POSUDEK BAKALÁŘSKÉ PRÁCE

Autorka bakalářské práce: Ondřej Vaverka
Název bakalářské práce: Historický vývoj kryptografie v období světových válek
Vedoucí práce: Doc. Jiří Ivánek, CSc.
Oponent práce: Ing. Martin Souček, Ph.D.
Hodnocení: výborně

Posudek: 29.8.2012

Cíl práce:
Cílem práce bylo popsat významné části kryptografické historie v období první a druhé světové války a dále popsat základy Shanonovy teorie informace, která v té době vznikala.

Shoda se zadáním bakalářského úkolu:
Cíl i struktura práce dobře sleduje zadání bakalářského úkolu.

Hodnocení práce:
Předložená bakalářská práce zpracovává období, ve kterém se rodila moderní kryptologická epocha i informační věda a kdy přístup k informacím rozhodoval o osudu milionů lidí. Kryptografie a kryptoanalýza během obou světových válek zásadním způsobem ovlivňovala vítězství i prohry jednotlivých bitev a v důsledku pak i výsledek války.
Tyto historické procesy práce popisuje nejprve na pozadí první světové války, pak podrobněji v rámci druhé světové války. V souvislosti s historickými událostmi autor sleduje teoretické principy, které byly pro kryptografii a kryptoanalýzu v této době používány. Během tohoto popisu prokazuje pochopení kryptologických postupů, pečlivost nastudování historických souvislostí i dostatečné porozumění matematickým principům, na kterých je kryptografie a kryptoanalýza postavena.
Čtivě je popsána atraktivní historie Enigmy i pozdějších šifrovacích strojů, zajímavým, byť částečně přejatým způsobem, je provedeno srovnání úspěšnosti spojenecké a německé kryptologie. Samotný závěr práce popisuje zrod oboru Information Science tak, jak byl založen v poválečném období Claudem Shanonem.
Práce je v dobrém slova smyslu kompilační, autor po nastudování velkého množství podkladů sestavil kryptologický pohled na období obou válek, který je zajímavý spojováním historických souvislostí s kryptografickou a informační teorií.

Volba informačních zdrojů:
Autor pracuje s rozsáhlým množstvím kvalitních českých i zahraničních informačních zdrojů, citace v textu jsou systematicky uváděny.

Stylistická úroveň práce:
Po této stránce nemám k práci výhrady, práce je dobře napsaná.

Formální úprava práce:
Po pravopisné stránce nemám výtky, grafická úroveň práce je velmi dobrá. Chybí odkaz na zdroje jednotlivých obrázků v příloze.

Doplňující otázky:

1. Jakým způsobem byly z tohoto historicky a kryptograficky bohatého období vybírány popisované epizody?
2. Pokud se střední a levý rotor Enigmy během šifrování netočí, jedná se o polyalfabetickou, nebo monoalfabetickoou substituční šifru?

Závěr

Celkově mohu říci, že práci považuji díky úrovni pochopení složité kryptologické problematiky za velmi dobrou, pečlivě zpracovanou. Doporučuji hodnocení výborně.

Martin Souček