Posudek oponenta bakalářské práce

Název: Metody odhalování denních klíčů u Enigmy
Autor: Dominika Kubániová

Shrnutí obsahu práce

Práce Dominiky Kubániové je věnována popisu a odůvodnění metod odhalování takzvaných denních klíčů šifrovacího stroje Enigma. Zatímco první kapitola obsahuje popis fungování Enigmy a tři verze protokolu šifrování (používaný před 15. zářím 1938, mezi 15.zářím 1938 a květnem 1940 a od května 1940), druhá kapitola prezentuje matematický model tohoto stroje. Nejrozsáhlejší třetí část textu se zabývá matematickým odůvodněním dvou metod odhalování denních klíčů navržených polskými matematiky známých pod názvy Rejewského bomba a Zygalského plachty. Čtvrtá kapitola je věnována principu a odůvodnění takzvané Turingovy bomby, která umožňovala získání denních klíčů chronologicky poslední verze protokolu.

Celkové hodnocení práce

Téma práce. Téma práce bylo sice poměrně obtížné, ale velmi zajímavé a tudíž vhodné pro zpracování v bakalářské práci. Zadání práce bylo studentkou podle mého mínění úspěšně naplněno.

Vlastní příspěvek. Studentka byla nucena formulovat a exaktně dokázat funkčnost metod, které jsou sice popsány v literatuře, ovšem bez dostatečně podrobné korektní matematické argumentace.

Matematická úroveň. Úroveň práce je vysoká. Matematický model problému je srozumitelně formulován a důkazy korektnosti postupu jsou přehledné a dobře srozumitelné.

Práce se zdroji. Text využívá větší množství zdrojů, na nichž zjevně není formulačně závislý. Jádro práce navíc spočívalo v tvorbě matematického modelu a vlastním odůvodnění známých postupů.

Formální úprava. Formální náležitosti práce nezasluhují žádnou výtku, text je napsán velmi čtivě kultivovaným jazykem. Jazykových a stylistických nepřesností jsem zaznamenal zanedbatelné množství.

Připomínky a otázky

1. strana 22: V závěru důkazu Tvrzení 3 je zdá se opomenut (symetrický) důkaz zpětné ekvivalence rovností (3.7) a (3.8).

Závěr

Práce Dominiky Kubániové „Metody odhalování denních klíčů u Enigmy" je podle mého názoru velmi zdařilá, bezpochyby splnila zadání a proto ji doporučuji uznat jako bakalářskou.

Návrh klasifikace oponent sdělí předsedovi zkušební (sub)komise.

Jan Žemlička
Katedra algebry
5.9.2018