Posudek oponenta

bakalářské práce p. Tomáše Tománka

„Použití kryptografie v prostředí Internetu“

Předložená bakalářská práce je napsána na aktuální téma teorie a praxe bezpečného přenosu dat. Autor si položil za cíl poukázat na nejdůležitější používané kryptografické algoritmy a jejich implementace do přenosových internetových protokolů.

Práce je vhodně strukturována do kapitol, dobrá je též celková grafická a jazyková úroveň předložené práce (i když pár chyb typu i/y, s/z jsem v práci našel). Co se týče použité literatury, její rozsah je více než dostatečný, nicméně něco přece jen autorovi uniklo – viz níže.

Autorovi se podařilo zpracovat pěkný přehled celé problematiky.Text svědčí o tom, že autor se v tématu velmi dobře zorientoval.

K práci mám několik připomínek týkajících se kryptologické terminologie a popisu šifrovacích algoritmů:

Str. 13 – řádek se vzorcem pro N je nesprávně uveden.

Str. 18 – popis DES není zcela konzistentní, značení použité ve vzorcích není plně zavedeno (např. sčítání mod 2).

Str. 19 – je v Triple DES klíč opravdu trojnásobně dlouhý?

Str. 20 – popis šifrování v IDEA není srozumitelný (jak se aplikují podklíče?)

Str. 20, posl. odst. – formulace „Počítá s výpočetně neproveditelným výpočtem …“ je opravdu nešťastná.

Str. 21, druhý odst. – vyjádření vlastnosti generátoru je nesrozumitelné, navíc použití písmene k způsobuje matoucí konotaci s označením tajného klíče k níže na téže stránce.

Str. 22, první odst. – formulace „obtížná faktorizace velmi vysokých prvočísel“ je matematicky nesmyslná.

Str. 23 – domnívám se, že formulaci „bloky, které mají délku kratší, než je číslo n“ je nutno doplnit na „bloky, které mají délku kratší, než je délka čísla n zapsaného ve dvojkové soustavě“.

Str. 23 – ve vzorcích zřejmě nemají být velká písmena C, M.

Tyto odpustitelné nedostatky souvisejí zejména s nedokonalým používáním matematického aparátu. Moje hlavní připomínka se však týká úplného opomenutí nového šifrového standardu AES (Advanced Encryption Standard), který před několika lety nahradil DES (klasický DES již asi deset let není považován za bezpečný a používá se případně pouze Triple DES). Autor by si měl pro obhajobu doplnit své informace a upřesnit patřičná místa ve své práci.

Přes uvedené výhrady předloženou bakalářskou práci doporučuji k obhajobě a hodnotím ji velmi dobře.

V Praze dne 26.4.2006

Doc. RNDr. Jiří IVÁNEK, CSc.