Posudek oponenta na bakalářskou práci

Vojtěch Brtník, *Rekonstrukce šifrovacího stroje ŠD-2*

V předložené práci se autor zabývá především rekonstrukcí struktury šifrovacího stroje ŠD-2, který byl zvažován pro použití v ČR v padesátých létech. Jde o šifrovací stroj podobného type jako byla německá Enigma, ovšem bez reflektoru a s vylepšeným protokolem.

Práce začíná úvodem napsaným vzletným jazykem, bohužel také s několika nepřesnostmi. Tak například ve druhém odstavci se mluví o tom, že k bezpečnosti Vigenérovy šifry stačí klíč stejné délky jakou má šifrový text. K bezpečnosti je ale potřeba také, aby byl klíč náhodnou posloupností znaků. Ve třetím odstavci je při posuzování bezpečnosti polyalfabetické šifry generované automatickým šifrátorem zmiňována pouze délka hesla. Hlavní předností těchto strojů ale byla skutečnost, že jednotlivé jednoduché záměny generované šifrátorem v různých polohách jsou obecné (ideálně náhodné) permutace, nikoliv pouze cyklická posunutí, jako u Vigenérovy šifry.

Jádro práce je v popisu fungování šifrátoru ve třetí a čtvrté kapitole. Tato část je napsána hodně srozumitelně, je nutné ovšem dodat, že popis nevyžaduje žádnou velkou matematickou zběhlost. Určité problémy jsem měl pouze s pochopením role kolíčků při přenosu rotací, zde bych autora požádal o pečlivější vysvětlení během obhajoby. Dále jsem nepochopil, jak se obě strany komunikace domlouvaly o nastavení kolíčků při vzájemné komunikaci, když ani v denním klíči a v jednorázovém klíči o tom není žádná informace. Další problém jsem měl s tím, proč je nutné při generování jednorázového klíče podle odstavce 4.2.5 tisknout klávesy a proč nejde klíč prostě zvolit volbou náhodné posloupnosti pěti písmen.

Dále práce pokračuje popisem jednoduchých statistických testů šifrového textu generovaného jedním nastavením přístroje. Autor v úvodu 5. kapitoly zmiňuje, že různá nastavení produkují texty s různými statistickými vlastnostmi. Znamená to, že v jiných nastaveních může stroj produkovat šifrové texty, které při jednoduchém statistickém zkoumání nevypadají jako náhodné? To by byla ale závažná slabina přístroje, svojí formulací asi autor myslel něco jiného. Nakonec je doplněna matematickým modelem šifrátoru. Ani zde není potřeba žádná složitá matematika, pouze jednoduché použití teorie permutací.

Práce nepochybně splnila svůj účel zaznamenat konstrukci a popis fungování šifrátoru pro případné další zkoumání. V jednom nastavení potvrdila očekávanou hypotézu, že stroj produkuje šifrové texty, které nelze jednoduchými statistickými testy odlišit od náhodných.

V práci není příliš mnoho překlepů, pouze dost chyb v interpunkci, autor často uvádí vedlejší větu správně čárkou, ta ale často chybí na konci vedlejší věty.

Navrhuji uznat práci jako práci bakalářskou a hodnotit ji známkou výborně případně velmi dobře (vzhledem k jednoduchosti tématu).

V Praze dne 23.6.2009

Doc. RNDr. Jiří Tůma, DrSc.