1 Cesta kryptografie do nového tisíciletí: Od Kámasutry k osobním zápiskům K. H. Máchy

RNDr. Pavel Vondruška, publikováno v ComputerWorld 37/2000–40/2000

Kryptologie (zjednodušeně věda o utajení obsahu zpráv) je věda, která má stále mezi lidmi nádech tajemna. Není to tak dávno, co se dokonce knihy o kryptologii daly v knihovnách najít ve stejném oddělení jako knihy o alchymii nebo hvězdopravectví. V oficiálním třídění matematických věd také nebyla kryptologie dlouho uvedena a trochu živořila ve stínu matematiky a informatiky.

Kryptologie se dělí na kryptografii a kryptoanalýzu a někdy se také uvádí, že obsahuje steganografii. Kryptografie se zabývá matematickými metodami se vztahem k takovým aspektům informační bezpečnosti, jako je důvěrnost, integrita dat, autentizace entit a původu dat. Ve starším chápání to byla především disciplína, která se zabývala převedením informace do podoby, v níž je obsah této informace skryt. Jejím úkolem bylo tedy především učinit výslednou zprávu nečitelnou i v situacích, kdy je plně prozrazená, zachycená třetí – nepovolanou – stranou. Tím se liší od steganografie, jejímž úkolem je skrýt samotnou existenci zprávy, ale zpráva samotná může být napsána nebo předána ve srozumitelné podobě. Kryptoanalýza je pak jakýsi "opak" kryptografie. Kryptoanalytici se snaží získat ze zašifrované zprávy její původní podobu (nebo alespoň část skrytých informací). Kryptoanalýza se zabývá analýzou odolnosti (síly) kryptografického systému a metodami vedoucími k proniknutí do kryptografického systému. Tento proces se nazývá luštění šifrové zprávy a pokud je kryptoanalytik úspěšný a podaří se mu vniknout do některého šifrového systému, řekneme, že šifra byla zlomena nebo rozbita.

Hlavním cílem kryptografie byl tedy rozvoj algoritmů, které lze použít ke skrytí obsahu zprávy před všemi s výjimkou vysílající a přijímající strany (utajení) a mnohem později také přibyl rozvoj algoritmů sloužících k jednoznačnému určení osoby odesílatele (identifikaci) a k ověření správnosti zprávy přijímající stranou (autentizaci) a další související algoritmy. Původní vysílanou zprávu nazýváme otevřeným textem. Tato zpráva je následně šifrována pomocí nějakého kryptografického algoritmu. Zašifrované zprávě říkáme šifrový text. Odšifrování je opačný postup vzhledem k zašifrování, je to převedení šifrového textu zpět do podoby otevřeného textu.

1.1 Starověká kryptografie

Kryptografie prodělala dlouhý vývoj. Prvé pokusy o utajení obsahu zpráv jsou známé již ze starého Egypta a Mezopotámie. Jednalo se o nejprimitivnější systémy, které spočívaly v nějaké mírné, zpravidla neobvyklé úpravě písma. Takovéto malé změny zcela postačovaly, již samotná znalost písma byla v té době jistým druhem umění a pro většinu populace zůstával obsah nápisu stejně utajen.

Ve staré Indii se situace změnila. Zalistujme ve známé učebnici erotiky Kámasútře. V části "Smyslná žena" se hned v úvodu dozvíme mezi 64 radami ženám, které chtějí mít úspěch u mužů : "Osvojte si tajná písma a šifry nebo si vynalezněte vlastní. Důležitá je také znalost nových způsobů mluvy, abyste mohla obratně měnit začátky a konce slov tak, jak právě potřebujete." V komentáři ke Kámasútře Yašodhara popisuje některé z používaných tajných písem. Jedním z uvedených systémů je "muladeviya", kde zašifrování spočívá pouze v použití reciproční abecedy. Existují záznamy, že tento systém byl používán i v mluvené podobě mezi obchodníky.

Kořeny skutečné kryptologie jsou však spjaty až s dějinami Řecka. Téměř každá učebnice šifrování začíná popisem toho, jak Řekové pro utajení zpráv používali poněkud (dnešní terminologií neoperativní) způsob – oholili svému poslu hlavu, napsali na jeho lebku vzkaz a když mu vlasy opět narostly, mohl se vydat na cestu. Ve skutečnosti je však zaznamenán jen jeden takový způsob použití, popsal jej Herodotos ve svých Dějinách. Odesílatelem zprávy byl Histiaeus a zprávu napsal na hlavu svému oddanému otroku, který ji takto dopravil do Milétu a pomohl tak ke koordinaci povstání proti Peršanům.

Jedna z nejdůležitějších zpráv pro existenci západní civilizace byla také předána utajeně. Jednalo se o zprávu, která pomohla Řekům v boji proti Peršanům. Demaratus, syn Aristona, zjistil

termín, kdy král Xerxes vytáhne s armádou proti Řekům. Rozhodl se o tom své krajany informovat, seškrábal vosk ze dvou dřevěných psacích destiček a přímo na dřevo zprávu napsal. Tyto destičky opět zalil voskem, aby to při náhodné kontrole vypadalo, že nejsou použité. Zpráva se dostala na místo určení, manželka krále Leonidase Gorgo odhalila tajemství destiček a zpráva byla přečtena. Zbytek známe z hodin dějepisu – následovaly slavné bitvy u Thermopyl, Salaminy a Plataea. Postup Peršanů do Evropy byl jednou pro vždy zastaven a v důsledku toho se mohla rozvinout západní civilizace.

Oba systémy – vyholená hlava a zápis na dřevo pod vosk – jsou představitelé systémů určených pro tajný přenos zprávy. Z hlediska dnešní terminologie jsme se tak seznámili s nejstaršími aplikacemi steganografie.

Řekové však neskončili jen u utajování přenosu zpráv – dokázali vyvinout skutečné šifrové systémy. Sparťané, nejbojovnější z Řeků, vymysleli a prokazatelně používali již v pátém století před naším letopočtem zařízení na utajení zpráv. Tento systém se skládal ze dvou holí ("skytale" nebo někdy psáno "scytale") přesně stanovené šířky (šířka = symetrický klíč zařízení), na prvou hůl se navinul pás látky, papyru nebo pergamenu. Na tento materiál se potom napsala zpráva, a to směrem dolů po délce hole. Pás s textem se sejmul a posel (komunikační systém) jej odnesl na místo určení. Tam byl pás látky navinut na druhou hůl a zpráva mohla být přečtena. Toto zařízení pracovalo na principu dnes nazývaném jako transpozice – promíchání otevřeného textu. Nepovolaná osoba sice mohla snadno přečíst všechna písmena otevřeného textu, ale díky použitému systému neznala jejich pořadí. Jedná se o nejstarší známé kryptografické zařízení.

Řecký spisovatel Polybius zase vynalezl systém signalizace, který byl později převzat jako další základní kryptografická metoda. Seřadil písmena do čtverce a jejich řady a sloupce očísloval. Každé písmeno je tak reprezentováno dvěma čísly – číslem řady a číslem sloupce. Polybius pak dále doporučoval, aby tato čísla byla předávána pomocí pochodní. Např. písmeno v prvém řádku a pátém sloupci by bylo odesláno pomocí jedné pochodně v levé ruce a pěti pochodní v pravé ruce. Zprávy tak mohly být odeslány bezpečně a rychle na velké vzdálenosti. Polybiův čtverec (šachovnice), který umožňuje převod písmen na číslice, se stal základem mnoha dalších šifrových systémů.

