Kryptografie a její aplikace

Michal Bulant

DCB Actuaries and Consultants

Abstrakt: **Kryptografie** se v současné době dostává do centra pozornosti zejména v souvislosti s uplatňováním zákona o elektronickém podpisu. Snahou tohoto příspěvku je objasnit některé souvislosti a poukázat na možné problémy při praktické aplikaci kryptografie.

1 Jemný úvod do terminologie

Kryptologie — z řeckého *kryptós* (skrytý) a *lógos* (slovo) — je vědní disciplína, zabývající se bezpečnou a tajnou komunikací. Zahrnuje v sobě **kryptografii** — *gráphein* (psát) a **kryptoanalýzu** — *analýein* (rozvázat, uvolnit).

Kryptografie studuje techniky, pomocí kterých lze srozumitelnou zprávu zašifrovat (nejčastěji pomocí dohodnutého hesla, resp. klíče) a později rozšifrovat tak, aby pro nezasvěceného držitele zprávy bylo nemožné nebo velmi obtížné tuto zprávu přečíst. A právě o rozšifrování zpráv bez znalosti klíče usilují kryptoanalytici.

Oblastí, kterými se zabývá moderní kryptografie je však mnohem více, než je naznačeno v předchozím odstavci. Těmi základními jsou zejména:

- **důvěrnost** (*confidentiality*) — služba, zajišťující ukrytí obsahu zprávy před jinými než autorizovanými zraky
- **integrita dat** (*data integrity*) — služba, zajišťující odhalení případné modifikace dat třetí osobou
- **autentizace** (*authentication*) — zahrnuje identifikaci komunikujících stran, spojení zprávy s původcem, časem původu, datem odeslání, obsahem atd.
- **nepopření** (*non-repudiation*) — služba, zabezpečující, že žádná z komunikujících stran nemůže později popřít provedení příslušné akce (např. odeslání nebo přijetí zprávy)

V některých situacích nejsou některé z těchto služeb vyžadovány, někdy je naopak důležité rozlišit i drobné nuance v rámci konkrétní služby (např. nepopření původu vs. nepopření podání — např. bude možné prokázat, že danou zprávu někdo napsal, ale už ne, že ji odeslal).

Některé prameny za součást kryptologie považují rovněž **steganografii** — *steganos* (ukrytý), která se zabývá zápisem (ne nutně zašifrovaných) zpráv v takové formě, aby je byl schopen přečíst pouze zasvěcený čtenář.

Jan Kasprzak, Petr Sojka (editoři): SLT 2001 – sborník semináře o Linuxu a TEXu, str. 169–177, 2001.

2 Exkurze do historie

2.1 Počátky

Na počátku používání metod pro utajení zpráv se objevují jednak primitivní kryptografické algoritmy, jednak zajímavé steganografické postupy. Často citován je např. Herodotos, který ve svých Dějinách zaznamenal patrně nejstarší využití steganografie. Odesílatel zprávy Histiaeus napsal text na oholenou hlavu svého otroka, který s ní, samozřejmě již opět vlasatý[1], dorazil do Milétu, kde přispěl k povstání proti Peršanům. Dalšími steganografickými metodami, které se postupem času objevovaly, jsou tajný inkoust či nějakým způsobem vyznačená písmena v běžném textu (propíchnutím, sklonem, pořadím ve slově aj.). Dnes se zřejmě steganografie používá jen doplňkově, mezi často zmiňované možnosti patří např. ukrytí v grafických souborech, v nevyužívaných bitech apod.[2] Mezi „zajímavé“ možnosti (zřejmě bez valné praktické použitelnosti), objevivší se v souvislosti s rozmachem elektronické komunikace, patří i ukrytí zprávy ve spamech (viz [4]).

Z Řecka (přesněji ze Sparty) pochází i nejstarší známé kryptografické zařízení — skytála. Jde o hůl přesně stanovené šířky, na niž se namotal proužek kůže, na který byla napsána zpráva. Ta mohla být přečtena opět jen na holi stejné šířky. v moderní terminologii se hovoří o tzv. **transpoziční metodě**.

Naproti tomu, ve starém Římě byly položeny zaklady druhému hojně používanému principu, tzv. **substitučním metodám**. Šlo o metodu, která se dnes (patrně neprávem) říká Caesarova šifra — každé písmeno textu bylo nahrazeno písmenem stojícím v abecedě o 3 místa za ním. Podobná metoda se používala pro šifrování hebrejštiny (viz obr. 1).

Tyto dva základní typy kryptografických metod jsou používány s různými modifikacemi v podstatě dodnes. Smyslem modifikací je snaha o to, aby šifrový text vykazoval co nejméně odchylek od textu statisticky náhodného a tak znesnadnit kryptoanalýzu.

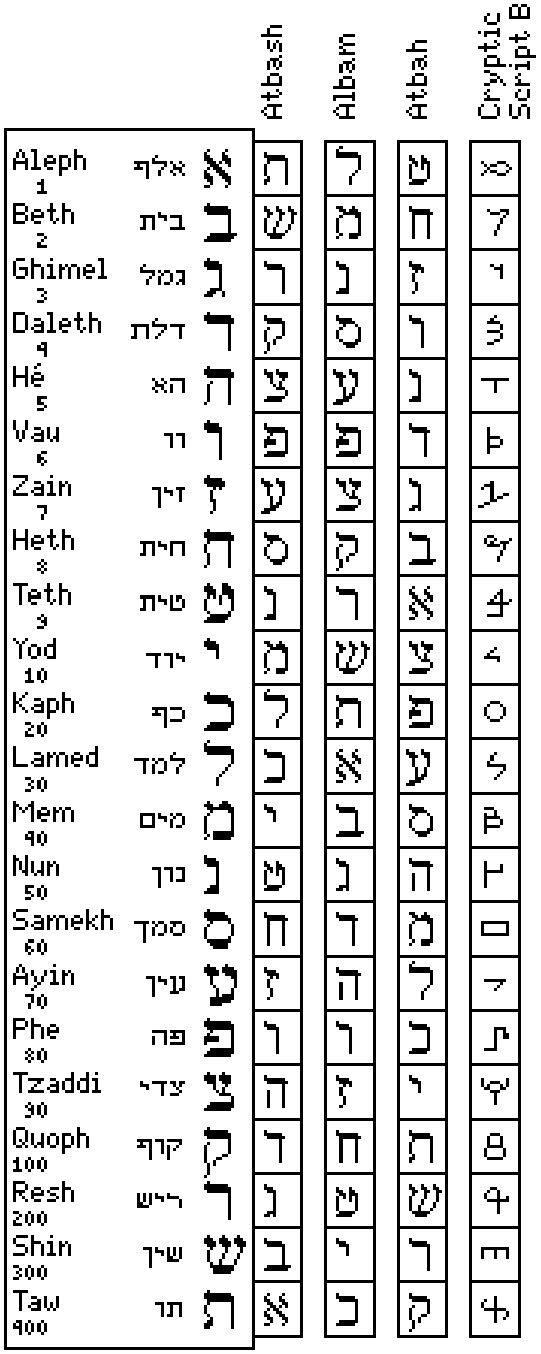
2.2 Kryptografické stroje

S rozvojem metod pro kryptoanalýzu (zejména Friedmann začátkem 20. století) se zjistilo, že pro ztížení kryptoanalýzy je výhodné často měnit tajný klíč. Pro tento účel se ukázaly velmi vhodnými mechanické stroje. Za všechny jmenujme alespoň mediálně nejznámější **Enigmu** (viz obr. 2).

