Michal Altair Valášek

PŘÍSNĚ TAJNÉ ŠIFRY

aneb velmi jemný úvod
do současné kryptografie

www.secpublica.cz

Obsah

Přísně tajné šifry: co byste měli znát o současné kryptografii

Když se řekne „šifra“, většina lidí si vzpomene na šifrovací hříčky z Pionýrského zápisníku (ti mladší pak z Příručky mladých svišťů). Současné šifrovací (a podepisovací algoritmy) s nimi ovšem nemají mnoho společného. Ve světě dnešních počítačů jsou šifry v podstatě všudypřítomné, pročež se vyplatí mít o nich alespoň základní povědomí.

Význam znakových transpozičních šifer – to jsou ty z našich dětských let nebo z historických knížek o druhé světové válce – začal upadat s příchodem digitálních počítačů, které mají dostatečný výkon, aby dokázaly většinu z nich louskat v reálném čase. Tato technologie koncem minulého století umožnila vývoj zcela nové generace šifer (a také si jej v podstatě vynutila), na jejich základech stavíme dodnes a nejspíš ještě pěknou řádku let stavět budeme.

Název této stručné příručky je jakousi soukromou poctou ke třicátému výročí vydání stejnojmenné knihy V. P. Borovičky. Tato kniha se snaží v mezích žánru literatury faktu rekonstruovat historické příběhy, v nichž hrála velkou roli kryptografie. Ačkoliv je to spíše „detektivka“, která se zaobírá povětšinou fyzickými aspekty těchto příběhů, stála u začátku mého zájmu o kryptografii.

Účelem tohoto textu je seznámit běžné uživatele a laické zájemce s naprostými základy kryptografie: se šifrováním, elektronickými podpisy a podobnými věcmi. v zájmu dodržení rozumného rozsahu a srozumitelnosti se zde dopouštím řady nepřesností, přílišných zjednodušení a dalších hříchů. Pokud se se zjednodušením nechcete spokojit, nebo pokud ve vás tato knížka vzbudí víc otázek, než kolik jich zodpoví, na konci najdete odkaz na spoustu mnohem podrobnějších zdrojů.

Klíč k tajemství

Jedna ze základních kryptografických pouček praví, že *šifrováním se tajemství neztratí, jenom se zmenší*. Každá šifra má svůj *klíč*, který slouží k zašifrování a dešifrování dat (případně k vytvoření a ověření elektronického podpisu). Tento klíč je nutné uchovávat v tajnosti – ve stejné tajnosti, jako původní citlivá data, která jsme zašifrovali. Proto říkáme, že se tajemství jenom zmenší: šifrování je jenom technologická pomůcka. Výhodou je, že je mnohem snazší uchovat v tajnosti pár bajtů až kilobajtů klíče, než gigabajty původních dat.

V konečném důsledku pak šifrování musí vždy končit v naší hlavě: „klíčem poslední instance“ je pak nějaké heslo (PIN, passphrase…) kterou si musíme zapamatovat. Na šifrování lze tedy hledět jako na proces zmenšování tajemství až do velikosti, kterou pohodlně udržíme v paměti.

Ochrana klíče je pak úhelným kamenem kryptografie. Pokud je klíč ztracen, k datům se již nikdo nedostane. Pokud je prozrazen, klenba kryptosystému se zhroutí a útočník získá naše data.

Klíč je také to jediné, co bychom ohledně šifrování měli držet v tajnosti. Šifrovací algoritmy samotné, tedy postupy, jakými se šifrování provádí, naopak tajné být nesmí. Všechny dnes běžně používané algoritmy jsou veřejné, otevřené standardy. Kdokoliv si může přečíst a podrobně prostudovat, jak funguje RSA nebo AES. Spousta chytrých lidí to také udělala – a právě proto můžeme důvodně předpokládat, že jsou tyto algoritmy bezpečné a důvěryhodné.

Proprietární, tajné a nezveřejněné algoritmy obvykle znamenají problém. Historická zkušenost praví, že obvykle nebývají příliš kvalitní a bývají relativně svižně prolomeny. Je to paradox, ale pouze zdánlivý:

tajemství musí spočívat v klíči, ne v postupu. Pokud tedy někdo v produktu citlivém na bezpečnost utajuje, jaké kryptografické algoritmy používá, je to obecně důvod k obavám a nedůvěře.

Šifrování versus kódování

Na závěr této kapitoly si necháme ještě jedno slovíčko, které se se šifrováním tak trochu neoprávněně pojí: *kódy* a *kódování*. v laické komunikaci a bohužel i některé populárně naučné literatuře se *šifrování* a *kódování* používá jako synonymum. Což v žádném případě není správné.

