Posudek vedoucího na bakalářskou práci

Barbora Galaczová, **Rejewského a Turingova bomba**

Tématem práce Barbory Galaczové jsou metody odhalování denních klíčů u německého šifrovacího přístroje Enigma. Tyto metody byly rozpracovány původně polskými matematiky v letech 1932–1938 a poté britskými matematiky v období druhé světové války.

K tomuto tématu není příliš mnoho podkladů. Několik původních prací Mariana Rejewského, mnohé pouze v polštině, nedávno zveřejněné části pojednání Alana Turinga a několik stran v knize L. Bauera. Autorka se s veškerou literaturou podrobně seznámila.

Metody odhalování denních klíčů se vyvíjely během celého sledovaného období současně s tím, jak německá armáda měnila pravidla (protokol) pro používání přístroje Enigma. Metody pro odhalování denních klíčů použitelné pro jeden protokol přestaly být účinné při změně protokolu a bylo nutné vytvořit metody nové.

Autorka v práci podrobně probírá a vysvětluje šest metod Mariana Rejewského a jeho kolegů a dále konstrukci Turingovy bomby.

Práce je zpracována velmi pečlivě, má kvalitní grafickou úpravu, jazyk je místy trochu expresivní, to ale souvisí se zdroji, ze kterých autorka čerpala..

Následuje několik připomínek.

Trochu mi v práci schází jednoduchý časový přehled vývoje jednotlivých metod. Tyto údaje jsou místy uvedené při popisu metod a jejich souvislosti s příslušnými změnami protokolu. Celkový přehled o vývoji metod ale neposkytují.

Autorka se do velké míry nechala ovlivnit stylem, kterým jsou napsány zdroje, ze kterých čerpala. S výjimkou jednoho článku Mariana Rejewského jsou tyto práce psané pro nematematické publikum a tomu odpovídá jejich styl. Důraz na jazykových popis metod, volnější přístup k terminologii a podobně. To se bohužel projevuje v hodnocení práci větší měrou, než by se mi zamlouvalo. Následuje pár ukázek tohoto volnějšího přístupu k pojmům.

Str. 10, řádek 1. Autorka píše o změnách *pozic rotoru* na ose, správně by ale mělo být *pořadí rotoru*. Pozicí rotoru se na jiných místech rozumí natočení rotoru na ose.

Str. 17, řádek 2. Zde autorka píše o *určitých charakteristických vlastnostech*, což patrně vzniklo překladem anglického (případně polského) pojmu *characteristic*, který má ale přesný matematický význam. Je používán pro složení permutací používaných pro šifrování prvního a čtvrtého (druhého a pátého, případně třetího a šestého) písmene indikátoru – klíče zprávy. Katalog, který byl pomocí cyklometru vytvořen, pak obsahoval cyklické typy těchto permutací.

Str. 30, prostřední odstavec. V poslední větě se mluví o nalezení *správné pozice*, hned v první větě následujícího odstavce se ale mluví o nalezení *zdánlivě správných možností poloh rotoru*.

V odst. 4.2 je používán pojem *větve grafu*, který není nikde definován a je ponecháno na čtenáři, aby si jej domyslel.

Také je třeba upozornit na nekonsistenci příkladu denního klíče konci části 2.1, kdy jsou při označení symbolů na abecedním kroužku (prstenci) použita čísla a u základního nastavení písmena, přitom jde o ty samé symboly.

Právě v nedostatečné exaktnosti některých formulací a malém důrazu na matematickou formulaci a zdůvodnění použitých metod vidím hlavní slabinu práce. Na konci je sice uvedený dodatek *Kapitola o permutacích*, obsahující elementární pojmy z teorie permutací, na které se Rejewski ve svých článcích odvolává, propojení této kapitoly s hlavním textem práce je ale minimální.

Naproti tomu musím jako klad zdůraznit ještě jednou pečlivost a výbornou grafickou úpravu práce.

Proto navrhuji, aby byla práce přijata jako práce bakalářská a hodnocena známkou *velmi dobře*.

V Praze 26.6.2007

Doc. RNDr. Jiří Tůma, DrSc.