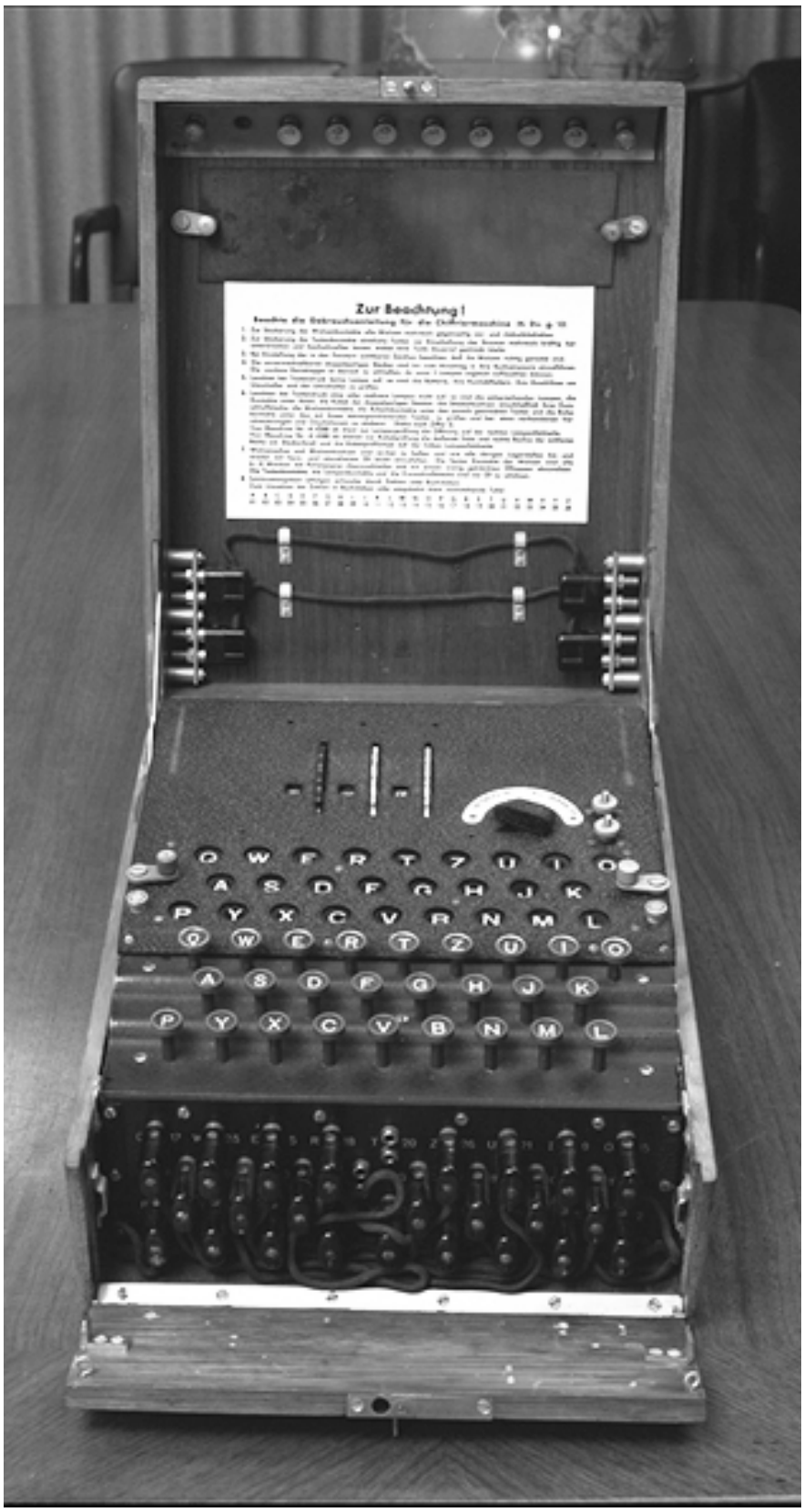
Tu (v několika variantách) používaly různé složky německé armády ve II. sv. válce. Byl to jakýsi psací stroj, který po stisku klávesy provedl několik permutací a po těchto operacích bylo rozsvíceno písmeno šifrového textu odpovídající

[1] Rychlost zřejmě nebyla v té době mezi hlavními kritérii.

[2] Jako nepříliš úspěšný pokus o steganografii se dá hodnotit i nedávný počin jistého britského novináře, který do prvních písmen vět svého zemědělského sloupku „ukryl“ nepříliš lichotivý vzkaz pro svého exšéfa. Už z těchto řádků je patrné, že s ukrytím příliš neuspěl.



Obrázek 1. Substituční tabulka používaná ve starověku pro šifrování hebrejštiny



Obrázek 2. Ukázka šifrovacího zařízení Enigma

stisknuté klávese. Enigma obvykle sestávala z 3–4 rotorů, 1 reflektoru a 26 sdířek, odpovídajících jednotlivým písmenům, které mohly navíc definovat dodatečnou permutaci. Po zašifrování jednoho znaku dojde k otočení nejpravějšího rotoru o jeden dílek, po jedné otáčce se otočí jeho soused o jeden dílek atd.[3] (podobně jako např. na počítadle přístupů na WWW stránku). Tajný klíč byl tvořen jednak výběrem rotorů, jejich inicialním nastavením a propojením sdířek. Šlo o poměrně komplikovaný stroj, který však neodolal kryptoanalýze spojenců (zejména díky zachycení jednoho exempláře Enigmy z ponorky U-505 a použití specialního, Poláky vyvinutého a Turingem zdokonaleného, stroje **Bombe**, který fungoval jako „hrubá síla“, testující všechny možné pozice rotorů a poskytující sadu možných otevřených textů.