- *Šifrování* dat slouží k jejich utajení. v případě moderních šifer se nijak nezabývá formátem nebo obsahem zprávy – vstupem i výstupem jsou obecná binární data.
- *Kódování* dat je technická úprava pro přenos nebo ukládání v nějakém systému, která sice může způsobit zdánlivou nečitelnost zprávy, ale neslouží k utajení jejího obsahu.

Příkladem kódování je třeba Morseova abeceda. Ačkoliv může být pro běžného uživatele, který ji neovládá, nesrozumitelná, jde jenom o způsob převodu dat do podoby, kterou lze přenést stylem „tečka čárka“. v oblasti výpočetní techniky se zpravidla setkáváme s Base64 kódováním, které slouží pro přenos či ukládání obecných osmibitových dat sedmibitovým či textovým způsobem – např. v rámci e-mailu.

Zmatení jazyků je navíc podpořeno ještě tím, že kryptografický materiál (šifrovaná data, klíče…) se rutinně právě Base64 kódují, protože pak je s nimi obecně snazší práce. Nicméně Base64 nebo podobné kódování je jenom technická pomůcka, z hlediska utajení informace nemá význam.

Jak vidno, použití (případně kombinace) šifrovacích algoritmů většinou vychází z principu jejich fungování a účelu použití a běžný uživatel nemá v tomto případě příliš na výběr. Nicméně i jemu se může hodit znát základní vlastnosti toho, co používá. Už jenom proto, aby věděl, že svůj tajný klíč musí chránit jako oko v hlavě.

Symetrické šifrovací algoritmy

První velkou rodinu postupů pro utajení dat tvoří *symetrické šifrovací algoritmy*. Jsou proto symetrické, že se pro šifrování a dešifrování používá stejný klíč.

Primitivním „symetrickým algoritmem“ je prostá logická operace XOR. Pokud máme k dispozici jednorázový náhodný klíč o délce shodné jako je objem šifrovaných dat, stačí je prostě zaXORovat a máme matematicky neprolomitelnou šifru. Nicméně to je přístup dosti fundamentalistický a pro většinu praktických scénářů nepoužitelný.

Používáme tedy poněkud sofistikovanější metody, které nám umožňují to, o čem jsem v úvodu pravil, že je obecně cílem šifrování – zmenšit tajemství do podoby klíče.

Typickým a v současnosti snad nejrozšířenějším symetrickým algoritmem je AES (Advanced Encryption Standard). Ve starších systémech se lze ještě místy setkat se starým (a dnes již nepostačujícím) algoritmem DES/3DES (Data Encryption Standard). Existuje i celá řada dalších algoritmů jako například Skipjack, Blowfish, Twofish, ale faktickým standardem je dnes AES.

Klíč k symetrické šifře je obvykle relativně krátký, v případě AES má 128-256 bitů (tedy 16-32 bajtů), a jeho délka je daná konstrukcí algoritmu, nemůžeme ji tedy libovolně měnit. Klíč pro symetrický algoritmus nemá žádnou vnitřní strukturu a jsou to pokud možno náhodně generovaná data.

Bezpečnost celého systému zásadně závisí na kvalitě klíče, potažmo na míře jeho náhodnosti. Problém je, že počítače neumějí digitální data generovat. Počítač, digitální procesor, je z principu neschopen generovat náhodná data, to nelze čistě matematickými postupy zařídit.

Pořádný chaos vyžaduje speciální hardware: ve chvíli, kdy potřebujeme získat opravdu kvalitní náhodná data ve velkém množství, používají se fyzikální jevy, které pokládáme za náhodné: kvantové jevy[1], atmosférický šum, radioaktivní rozpad… Běžné počítače nicméně postupují tak, že sbírají „náhodné“ podněty zvenčí: sledují se intervaly příchodu paketů, pohyby myší, psaní na klávesnici… Filtrují z nich predikovatelné sekvence a snaží se získat entropii. Pro běžné použití a většinu situací to postačuje.

Nejnovější procesory od Intelu obsahují hardwarový generátor náhodnosti přímo v sobě, dostupný pomocí instrukce RDRAND[2]. Zatím je ale jenom málo programů, které tento generátor umějí využít.

