Ukázka z kapitoly *5. Důležitá data a mezníky v dějinách kryptologie*

1415

Pravděpodobně prvním dochovaným dokladem o používání šifer v Čechách jsou listy Mistra Jana Husa z Kostnice. Jeho šifrový systém byl velice jednoduchý, šifroval pouze samohlásky a to tak, že je nahradil písmenem, které jej v abecedě následuje. Místo A psal B, místo E napsal F atd. OKO, ALBATROS by zašifroval jako MKM, BLBBTRMS. Systém je z kryptologického hlediska velmi slabý a navíc nejednoznačný. Příjemce může mít v některých případech problém s dešifrováním, neboť nemusí být na první pohled zřejmé, které písmeno je v otevřeném tvaru (souhláska) a které je šifra (samohláska). Nejednoznačnosti mohou vzniknout především v krátkých textech.

1835

Používání slabé šifry k uchování osobního tajemství nám zanechalo i zajímavé svědectví ze života Karla Hynka Máchy (1810-1836). Máchův Deník z roku 1835 obsahoval i šifrované pasáže, které se podařilo rozluštit novináři a historikovi Jakubu Arbesovi v 80. letech 19. století. Vzhledem k jejich intimní povaze a s ohledem na budovaný kult Karla Hynka Máchy nebyly zahrnuty do žádného vydání Máchových spisů. Poprvé vyšly v 70. letech 20. století (česky jako bibliofilie v počtu 20 kusů, italsky v Benátkách). Oficiální úplné české vydání Deníku, včetně překladu zašifrovaných částí, pochází až z roku 1993.

Mácha použil jednoduchou záměnu, kdy šifrový text nejprve píše podle běžného zvyku zleva doprava, ale na konci řádku nepřejde na začátek nového řádku, ale píše zprava do leva – tj. jako když kůň oře pole.

1914-1918

Tajná komunikace české protirakouské politické opozice během první světové války je dobře vylíčena v knize Karla Čapka „Hovory s T.G.Masarykem“.

Prezident Tomáš Garrigue Masaryk v ní vzpomíná :

„Mnoho práce a starostí bylo s vypravováním poslů do Prahy. Nechtěl jsem užívat obvyklých a rakouským úřadům jistě známých prostředků, jako je zašít zprávy do límce nebo je vložit do podpatků a podobně. To byly někdy dost těžké technické problémy: například dát papírek pod regulátor rychlosti do hodinek; vhodně navrtat deštník, dát stočený dopis do plavajzu

(zastaralý název pro tužku), ze kterého se musel šikovně odstranit kousek tuhy; ty kumšty prováděl hlavně inženýr Baráček. Jeden český stolař nám dělal kufry ne s dvojím dnem, ale s dvojitou stěnou; hlavní vtip byl, aby ta stěna při zaklepání nezněla dutě, ale aby zrovna zvonila - ten stolař to dovedl. Jindy jsme dali své zprávy do sudů s olejem, a to se zas musely nenápadně označit ty sudy."

Pro psaní senzitivních zpráv mezi domácím a zahraničním odbojem se používal i neviditelný inkoust, který byl za I.světové války velmi rozšířen a s oblibou používán špióny na všech frontách. Konkrétně to bylo v korespondenci mezi pražským průmyslníkem J. J. Fričem a jeho obchodním zástupcem v Itálii a Švýcarsku Z. Rohlou.

Mimo těchto typických steganografických metod se používalo i šifrování. Svědectví o jeho použití se dochovalo v již zmíněné knize, kde prezident Masaryk uvádí, že inženýr Baráček v Ženevě pro účely odboje zkonstruoval dokonce šifrovací stroj.

1939

V předvečer obsazení Československa Německem odlétalo 14.3.1939 do Londýna v tajnosti letadlo, kde bylo vyčleněno 11 míst pro československé zpravodajské důstojníky. Do výběru se nedostal nikdo z tehdejších kryptologů a to ani vedoucí českých šifrérů - zkušený kryptolog Rohatý. Ten pouze stačil připravit popis doporučených šifrových systémů pro komunikaci s Londýnem a předat jej plukovníku Moravcovi, který odpovídal za vytvoření československé zpravodajské londýnské centrály. Moravec však zjistil, že navrženým postupům nerozumí, a tyto systémy proto nebyly použity. Důsledkem tohoto jeho rozhodnutí pak bylo použití slabých šifer a řada dalších osudových chyb naší centrály.

1941

V Londýně nebyl v době války k dispozici žádný český kryptolog, a proto depeše mezi centrálou a českým odbojem trpěly řadou základních chyb. To bohužel mělo za následek i to, že pravděpodobně byly některé odbojové skupiny odhaleny na základě analýzy dešifrované komunikace.

Jako příklad chyb, kterých se centrála dopouštěla, si uvedeme ukázku textu depeše odeslané 24.6.1941 z Londýna do Prahy.

DOM. Pro tajné depeše navrhuji jiný šifrovací způsob. Pod zašifrovací heslo se píší místo písmen a jiných znaků už jejich šifry a to do každého čtverečku jedna číslice. Počet čtverečků pod heslem musí být dělitelný pěti. Není-li, přidá se v poslední řádce tolik nul, aby se dosáhlo

nejbližšího tohoto čísla. Ze zašifrovacího obrazce se pak čtou sloupce s čísly svisle podle číselného pořadí hesla a píší se vodorovně pod zašifrovací heslo. Zde se opět čtou svisle ve sloupcích podle číselného pořadí hesla a tvoří se pětimístné šifrové skupiny. Způsob je naprosto jistý, protože šifrové dvojice jsou transpozicí rozlomeny. Není však to rychlé jako způsob dosud používaný. Pro tento šifrovací způsob platná jen jedna jediná abeceda a to pro prvý den v měsíci. Dá se tedy naučit nazpaměť. Sdělte mi váš názor. Dík. SUDAR.

V české centrále se dopustili hned dvou velkých chyb:

1) předpokládali, že navržený kombinovaný šifrový systém STT – substituce a úplná dvojitá transpozice - je bezpečný („jistý“), přestože způsob luštění systému byl již na začátku třicátých let popsán v dostupné kryptologické literatuře,
2) domluva na šifrovém systému touto cestou je klasické porušení základních pravidel konspirace.

2004

Čínští vědci Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu na konferenci Crypto 2004 oznámili, že dokáží prolomit hašovací funkci MD5 a dále méně odolné funkce MD4, RIPEMD a HAVAL-128. Vědci nalezli nové obecnější techniky využití slabin iterativních hašovacích funkcí pomocí diferenciální kryptoanalýzy. Prolomením hašovací funkce zde máme na mysli praktické nalezení kolize, tj. dvou různých zpráv vedoucích na stejnou haš. Problematika byla intenzívně studována i v ČR. Kryptolog Vlastimil Klíma jako druhý na světě našel metodu, jak hledat kolize hašovacích funkcí. Jeho metoda je rychlejší než původní čínská metoda. V Čechách byla také zveřejněna prvá práce (autor Ondrej Mikle) ukazující, jak lze nalezené kolize využít k útoku, který zpochybňuje důvěru v předaná podepsaná data.