Ukázka z kapitoly *6. VYZKOUŠEJTE SI …*

Šifrové texty

Na závěr si můžete zkusit luštění následujících třiceti šifrových textů. Otestujete si tak, jak pozorně jste knihu přečetli, co jste si z ní zapamatovali, ale hlavně vám to umožní zažít krásný a neopakovatelný zážitek, kdy se ze šifrového textu začne díky vašim znalostem, fantazii a trpělivosti vynořovat otevřený text. Pro luštitele to je vrcholný a nezapomenutelný okamžik a vy máte nyní možnost jej také prožít. Není vyloučeno, že to pro vás bude tak krásný zážitek, že se rozhodnete se této nádherné, ale velmi složité vědě – kryptologii - profesionálně věnovat. Držím vám na této těžké cestě palce.

Úlohy jedna až čtrnáct jsou velmi lehké a měli byste je při troše trpělivosti vyluštit. Jedná se zpravidla o systémy, jež jsme označili jako šifry, které skutečnými šiframi nikdy nebyly. K jejich vyluštění stačí správně odhalit konkrétní použitý šifrový nebo kódový systém. Pokud se chcete ujistit, že jste se vydali správnou cestou, můžete nahlédnout do prvé nápovědy, která obsahuje obecné určení systému (transpozice, jednoduchá záměna, steganografie atd.). Úlohy patnáct až dvacet jsou již pro přímé luštění o něco složitější. Jedná se o klasické šifrové systémy, k jejichž vyluštění však stačí správné určení použitého šifrového systému. Tyto šifry (až na úlohu šestnáct) patří do skupiny šifer, které jsou založeny na tzv. omezených algoritmech. Jedná se tedy převážně o šifry, které nepoužívají klíč. Úlohy dvacet jedna až dvacet sedm patří mezi klasické šifrové systémy. Tyto šifry používají klíčové hospodářství a tedy pouhé odhalení systému ještě automaticky nevede k získání otevřeného textu. Vzhledem k tomu, že tato kniha obsahuje jen velmi stručné poznámky k luštění těchto šifer, lze je považovat za těžké. Pokud se však budete věnovat kryptologii, bude řešení těchto úloh pro vás velmi lehké a samotné hledání otevřeného textu patří mezi základní kryptoanalytické metody a lze jej zcela zautomatizovat. Pokud při jejich řešení budete neúspěšní, můžete využít druhou nápovědu, kde je uveden použitý konkrétní šifrový systém a klíče. Luštění příslušného šifrového textu se díky tomu změní na jeho dešifrování. Pokud jste pochopili popis šifrového systému, nemělo by vám dešifrování úlohy, a tedy nalezení otevřeného textu, dělat problém. Poslední tři úlohy jsou velmi těžké. Jedná se o šifry, kde i profesionálové měli v době jejich vzniku problém do nich proniknout. Vyřešit úlohu z jediného textu je opravdu obtížné a doporučuji u těchto příkladů využít informací uvedených ve druhé nápovědě.

Poznámka:
Úlohy z této kapitoly byly použity v v roce 2006 v tradiční soutěži v luštění jednoduchých šifer, která probíhá vždy na podzim pod záštitou e-zinu Crypto-World.

Úlohy a informace o soutěži můžete proto najít na stránce soutěže:
http://crypto-world.info/souteze.php
resp.
http://soutez2006.crypto-world.info/