Základní výhodou symetrických algoritmů (zejména v porovnání s asymetrickými, o nichž bude řeč příště) je jejich rychlost a principiálně neomezený objem dat, které jsou schopné zašifrovat. Navíc současné procesory[3] mají často vestavěnou hardwarovou akceleraci AES, která dokáže kryptografické operace výrazně zrychlit – i několikanásobně. To má význam například při šifrování dat na pevném disku: šifrování na takto vybaveném počítači neznamená měřitelné zpoždění při práci s uloženými daty.

Základní nevýhodou symetrických algoritmů je pro řadu případů právě to, že jsou symetrické. Jsou perfektně použitelné pro scénář, kdy šifrujeme data „sami pro sebe“, například u výše zmíněného šifrování disku. Samy o sobě jsou ale zcela nevyužitelné v dalším klasickém případě: pokud si dvě komunikující strany chtějí vyměňovat data a mají k dispozici pouze kanál, který není bezpečný, protože

[1] Příkladem jsou třeba kvantové generátory náhodnosti od ID Quantique: http://www.idquantique.com/
[2] http://software.intel.com/en-us/blogs/2011/06/22/find-out-about-intels-new-rdrand-instruction
[3] Opět nejnovější řada Core i3/i5/i7 od Intelu, ale i některé starší procesory VIA a další.

může být například odposloucháván. Pokud chcete symetricky šifrovaná data poslat někomu dalšímu, musíte mu také předat šifrovací klíč. Pokud jste to schopni učinit bezpečně, způsobem odolným proti odposlechu, je všechno v pořádku. Pokud ale takovou příležitost nemáte, jste ztraceni.

Bezpečnost klíče také klesá s počtem jeho použití. Ideální tedy je pro každou zprávu používat jiný klíč, což práci s nimi dále komplikuje. Je nutné používat nějaký systém generování a synchronizace klíčů.

Pokud ale potřebujete zašifrovat disk nebo konkrétní datový soubor, aby se například v případě ztráty notebooku nedostal do nepovolaných rukou, je symetrické šifrování řešením pro vás. Programy jako BitLocker (který je součástí vyšších edic Windows 7 a Windows 8), nebo open source TrueCrypt[4] jsou založené právě na symetrických algoritmech.

[4] http://www.truecrypt.org

Asymetrické šifry

Symetrické algoritmy, o nichž byla řeč v minulé kapitole, jsou obvykle dosti skryté, běžný uživatel s nimi a s jejich klíči přímo pracuje zřídkakdy. U asymetrických algoritmů je tomu jinak: s jejich klíči se, nejčastěji v podobě certifikátů, setkáváme celkem často. S postupující elektronizací státní správy také nabývá na důležitosti elektronický podpis, který je na nich založen.

Zlé jazyky říkají, že *asymetrické šifrovací algoritmy* se tak nazývají, protože abyste je pochopili, musíte prostudovat asi metr vysokou hromadu knih. Něco na tom bude, protože ve slabších povahách zdeptaných výukou matematiky na českých školách dokáží vzbudit hrůzu již prostá slova „celočíselná faktorizace“ nebo „diskrétní logaritmy“ – tedy matematické postupy, které se pro asymetrické algoritmy vnitřně používají.

Asymetričnost diskutovaných algoritmů nicméně spočívá především v tom, že používají klíče dva: soukromý (také se mu říká tajný) a veřejný.

- **Soukromý (tajný) klíč** slouží k dešifrování dat a k vytvoření elektronického podpisu. Musíte ho tedy střežit stejně žárlivě, jako klíč symetrické šifry. Jeho výhodou nicméně je, že jej nikdy nemusíte nikam dopravovat a přenášet: budete ho potřebovat jenom vy sami.
- **Veřejný klíč** slouží k šifrování dat a k ověření elektronického podpisu. Není nutné jej nijak zvlášť střežit – ba právě naopak. Musíte jej dát k dispozici každému, s kým chcete bezpečně komunikovat. Jeho vyzrazení nepředstavuje nejmenší problém. Problémem by mohlo nicméně být jeho podvržení – od toho ovšem máme certifikační autority, o kterých bude řeč v některém z dalších článků.

Typickým zástupcem asymetrického šifrovacího algoritmu je RSA (pojmenovaný podle jmen svých vynálezců, Rivest – Shamir – Adleman).

Klíč asymetrického algoritmu je řádově delší, že u symetrického: má obvykle tisíce bitů. Jeho délka není povahou algoritmu prakticky nijak omezena, a dá se říci čím delší, tím lepší. Ovšem také tím náročnější na vygenerování a následné operace. Vytvoření asymetrického klíče je výpočetně velmi náročná operace, přičemž její náročnost exponenciálně stoupá s délkou klíče: při zdvojnásobení délky klíče se 16× zpomalí jeho generování, 8× operace se soukromým klíčem a 4× operace s veřejným klíčem.

Délku klíče tedy volíme s ohledem na momentálně dostupné výpočetní kapacity a se zřetelem k době, po kterou budeme data chtít utajovat: čím delší životnost dat, tím delší klíče. v současnosti lze za minimum považovat klíče o délce 1024 bitů, za optimum pro běžné použití 2048-4096 bitů a pro obzvláště důležité klíče nebo dlouhodobě uchovávaná data dokonce 8192 nebo 16384 bitů.

Nedá se paušálně říct, že by RSA bylo lepší než AES, protože má delší klíč. Jedná se o funkcionálně zcela odlišné mechanismy. Do jisté míry lze dokonce symetrické algoritmy považovat za fundamentálně bezpečnější, než asymetrické. Druhé jmenované jsou totiž vesměs založeny na obtížnosti faktorizace velkých čísel. To sice neumíme, ale nikdo nikdy nedokázal, že to nejde – nelze teoreticky vyloučit, že se zítra ráno probudí matematický génius, který přijde na způsob, jak ji jednoduše provést a v tom okamžiku nám celá současná asymetrická kryptografie bude k ničemu.

Hlavní výhodou asymetrické kryptografie je její asymetričnost: velice snadno jsme schopni zabezpečit šifrovanou komunikaci i na nedůvěryhodném komunikačním kanálu: stačí, aby si obě strany vyměnily

veřejné klíče, které nepředstavují tajemství a mohou komunikovat důvěrně. Vyzrazení veřejných klíčů například odposlechem nepředstavuje problém. Právě schopnost zajistit důvěrnou komunikaci i na nedůvěryhodném kanále je pro nás velmi podstatná.

Dále se pak hodí oddělení šifrování a dešifrování – data může zašifrovat kdokoliv, ale dešifrovat jenom vlastník příslušného soukromého klíče. Kromě toho lze asymetrické algoritmy využít i k vytváření elektronického podpisu a k autentizaci, tedy ověřování totožnosti, nebo chcete-li k přihlašování, jak bude pojednáno později.

Hlavní nevýhodou asymetrických algoritmů je jejich pomalost a omezený objem dat, pro který ji můžeme použít. Vzhledem ke své nemalé výpočetní náročnosti jsou asymetrické šifrovací operace pomalé. Velmi pomalé. Řádově pomalejší, než symetrické. Pomalé až k praktické nepoužitelnosti pro většinu účelů.

V praxi tedy, pokud používáme asymetrické algoritmy k šifrování, oba druhy algoritmů kombinujeme: vlastní objemná data zašifrujeme symetrickou šifrou s náhodným klíčem. Ten pak zašifrujeme asymetrickým algoritmem – protože má doslova pár bajtů, tak to výpočetně zvládneme. Zašifrovaný symetrický klíč pak přihodíme k původním datům a máme je tak fakticky zabezpečená asymetrickým klíčem.

Asymetrickou kryptografii používáme v praxi téměř vždy, když chceme zajistit důvěrnost přenášených (nikoliv staticky uložených) dat: při šifrování e-mailů nebo třeba zabezpečeném přístupu k webovým serverů protokolem HTTPS.

Hashovací algoritmy

V předchozích kapitolách jsme se zabývali symetrickými a asymetrickými šifrovacími algoritmy. Smyslem jejich existence je utajit obsah přenášené informace. Dalším z kryptografických primitiv, tedy (relativně) jednoduchých algoritmů, ze kterých se pak staví rozsáhlejší systémy, jsou hashovací (čti *hešovací*) funkce.

Jedná se o výpočet jakéhosi „kontrolního součtu“ libovolné zprávy („zprávou“ zde, jako všude v kryptografii, opět nazýváme obecně jakákoliv data). Hashovací algoritmy fungují tak, že matematickými prostředky z libovolných (a libovolně velkých) vstupních dat vytvoří zprávu kratší. Povaha hashovacího algoritmu přitom zajišťuje tři důležité vlastnosti:

1. Pro tutéž zprávu (tatáž vstupní data) bude výsledek vždy stejný.
2. Ze znalosti výsledku nebude možné zpětně dopočítat původní zprávu.
3. Pravděpodobnost kolize, tedy možnost nalezení dvou různých vstupních dat, která budou mít stejný výsledek, je extrémně malá.

Výsledek hashovacího algoritmu se nazývá různě: časté je prostě pojmenování „hash“ (čti heš), „fingerprint“ nebo „thumbprint“. Lze se setkat i s českými překlady „miniatura“ nebo „otisk“. Jedná se ale vždy o totéž.

S velmi vysokou pravděpodobností (ba téměř jistotou) se můžeme spolehnout na to, že mají-li dvě zprávy totožný hash, jsou totožné. Této vlastnosti se využívá velmi často v kryptografii i mimo ni.

Hashovací algoritmy

Nejstarším hashovacím algoritmem, se kterým se dnes běžně setkáme, je **MD5**. Navrhl ho v roce 1991 Ron Rivest (písmeno „R“ v názvy šifry RSA, o které byla řeč minule). Pro kryptografické účely nelze v současnosti MD5 pokládat za bezpečný, protože již před několika lety byly objeveny způsoby, jak získat kolizní dokumenty a pomocí rainbow tables lze za určitých okolností získat i části původních zpráv, zejména tedy hesel.

Novějším algoritmem je **SHA-1**, který vytvořila americká NSA. Staví na stejných principech jako MD5, ale její návrh je poněkud robustnější a je také o něco delší (160 místo 128 bitů). Jsou známé některé její principiální nedostatky, ale zatím nebyla kompromitována takovým způsobem, jako MD5. Je to nicméně jenom otázkou času a obecně se nedoporučuje ji používat pro nové systémy.

Tím nejlepším, co máme v současné době prakticky k dispozici, je **SHA-2**. Tento algoritmus se vyskytuje ve dvou variantách, **SHA-256** a **SHA-512**, přičemž toto číslo určuje též délku výsledku v bitech (lze se setkat i s variantami SHA-224 a SHA-384, což je ale prakticky totéž, jenom s “uříznutým koncem“). Algoritmy této rodiny jsou opět založeny na obdobných principech jako MD5 a SHA-1, jen jsou ještě o něco delší a robustnější. v současnosti je pokládáme za dostatečně bezpečné, a vhodné pro návrh nových systémů. Řada systémů byla upgradována tak, aby podporovala SHA-2, což se týká mimo jiné i českých kvalifikovaných certifikačních autorit.

Hashovací (a šifrovací) algoritmy pro standardizační účely se vybírají ve veřejné soutěži. Jedna taková skončila 2. října 2012, kdy byl americkým Národním institutem pro standardy a technologie (NIST) vyhlášen vítězný algoritmus soutěže **SHA-3**. Tento algoritmus má zcela odlišnou konstrukci, než všechny dosud zmíněné. Pro svou novost nicméně není dosud standardně implementován v běžných kryptografických knihovnách – to nás čeká v následujících letech.

Použití hashe

Hashe lze využít například pro vyhledávání duplicit, souborů s totožným obsahem: spočítáme hashe a pak porovnáváme jenom ty – není třeba stylem „každý s každým“ porovnávat původní zdrojové soubory.

Další typické užití je pro ověření integrity dat, například při přenosu nebo při uložení na ne zcela spolehlivé médium: před přenosem spočítáme hash, po přenosu také a pokud hashe po porovnání souhlasí, data se přenesla správně.

Hash samotný nám bez dalšího zabezpečení nepomůže proti záměrné manipulaci. s drobnou úpravou se nicméně může stát nejjednodušší formou elektronického podpisu (formálně vzato, nejedná se o elektronický podpis ve smyslu českého práva).

K datům, jejichž autenticitu chceme ověřit, přidáme před výpočtem hashe ještě něco navíc, náhodně vygenerovaná tajná data. Těm se říká klíč, nebo někdy také sůl. Útočník bez znalosti klíče nemůže vygenerovat podvržený hash. Tento postup a jeho výsledek se označuje jako HMAC – Hash Message Authentication Code.

Hashovací algoritmy jsou také nezbytné pro ověřování pravosti certifikátů a pro vytváření a ověřování „opravdových“ elektronických podpisů založených na asymetrické kryptografii.

Elektronický podpis a přihlašování pomocí asymetrických algoritmů

Elektronický podpis má dvě základní funkce: umožnit prokázat, že se obsah zprávy od okamžiku podpisu nezměnil a svázat identitu podepisujícího klíče s obsahem zprávy. V tomto směru je schopnější, než klasický podpis na papíře: ten totiž neumožňuje prokázat, že se obsah dokumentu nezměnil, že např. na listinu někdo něco dodatečně nepřipsal. To bychom museli dokazovat dalšími, mnohem složitějšími postupy.

Populárním omylem je přesvědčení, že elektronický podpis zabrání modifikaci dokumentu. Není to pravda, modifikaci zabránit nelze. Ale lze ji detekovat, pokud podpis ověříme: nebude souhlasit. To je ale vše, podpis nám neumožní zjistit, jak byla změna velká nebo co konkrétně bylo změněno a jak. Jenom se dozvíme, že změna nastala.

Co dalšího elektronický podpis znamená, to záleží na okolnostech jeho použití a na smluvních nebo zákonných podmínkách. Intuitivně předpokládáme, že elektronický podpis znamená vyjádření souhlasu s obsahem zprávy, ale to nemusí být vždycky pravda. Například v případě autorizované konverze, tedy převodu dokumentu z listinné do elektronické podoby, připojí konvertující osoba k elektronické verzi svůj elektronický podpis. v tomto kontextu to nicméně neznamená souhlas s obsahem dokumentu, ale jenom potvrzení, že elektronická podoba je věrným obrazem té listinné.

Jak elektronický podpis funguje?

V jednom z předchozích dílů jsme si ukázali, jak funguje asymetrický šifrovací algoritmus RSA. Máme dva klíče: veřejný (slouží k zašifrování zprávy) a soukromý (slouží k dešifrování). Elektronický podpis pomocí RSA je tak trochu šifrování naruby.

Začneme tím, že z podepisovaných dat spočítáme hash (např. SHA-1 nebo SHA-2, viz předchozí kapitola). Tento hash potom zašifrujeme soukromým klíčem. Tedy obráceně, než je zvykem, normálně se šifruje veřejným klíčem. a hash dokumentu zašifrovaný tajným klíčem je elektronický podpis v surové podobě.

Pokud chceme podpis ověřit, tak začneme tím, že jej dešifrujeme veřejným klíčem osoby, která podpis vytvořila (musíme jej tedy mít k dispozici). Tím získáme hash původně podepisovaných dat. Ve druhém kroku pak sami spočítáme hash zprávy, kterou jsme obdrželi. Pokud oba hashe souhlasí, jedná se o tutéž zprávu, můžeme si být jisti, že nebyla nijak modifikována.

V reálné praxi je samozřejmě podpis poněkud složitější. Jeho datová struktura kromě surového podpisu (zašifrovaného hashe) obsahuje ještě řadu dalších informací. Například popis použitých algoritmů a jejich parametrů, identifikaci veřejného klíče, případně přímo ten klíč samotný atd.

Formáty, v nichž jsou podpisy a související údaje uchovávány, jsou definovány mezinárodními standardy, což umožňuje vzájemnou interoperabilitu jednotlivých technologií. Standardů souvisejících s elektronickými podpisy je celá řada, ale jsou vesměs založeny na PKCS#7/CMS (Public Key Cryptography Standard #7, Cryptographic Message Syntax). Tato norma říká, jak se obecně ukládá kryptografický materiál: podpisy, jeho metadata, související klíče, časová razítka a další.

Od ní jsou pak odvozeny normy z rodiny AdES (Advanced Electronic Signature), které přesně určují, jaké konkrétní údaje a v jaké podobě mají být jako součást podpisové struktury uvedeny. PAdES to určuje pro formát PDF, XAdES pro XML dokumenty atd.

Elektronický podpis může být přímo součástí struktury dokumentu samotného, pokud to jeho formát umožňuje. Typickým případem je třeba PDF nebo Office OpenXML ve Wordu. Tomuto postupu se říká „interní podpis“ a setkáte se s ním nejčastěji při podpisu běžných dokumentů, například v rámci služeb eGovernmentu. Podpis může nicméně existovat i jako samostatný soubor („externí podpis“) a pak lze podepsat jakákoliv data. Takový podpis obvykle mívá název shodný jako je název podepisovaného souboru a příponu „`.sig`“, „`.p7b`“ nebo „`.p7s`“. Tj. např. k souboru `data.txt` bude existovat podpis `data.txt.p7s`.

Elektronický podpis sám umožňuje propojit podepisovaná data pouze s klíčem. My ale většinou chceme zjistit, která konkrétní osoba podpis vytvořila. K tomuto účelu, tedy ke spojení klíče s konkrétním subjektem, slouží certifikáty a certifikační autority.

Certifikáty a certifikační autority

Klíč asymetrického algoritmu (typicky RSA) je nezbytný pro šifrování a elektronické podepisování dat. Pro praktické použití ale musíme vědět, komu ten který klíč patří, jaké konkrétní osobě, systému a podobně. Kromě toho potřebujeme ukládat ještě další metadata, jako například účely použití nebo časové omezení platnosti. Proto se asymetrické veřejné klíče obvykle po světě potulují nikoliv ve své holé podobě, ale v podobě certifikátu, který všechny tyto údaje umí uchovávat.

