Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Ondrejková Ľubica** **Oponent:** **Doc. Burda Karel, CSc.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Informační technologie**
Akademický rok: **2012/2013**

Téma diplomové práce: **Současné technologické možnosti kryptografické ochrany**

Hodnocení práce:
Hlavním předmětem diplomové práce je popis možností soudobé kryptografie z hlediska ochrany utajovaných informací a popis současného stavu kryptografické ochrany komunikace s dohledovými přijímacími a poplachovými centry (DPPC). Stanovené téma je ve světle rostoucích požadavků na bezpečnost informací aktuální a obtížnost zadání je průměrná.

Studentka vypracovala práci, která je poměrně rozsáhlá (118 stran), avšak která je zároveň povrchní, matoucí a se spoustou věcných chyb. Například steganografie není součástí kryptografie (s. 11), jednosměrné šifrování (s. 33) je nesmysl (heš je kryptografický reprezentant zprávy a nikoliv zašifrovaná zpráva), klíče symetrických kryptosystémů o délce 56 bitů (s. 34) jsou z bezpečnostního hlediska naprosto nepostačující, provozní režim blokové šifry CFB není totéž co režim CBC (s. 39), v algoritmu 3DES je prostřední operace dešifrování a nikoliv šifrování (s. 40) atd. Autorka se rovněž často zabývá naprosto okrajovými aspekty (např. 15 stran o historii kryptografie v práci, v jejímž názvu se nachází slovo „současné“) na úkor úloh stanovených zadáním.

Podle zadání měla studentka vypracovat pět úloh. V první úloze měla zpracovat manuál k orientaci manažerů bezpečnostní komunity. Vzhledem k výše uvedeným věcným chybám, rozplizlosti a neujasněnosti (měla být řešeno utajení zpráv a nikoliv i jejich autentičnost) je práce pro uvedený účel nepoužitelná. Druhým úkolem byla analýza současného stavu legislativy související s kryptografickou ochranou utajovaných informací. Tento úkol autorka vyřešila jako pouhé seznámení s obsahem nejdůležitějších ustanovení příslušného zákona a vyhlášek, bez jakéhokoliv pokusu o analytický přístup. Třetím úkolem byl popis možností kryptografických ochran z technického hlediska. Autorka však namísto popisu dostupných šifrátorů, kryptografických generátorů apod. popsala principy některých metod technické ochrany prostor a zařízení (např. generátory šumu nebo stínící komora). S těmito metodami však kryptografie nemá nic společného. Poslední dva úkoly se týkají kryptografické ochrany komunikace s dohledovými přijímacími a poplachovými centry (DPPC). Zde studentka opět neřešila podstatu (tj. např. popis kryptografického zabezpečení podle standardu ANSI/SIA DC-09-2007), ale popisuje standardy, které s kryptografií nemají vůbec nic společného (např. požadavky kladené na stavební řešení DPPC).

Celkově konstatuji, že předložená práce splňuje zadání pouze částečně, je zpracována povrchně, bez hlubší znalosti problematiky a obsahuje řadu věcných chyb. Z těchto důvodů jí hodnotím stupněm E, tj. Dostatečně.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Vzhledem k nesplněným úkolům zadání mám na diplomantku k obhajobě následující požadavky:

1. Uveďte stručný přehled technických prostředků pro šifrování komunikace, které jsou komerčně dostupné (ISDN šifrátory, IP šifrátory atd.).
2. Vysvětlete podstatné rysy kryptografického řešení komunikace podle standardu ANSI/SIA DC-09-2007.

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

E - dostatečně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 3.6.2013 Podpis oponenta diplomové práce