Obsah

O české kryptologii

Motto:
Šifrování je často jedinou možností,
jak chránit cenná data.

Kryptologie není naukou o kryptách, jak si hodně lidí myslí, ale o šifrách, a její vliv na světovou historii je fascinující. A jaká je česká kryptologie? Máme také my nějaké tajné pracoviště nebo podzemní město, jako je tomu v Anglii v Menwith Hill, kde se luští a vyhodnocují zachycené komunikace? Tahle tichá pracoviště totiž ovlivňovala výsledky všech válek, na něž si vzpomenete. Také naše šifrogramy, proudící za druhé světové války mezi Londýnem a domácím odbojem, byly luštěny, jak ostatně po válce potvrdili sami zajatí Němci, kteří luštění prováděli. Začal jsem druhou světovou válkou, protože v předválečné české kryptologii se nedělo nic významného. Po válce se česká kryptologie stabilizovala a vyvíjela až do roku 1989 v závislosti na tehdejším SSSR. Přestože nejexponovanější vládní spoje byly zajištěny sovětskou technikou, byly vyvíjeny šifrátory také ryze české a úroveň kryptologie nebyla malá. Soustředila se však výhradně na zajištění potřeb ministerstev (zahraničí, vnitro, armáda) a státně-mocenského aparátu. Po sametové revoluci došlo k odlivu pracovníků příslušných služeb do komerční oblasti, kde vznikala poptávka po šifrovacích zařízeních, programech pro ochranu dat apod. Zařadili jsme se dokonce mezi vývozce šifrovacích zařízení a softwaru. Během uplynulých 13 let se také samostudiem vyškolilo několik desítek vysokoškoláků v oblasti počítačové bezpečnosti a částečně i aplikované kryptologie. Všude ve vyspělých zemích se však kryptologie už řadu let vyučuje na vysokých školách a o bezpečnosti a kryptologii zde vycházejí stovky knih. Přesto i tam je po těchto specialistech velká poptávka. Prudký nárůst zaznamenala také teorie. Před dvaceti lety proběhla během roku jediná světové kryptografická konference, nyní se jich každoročně koná více než pět. Lidé, kteří rozumí metodám ochrany dat, jsou a budou potřební v mnoha bankách, na ministerstvech a v jiných státních institucích, u mobilních operátorů, v průmyslu informačních a komunikačních technologií apod. Dnes tu ale tito lidé chybí – a chybí i příslušná

česká terminologie. I když jsem se snažil po celých deset uplynulých let kryptologii popularizovat – zejména každý měsíc v časopise *Chip*, ale i na různých bezpečnostních konferencích – výsledek je nevalný. Každý druhý technik místo šifrovat řekne „kryptovat" a místo autentizace „autentikace". Chce to zkrátka ještě čas. Získal jsem však mladého kolegu Tomáše Rosu, jednoho z mála porevolučních vysokoškoláků, který si může říkat kryptolog. V takto vzniklém tandemu jsme při práci na jednom projektu pro Národní bezpečnostní úřad také objevili závažnou chybu v programu PGP. Tím jsme dostali „českou kryptologii" i na stránky *The New York Times* (PGP používají miliony Američanů a jsou na něj hrdí, viz 8. kapitola této knihy). Podařilo se nám přispět i k rozvoji teorie a popsat možné útoky na algoritmus RSA tam, kde by to nikdo nečekal. Po dvaceti letech konání světových kryptografických konferencí tak v Kalifornii letos zazněl i náš příspěvek. Český kryptologický výzkum stále tvoří roztroušené a izolované ostrůvky, na tom jsme nic nezměnili, ale Češi jsou chytrý národ, takže za několik let může situace vypadat mnohem nadějněji.

Co v knize nenajdete

A teď ještě pár slov o tom, jaké významné události se odehrály až po napsání knihy, takže v ní již nemohly být zaneseny. V roce 1998 byl za čtvrt milionu dolarů sestrojen DES-Cracker – stroj, který je během devíti dnů schopen vyzkoušet všech 2^{56} (tj. 72 057 594 037 927 936) možných klíčů šifry DES. Dále se na internetu spojilo 300 000 dobrovolníků a po čtyřech letech práce jejich počítače vyluštily 64bitový klíč k šifře RC5. Nejpodstatnější událostí bylo však přijetí nového amerického šifrovacího standardu AES v roce 2002. Byl vybrán po čtyřech letech veřejné soutěže a i jeho nejkratší klíč má cca 3.10^{38} možných hodnot, je tedy tak velký, že vyzkoušení všech možností dostupnými hmotnými pozemskými zdroji je vyloučené. Ledaže by došlo ke zcela převratnému pokroku, například na poli tzv. kvantových počítačů, o nichž se v knize také dočtete. Jako obrana proti kvantovým počítačům už byly také zkonstruovány nové kvantové šifrátory. Jinými slovy, neustálý souboj kryptografů a kryptoanalytiků se nezastavil. Už už se zdálo, že kryptografové vyhráli, neboť AES bude dost silná, ale luštitelé přišli s novým objevem, který do-

