Posudek oponenta na bakalářskou práci

Jan Říha, Konstrukce a kryptoanalýza AES

AES (Advanced Encryption Standart) je nejpoužívanější blokovou symetrickou šifrou současnosti. Práce Jana Říhy popisuje nejprve vznik této šifry, od vypsání soutěže až po vybrání vítězného návrhu, šifry Rijndael, od autorů Rijmena a Daemena. Poté práce popisuje zevrubně její konstrukci. V další části se věnuje softwarové a hardwarové implementaci a v závěru stručně podává některé výsledky kryptoanalýzy této šifry.

V první kapitole je podrobně popsán vznik této šifry. Americký NIST (National Institute of Standards and Technology) vypsal v roce 1997 konkurs se zadanými požadavky na novou blokovou symetrickou šifru, která měla nahradit používané, ne však již bezpečné šifry. Z patnácti návrhů a posléze pěti finalistů byl v říjnu 2000 vybrán vítěz, šifra Rijndael. Tato kapitola je napsána velmi dobře a přehledně.

Ve druhé kapitole je podrobně popsán algoritmus AES. Po uvedení používaných matematických poznatků z algebry jsou popsány jednotlivé části algoritmu a posléze inverzní šifra a její alternativa. V tomto popisu je kladen důraz právě na matematické vlastnosti šifry, což nebývá zcela vždy zvykem. Kapitola je členěna velice dobře, nejprve je stručně popsána šifra celá a poté podrobně její části, popis je dobře srozumitelný.

Ve třetí kapitole jsou popsány implementační výhody šifry AES na jednotlivých platformách. Je uvedeno, jak lze efektivně implementovat jednotlivé dílčí operace šifry, což osvětluje jeden z důvodů, proč právě tato šifra byla vybrána. Protože v této kapitole jsou uváděna ne vždy zcela triviální fakta a problematika implementace je velmi široká, neškodilo by dodat přesný odkaz na literaturu, z které byly právě tyto informace čerpány.

V poslední kapitole autor zmiňuje nejrůznější přístupy kryptoanalýzy. Tato oblast je velmi rozsáhlá a zároveň rychle se vyvíjející. Na téma kryptoanalýzy bylo publikováno velké množství článků i v relativně nedávné době a není lehké tuto oblast plně uchopit. Jistě by bylo přínosné popsat stručně současné výsledky, ale především směry, kudy se současný vývoj ubírá, případně uvést odkazy na týmy, které se nejvíce touto problematikou zabývají.

V práci však nikde není výslovně uvedeno, co si vlastně čtvrtá kapitola (potažmo celá práce) klade za cíl, proto je i těžké hodnotit, zda tohoto cíle dosáhla. Odkazy na články jsou uvedeny neúplné pouze v textu, v seznamu literatury chybí, navíc jsou články většinou dost starého data (což se člověk dozví, až když si je dohledá). Není jasné, proč autor zmiňuje v textu právě tyto zdroje, čtvrté kapitole chybí minimálně nějaký úvod, který by toto osvětlil. Poslední dva odkazy ze čtyř celkem uvedených zdrojů v seznamu literatury jsou uvedeny chybně.

Celkově je práce vyvážená, s minimem překlepů, splňuje požadavky kladené na bakalářskou práci. Vzhledem k uvedeným nedostatkům navrhuji hodnocení

Velmi dobrý (2)

V Praze, 9.9.2006

[redacted]

Mgr. Jiří Vábek.
Oponent práce