Posudek bakalářské práce

Matematicko-fyzikální fakulta Univerzity Karlovy v Praze

Autor práce	Marek Behún
Název práce	Post-quantum alternative to secure sockets
Rok odevzdání	2017
Studijní program	Informatika
Studijní obor	Obecná informatika [IOI]
Autor posudku	Mgr. Miroslav Kratochvíl Vedoucí
Pracoviště	Katedra softwarového inženýrství

K celé práci

	lepší	OK	horší	nevyhovuje
Obtížnost zadání	X			
Splnění zadání	X			
Rozsah práce *... textová i implementační část, zohlednění náročnosti*		X		

Cíle práce se týkají aktuálního vývoje na poli kryptografie a informační bezpečnosti, jsou jasně definované a práce je splňuje.

Textová část práce

	lepší	OK	horší	nevyhovuje
Formální úprava *... jazyková úroveň, typografická úroveň, citace*	X			
Struktura textu *... kontext, cíle, analýza, návrh, vyhodnocení, úroveň detailu*		X		
Analýza	X			
Vývojová dokumentace		X		
Uživatelská dokumentace			X	

Práce je napsaná kvalitní angličtinou, čte se velmi dobře. Zřídka se vyskytne drobná chyba typu a/an nebo interpunkce navíc. Několik vět v práci kombinuje příliš mnoho informací na to, aby šly pochopit napoprvé, celkový dobrý dojem to ale nenarušuje.

Zhruba polovinu práce autor věnuje popisu potřebných matematických konstrukcí — přehledně shrnuje použití konečných těles a eliptických křivek v kryptografii a popisuje poměrně nový algoritmus SIDH.

Popis implementace je rozdělen na dokumentaci autorem vytvořeného protokolu, dílčích součástí knihovny a zevrubnou dokumentaci knihovního API.

Implementační část práce

	lepší	OK	horší	nevyhovuje
Kvalita návrhu *... architektura, struktury a algoritmy, použité technologie*		X		
Kvalita zpracování *... jmenné konvence, formátování, komentáře, testování*		X		
Stabilita implementace		X		

Knihovna implementuje algoritmus SIDH a podpůrný protokol zajišťující správný průběh odvození tajných klíčů a následný přenos šifrovaných dat. Zvolený programovací jazyk je C++. Autor nepoužívá STL kvůli zachování kompatibility s embedded hardwarovými platformami, konstrukce se proto občas stylově blíží spíše C. Kód je čitelný a dobře strukturovaný, celkové přehlednosti ale škodí absence komentářů, hlavně např. v popisech rozhraní a datových struktur.

Ukázkový program 'post-kvantový telnet' je stabilní a po drobných modifikacích (autentizaci uživatele v cílovém systému) může sloužit jako bezpečná náhrada SSH.

Celkové hodnocení Výborně

Práci navrhuji na zvláštní ocenění Ne

Datum

Podpis