Římané nepřevzali tyto systémy od Řeků, vydali se vlastní cestou. Kolem přelomu našeho letopočtu prokazatelně zavedli vojenskou kryptografii. Zprávy mezi legiemi nebyly zasílány otevřeně, ale pomocí záměny otevřeného textu za šifrový text. Julius Caesar vypráví o využití těchto systémů v "Zápiscích o válce galské". Známý životopisec Suetonius pak dokonce prozrazuje, jak systém přesně vypadal. Každé písmeno zprávy bylo zaměněno za písmeno, které leželo o tři místa dále v abecedě. Suetonius dále popisuje, že Caesarův synovec Augustus používal podobný systém, ale nahradil písmeno otevřeného textu písmenem stojícím v abecedě těsně za ním. Výjimkou bylo poslední písmeno X, které nahradil dvojicí AA. Kryptografie ve starém Římě se stala naprostou samozřejmostí. Mimo podobných záměn se ještě používalo vkládání kódů pro jména osob, zemí apod.

Hlavní systémy pro bezpečný přenos dat byly na světě: utajování přenosu dat, transpozice, používání kódů a záměny znaků otevřeného textu podle určitých pravidel za jiné znaky. Všechny výše uvedené systémy jsou symetrické – příjemce i odesílatel jsou dohodnuti na stejném principu a klíči.

1.2 Středověká kryptologie

Skutečná kryptologie se však zrodila teprve díky vynikajícím arabským matematikům. Roku 855 našeho letopočtu popisuje Abú Bakr Ahmad ve své práci různé šifrové záměnné systémy. Jedna z popisovaných substitučních abeced se v arabském světě dokonce beze změny používala ještě v roce 1775(!!!), kdy jí bylo použito v dopise s choulostivými informacemi pro alžírského vládce.

Arabové byli první, kdo objevili a popsali metody kryptoanalýzy. Souhrn arabských poznatků je uveden v jednom oddíle ("Utajování tajných zpráv v dopisech") rozsáhlé čtrnáctidílné encyklopedie Subh al-á sha, která byla dokončena r. 1412.

Na práce arabských matematiků a kryptologů navázala středověká Evropa. Významným představitelem evropské kryptografie byl benediktinský opat ze Spanheimu Johannes Trittheim (1452

– 1518). Kolem roku 1500 napsal první významnější evropskou knihu o šifrování. Trittheim se zabýval převážně substitučními systémy. Zavedl a doporučoval vkládání klamačů do šifrového textu. Jednalo se o náhodné vkládání znaků do textu za účelem ztížení statistického rozboru. Panovnické rody (které běžně šifru ke komunikaci používaly) se však zalekly, že vyzradil příliš mnoho tajemství, a snad proto jej označily za čarodějníka.V 16. století se objevili i první slavní luštitelé. Jedním z největších byl francouzský právník a matematik Francois Viete (1540 – 1610), který luštil zašifrované depeše španělského krále a předával je francouzskému panovníkovi Jindřichu IV. Navarrskému. Trvalo několik let, než na to Španělé přišli. Nevěřili, že je možné jejich složitou záměnu rozluštit a žádali Svatou stolici, aby postavila Vieta před soud, protože musí být spojen s ďáblem. I další významný kryptograf a kryptoanalytik Giovanni Battista della Porta (1541 – 1615) byl obviněn ze spojení s ďáblem. Porta navrhl tabulku složité záměny (odlišnou od systému Trittheima), v jejichž luštění byl také velice úspěšný. Jeho hlavní povolání však byla alchymista a dramatik. Do dějin se zapsal vedle kryptologie i přípravou kysličníku cíničitého.

Nechci se zde však zabývat systematickým vývojem, který vedl dále přes různé formy záměn, nomenklátorů a polyalfabetických šifer. Základem všech těchto šifrových systémů byla vždy kombinace transpozice a jednoduché záměny již s vědomou snahou zakrýt charakteristiky jazyka.

Poznání, že výsledné šifrové texty lze na základě statistických metod luštit, vedlo ke zdokonalování šifrových systémů. Snahou bylo zahladit dodatečné informace, které byly v textu obsaženy, a tím zabránit analýze šifrového textu, která by mohla vést ke kompromitaci textu otevřeného. Spolehnutí se na nedokonalý systém tak například stálo skotskou královnu Marii Stuartovnu (1542 – 1587) život, neboť dopisy, ve kterých dala souhlas k připravovanému povstání a zavraždění anglické královny Alžběty, posloužily jako důkaz při soudním líčení. Používání slabé šifry k uchování osobního tajemství nám zanechalo i zajímavé svědectví ze života K.H.Máchy, který ve svých denících popisuje zašifrovaně své zážitky způsobem, který by mohl být po odšifrování přetištěn i dnešními erotickými časopisy.

2 Cesta kryptologie do nového tisíciletí: Od zákopové války k asymetrické kryptografii

V dnešní kapitole z historie kryptologie bude řeč o tom, jak nedokonalé zašifrování zpráv dokázalo pohnout osudy stovky lidí. Nejvíce se v tomto díle zaměříme na úspěchy kryptoanalýzy, která v obou světových válkách slavila velké úspěchy a často rozhodla o vítězství či porážce velkých armád dávno před vypuknutím prvním bitvy. Ale již dost úvodu, další díl fascinující historie kryptologie právě začíná.

2.1 První polovina dvacátého století

První světová válka nepřivedla na svět jen letadla a tanky, ale i první masové použití šifrování v polních podmínkách. Podnětem k rozvoji kryptologie nebyla jen válka jako taková, ale i rozšíření bezdrátového telegrafu. Ten dával možnost snadného odposlechu a bylo proto potřeba zavést jednoduché a bezpečné systémy šifrování. Dále se prokázala úžasná síla kryptoanalytiků (luštitelů). Pokud dokázali prolomit příslušný používaný systém, pak takto získané informace byly pro výsledek ofenzívy nebo dokonce celé války důležitější než roty vojáků a letadla. Samotný vstup USA do války byl důsledkem vyluštění obsahu šifrového telegramu – dnes známého jako tzv. Zimmermannův telegram. Německý ministr zahraničí Zimmermann v telegramu mexické vládě vyzývá Mexiko k válce proti USA. Slibuje v ní mexické straně podporu a územní zisk. Britové telegram zachytili, rozluštili jej a předali USA (přičemž neprozradili svůj zdroj). Poté, co se prezident Wilson s obsahem telegramu seznámil, svolává Kongres. Ten 2.4.1917 schvaluje vstup USA do války proti Německu. Tento akt rozhodujícím způsobem změnil poměr sil na evropském bojišti. První světová válka vychovala i prvního z velikánů kryptografie dvacátého století. Stal se jím William Frederic Friedman (1891 – 1969). V roce 1915 nastoupil dráhu úspěšného kryptologa v americké armádě a vybudoval pro USA vzorně fungující kryptoanalytickou službu. Opravdovou biblí všech

kryptologů prvé poloviny dvacátého století se stalo jeho čtyřsvazkové dílo "Základy kryptoanalýzy" z roku 1923. Obsah této knihy zásadně ovlivnil rozvoj kryptografie ve všech státech mezi dvěma světovými válkami a dá se říci, že se znalosti právě díky tomuto dílu "na všech frontách" vyrovnaly. Tato kniha by pravděpodobně asi nikdy nebylo vydáno, kdyby Friedman neměl existenční problémy a nemusel se živit psaním. Američané se totiž dopustili neuvěřitelné chyby, která je stála těžce získaný náskok – zrušili kryptoanalytické oddělení a členy tohoto oddělení propustili! Americký ministr zahraničí Henry Stimson to komentoval dnes již proslulou větou "Gentlemani si navzájem nečtou dopisy". Velice brzy si tuto chybu uvědomují a povolávají Friedmana zpět ke službě a dávají mu k dispozici na tu dobu veliké prostředky; je pověřen zřízením dešifrovacího oddělení. Od tohoto okamžiku se již odborná veřejnost po dlouhou dobu nebude dovídat o tom, co se děje v kuchyních tajných služeb. Tyto služby – vzhledem ke svým prostředkům a možnosti naverbovat schopné lidi – získávají před akademickou a komerční veřejností obrovský náskok. Většina států si vzala z této události poučení a jen zcela výjimečně docházelo k propuštění kryptoanalytiků. Jednou ze známých výjimek byla Československá republika, která neváhala v rámci velkých politických čistek oslabit i toto své oddělení.