Alice, Bob a Eva

Abychom si ukázali nutnost a funkci certifikační autority, seznámíme se s Alicí, Bobem a Evou. Alice a Bob se poprvé objevili v roce 1977 v článku Rona Rivesta (o kterém už byla řeč, jako o jednom z autorů RSA a MD5) a od té doby se tradičně používají jako ukázkové osoby v kryptografických příkladech. Jejich protivníkem je Eva, která na Alici už pětatřicet let žárlí a snaží se její komunikaci s Bobem odposlouchávat nebo různým způsobem mařit.

Chtějí-li Alice a Bob bezpečně komunikovat pomocí asymetrické kryptografie, musí si každý z nich vygenerovat pár klíčů (tajný a veřejný) a ten veřejný potom předat protistraně – musejí si vyměnit klíče. Pokud může Eva jejich komunikaci pouze odposlouchávat, nebude jí to nic platné: získá jenom veřejné klíče, které – jak jsme si již řekli v předchozích dílech – nepředstavují žádné tajemství.

Nicméně pokud Eva může jejich komunikaci nejenom odposlouchávat, ale také modifikovat, mají problém. Eva může zasílaný veřejný klíč odchytit a místo něj podvrhnout svůj vlastní, který si pro tento účel vygenerovala. Potom bude schopna dešifrovat, modifikovat a zpětně zašifrovat jakékoliv zprávy, které si Alice a Bob vymění. Tomuto typu útoku se říká „man in the middle attack“.

Pokud tedy chce Alice Bobovi posílat šifrované zprávy (nebo si ověřit jeho elektronický podpis), musí mít jistotu, že získaný veřejný klíč patří skutečně jemu. Problém s veřejnými klíči tedy nespočívá v jejich prozrazení, ale v možnosti jejich podvržení. Pokud chce Alice mít jistotu, že Bobův klíč patří skutečně jemu, má na výběr v zásadě ze třech možností:

a) Musí jej získat důvěryhodným způsobem. Tedy takovým, kde má jistotu, že komunikuje skutečně s Bobem. Ideálně tak, že jí ho Bob fyzicky předá třeba na flash disku.
b) Může jej získat jakkoliv, ale musí si ověřit, že patří skutečně Bobovi. Například tak, že spočítá jeho otisk (hash – byla o nich řeč v jednom z minulých dílů) a pak se bezpečným způsobem spojí s Bobem a ověří si, že hashe klíče souhlasí. Musí tak učinit jiným kanálem, než jakým získala klíč, jinak je takové ověření bezcenné. Tj. např. pokud obdrží klíč e-mailem, může Bobovi zatelefonovat – pokud je rozumné předpokládat, že Eva může zasahovat do komunikace mailem, ale ne po telefonu.
c) Může využít služby nezávislé důvěryhodné třetí strany, která se vahou své důstojnosti zaručí za to, že klíč je pravý.

Prvně zmíněné varianty jsou pro rutinní použití většinou nepraktické (i když mají své místo) a většinou se tedy v praxi vydáváme tou třetí cestou. a onou nezávislou důvěryhodnou třetí stranou je **certifikační autorita**.

Certifikační autorita

Certifikační autorita je instituce, která ověřuje totožnost libovolného žadatele. Na základě tohoto ověření potom ke klíči přidá informace o jeho vlastníkovi a celý tento balíček digitálně podepíše vlastním klíčem.

Celé to funguje v několika krocích:

1. Certifikační autorita publikuje svou **certifikační politiku**. To je dokument, který popisuje postupy, které certifikační autorita používá, jak si ověřuje totožnost žadatelů a jaké poskytuje záruky. Každá certifikační autorita si je stanovuje po svém a s ohledem na účel, pro který mají být její certifikáty používány.
2. Uživatel, který prahne po certifikátu, si vygeneruje pár klíčů, přidá k tomu veřejnému požadovaná metadata a to celé podepíše svým soukromým klíčem. Této datové struktuře se říká **certificate signing request** (CSR, žádost o podpis certifikátu) a popisuje ji standard PKCS#10. Žádost zašle certifikační autoritě.
3. Certifikační autorita si v souladu se svou politikou nějakým způsobem ověří, že v žádosti uváděné údaje jsou pravdivé. Pokud je v tomto ohledu uspokojena, vezme veřejný klíč, přidá k němu identifikaci vlastníka, identifikaci svoji, označení doby platnosti a další údaje. Celý tento datový balíček pak podepíše svým vlastním klíčem a vrátí uživateli. Tomuto výsledku se pak říká **certifikát**.

