POSUDEK bakalářské práce

Název:	**Rekonstrukce šifrovacího stroje ŠD-2 (NSSZ6026)**
Vedoucí bakalářské práce:	**Vondruška Pavel**
Řešitel:	**Vojtěch Brtník**
Zadáno a potvrzeno:	12. 11. 2009
Datum odevzdání:	**28. 5. 2009** (termín splněn, zápočet udělen)

Zadání:
Obsahem práce je rekonstrukce historického šifrovacího stroje ŠD-2 (1957) a to na základě částečně zachované a neúplné technické dokumentace.
Práce má obsahovat tyto části:
- úvod s popisem rotorových šifratorů
- popis šifrovacího stroj ŠD-2 a jeho funkcí
- matematický model šifrovacího stroje
- kryptografická bezpečnost zařízení
- softwarový simulátor zařízení

Posudek:
Řešitel zpracoval téma dle zadání a mých pokynů zcela samostatně. Při práci vycházel z dochovaných neúplných historických materiálů a dvou stručných velmi obecných historických článků, které byly jedním z pamětníků publikovány (K.Šklíba, Crypto-World).

Po stručném úvodu do problematiky (větší hloubka nebyla vyžadována) se student soustředil na rekonstrukci zařízení a pochopení a vysvětlení, jak šifrátor pracoval (jednotlivé směnné prvky – krátkodobé a dlouhodobé klíče, šifrovací algoritmus, tvar a způsob přenosu zprávy a režimy práce stroje). Výsledky jsou uvedeny v kapitolách 3 a 4 bakalářské práce. V této části prokázal student, že zařízení dokonale porozuměl. Tato část byla stěžejní, protože mým osobním cílem bylo vytvořit popis stroje tak, aby se uchoval pro případné další studium a zařízení neupadlo v úplné zapomnění. Výklad je srozumitelný a popis je úplný.
Na základě této rekonstrukce student sestavil simulátor. Simulátor (stručně představen v kapitole 7) byl využit pro následnou statistickou analýzu kvality šifrových textů. Úkol (vyhotovení softwarového simulátoru) byl splněn velmi kvalitně. Simulátor je funkční a jeho ovládání je intuitivní a uživatelsky přítulné. Zpracování simulátoru hodnotím velmi kladně.
Šifrové texty – výstupy z ŠD-2 - jsou uvedeny v kapitole 5. Prováděné statistické testy byly poměrně rozsáhlé. V kapitole jsou uvedeny výstupy včetně stručné interpretace jednotlivých testů. V kapitole 6 je uveden velmi stručný matematický popis šifrátoru bez toho, že by byl dále využit k zisku nějakých výsledků.

Závěrečné hodnocení: řešitel splnil zadání bakalářské práce, prokázal schopnost samostatné práce, práce je srozumitelně napsána, simulátor šifrátoru je funkční a intuitivně ovladatelný.

Návrh hodnocení: z výše uvedených důvodů navrhuji udělit známku výborně

V Praze 10. 6. 2009