Nové vyzbrojování ve třicátých letech se tedy nesoustředilo jen na vývoj zbraní, ale i na výrobu šifrovacích zařízení. V Německu bylo sestrojeno snad nejznámější šifrovací zařízení všech dob – legendární ENIGMA, ale i řada dalších důmyslných zařízení, např. kryptografické zařízení LORENZ nebo poněkud slabší zařízení Kryha. Svá řešení vyvíjelo i Japonsko (97-ši-ki-O-bun in-ji-ki – PURPLE, J19-K9), USA (Sigaba, Hagelin C-38, M-209), Anglie a další státy, které se připravovaly k válce. Jména tvůrců těchto kryptografických zařízení jsou Edward H. Hebern, Hugo Koch, Arvid Gerhard Damm, Alexandr von Kryha, Gilbert Vernam, Boris Hagelin a další ..

Druhá světová válka prověřila kvalitu přichystaných šifrovacích zařízení. Zní to až neuvěřitelně, ale s odstupem času, kdy byly příslušné materiály postupně odtajněny, se ukázalo, že většinu tehdy používaných šifrových systémů se podařilo druhé straně prolomit a příslušné zprávy z těchto kanálů využívat. Utajení před veřejností bylo dokonalé. V zájmu neprozrazení, že v Bletchley Parku (hrabství Buckinghamshire) luští zprávy z Enigmy, nezabránil W.Churchil rozbombardování Coventry. Vzhledem k luštění zpráv předávané Enigmou a i Lorenzem o chystaném náletu předem věděl, ale dlouhodobé strategické využívání zpráv z těchto zdrojů postavil nad životy tisíců lidí z tohoto anglického města. Cesta k prolomení tehdejších systémů již nebyla jednoduchá - na luštění se podíleli nejlepší matematici a pro účely luštění zařízení Enigma a Lorenz byly postaveny první stroje, které můžeme dnes nazvat počítače. Úplný popis zařízení Colossus, které sloužilo k luštění zpráv kryptografického zařízení Lorenz, byl například uvolněn teprve letos v květnu.

V luštění byli úspěšní nejen Angličané a Američané. Řadu šifer USA prolomili i Němci. Ti četli i většinu zpráv naší exilové vlády v Londýně, které vysílala domácímu odboji. Luštění těchto zpráv prokazatelně přispělo k likvidaci některých výsadků a odbojových skupin.

Veřejnost se sice dozvěděla některé částečné informace hned po válce, ale řada zpráv se objevovala až v průběhu desítek let po skončení války. K tomu bylo několik důvodů – především i po válce řada států ještě používala své válečné systémy, o nichž se nevědělo, že v průběhu války byly prolomeny, nebo naopak byly tyto systémy úspěšné a vlády nechtěly zveřejněním informací o nich oslabit možnost jejich využití.

Příkladem může být poválečné používání kryptografických zařízení z dílny Kryha Maschinen Gesselschaft v německé diplomatické službě, ale i v československém Obranném zpravodajství. Tato zařízení se s malou obměnou používala ještě začátkem roku 1952. Ve skutečnosti zařízení produkovalo nekvalitní, krátké periodické heslo a již roku 1933 Friedmann se svými kolegy přišel na to, jak zprávy zašifrované tímto strojem luštit.

Druhým příkladem může být využití úspěšného systému i po válce. Za druhé světové války bylo využíváno indiánů kmene NAVAJO u americké námořní pěchoty k předávání tajných zpráv rádiem. Kódovou řeč, kterou Indiáni předávali ve své mateřštině, se Japoncům nepodařilo odhalit. Američané tento způsob s úspěchem použili ještě ve válce v Severní Koreji a dokonce i v 60. letech ve Vietnamu. Veřejnost byla o úspěchu těchto Indiánů informována až koncem šedesátých let a úplná kódová kniha byla uvolněna k publikování teprve zhruba před rokem.

V době studené války byla kryptografie chápána jako tajná zbraň. Informace o ní byly záměrně potlačovány. Na civilních školách se nevyučovala. Instituce, které se použitím a vývojem

šifrových technik zabývaly, si vybíraly do svých služeb nejschopnější matematiky už během studia a po nástupu do svých služeb je teprve seznamovaly s dosaženými výsledky, které patřily mezi nejutajovanější informace. Tento systém přispěl k tomu, že v šedesátých a sedmdesátých letech byl náskok těchto agentur (a nemyslím tím jen NSA a KGB) až desítky let před světovou odbornou veřejností, která se ovšem prakticky ještě nezformovala a vlastně tedy téměř neexistovala.

2.2 Druhá polovina dvacátého století

Jako blesk z čistého nebe proto zapůsobily dvě práce dalšího z velikánů kryptologie dvacátého století Claude Elwood Shannona. V časopise Bell Systém Technical Journal v roce 1948 a 1949 otiskuje články "Matematická teorie sdělování" a "Sdělovací teorie tajných systémů". Prvý z článků dal vznik teorii informací, druhý článek pojednával o kryptologii v termínech informační teorie. Pojetí nadbytečnosti (redundancy) je hlavním termínem, který Shannon zavedl. Oba články fakticky odstartovaly moderní pojetí matematického zkoumání základů kryptografie a kryptoanylýzy a staly se pro rozvoj veřejné kryptologie stěžejními díly a pravděpodobně nejcitovanějšími pracemi v tomto oboru do konce sedmdesátých let.

Nová kvalitní kryptografická zařízení, která se v této době začala vyrábět po celém světě, byla zpravidla založena na velice jednoduchém principu, sčítání otevřeného textu s náhodným heslem. Systém navrhl již roku 1917 Gilbert Vernam, ale z publikované teorie amerického vědce Shannona vyplynulo, že jediný absolutně bezpečný systém je právě sčítání otevřené zprávy se stejně dlouhým náhodným heslem. Velice jednoduché – jenže je zde malý problém. K odšifrování samozřejmě potřebujeme mít k dispozici příslušné náhodné heslo, které jsme přičetli k původní zprávě. A to je právě onen základní problém celého systému. Místo tajného doručení původního otevřeného textu délky N musíme na místo určení doručit heslový materiál – náhodnou posloupnost stejné délky, tedy délky N. Problém je to tedy téměř ekvivalentní (samozřejmě, heslový materiál lze doručit ve velkém množství a do zásoby ještě před nutností vyslat zprávu). Při objemu dnes předávaných zpráv je tento systém nevyhovující. Jeho význam je v tom, že se jedná o jediný absolutně bezpečný systém – pokud jsou dodrženy následující podmínky:

- umíme vyrobit náhodné, stejně pravděpodobné heslo (výroba takového hesla byla v 60. letech velkým problémem)
- máme dostatečně důvěryhodný kanál k transportu hesla na místo určení
- korespondence je tak slabá, že nám nevadí velká spotřeba hesla
- každé heslo lze použít pouze jednou a je tedy potřeba dodržovat určitá přesně daná pravidla pro zacházení s heslovým materiálem.