Mezi velmi úspěšné kryptografické stroje použité během II. sv. války (a údajně i během války ve Vietnamu) se dají (s jistou nadsázkou) zařadit tzv. Code-talkers — příslušníci indianského kmene Navajo. Často používané výrazy měly přímo definovaný kód v navajštině, u ostatních slov bylo jejich každé písmeno při šifrování nahrazeno anglickým slovem (z pevně definované sady), na toto písmeno začínajícím a to bylo posléze převedeno do Navajštiny (buď jako ekvivalent nebo opis původně v tomto jazyce neexistujícího slova). Díky pečlivě volenému kódovaní slov (viz např. [8]) nebylo toto šifrování během války prolomeno ani přesto, že Japonci mohli využít příslušníka kmene Navajo pro překlad zachycených termínů.

2.3 Kryptografická moderna

Přes poměrně dlouhou historii kryptografie a některé teoretické výsledky (např. prokazatelná bezpečnost one-time padu (Vernam)[4] stále přetrvávaly některé problémy, které se s rozvojem komunikačních médií ještě prohlubovaly. Těmi byly zejména:

- nutnost znalosti (a utajení) klíče na obou stranách komunikace
- pro každý pár komunikujících nutnost existence speciálního klíče, díky čemuž počet potřebných klíčů roste kvadraticky s počtem komunikujících

Tyto problémy vedly v polovině 70. let 20. století k objevu **kryptografie s veřejným klíčem** (*public-key cryptography*).[5] s tím souviselo následné použití v oblasti digitálního podpisu a algoritmus pro výměnu tajných klíčů. Mezi nejzávažnější nevýhody tohoto typu šifrovaní patří:

[3] Zde poněkud zjednodušeno — ve skutečnosti práci kryptoanalytiků velmi ztěžovaly právě drobné nepravidelnosti v otáčení rotorů.

[4] Tento systém se podle nedávno odtajněných materiálů používal během studené války pro komunikaci mezi Moskvou a Washingtnem. Distribuci klíčů zajišťoval důvěryhodný kurýr. Údajně došlo k tomu, že některé klíče byly Moskvou použity opakovaně, což velmi usnadnilo kryptoanalýzu.

[5] Ve skutečnosti byl tento objev učiněn zřejmě o něco dříve — již počátkem 70. let v utajovaném výzkumu britské GCHQ a zřejmě i americké NSA.

- velikost klíče, která je obecně řádově větší pro dosažení stejné úrovně bezpečnosti
- rychlost — tyto metody jsou obvykle založené na matematických problémech obtížně řešitelných bez dodatečné informace (např. problém diskrétního logaritmu, odmocňování modulo složené n, dělení v grupě bodů na eliptické křivce apod.), což s sebou nese nutnost pracovat se složitějšími strukturami a následně pomalost výsledného systému
- není teoreticky prokázána bezpečnost žádného takového systému, dokonce se o matematických problémech, tvořících princip algoritmů s jistotou ani neví, zda skutečně nejsou řešitelné v rozumném čase

Proto se často používá systémů, využívajících lepších vlastností obou těchto základních typů — pro vlastní šifrovanou komunikaci se používá tajného klíče, který se předává prostřednictvím veřejného klíče. Rovněž se objevují pokusy o přenos klíčů a ustavení one-time pad spojení pomocí kvantových generátorů spolu s protokoly, které znemožňují jejich odposlech.

Jedním z nejdůležitějších v současné době používaných kryptografických primitivů jsou tzv. **hešovací funkce** (*one-way hash functions*). Tyto funkce mapují řetězec libovolné délky na řetězec pevné, předem zadané, délky, a to takovým způsobem, že jsou zejména splněny následující dvě podmínky:

- *preimage resistance* — nesnadnost nalézt zprávu s předem zadanou hodnotou hešovací funkce
- *collision resistance* — nesnadnost nalézt dvě zprávy se stejnou hodnotou hešovací funkce

Hešovací funkce (mezi nejznámější patří `MD5`, `SHA1`, `RIPEMD-160` nebo `MASH-1` slouží především při vytváření elektronických podpisů, při zajišťování integrity dat nebo jako první fáze zašifrování, kdy je jejich prostřednictvím zvyšována entropie šifrovaného textu. Jsou ale s výhodou používány také při autentizačních protokolech, které umožňují přesvědčit o určité znalosti bez jejího odhalení (viz např. protokol SRP popsaný v [10]).

3 Aplikace kryptografie a s tím spojené problémy

3.1 Vybrané aplikace

Elektronický podpis Je bezesporu chvályhodné, že jsme se velmi rychle zařadili mezi státy, které mají ve svých zákonných osnovách i zákon o elektronickém podpisu (viz [13]). Na druhé straně je třeba si uvědomit, že právě zákony spojené s využíváním výpočetní techniky a masové komunikace mohou být ještě náchylnější na drobné nepřesnosti než běžné zákony.

Odhlédneme-li od právních kliček, můžeme vidět některé další potenciální problémy využívání kryptografie s veřejným klíčem (ty nejsou samozřejmě zavedeny citovaným zákonem, ale tvoří obecný problém této infrastruktury):

– certifikační autorita — tzv. důvěryhodná třetí strana, která zajišťuje přiřazení veřejného klíče k jeho majiteli. Jejím úkolem je provádět dostatečně bezpečnou politiku v oblasti vydávání certifikátů (to doufejme vyřeší zmíněný zákon a hrozba vysokých pokut).
– ochrana soukromého klíče — ze zákona např. vyplývá, že majitel tzv. kvalifikovaného certifikátu odpovídá za škodu, způsobenou jeho použitím bez ohledu na to, způsobil-li tuto škodu on nebo např. trojský kůň či zloděj počítače s nedostatečně zabezpečeným soukromým klíčem.[6]
– seznam certifikačních autorit — problémem je udržování seznamu certifikačních autorit a jejich veřejných klíčů na počítači každého uživatele, které je nutnou podmínkou platnosti jí vydaných certifikátů. V případě, že bude v uživatelově počítači instalována podvržená certifikační autorita, bude pak automaticky každý jí vydaný (podvržený) certifikát a s ním i příslušný veřejný klíč považován za platný.

Problémů s praktickým zavedením elektronického podpisu se může objevit ještě více, přitom jde ale mezi kryptografickými protokoly o jeden z nejjednodušších. V následujícím odstavci se zmíníme o komplikovanější aplikaci, která má do své zákonné podoby před sebou ještě dlouhou cestu.

Volby

> *A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created in the history of computers.* — Bruce Schneier

V souvislosti s vývojem nedávných prezidentských voleb v USA, kde došlo k výraznému ovlivnění výsledků nejen jejich systémem, ale zejména jejich technickým provedením[7], se hodně hovoří o zavedení volebních automatů do procesu volby (tak, jak jsou využity např. v Brazílii a jak je zřejmě hodlají vyvinout ve spolupráci firmy Unisys, Microsoft a Dell) nebo přímo o volbách přes Internet. Zároveň je však požadováno, aby takové volby dostály těmto základním požadavkům: **anonymita**, **možnost auditu**, **rychlost**, **rozšiřitelnost** (**scalability**), **přesnost**. Přestože zejména nutnost autentizace je v relativně ostrém protikladu s požadavkem anonymity, je takový systém teoreticky zaveditelný (s některými drobnými ústupky, jako je např. existence důvěryhodné instituce, vydávající klíče). Jeho komplikovanost a riziko, s jeho zavedením spojené, je takové, že se zatím jeví v kontextu panujících poměrů veřejné sítě volby přes Internet jako nereálné.[8] Přesto jsou snahy některých firem (jistě do značné míry vyprovoko-

[6] Na druhou stranu je v zákoně formulka, podle níž zaručený elektronický podpis musí splňovat, že „*byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou*“.

[7] Údajně došlo např. v jistém okrsku v Michiganu ke dvouhodinovému zpoždění v dodání výsledku voleb kvůli tomu, že dobrovolníci byli s hlasovacími lístky uvězněni v budově medvědem.

[8] Máloco asi přítáhne pozornost hackerů a nasměruje ji jedním směrem tak bezpečně jako volby přes Internet, kterých se účastní desítky miliónů lidí.

vané volební ostudou) v USA vedeny i tímto směrem a je možné, že v menším měřítku budou takové systémy provozovány již v brzké době (viz např. [12]).