stal divné jméno – postranní kanály. Kryptoanalytici ukázali desítky možností, jak čerpat informace nejen z vlastních šifrogramů, ale i ze způsobu jejich vzniku, ze způsobu, jak šifrátory pracují nebo komunikují se svým okolím. Dokáží užitečnou informaci získat z těch nejnicotnějších detailů, například z chybových hlášení typu „dešifrování této zprávy nedopadlo dobře“, z časového trvání operací nebo z elektromagnetického vyzařování šifrátoru. Tyto fantastické objevy nových možností kryptoanalýzy vyvolají protiakci kryptografů. Mnoho zařízení nebo počítačových programů se dostane do nového ohrožení, mnozí výrobci nebudou na tato nová nebezpečí reagovat a mnoho lidí bude stále dělat tytéž chyby jako před sto lety. A tajné služby? Ty se po pádu železné opony přeorientovaly více na ekonomickou špionáž. K tomu přistupuje nový protivník – mezinárodní terorismus. Proto zápas mezi kryptografy a kryptoanalytiky vůbec nekončí, naopak je stále dramatičtější. Ani velký bratr nespí, neboť – jak se říká v NSA: „V Boha věříme, vše ostatní monitorujeme.“

RNDr. Vlastimil Klíma, prosinec 2002

Úvod

Králové, královny a generálové po tisíce let spoléhali na účinné komunikační systémy, jež jim umožňovaly vládnout jejich zemím a velet armádám. Zároveň si vždy byli vědomi, jaké následky by mělo, kdyby jejich zprávy padly do nepovolaných rukou: vyzrazení cenných tajemství cizincům, odhalení klíčových informací nepříteli. Bylo to právě riziko vyzrazení, co vedlo k rozvoji kódů a šifer, tedy technik určených k ukrytí smyslu zprávy před všemi kromě zamýšleného příjemce.

Ve snaze dosáhnout utajení provozují jednotlivé státy svá šifrová pracoviště zodpovědná za bezpečnost komunikací, kde se vyvíjejí a uvádějí do praxe nejlepší možné šifry. Cizí luštitelé šifer se naopak snaží tyto šifry rozluštit a získat ukrytá tajemství. Luštitelé šifer jsou lingvističtí alchymisté, jakési mystické společenství, které se snaží vyluštit z nesrozumitelných symbolů jejich skrytý význam. Historie kódů a šifer je příběhem boje mezi tvůrci a luštiteli šifer, boje probíhajícího po staletí, intelektuální bitvy, jež měla a má hluboký dopad na světové dějiny.

Při psaní této knihy jsem sledoval dva hlavní cíle. Prvním z nich je zmapovat vývoj kódů. Slovo vývoj je případné, protože rozvoj šifrovacích technik lze chápat jako evoluční zápas. Kód je vždy v ohrožení. Jakmile luštitelé vyvinou nový způsob, jak odhalit slabinu kódu, ztratí tím kód svůj význam. Buď zmizí, nebo se přetvoří v nový, účinnější kód. I ten pak prosperuje pouze do té doby, než se podaří odhalit jeho slabiny – a tak dále. Jde o analogii situace, v níž se nachází například bakteriální kmen nakažlivé nemoci. Bakterie žijí, prosperují a přežívají do té doby, než lékaři najdou antibiotika, jež jsou namířena proti slabému místu daných bakterií a dovedou je zabít. Bakterie jsou tak nuceny dál se vyvíjet a antibiotika „přelstít“. Pokud se jim to povede, budou znovu přežívat a prosperovat. Jsou pod neustálým evolučním tlakem, jímž působí nasazení nových a nových léků.

Neustálý boj mezi tvůrci a luštiteli šifer vedl k celé řadě významných vědeckých objevů. Tvůrci šifer vždy usilovali o stále dokonalejší utajení komunikací, zatímco jejich luštitelé vyvíjeli ještě rafinovanější techniky útoku. V této snaze o uchování i odhalení tajemství musely obě strany zvládnout rozmanité obory a technologie od matematiky po lingvistiku, od teorie informace po kvantovou fyziku. Vynaložené úsilí bylo pro všechny zmíněné obory přínosem a jejich práce vedla často k urychlení technického pokroku. Nejvýraznějším příkladem je vznik moderních počítačů.

Kódy stojí v pozadí mnoha historických mezníků. Někdy rozhodovaly o výsledcích bitev, jindy zapříčinily smrt korunovaných hlav. Pro ilustraci klíčových okamžiků evolučního vývoje kódů vám předkládám příběhy o politických intrikách, o životě a smrti. Historie kódů je natolik bohatá, že jsem byl nucen mnoho fascinujících příběhů vynechat – má práce rozhodně nevedla k vyčerpávajícímu výsledku. Pokud se chcete dovědět více a prostudovat problematiku detailněji, odkazuji vás na seznam doporučené literatury.

Vedle souhrnu vývoje kódů a jejich důsledků pro historii je druhým cílem knihy ukázat, že tato tematika je dnes důležitější než kdy dříve. V době, kdy se informace stávají stále cennější komoditou, kdy komunikační revoluce mění podobu společnosti, začíná hrát šifrování v každodenním životě stále důležitější roli. Naše telefonní hovory se dnes běžně spojují přes satelity, naše e-maily procházejí po cestě celou řadou počítačů. Takové komunikace lze snadno odposlouchávat, což ohrožuje naše soukromí. Podobná úvaha platí i pro obchodní záležitosti; stále větší podíl obchodu se realizuje prostřednictvím internetu, takže je nezbytné zajistit firmám a jejich zákazníkům bezpečnost. Jedinou metodou, jež může ochránit soukromí a zaručit úspěch elektronického obchodu, je šifrování. Umění tajné komunikace, známé též jako kryptografie, poskytne zámky a klíče informačního věku.

Zároveň je nutno říci, že rostoucí poptávka široké veřejnosti po kryptografii je v rozporu s požadavky vymahatelnosti práva a národní bezpečnosti. Policie a tajné služby po desetiletí užívaly odposlechů v boji proti teroristům a organizovanému zločinu, ale současný vývoj velmi silných kódů hrozí tím, že by takový postup mohl ztratit účinnost. S nadcházejícím 21. stoletím vyvíjejí zastánci občanských práv stále větší tlak na široké využití kryptografie v zájmu ochrany práv jednotlivce. Spolu s nimi zastávají stejné stanovisko

zástupci podnikové sféry, kteří se dožadují silné kryptografie kvůli bezpečnosti transakcí v rychle se rozvíjejícím světě elektronického obchodu. Ti, kteří jsou odpovědní za právo a pořádek, naopak apelují na vlády, aby použití kryptografie omezily. Otázkou je, čeho si ceníme výše – soukromí, nebo efektivně pracující policie? Existuje nějaký kompromis?

I když má kryptografie v dnešní době velký význam i pro občanské aktivity, je třeba zdůraznit, že ani vojenská kryptografie neztrácí své opodstatnění. Říká se, že první světová válka byla válkou chemiků, neboť v ní byl poprvé použit chlór a hořčičný plyn; druhá světová válka je označována kvůli atomové bombě jako válka fyziků. Třetí světová válka by pak mohla být válkou matematiků, neboť právě oni mají pod kontrolou její nejdůležitější zbraně – informace. Matematici vyvinuli kódy, s jejichž pomocí se dnes chrání vojenské informace. Jistě není překvapením, že existují jiní matematici, kteří se snaží tyto kódy luštit.

Při popisu evoluce kódů a jejich významu pro historii lidstva jsem si dovolil malou odbočku. Kapitola 5 popisuje vyluštění některých starověkých písem včetně lineárního písma B a egyptských hieroglyfů. Z technického hlediska tu je patrný jeden rozdíl: kryptografie se zabývá komunikací, jež byla záměrně navržena tak, aby skryla tajemství před nepřítelem, zatímco písma starověkých civilizací takový účel neměla; prostě jsme jen postupem věků ztratili schopnost je číst. Avšak dovednosti potřebné k odhalení smyslu archeologických textů se velmi podobají těm, jež potřebují luštitelé šifer. Ještě dříve, než jsem si přečetl knihu Johna Chadwicka *The Decipherment of Linear B* (Rozluštění lineárního písma B), která popisuje nalezení smyslu textu starověké středomořské civilizace, jsem byl fascinován skvělými intelektuálními výkony těch, kteří dokázali rozluštit písmo našich předků a umožnili nám tak dovědět se více o jejich civilizaci, víře a každodenním životě.