Touto – v té době moderní cestou – se vydala i tehdejší česká kryptografie. Autorem návrhu příslušného systému byl Alojz Lorenc, který o dvacet let později, již ve funkci prvního náměstka ministra vnitra, nechvalně proslul v listopadových událostech.

Kubánská krize na začátku šedesátých let vyvolala potřebu rychlého a bezpečného spojení mezi USA a SSSR. Obě mocnosti se domluvily na vybudování horké linky mezi hlavami obou států. Pro tuto linku byl také zvolen výše popsaný systém. Horká linka byla uvedena do provozu 30. 8. 1963 . Kreml i Bílý dům si vzájemně vyměnily heslové materiály – pásky. Otevřené texty se převedly do dálnopisného kódu a sčítaly se s heslovým materiálem, heslová páska byla ihned po použití automaticky ničena, čímž se mělo zamezit jejímu nechtěnému opětovnému použití. Při zavedení tohoto systému se použilo zařízení ETCRRM-II (Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II). Každou hodinu se přenášely zkušební relace. Ze strany americké se přenášely výsledky basebalových zápasů a ze strany ruské výňatky z Lovcových zápisků od Turgeněva. Použití kódových pásků, které se vyměňují prostřednictvím velvyslanectví jednotlivých států, zajišťuje naprostou bezpečnost přenášených zpráv a také – což je velmi důležité – nemožnost vpašování falešné zprávy.

Rozsah provozu právě v této době závratně rostl. V r. 1930 představoval telegrafní provoz v celých USA 2,2 miliony slov, v lednu 1960 jen Ministerstvo zahraničních věcí USA vyslalo a

přijalo stejné množství slov za 14 dní. V červnu 1961 již bylo přeneseno 6,929 milionů slov za jeden měsíc. Jednalo se tedy o zvýšení zátěže provozu o 40% za rok a půl!

Potřeba důvěrné komunikace mezi subjekty se dále zvyšovala a náklady na výrobu a transport heslového materiálu stále rostly. Současně se stávalo, že při nedostatku heslového materiálu byla porušena zásada nepoužít stejné heslo dvakrát, a také při distribuci tak ohromného množství šifrového materiálu se stávalo, že se k heslovému materiálu dostala nepovolaná osoba.

Absolventi vojenských kateder 70. let si jistě pamatují na stále vtloukaný slogan: "Bez spojení není velení", a tak nastala doba inovace. Bylo nutno opustit předávání heslového materiálu délky zprávy a přejít na jiný systém. Řešením se zdálo generování hesla přímo kryptografickým zařízením. Přijímač a vysílač generoval pseudonáhodné heslo. Počáteční nastavení bylo dáno zpravidla tzv. inicializačním vektorem a klíčem. Stačilo se jen domluvit na počátečním nastavení. Kvalita tohoto systému závisí na kvalitě pseudonáhodné posloupnosti a počtu možných počátečních stavů, které pak generují různé pseudonáhodné posloupnosti. Tento problém je z matematického hlediska velice složitý a byl slabinou některých komerčně vyráběných zařízení té doby.

Kryptologie se v sedmdesátých letech přestala pěstovat jen v uzavřených komunitách tajných služeb a začala se stávat součástí světové vědy. Objevily se první významné výsledky této akademické obce. V roce 1976 publikovali Whitfield Diffie, Martin Hellman a Ralph Merkle článek o nové závratné myšlence – asymetrické kryptologii. Až dosud všechny šifrové systémy byly systémy tzv. symetrické. Odesílatel i příjemce museli znát stejný klíč a jím buď zašifrovali nebo odšifrovali. Pokud takto komunikovalo n lidí a zprávám měli rozumět vždy jen dva z nich, bylo zapotřebí distribuovat n*(n-1)/2 různých klíčů. Dále bylo nutné přesně dodržovat tzv. pravidla klíčového hospodářství, tedy kdy který klíč začal platit, přestal platit, řešit kompromitace, záložní klíče, skupinové klíče apod. Správa takovéhoto systému se začala stávat nepřehlednou, těžkopádnou a hlavně byla slabinou většiny šifrových systémů té doby.

3 Cesta kryptologie do nového tisíciletí: Od asymetrické kryptografie k elektronickému podpisu

V minulém díle jste se mohli seznámit s historií kryptologie od prapočátků ve starověku, podívali jsem se i na středověk a přes nedávné dějiny obou světových válek jsme se dostali až k objevu asymetrické kryptologie. A bude to právě tato revoluční metoda, která spolu se standardem DES a jemu podobnými bude ústředním tématem tohoto dílu. Putování historií pak bude uzavřeno opravdu tou nejžhavější současností — elektronickým podpisem.

3.1 Asymetrická kryptografie

Asymetrická kryptografie je založena na této myšlence: Každý subjekt má svůj tajný (soukromý) klíč a k němu veřejný klíč. Tajný klíč je určen k zašifrování a veřejný klíč k odšifrování. V síti o n subjektech je tak potřeba připravit jen 2n klíčů, přičemž veřejné klíče lze opravdu zveřejnit a odpadá tedy nutnost složité, nákladné a nebezpečné distribuce těchto klíčů. Šifrování mezi subjekty A a B pak probíhá takto: A má dvojici klíčů "AS" (soukromý klíč), "AV" (veřejný klíč), B má k dispozici obdobně klíče "BS" a "BV". Klíče "AV", "BV" jsou zveřejněny a jsou tedy A i B známy. Subjekt A připraví text, který chce utajit, zašifruje jej svým klíčem "AS" a dále jej zašifruje veřejným klíčem příjemce "BV" (jinak by zprávu mohl odšifrovat každý, kdo má přístup k veřejnému klíči "AV"). Příjemce B potom nejprve zašifruje přijatou zprávu pomocí svého soukromého klíče "BS" (ten zná jen on) a dále pomocí veřejného klíče odesílatele.

Brzy po zveřejnění teoretického schématu asymetrické kryptografie (1978) se objevuje první šifrový systém založený na této myšlence. Vžil se pro něj název RSA (zkratka z prvních písmen tvůrců systému Rivest, Shamir a Adelmann). Tento systém se po malých úpravách (především prodloužení klíče a stanovení jistých pravidel, která musí klíče splňovat) používá dodnes. Je založen na obtížném matematickém problému – faktorizaci (rozkladu na prvočísla) velkých čísel. Vše si nejlépe uvědomíme na následujícím jednoduchém příkladě. Zkusíte najít celočíselné dělitele čísla

217502279? Jsou jimi dvě prvočísla 14713 a 14783. Zatímco vyhledání těchto čísel vyžadovalo relativně dost práce, pak vynásobení těchto dvou čísel je velice jednoduchým úkonem.

Vzhledem k tomu, že RSA ovlivnilo kryptologii konce 20. století a význam celého systému v souvislosti se zavedením elektronických podpisů neustále roste, řekněme si něco více o matematických principech tohoto systému.

Postup při vytváření dvojice klíčů (veřejného a tajného) pro RSA je následující: a) Nejprve náhodně (a nepredikovatelně) vygenerujeme dvě dostatečně velká prvočísla (jejich přibližná velikost, tj. počet bitů, je zadána).

b) Spočteme n = p*q a F (n) = (p-1)*(q-1), kde F (n) je Eulerova funkce určující počet přirozených čísel nesoudělných s n.

c) Zvolíme náhodné číslo e, kde 1 ¡ e ¡ F (n), tak, že největší společný dělitel (e, F (n)) = 1 (tj. e a F (n) jsou nesoudělná).

d) Užitím Eukleidova algoritmu spočteme jednoznačně definované číslo d takové, že 1 ¡ d ¡ F (n) a e*d 1 mod F (n).

Veřejným klíčem je potom dvojice (n,e), tajným klíčem uživatele je d. Číslo n nazýváme modulem, číslo e šifrovacím exponentem a číslo d dešifrovacím exponentem. Patent na algoritmus RSA drží již od jeho vzniku americká společnost RSA Data Security Inc. Právě nyní (tedy přesněji 20. 9. 2000) tento patent vyprší a algoritmus bude uvolněn k veřejnému použití bez poplatků. Jak se dále dozvíme, stane se tak právě v době, kdy může tento algoritmus sehrát rozhodující úlohu v zavádění elektronických podpisů dokumentů.

Jsme ale stále ještě na začátku 80. let. Světová odborná společnost vývojem asymetrické kryptografie slaví velký úspěch. Tajné služby USA a Anglie mlčí a neprozrazují, že jim je celý systém asymetrické kryptografie již znám. Teprve v roce 1997 byl uveřejněn článek Jamese Ellise z britské CESG (Communications – Electronics Security Group), nazvaný "The history of Non-Secret Encryption" , ve kterém jeho autor popisuje, jak princip asymetrické kryptografie (jím nazývaný jako Non-Secret Encryption, NSE) objevil už v roce 1970. Dále uvádí, že speciální variantu RSA objevil jeho kolega Clifford Cocks v roce 1973. Tajným službám je však přesto jasné, že jejich náskok před světovou veřejností se zmenšuje.

3.2 První symetrický standard – DES

Přes zjevné výhody systému RSA se systém na přelomu 70. a 80. let ještě moc neprosazuje. Výpočetní složitost je obrovská a tehdejší slabé počítače pracují pomalu. Šifrování dlouhých textů je tak pomalé, že není prakticky použitelné. Je stále potřeba používat symetrickou kryptografii. Asymetrická kryptografie má sloužit v budoucnu jen k distribuci klíčů a k identifikaci a autentizaci. Kryptologové se začínají zabývat hybridními systémy. Pomocí asymetrického šifrového systému se přenese klíč pro symetrický systém, a tím se dále šifruje. Na každou zprávu tak lze použít jiný symetrický klíč. Tato kombinace prakticky řeší a odstraňuje většinu problémů s distribucí klíčů. Zbývá maličkost – silný a bezpečný symetrický algoritmus. Na scéně se objevuje první celosvětově uznávaný symetrický algoritmus DES (Data Encryption Standard).

Vývoj DES navazuje na vývoj šifrovacího algoritmu Lucifer od Thomase Watsona (IBM). Potřeba standardu jeho vývoj urychluje a DES je v roce 1977 v USA formálně přijat za veřejný standard pro ochranu senzitivních informací, nikoliv však pro ochranu informací utajovaných. Způsob ochrany tajných informací v USA není zveřejněn.

DES šifruje text po blocích délky 64 bitů, aktivní délka klíče je 56 bitů, hlavní prvek tvořící potřebnou nelinearitu, která chrání šifrový text před útoky analytiků, jsou tzv. S-boxy. Hned od počátku jsou zde určité nejasnosti okolo návrhu celého systému. NSA (National Security Agency) přesvědčila IBM o "vhodnosti" redukce délky klíče z původních 128 bitů na 56 bitů. NSA také změnila vnitřní strukturu jednoho z S-boxů. Martin Hellmann poukazuje na nebezpečí, které vyplývá z malé délky symetrického klíče. Celkově se však zdá, že algoritmus DES je prvním opravdu bezpečným algoritmem tohoto typu.

O tom, jaký byl náskok pracovníků NSA před odbornou veřejností, svědčí událost, která se váže se k procesu přijímání DES za standard. V roce 1976 uspořádal NBS (Národní úřad pro standardizaci) dvoudenní konferenci k diskuzi o DES. Na tuto konferenci byli pozváni všichni

zástupci výzkumných organizací, univerzit, firem a další zájemci o kryptologii. Zástupce NSA pak ve svých vzpomínkách popisuje, že již během prvního dne bylo jasné, že toto shromáždění nemá dostatečné znalosti pro posouzení tohoto šifrového algoritmu. Dokonce tvrdí, že měl pocit, jako by byla pozvána skupina alchymistů k posouzení atomové bomby...

3.3 International Association for Cryptologic Research

Dalším možným mezníkem na naší pouti světem kryptologie je rok 1980. V tomto roce se koná v Santa Barbaře veliká konference věnovaná kryptologii. Konference má výjimečný ohlas a její další konání v roce 1981 (již pod názvem Crypto) zakládá tradici, která nepřetržitě trvá dodnes. Vytváří se nezávislá akademická skupina odborníků, kteří v roce 1982 zakládají IACR (International Association for Cryptologic Research). Od roku 1982 se také pod záštitou IACR konají pravidelná setkání vědců na evropském kontinentu – Eurocrypty. Tyto pravidelné konference Crypto a Eurocrypt se stávají synonymem pro toto sdružení. Od svého založení vydává tato společnost vlastní a ve své době jediný časopis svého druhu – Journal of Cryptology. Velice brzy získalo toto sdružení vůdčí postavení ve vědeckém a odborném světě kryptologie. V prostředí, kde po dlouhou dobu trvala absence jakýchkoliv odborných informací, sehrálo neocenitelnou roli a své vůdčí postavení si udržuje dodnes.

Kryptologická veřejnost sdružená v IACR podrobuje analýze blokovou šifru DES. Objevují se jisté teoretické útoky, lineární analýza, diferenční analýza. DES odolává. Dokonce jsou vyslovovány hypotézy, že NSA znala tyto metody již v době návrhu S-boxů.

Koncem osmdesátých a začátkem 90. let se objevuje celá řada dalších symetrických blokových algoritmů – FEAL, GOST, IDEA, CAST, BLOWFISH atd. Autoři těchto systémů jsou výrazné postavy z komunity IACR. Tato komunita spolu soutěží o vytvoření silného, rychlého a bezpečného symetrického algoritmu. Kompatibilita veřejných systémů se tím sice snižuje, ale DESu se v této komunitě nevěří a hlavně prodej licencí na nové šifrové algoritmy se stává obchodně zajímavý. V ČR se v té době komerčně vyvíjí vlastní šifrovací čip SIC5000 (s algoritmem DVK). Současně se zjišťuje, že některé z těchto systémů, ač na první pohled velice podobné svoji strukturou DES, nejsou tak kvalitní a jsou rozbitelné. Japonský FEAL je totálně rozbit. Je to upozornění – amatéři a poloprofesionálové nemají na poli kryptologie místo. Bez hluboké znalosti souvislostí nelze navrhnout bezpečný šifrový algoritmus.

Co však nedokázali kryptologové svými analytickými útoky, docílil rozvoj síly výpočetní techniky. Vyluštit šifrový text tzv. hrubou silou znamená, že odzkoušíme všechny možné klíče. Právě velikost klíče "pouze" 56 bitů se stala pro DES osudná. V roce 1993 J. Wiener z Bell Northern Research publikoval zprávu, v níž popsal zařízení, které vyzkouší všechny klíče DES do 7 hodin. Cenu takového zařízení odhaduje na jeden milion dolarů. V roce 1995 se na veřejnost dostává informace, že NSA vlastní stroj, který je schopen DES vyluštit do 15 minut. Toto zařízení sestrojila firma The Harris Corporation. Pro ty, kteří stále pochybovali, bylo komerčně sestrojeno a předvedeno speciální zařízení DES-cracker (1998), které je schopno otestovat všech 256 klíčů do 9 dnů a nalézt tak příslušné řešení.

DES musel být nahrazen jiným standardem. Prozatímně jej NIST (National Institute of Standards and Technology) nahrazuje implementací 3DES (TripleDES). V podstatě se jedná o opakované použití algoritmu DES. Zašifrování nyní probíhá takto: zpráva se zašifruje pomocí algoritmu DES a klíče K1, odšifruje se pomocí klíče K2 a opět se zašifruje pomocí klíče K3 (resp. v jiné verzi klíčem K1). Délka klíče se tak vlastně 3x (resp.2x) prodloužila a toto řešení se tímto stalo odolné proti útoku hrubou silou. FIPS-PUB-46-3 ustavuje jako současně platnou normu obě výše popsané verze algoritmu 3DES. Kryptologické veřejnosti je jasné, že řešení není optimální, a proto v roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.

3.4 Advanced Encryption Standard

Pro název tohoto nového algoritmu se vžilo označení AES (Advanced Encryption Standard). Vybraný standard má být velice flexibilní, lehce implementovatelný, má pracovat s 32bitovým mi-

kroprocesorem, 64bitovým procesorem, ale i 8bitovým (v tzv. režimu smart card). AES má být 128bitová bloková šifra, musí podporovat klíče délky 128, 192 a 256 bitů. Výběr takového algoritmu, který je určen pro všechny typy aplikací a nasazení (klasický software pro PC, terminály pro elektronickou komerci, čipové karty), není opravdu lehký. Autoři tvrdí, že nově vzniklý standard by snad mohl být standardem pro celé 21. století! Algoritmus nesmí být patentován a pro vítěze je připravena odměna – prestižní uznání kryptologické veřejnosti – tzv. "zlatý vavřín kryptologie".

3.5 Elektronický podpis

Vraťme se ale zpět k asymetrické kryptografii. Dalším závažným využitím, mimo šifrování, je možnost elektronicky podepisovat dokumenty. Popišme si stručně, jak obecně probíhá proces elektronického podpisu nějakého dokumentu.

K výkladu potřebujeme ještě jeden kryptografický modul kromě asymetrické šifry, o které jsme se již podrobně zmínili. Tím modulem je hash. Hashovací funkce mají za úkol vytvořit takzvaný otisk zprávy. Vstupem hashovací funkce může být libovolná zpráva (libovolně dlouhá), na výstupu obdržíme její otisk, který má pevnou délku (128 nebo 160 bitů). Pokud bychom ve zprávě změnili byť i jediné písmenko, dostaneme na výstupu úplně jiný otisk. Hashovací funkce jsou obecně známé a kdokoli si může z jakékoliv zprávy takový otisk udělat. Navíc platí, že je výpočetně velice obtížné vytvořit k libovolné zprávě jinou zprávu, která má stejný otisk. Obtížnost tohoto úkonu je ekvivalentní obtížnosti rozšifrování zprávy bez znalosti klíče.

Nejznámějšími a nejpoužívanějšími představiteli hashovacích funkcí jsou MD5 (message digest, otisk délky 128 bitů) a SHA-1 (Secure Hash Algorithm, otisk délky 160 bitů).

Podepisující osoba musí mít dále připravenu sadu svých klíčů (soukromý a veřejný klíč) pro některý asymetrický algoritmus . Nejznámějším je RSA, ale mohou se použít i asymetrické algoritmy založené na diskrétním logaritmu nebo eliptických křivkách.

Proces elektronického podpisu pak probíhá takto: Podepisující osoba vypočte hash dokumentu, který chce podepsat, hash dále zašifruje pomocí zvoleného asymetrického algoritmu a pomocí svého soukromého klíče. Získaný výsledek "V" je přiložen k původní zprávě. Takto upravená zpráva je tzv. elektronicky podepsána. Jak postupujeme při ověření? K otevřenému textu vypočteme hash, označme jej "H1". Odšifrujeme "V" pomocí veřejného klíče podepsané osoby a dostaneme jím spočtený hash "H2". Nyní porovnáme "H1" a "H2". Pokud jsou tyto hodnoty shodné, pak nebyl dokument cestou změněn (hashe jsou shodné) a dokument podepsala osoba, které přísluší veřejný klíč (jen ta mohla "H2" zašifrovat pomocí svého soukromého klíče).

V praxi celý systém vyžaduje ještě třetí důvěryhodnou stranu. Tato třetí strana eviduje veřejné klíče a stvrzuje identitu jejich majitelů. Takováto strana se nazývá certifikační autorita. Používání elektronických podpisů však potřebuje zákonnou úpravu. Velice zhruba řečeno, musí být elektronický podpis (a jeho jednotlivé bezpečnostní varianty) přesně definován, je potřeba uznat rovnost elektronického podpisu s podpisem normálním, zajistit neodmítnutí elektronického podpisu z důvodu, že je proveden elektronicky a musí být stanovena pravidla chování certifikačních autorit a podmínky, které musejí tyto instituce splňovat, případně musí být stanoven určitý režim a dohled nad službami certifikačních autorit. Koncem roku 1999 přijala evropská komise Směrnici o elektronických podpisech (1999/93/EC) v rámci Evropské unie. Tento dokument je pro členy EU závazný a své zákony musí s tímto dokumentem postupně harmonizovat. Zároveň probíhal proces schvalování zákona o elektronickém podpisu i v České republice. Do tohoto zákona se podařilo včlenit většinu požadavků Směrnice. Po schválení v parlamentu a senátu podepsal 11. 7. 2000 tento důležitý zákon i prezident České republiky.

4 Cesta kryptologie do nového tisíciletí: Od NESSIE ke kvantovému počítači

Dnes vás čeká poslední část našeho 4dílného seriálu o historii kryptologie, která se poprvé objevila v temném dávnověku a která nyní češe zasloužené ovoce několikatisícového vývoje. A právě ony triumfy budou náplní dnešního dílu, kde se budeme věnovat žhavé současnosti. A ta je opravdu

velice zajímavá, poslední dva roky totiž kryptologie nabývá stále více na vážnosti a to zejména díky Internetu. Neboť je to právě ona a její algoritmy (elektronický podpis, asymetrické šifrování), které umožňují bezpečné placení po Síti.

Kryptologie již tak dávno není jen akademickou záležitostí, ale začíná být zajímavá i po obchodní stránce a je jedno, jestli chcete vytvořit neprůstřelnou šifru a nebo naopak nějakou zlomit. V každém případě se jedná o velice ceněnou informaci, za kterou jsou někteří ochotni zaplatit opravdu zajímavé částky.

