepodařilo.

Další dvě kapitoly jsou pak věnovány přehledu nejpoužívanějších metod pro řešení soustav algebraických rovnic nad konečnými tělesy.

Práce je napsána jasným, i když někdy až příliš úsporným jazykem.

Za největší vadu práce považuji poměrně malý vlastní přínos a celkově malý rozsah vzhledem k tomu, že jde o práci převážně kompilační.

Práce vyhovuje podmínkám pro diplomovou práci a navrhuji ji hodnotit známkou **velmi dobře.**

Doc. RNDr. Jiří Tůma, DrSc.

V Praze dne 2.2.2009