3.2 Aktuální stav (veřejné) bezpečnosti

Problémem, se kterým se v současné době budeme zřejmě stále častěji setkávat, je náskok, který má vývoj a analýza jednotlivých algoritmů před specifikací protokolů, jejich implementací a zejména před uvážlivostí jednotlivých uživatelů. Tak máme např. povědomí o tom, že lze sestrojit stroj, který je schopen za relativně rozumnou cenu (milióny $) v takřka reálném čase rozšifrovat v současné době běžně používané šifry s nepříliš paranoidně nastavenými parametry. Nebo jsme schopni provést v relativné krátké době útok při znalosti 2^{10} párů `(otevřený text, šifrový text)`. Podstatně jednodušší ale zřejmě bude pro případného (nikoliv náhodného) útočníka použít levnější a zaběhanější formy útoku — např. krádež média s nedostatečně zabezpečeným soukromým klíčem, instalace „čmuchajícího“ hardwaru, který eviduje veškeré stisky kláves (viz např. článek [11]) nebo sledování toku dat po lokální síti nebo internetu. Je to dokladem často opakovaného tvrzení, že *systém je maximálně tak bezpečný, jako jeho nejslabší část*.

Podobným příkladem je tzv. *man-in-the-middle* (MITM) útok. Je to často zmiňovaná možnost, jak napadat „tajnou“ komunikaci, vedenou prostřednictvím kryptografie s veřejným klíčem. v případě, že komunikující nejsou schopni zabezpečit dostatečně spolehlivou metodu výměny věřejných klíčů, je schopen aktivní útočník, nejen číst, ale i měnit jejich zprávy. Podobných útoků je teoreticky popsána celá řada, běžný software však obvykle nechává na klientovi, či svém správci, jakou bezpečnostní politikou se bude řídit. Situace se stává závažnější ve chvíli, kdy existuje softare automatizující tyto postupy (viz např. [9], který v nové verzi dokáže implementovat MITM útok proti SSH verze 1).

Na obranu softwaru, zmiňovaného v předešlém odstavci (SSH, SSL, apod.), je třeba říci, že jejich existenci vděčíme za to, že alespoň část komunikace je vedena šifrovaně — vždyť kolik uživatelů stále nevidí velký problém v používání nezabezpečených aplikací typu `telnet` nebo protokolu `HTTP` i pro důvěrné účely. Mnoho aplikací (i placených) na Internetu je stále ještě „zabezpečeno“ pouze prostřednictvím tzv. *basic authorization*, což v postatě znamená, že heslo sice není posíláno v otevřené podobé, ale je pouze zakódováno prostřednictvím `Base64` kódování.

Z uvedeného je zřejmé, že kryptografie jako taková je v podstatě připravena na nasazení v praktickém životě, kvůli očekávaným problémům implementačním, bezpečnostním a jistě v neposlední řadě i byrokratickým si asi budeme muset na masové rozšíření těchto nástrojů ještě počkat.

Reference

1. http://www.counterpane.com/crypto-gram.html BRUCE SCHNEIER, Crypto-Gram, elektronický měsíčník o bezpečnosti a kryptografii.
2. A. MENEZES, P. VAN OORSCHOT, AND S. VANSTONE, *Handbook of Applied Cryptography*, CRC Press, 1996.
3. http://fn2.freenet.edmonton.ab.ca/~jsavard/crypto.htm, John Savard's cryptography page.
4. http://www.spammimic.com/.
5. PAVEL VONDRUŠKA, Cesta kryptografie do nového tisíciletí, Computer World, září 2000.
6. V. MATYÁŠ A KOL., Bezpečnost pro všechny, soukromí pro každého, Computer World 10/97 až 40/98.
7. http://homepages.tesco.net/~andycarlson/enigma/enigma_j.html, Enigma simulation applet.
8. http://www.history.navy.mil/faqs/faq61-4.htm, Navajo Code Talkers' Dictionary.
9. http://www.monkey.org/~dugsong/dsniff/, dsniff v. 2.3.
10. http://srp.stanford.edu/, Secure Remote Password protocol, Stanford University.
11. JOHN LEYDEN, Mafia trial to test FBI spying tactics, The Register, 17. prosince 2000 (http://www.theregister.co.uk/content/4/15268.html)
12. http://votehere.net/VH-Content-v2.0/techbriefs/security.html, Internet Voting Security, VoteHere.net.
13. ÚŘAD NA OCHRANU OSOBNÍCH ÚDAJŮ, Elektronický podpis (http://www.uoou.cz/epodpis.php3)