4.1 Zlomové roky 1999–2000

Odborná veřejnost na konci 90. let je již dostatečně sebevědomá. Cítí, že dospěla do situace, kdy je schopna konkurovat pečlivě střeženým tajemstvím agentur velkých mocností. Již se neobjevují slabé šifrové systémy, které ještě v polovině 90. let byly předkládány veřejnosti jako bezpečné (např. Crypt, Rot13, SuperKey, N-Code). Odborná veřejnost umí velice dobře a rychle ocenit kvalitu určitého systému. V produktech Microsoftu (Word, Excel), Lotusu, WordPerfectu se však stále používají nekvalitní šifrové systémy, které lze lehce rozbít. Postupně je Microsoft sice nahrazuje za kvalitní šifru, ale z důvodu vývozních omezení je oslabuje úpravou klíče na délku pouhých 40 bitů. Takto úmyslně upraveným algoritmům se říká slabá kryptografie. Mimo území USA a Kanady se tak stále v těchto produktech nacházejí slabé šifrové produkty. Toto je ovšem výhodná situace pro evropské komerční firmy, které se snaží obsadit evropský trh svými produkty. Americké velké firmy se snaží donutit vládu USA k omezení vývozních restrikcí, ale ta neustupuje. Komerční produkty vybavené kvalitními symetrickými algoritmy (např. 3DES, CAST, RC4, Twofish) a asymetrickými algoritmy (RSA, algoritmy na bázi diskrétního algoritmu, algoritmy na bázi eliptických křivek) se začínají vyrábět a vyvážet nejen v Německu, Francii, Anglii, Finsku, ale i u nás. Česká firma Decros úspěšně vyváží své produkty nejen do Evropy, ale i do Asie. Firma AEC se stává průkopníkem v použití asymetrické kryptografie na bázi eliptických křivek. Produkty se stávají bezpečnými a začínají je "prodávat" již jiné vlastnosti – uživatelská přítulnost, kvalita klíčového hospodářství apod.

Květen 1999 je pro Českou republiku určitým ohodnocením naší vyspělosti v této oblasti. Výbor IACR v roce 1997 rozhodl, že konference Eurocrypt 1999 se bude konat v Praze. Na konferenci je profesorem Shamirem předvedeno optické zařízení Twinkle, které je schopno zrychlit jednu z fází faktorizace velkých čísel a dochází tak k faktickému ohrožení klíčů RSA o délce 512 bitů. O Shamirově přednášce se píše po celém světě, informaci otiskuje i NewYork Times. Teprve tehdy se v několika českých novinách objevuje zmínka o konferenci.

V srpnu 1999 pak bylo skutečně dosaženo vytouženého cíle, bylo rozbito číslo ze souboru RSA s délkou klíče 512 bitů (155ciferné dekadické číslo). Dodnes však nebyl přechod na klíče délky 1 024 bitů (doporučená bezpečná délka klíčů pro RSA nejméně do roku 2002) důsledně proveden.

V létě 1999 německá vláda vydává prohlášení, ve kterém jasně proklamuje, že na dobu dvou let ruší všechny restrikce v používání silné kryptografie a dává celému světu najevo, že chce zaujmout rozhodující pozici v evropském trhu s kryptografií.

Tlak amerických firem, které přicházejí o miliony dolarů, nakonec slaví úspěch. V listopadu 1999 dochází k prvnímu uvolnění vývozních restrikcí a další uvolnění následuje v lednu 2000. S konečnou platností je tak uvolněn export šifrovacích algoritmů ze Spojených států (včetně zdrojových textů).

4.2 NESSIE

Jak již jsme se zmínili, na jaře roku 2000 se provádělo důkladné hardwarové vyhodnocení algoritmů – kandidátů AES.

Především evropská veřejnost však není úplně jednotná v hodnocení kandidátů, v procesu výběru kandidátů a jejich hodnocení, a vznikly proto v jejich kruzích určité rozpaky. Možná, že právě tento moment byl jedním z faktorů nové aktivity v rámci Evropské unie, kde vznikla vlastní iniciativa na výběr vhodných kryptografických modulů.

Jedná se o projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption) programu IST Evropské komise (http://cryptonessie.org).

NESSIE je tříletý projekt, který byl zahájen 1. ledna 2000 a oficiálně vyhlášen v květnu na konferenci Eurocrypt 2000. Jednotlivé moduly budou vytvářeny na základě veřejných návrhů a rovněž tak vyhodnocení těchto návrhů proběhne otevřenou a transparentní cestou.

Celkem se jedná o celý systém kryptografických primitivů (blokové šifry, synchronní proudové šifry, samosynchronizující se proudové šifry, autentizační kódy zpráv – MAC, hashovací funkce, jednosměrné hashovací funkce, pseudonáhodné funkce, asymetrická schémata pro šifrování, asymetrická schémata pro digitální podpis, asymetrická schémata pro identifikaci). Nejedná se tedy jako v projektu NIST o výběr standardu pouze pro symetrický blokový algoritmus (AES), ale o výběr standardů pro celou oblast kryptografie.

V rámci každé třídy budou existovat dvě bezpečnostní úrovně (normální a vysoká), s výjimkou blokových šifer, kde bude ještě třetí úroveň (historická-normální). To znamená, že např. blokové šifry vysoké bezpečnostní úrovně mají pracovat s bloky textu v délce 128 bitů a s klíčem nejméně v délce 256 bitů. Blokové šifry normální bezpečnostní úrovně pracují rovněž s bloky otevřeného textu v délce 128 bitů a musejí mít klíč dlouhý nejméně 128 bitů. Zmíněná třetí úroveň ponechává možnost existence blokových šifer, které pracují s bloky otevřeného textu v délce 64 bitů (jako je tomu u většiny současných algoritmů). Délka klíče i u této třetí úrovně však musí být minimálně 128 bitů.

První kolo končí v září 2000. Do tohoto data mají být odevzdány výchozí návrhy. Jedním ze základních cílů projektu je také posílit pozice evropského kryptografického průmyslu v návaznosti na výsledky evropského výzkumu.

5 Zdroje

Prošli jsme se dějinami kryptologie od starověku po dnešní dobu. Shrneme-li celý několikatisíciletý vývoj, máme nyní k dispozici matematickou a informační teorii. Kryptologie se stala uznávanou vědou, která se z kanceláří tajných služeb přesunula do laboratoří velkých počítačových firem a na akademickou půdu. Přestala být tajemstvím. Kryptologii je možné studovat. Základní kurzy jsou dostupné i pro naše studenty na Masarykově univerzitě v Brně, na Matematicko-fyzikální fakultě UK v Praze nebo na ČVUT. Byly zrušeny vývozní a jiné administrativní překážky. Legislativa upravuje použití elektronických podpisů. Vědci umí navrhnout bezpečné šifrovací algoritmy, které se liší spíše jen parametry implementačními (rychlost, nároky na paměť) než bezpečnostními. Jsou vypracovávány a přijímány mezinárodní standardy a normy. Zdá se, že vývoj je v podstatě ukončen.

5.1 Teoretické hrozby současné kryptografii

Je vůbec něco, co může ohrozit současné symetrické nebo asymetrické algoritmy mimo hrubou sílu – mimo zvyšující se výpočetní potenciál? Zvyšujícímu se výpočetnímu potenciálu, který má kryptoanalytik k dispozici, se dá lehce čelit zvětšováním klíčů. Současné používané délky klíčů 128 bitů by měly při zachování rychlosti vývoje výpočetní techniky (zdvojnásobení výkonu zhruba každé dva roky) odolat desítky let. Autoři Lenstra a Verheul na základě hluboce sofistikované analýzy docházejí přitom k poměrně velice přísným doporučením pro rok 2020 (aby bezpečnost elektronické informace byla garantována pro období 20 let); symetrické klíče by měly mít minimálně délku 86 bitů, modul RSA minimálně 1 881 bitů, analogicky i modul pro diskrétní logaritmus, pro eliptické křivky by měla být minimální délka klíče 161 bitů.

Nyní zdánlivě odbočíme. CMI (Clay Mathematics Institut of Cambridge) vyhlašuje na konferenci v Paříži 24. 5. 2000 sedm matematických problémů tisíciletí. Současně je připraven fond se sedmi miliony dolary. Za řešení každého z problémů je vypsána odměna jeden milion dolarů. Neočekává se, že budou vyplaceny příliš brzy. První z problémů má velice jednoduchý název: "P versus NP." Problém vychází z teorie složitosti. Složitost algoritmu je dána výpočetním výkonem nárokovaným pro jeho realizaci. Často se hodnotí dvěma proměnnými – časovou nebo prostorovou náročností. Obecně se výpočetní složitost algoritmu vyjadřuje "velkým" O – řádem (Order) – hodnoty výpočetní složitosti. Bude-li například T=O(n), pak zdvojnásobení velikosti vstupu

zdvojnásobí dobu zpracování; takový algoritmus nazveme lineární. Je-li složitost na n nezávislá, píšeme O(1). Doba zpracování algoritmu se při zdvojnásobení vstupu nezmění. Bude-li T=O (2n), pak zvětšení velikosti vstupu o 1 bit prodlouží dobu zpracování na dvojnásobek. Algoritmy mohou být z hlediska složitosti kvadratické, kubické apod. Všechny algoritmy typu O(nm) se nazývají polynomiální. Třída P potom obsahuje všechny algoritmy, které mohou být řešeny v polynomiálním čase.

Dále definujme Turingův stroj jako konečný automat s nekonečnou čtecí-zapisovací páskovou pamětí. Čtenář si může představit klasický domácí počítač, ale rozšířený o nekonečnou paměť. Třídu NP definujeme jako všechny problémy, které mohou být řešeny v polynomiálním čase pouze nedeterministickým Turingovým strojem: tj. variantou normálního Turingova stroje, která může provádět odhady. Stroj odhaduje řešení problémů – buď tak, že metodou pokusů hádá správné řešení nebo tak, že paralelně provede všechny pokusy – a výsledky těchto pokusů prověřuje v polynomiálním čase. Třída NP zahrnuje třídu P, protože jakýkoliv problém řešitelný v polynomiálním čase deterministickým Turingovým strojem je také řešitelný v polynomiálním čase nedeterministickým Turingovým strojem. Jestliže všechny problémy NP jsou také řešitelné v polynomiálním čase deterministickým strojem, pak NP = P. Otázka platnosti P = NP je ústředním nevyřešeným problémem teorie výpočetní složitosti. Nyní se z naší zdánlivé odbočky vrátíme k samotným základům současné kryptografie. Kdyby někdo prokázal, že P = NP, pak bychom většinu toho, na čem je založena současná moderní kryptologie, mohli odepsat. Znamenalo by to, že pro všechny symetrické problémy existuje kryptoanalytický (luštitelský) algoritmus, který je časově polynomiální. Pro lepší pochopení jen podotkneme, že útok hrubou silou je "nesrovnatelně" horší – jeho složitost je tzv. superpolynomiální. V takovém případě by naše neschopnost řešit algoritmy typu 3DES a AES v rozumném čase znamenala jen to, že se nám zatím nepodařilo najít vhodný luštící algoritmus. Většina současných odborníků se však domnívá, že rovnost tříd problémů P a NP neplatí. Vyplacení jednoho milionu dolarů matematikovi v případě, že dokáže nerovnost tříd P a NP (a tím zároveň dokáže, že současné blokové algoritmy jsou opravdu bezpečné), není ve světle právě popsaných skutečností přehnaně vysoké ocenění.

Je zde ještě jedna cesta, která může ohrozit pracně dostavěnou budovu kryptografie nebo alespoň některou z nejdůležitějších částí. Toto nebezpečí se nazývá kvantový počítač. Na rozdíl od klasického počítače, kde bit má jen dva stavy, u kvantového počítače je základem přenosu informace kvantový bit (qubit). Qubit může být podle kvantové mechaniky v lineární superpozici dvou klasických stavů. Heisenbergův princip neurčitosti formuluje základní vlastnosti tohoto qubitu. Východiskem algoritmů zatím hypotetického kvantového počítače jsou tzv. unitární transformace pracující s vektory qubitů. Na rozdíl od transformací probíhajících v klasickém počítači jsou unitární transformace vždy reversibilní, tj. vždy existuje možnost jít algoritmem pozpátku. V roce 1994 Shor prokázal existenci kvantového polynomiálního algoritmu pro řešení diskrétního algoritmu a úlohu faktorizace velkých čísel.To znamená, že pokud se zdaří konstrukce kvantového počítače, bude nutné přestat používat v podstatě všechny současné systémy s veřejným klíčem (RSA, Diffie-Hellman), které jsou založeny na obtížné řešitelnosti úlohy faktorizace a úlohy diskrétního logaritmu (tyto úlohy nepatří do třídy NP problémů, ale jen do speciální třídy těžce řešitelných problémů). Konstrukce kvantového počítače podle některých odborníků není takovou utopií, jak by se na prvý pohled mohlo zdát. Někteří experti odhadují, že doba k faktické realizaci by mohla být kolem dvaceti let.

Na úplný závěr se vrátíme zpět do poloviny našeho roku 2000. Jaký dopad může čtenář osobně očekávat od celého tohoto vývoje ? Nastala doba, kdy softwarové a hardwarové firmy mohou tvořit na základě standardů a norem bezpečné aplikace. Pokud firmy vyřeší bezpečné a uživatelsky jednoduché uchovávání klíčů, pak se nebude muset čtenář bát, že produkty, které nějak prokáží svoji shodu s těmito celosvětovými standardy (na základě validace, certifikace apod.) jsou děravé. Bezpečné kryptografické produkty (společně s právními akty – zákony, vyhláškami) povedou k nebývalému rozšíření kryptografie. Zatímco aplikovaná kryptologie byla dříve výsadou tajných služeb, armád a diplomacie, stává se během posledních deseti let věcí veřejnou a současně i výnosným obchodem. Zahajuje svoje masové tažení za všemi uživateli výpočetní techniky. Pojmy jako státní informační systém, e-business, e-commerce, e-obchodování, elektronický notář, kvalifikovaný certifikát, ochrana osobních dat a další se stanou samozřejmou součástí našeho ja-

zyka a jejich realizace bude možná právě díky kvalitním kryptografickým produktům a právnímu zajištění.

Zajímavé odkazy:

- `http://www.aec.cz/` – zajímavé texty věnované šifrovaní, určitě si pak přečtěte firmou vydávaný bulletin
- `http://www.decros.cz/Security_Division/Crypto_Research/publikace.htm` – stránky další známé české firmy obsahují také řadu cenných materiálů
- `http://www.fi.muni.cz/usr/staudek/vyuka/security/P017.html` — řada zajímavých textů určená k výuce vysokoškolských studentů
- `http://www.mujweb.cz/veda/gcucmp/` – domovské stránky GCUCMP(Group of Cryptology Union of Czech Mathematicians and Physicists), kromě řady informací od autora tohoto textu se můžete přihlásit k odběru e-zinu Crypto-World
- `http://www.mujweb.cz/veda/bitis/` – stránky BITIS (Sdružení pro bezpečnost informačních technologií a informačních systémů), informace o veřejně pořádaných seminářích
- `http://www.obluda.cz/crypt.htm` – řada informací, včetně zajímavých odkazů
- `http://www.pgp.cz` – stránka věnovaná známému standardu PGP
- `http://www.cw.cz` – kromě denního zpravodajství si můžete stáhnout Seriál "Bezpečnost pro všechny, soukromí pro každého"