

Posudek diplomové práce

název práce: Bezpečné kryptografické metody

autor práce: Bc. Zdeněk Müller

Stručné zhodnocení práce:

Diplomová práce přináší velmi podrobné srovnání historických a zejména moderních kryptografických metod. Popisuje některé významné symetrické a asymetrické šifry, hashovací funkce a několik metod jejich prolomení. Dále se zabývá generátory pseudonáhodných čísel a autentizačními protokoly. V praktické části jsou některé algoritmy implementované.

Jak práce splnila cíle uvedené v zadání:

Práce splnila cíle uvedené v zadání s jednou výjimkou: nebyla provedena implementace útoku na SSL spojení. Nutno ovšem dodat, že je tato problematika dosti technicky náročná. Student ji podrobně teoreticky popsal a detailně se zabýval optimalizačními technikami jednoho z popisovaných útoků. Tento odklon od zadání tedy nepovažuji za závažný.

Přináší práce nové výsledky? Jaké (teoretické, algoritmy, nový SW nástroj, experimenty apod.)?

Hlavní přínos vidím v přehledném a podrobném popisu moderních kryptografických metod. Velmi pěkně jsou zpracovány útoky na šifu RSA pomocí postranních kanálů (Bleichenbacherův útok a Klíma-Pokorný-Rosa útok). Pokud je mi známo, tak tímto souhrnným způsobem nebyly zmíněné útoky v literatuře zatím popsány.

Jaká je jazyková úroveň práce? Jaké je formální zpracování (překlepy a jiné formální nedostatky)?

Práce obsahuje mnoho typografických chyb a překlepů. Např.:

- použití stejného symbolu ($\rightarrow$) pro zápis zobrazení (např. na str. 164 v definici Bad-Version orákula) a pro zápis přiřazení jednoho konkrétního prvku jinému prvku v daném zobrazení (např. na str. 16 při popisu zobrazení D_k),
- špatné dělení odstavců (např. na str. 18, 20, 42, 157, 170),
- na str. 19 patří „Vernamova” místo „Vermanova”,

- chybné použití uvozovek (např. na str. 19, 20),
- na str. 23 patří „Vigenerovy” místo „Vigenerovi”,
- na str. 30 patří „Kryptoanalýza symetrických šifrovacích systémů” místo „Kryptoanalýza u symetrických šifrovacích systémů”,
- na str. 57 nepatří tečka za „viz”,
- na str. 97 patří „nalezení základu” místo „nalezení kořenu”,
- na str. 98 je použito dvou různých symbolů pro označení Eulerovy funkce (φ a ϕ),
- na str. 98 patří „Jestliže” namísto „Jesliže”,
- na str. 98 patří „je dán . . . modulem n ” místo „je dán . . . operací modulo n ”,
- špatné vysázení odkazů na koncích vět (konkrétně na str. 99, 126, 134, 136, 153),
- na str. 100 patří $r_2 \cdots r_u$ místo $r_2 \cdot \cdots \cdot r_u$,
- chybějící interpunkce za matematickými výrazy (např. na str. 107, 109, 111, 114, 116, 118, 120).

Výše uvedené chyby nejsou zásadního charakteru. Jejich velký počet je možné vysvětlit značnou rozsáhlostí práce (celkem 178 stran).

Dále upozorňuji na velmi špatný překlad anglicky psaného závěru a na nahodile řazený seznam použité literatury, ve kterém jsou navíc chybně uvedené odkazy na zdroje z internetu.

Další (chyby, slabé a silné stránky práce, apod.):

Diplomová práce zahrnuje rozsáhlou část zejména moderní kryptologie. Popis některých metod je velmi detailní. Výhradu mám pouze k úvodní kapitole týkající se teoretických aspektů, zejm. se jedná o kapitolu 3.3. Uvádím pouze některé svoje výtky:

1. Definice *maximální entropie* na str. 19 je zavádějící. Spíše než o definici by se mělo jednat o tvrzení, které říká, kdy je entropie největší.
2. Definice *vzdálenosti jednoznačnosti* je těžko srozumitelná.

3. První odstavec v sekci 3.3.3 na str. 20 uvádí mylnou informaci. Nadbytečnost přirozeného jazyka není totiž dána opakováním se určitých slov v daném textu (např. odborných výrazů v matematickém textu), ale skutečností, že se jednotlivé n -gramy vyskytují ve slovech s různou, pro daný jazyk specifickou, pravděpodobností.
4. K definici *absolutní obsažnosti jazyka* mám podobnou výhradu jako v bodě 1. Definice budí dojem, že absolutní obsažnost je vlastností nějakého přirozeného jazyka. Ve skutečnosti se ovšem jedná o hodnotu obsažnosti jazyka, jehož jednotlivé znaky se v textu vyskytují se stejnou pravděpodobností.

Navrhované hodnocení práce:

Práci doporučuji k obhajobě a navrhuji udělit známku **C**.

datum: 26. 8. 2012

jméno: Mgr. Eduard Bartl, Ph.D.

podpis: