

POSUDEK DIPLOMOVÉ PRÁCE

Název práce: Bezpečné kryptografické algoritmy

Autor práce: Bc. Zdeněk Müller

Stručné zhodnocení práce:

Diplomant si téma práce vybral sám. Teoretická část práce se zabývá uceleným popisem kryptologie. V praktické části jsou implementovány čtyři symetrické (AES, BlowFish, IDEA, RC532) a dva asymetrické šifrovací systémy (Rabin, RSA) a tři šifrovací hašovací funkce (RIPEMD 160, SHA1, SHA256).

Jak práce splnila cíle uvedené v zadání:

Cíle práce (viz zadání) byly splněny.

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

Výsledkem diplomantovy práce je obsáhlý odborně zaměřený text, který se věnuje moderní kryptografii, symetrickým a asymetrickým šifrovacím systémům, kryptoanalýze, hašovacím funkcím, generátorům pseudonáhodných čísel, kvantové kryptografii, autentizačním protokolům a popisu úspěšného útoku na SSL spojení. Svým rozsahem je práce ojedinělá a může dobře posloužit jako učební materiál s dostatkem odkazů na další literaturu. V rámci diplomové práce vznikla i nová aplikace, ve které je implementováno několik známých algoritmů (viz výše).

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

Jazyková úroveň je velmi dobrá. Některé pasáže mohly být zkráceny či úplně vynechány. V práci se vyskytuje přiměřené množství překlepů a typografických prohřešků (zejména výskyt neznělých předložek na konci řádků, používání spojovníků namísto pomlček a používání nečeských uvozovek). Bohužel se v textu vyskytuje i několik hrubých chyb, například „Vigenerovi šifry“ na str. 24 nebo spojení „se objevili výzkumy“ na str. 62 či v textu „se získaných“ na str. 90.

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

- V aplikaci, po vybrání šifry Rabin kliknutí na tlačítko „Generovat prvočíslo“ se dá chybně kliknout na tlačítko „Otestovat E“. Uživatel je následně vyzván k modifikaci čísla E, což ale není možné.
 - Chybové hlášky v dolním řádku aplikace se po vyřešení problému nesmažou a mohou tak mást uživatele.
 - Diplomanta se ptám, proč se při používání „Nápovědy aplikace“ objevuje text „This help file was created with an unregistered evaluation copy of ...“.
 - Ještě by mohl diplomant u obhajoby objasnit rozdíl mezi 4. a 5. bodem v textu na str. 102.
- Výše zmíněné chyby jsou snadno odstranitelné. Je škoda, že diplomant před dokončením práce nevyužíval konzultace s vedoucím práce.

Navrhované hodnocení práce:

Práci hodnotím známkou „B“.

Datum: 24. 8. 2012

Jméno: RNDr. Miroslav Kolařík, Ph.D., Katedra informatiky PřF UP v Olomouci

Podpis: