Posudek oponenta na bakalářskou práci

Petr Veselý, **Luštění německého šifrovacího stroje Lorenz**

Petr Veselý se ve své práci zabývá rozluštěním německého šifrovacího stroje Lorenz za druhé světové války. Jeho práce není přímou rekonstrukcí odhalení konstrukce tohoto přístroje, spíše předkládá alternativní postup této rekonstrukce využívající současné počítače. Na druhou stranu je jeho postup realizovatelný i ručně, pouze by jeho realizace trvala mnohem delší dobu.

Po stručném historickém úvodu a popisu stroje Lorenz autor uvádí několik kroků, kterými se britská přiblížila odhalení vnitřní konstrukce přístroje. Počátečním bodem jeho analýzy je chyba šifranta, která umožnila britským kryptoanalytikům zjistit 3976 znaků dlouhou pseudonáhodnou posloupnost klíče generovaného přístrojem.

Odvozením konstrukce přístroje začíná nalezením vzorků pro nastavení rotorů K_i. To lze převést na luštění Vigenérovy šifry, kde klíčem jsou znaky generované rotory K_i a otevřeným textem jsou znaky generované rotory S_i, v obou případech pro i=1,2,3,4,5. Protože se rotory K_i pohybovaly v šechy současně, stejně jako rotory S_i, lze rekonstrukci nastavení rotorů K_i provádět samostatně pro jednotlivá i. Autor používá standardní metody pro zjištění délky periody klíče, Kasinského test a index koincidence. Vzhledem k tomu, že klíč i otevřený text jsou posloupnosti 0 a 1, aplikuje test koincidence na bigramy. Tím získá nejen periody rotorů K_i, ale také posloupnost klíče a otevřený text, tj. posloupnost generovanou rotorem S_i.

Pro odhalení period a nastavení rotorů S_i používá statistické testy, které vedou ke správnému výsledku, zdůvodnění proč k nim vedou, je ale trochu nejasné. Nakonec zjišťuje periody a nastavení dvou řídících rotorů, zde jde patrně o stejný postup, jaký vedl k cíli i v Bletchley Park.

Práce je napsaná velmi pečlivě a čtivě, po stránce stylistické jí lze sotva něco vytknout. Následuje jenom pár připomínek k prezentaci výsledků a jeden dotaz.

- Při prvním čtení mě trochu zmátlo použití slova *aktivní* ve dvou různých významech v úvodu části 2.3. na straně 10. I když je toto slovo použito ve dvou různých souslovích, asi by stálo za zvážení nahradit v jednom případě slovo *aktivní* jiným slovem.
- V definici 3.1 se mluví o *aditivní grupě*. Aditivní grupa není definována bez uvedení tělesa, ve kterém touto aditivní grupou je. Autor má patrně na mysli *abelovskou grupu*.
- Trochu matoucí je také používání slova *impuls* pro posloupnost generovanou rotorem K_i v části 3.5. a následujících, zejména proto, že dříve na straně 10 je termín impuls používán pro jeden bit.
- Na straně 25 autor používá pojmy Vigenérova šifra a polyalfabetická substituce ve stejném významu. Častější je asi používání pojmu polyalfabetická substituce v širším významu, kdy jednotlivé substitue jsou obecné permutace, nikoliv pouze cyklická posunutí abecedy jako je tomu v případě Vigenérovy šifry. Z tohoto důvodu je slovní popis odhalení posloupnosti generované rotorem K_i trochu nejasný.
- Trochu mi také scházelo zdůraznění souvislosti nepravidelné frekvence bigramů v posloupnosti S'_i (tj. v „otevřeném textu" při luštění Vigenérovy šifry odhalujícím

posloupnost K_i) s pohybem rotoru S_i při generování klíče. Ta je uvedena až na straně 40.

Otázka. Čím je způsobený velký rozdíl mezi odhadem velikosti průměrů výběrových rozptylů na straně 32, odhad je 1,86, a skutečně vypočítanými hodnotami v tabulce 3.19, které jsou kolem 1,04 ? Velikost tohoto rozdílu vyvolává jisté pochybnosti o zdůvodnění statistické metody, která vedla k odhalení počtu jednotlivých běhů v posloupnosti S_i.

K práci je přiloženo CD s podrobnějšími informacemi o výpočtech a kvalitním simulátorem s velmi jednoduchým ovládáním.

Práce je velmi kvalitní a bohatě naplňuje požadavky kladené na bakalářskou práci. Proto navrhuji, aby byla práce přijata jako práce bakalářská a hodnocena známkou *výborně*.

V Praze 26.6.2007

Doc. RNDr. Jiří Tůma, DrSc.