Puristům se musím omluvit za název knihy v anglickém vydání – *The Code Book*. Nejde v ní jen o kódy. Termín „kód" se vztahuje ke zcela konkrétnímu typu tajné komunikace, jenž během staletí ztratil na významu. V rámci kódu se slovo či fráze nahrazuje jiným slovem, číslem či symbolem. Například tajní agenti mají svá krycí (kódová) jména chránící jejich identitu, tedy slova používaná namísto skutečných jmen. Podobně lze slovní spojení **Útok za úsvitu** nahradit kódovým slovem **Jupiter** a to zaslat veliteli na bitevní pole, aby

informace zůstala nepříteli skrytá. Pokud se štáb a velitel předem dohodli na kódu, pak význam slova **Jupiter** bude oběma stranám jasný, zatímco nepřítel, který je zachytí, nebude rozumět ničemu. Alternativou ke kódu je šifra – technika působící na nižší úrovni, která nahrazuje písmena namísto celých slov. Pokud například nahradíme každé písmeno tím, jež následuje po něm v abecedě (tedy namísto **A** píšeme **B**, namísto **B** píšeme **C** a tak dále), pak **Útok za úsvitu** přepíšeme jako **Vupl ab vtwjuv**. Šifry jsou ústředním pojmem kryptografie, takže by se tato kniha měla správně jmenovat *The Code and Cipher Book*, obětoval jsem však přesnost zvučnosti. [My v českém překladu nikoli – pozn. překl.]

Tam, kde bylo třeba, jsem uvedl definice různých technických pojmů používaných v kryptografii. Přestože se jimi obecně vzato řídím, místy jsem použil i termín, který možná není technicky přesný, je však u laické veřejnosti známější. Dovolil jsem si to učinit jen tehdy, je-li význam slova z kontextu zcela jasný. Na konci knihy najdete slovníček pojmů. Žargon kryptografie je ostatně zpravidla zcela průhledný: tak například *otevřený text* je zpráva před zašifrováním, *šifrový text* zpráva po zašifrování. Než ukončím tento úvod, musím se ještě zmínit o problému, jemuž čelí každý autor, jenž se dotkne oblasti kryptografie: věda o tajemství je převážně sama o sobě tajná. Mnozí z hrdinů této knihy nedosáhli během svého života veřejného uznání, neboť jejich práce stále ještě měla diplomatickou či vojenskou hodnotu. Během přípravných prací pro tuto knihu jsem měl možnost hovořit s experty britské Government Communications Headquarters (GCHQ), kteří mě seznámili s detaily právě odtajněného pozoruhodného výzkumu ze 70. let. Díky tomuto odtajnění se tři z největších světových kryptografů dočkali ocenění, jež jim právem náleží. Toto odhalení mi však připomnělo, že podobných případů, o nichž nevím nic ani já, ani jiní publicisté, je jistě více. Organizace jako GCHQ nebo americká NSA (National Security Agency) pokračují v utajeném výzkumu na poli kryptografie, takže jejich výsledky jsou tajné a jejich pracovníci anonymní.

Navzdory problémům souvisejícím s utajením jsem věnoval poslední kapitolu knihy spekulacím o budoucnosti kódů a šifer. Zároveň se v ní pokouším zjistit, zda dovedeme odhadnout, kdo v evoluční bitvě mezi tvůrci a luštiteli šifer zvítězí. Navrhnou tvůrci šifer někdy kód, jenž nelze nijak rozluštit, a dosáhnou tak svého cíle – absolutního utajení? Nebo to snad budou luštitelé šifer, kteří posta-

ví stroj schopný dešifrovat cokoli? Jsem si vědom toho, že nejlepší mozky oboru pracují v tajných laboratořích, kde mají k dispozici dostatek prostředků pro svůj výzkum; má tvrzení v poslední kapitole proto mohou být nepřesná. Uvádím například, že kvantové počítače – stroje schopné vyluštit jakoukoli dnešní šifru – jsou dosud ve velmi primitivním stadiu vývoje, je však klidně možné, že někdo již takový počítač sestrojil. Jediní lidé, kteří by mohli poukázat na mé omyly, jsou však ti, kteří to udělat nesmějí.