Posudek oponenta na bakalářskou práci

Barbora Galaczová, Rejewského a Turingova bomba.

Bakalářská práce má za cíl podat přehled metod na určování denního klíče šifrovacího přístroje Enigma.

První část obsahuje popis přístroje Enigma a jeho fungování, popis jejího použití společně s tzv. denními klíči a klíči zpráv.

Ve druhé, nejrozsáhlejší části jsou popsány metody polských kryptoanalytiků na odhalování denních klíčů, postup je vysvětlován na příkladech. Tato část by si zasloužila přesnější matematický popis a rozbor používaných algoritmů. Odkazy na část o permutacích nejsou přesně zacílené a znesnadňují tak orientaci.

Ve třetí části je poté popsán navazující postup anglických kryptologů při odhalování denních klíčů. Popsána je konstrukce Turingovy bomby a Welchmanovo vylepšení. Také u této části by byl možný rozsáhlejší matematický popis a rozbor.

Závěrečná kapitola o permutacích obsahuje základní definice, tvrzení a poznatky, které jsou využívány v předchozích kapitolách. Schází číslování definic a tvrzení, což znemožňuje přesnější odkazování z předchozích částí.

Celkově práce obsahuje minimum věcných a tiskových chyb, grafická a jazyková úroveň je velmi dobrá. Práce by mohla být více strukturovaná a obsahovat více matematického pohledu a přesnějšího popisu algoritmů. Práce splňuje požadavky kladené na bakalářskou práci. Navrhuji hodnocení

Velmi dobrý (2)

V Praze, 21.6.2006

Mgr. Jiří Vábek.
Oponent práce