

Posudek oponenta diplomové práce

Student: Pekař Tomáš, Bc.
Téma: Šifrování webových stránek na straně prohlížeče (id 16900)
Oponent: Burget Radek, Ing., Ph.D., UIFS FIT VUT

1. **Náročnost zadání** průměrně obtížné zadání
2. **Splnění požadavků zadání** zadání splněno
Zadání bylo bez výhrad splněno.
3. **Rozsah technické zprávy** je v obvyklém rozmezí
Technická zpráva svým rozsahem odpovídá rozmezí obvyklému pro diplomovou práci.
4. **Prezentační úroveň předložené práce** 92 b. (A)
Technická zpráva pokrývá velmi detailně jak teoretickou část, zejména relevantní problémy kryptografie a související technologie dostupné na platformě JavaScript, tak i praktickou část spočívající v návrhu řešení pro šifrování obsahu webových stránek. Celá technická zpráva je výborně strukturovaná a srozumitelná, všechna související témata jsou podrobně diskutována.
5. **Formální úprava technické zprávy** 90 b. (A)
Z formálního pohledu je technická zpráva velmi pečlivě zpracována. Jedinou drobnou výhradu mám k obrázku 4.3 nešťastně osiřelému na str. 44.
6. **Práce s literaturou** 90 b. (A)
Seznam použité literatury je poměrně obsáhlý a zdroje pokrývají celou řešenou problematiku. V textu práce jsou všechny zdroje řádně citovány.
7. **Realizační výstup** 94 b. (A)
Realizačním výstupem je řešení pro šifrování statických HTML dokumentů a jejich částí, které se skládá z klientské části v jazyce JavaScript zajišťující zejména dešifrování stránek v prohlížeči a oddělené aplikace v jazyce Python pro přípravu zašifrovaných dokumentů. Celé řešení je velmi pěkně navrženo a autor zvládl i integraci do existujícího generátoru statických stránek.
8. **Využitelnost výsledků**
Implementované řešení je veřejně publikováno na serveru GitHub a je obecně použitelné k výše uvedenému účelu.
9. **Otázky k obhajobě**
 1. Mohl byste blíže vysvětlit způsob přidělování přístupu k obsahu jednotlivým rolím pomocí šifrování? Je možné, aby měla stránka různý obsah v závislosti na roli uživatele?
10. **Souhrnné hodnocení** 92 b. výborně (A)
Pan Pekař prostudoval poměrně komplexní problematiku šifrování s důrazem na aplikaci ve webovém prohlížeči a navrhl a implementoval poměrně rozsáhlou a technicky pěkně realizovanou aplikaci. Rovněž technická zpráva je pečlivě zpracována a jak do obsahu, tak z formálního hlediska jí téměř není co vytknout.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 7. června 2017

.....
podpis