Platí tedy, že certifikát je veřejný klíč, plus metadata, to celé podepsané certifikační autoritou.

Nutnost ověřovat si pečlivě identitu každé komunikující protistrany zvlášť je pak nahrazena nutností ověřit si identitu certifikační autority (stejným způsobem, jaký byl popsán výše). Což je úkon řádově jednodušší, protože pro praktické použití lze předpokládat, že certifikačních autorit bude málo a bude snazší si ověřit jejich totožnost.

Na druhou stranu, certifikační autorita se stává slabým bodem celého systému. Pokud uživatel za důvěryhodnou prohlásí nepravou autoritu, kompromituje tím bezpečnost svého systému. Stejně tak, pokud certifikační autorita vydá z nějakého důvodu certifikát nepravé osobě – jako se stalo v relativně nedávné minulosti například dnes již neexistující holandské autoritě DigiNotar[5].

Výměnu zpráv mezi Alicí a Bobem, stejně jako popis funkce certifikátů a certifikačních autorit, si můžete prohlédnout v krátkém videu na YouTube: http://youtu.be/LTa7JOjAtQ4

Jakou certifikační autoritu zvolit?

Z hlediska čisté kryptografické teorie na konkrétní zvolené certifikační autoritě nezáleží. Záleží na použitých algoritmech, délce klíčů a dalších parametrech. v praxi nicméně záleží na certifikačních politikách té které certifikační autority a účelu, pro který certifikáty potřebujeme.

Certifikáty podle českého zákona o elektronickém podpisu: pro komunikaci s úřady

Kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb [6]. S touto možností se setkáte velmi často v oblasti eGovernmentu. Hovoří-li se o elektronickém podpisu v kontextu českého zákona, téměř vždy se jedná o tento. Tento typ certifikátu potřebujete, pokud jste orgánem veřejné moci, nebo s nimi hodláte elektronicky podepsaným způsobem komunikovat.

Vydávání a použití těchto certifikátů je poměrně podrobně upraveno zákonem a jeho prováděcím předpisem. Podle stanoviska Ministerstva vnitra, které je v tomto oboru dohlédacím orgánem, lze kvalifikované certifikáty použít pouze pro účely elektronického podpisu. Technicky vám nicméně nic nebrání používat jej třeba pro šifrování nebo pro autentizaci. Ačkoliv je právní konstrukce za tímto

[5] http://www.f-secure.com/weblog/archives/00002228.html
[6] Ve smyslu zákona 227/2000 Sb. o elektronickém podpisu

omezením dost vachrlatá a její legalita pochybná, obecně je dobrý nápad nepoužívat tentýž klíč pro několik různých účelů.

Pro úplnost dodávám, že zákon rozeznává „kvalifikovaný certifikát“, který se používá pro vytváření elektronického podpisu živým člověkem a „kvalifikovaný systémový certifikát“, který se používá pro vytváření elektronických značek automatickým zařízením (např. programem na generování faktur). Genialitu myšlenkového pochodu zákonodárce, který vedl k této dvojkolejnosti, se autorovi nepodařilo docenit za celých dvanáct let, co se elektronickými podpisy zabývá.

Certifikát vydaný akreditovaným poskytovatelem certifikačních služeb (tedy ne kvalifikovaný, obvykle se mu říká „komerční“ nebo „veřejný“). Pohybuje se z hlediska zákona o elektronickém podpisu v jakémsi právním vakuu, protože ho sice vydává ministerstvem akreditovaná certifikační autorita, ale jinak s ním obecně české právo příliš nepočítá. Pokud je mi známo, je zákonem (resp. prováděcí vyhláškou) předpokládán pouze jako jedna z autentizačních metod pro přihlášení k datovým schránkám.

Tento certifikát můžete použít pro autentizaci a šifrování (a samozřejmě též pro elektronický podpis, ovšem ten vám v kontextu eGovernmentu nebude k ničemu). v praxi je jeho využitelnost dosti omezená. v soukromoprávní sféře může mít výhodu, pokud chcete využít relativně rozsáhlou infrastrukturu na území ČR a hodí-li se vám, že s vámi příslušné firmy budou komunikovat česky.

Certifikáty v režimu dle zákona o elektronickém podpisu (kvalifikované i veřejné) vydávají tři společnosti. Seřazeny podle doby působení na trhu to jsou:

- I.CA – první certifikační autorita (www.ica.cz)
- Post Signum – certifikační autorita provozovaná Českou poštou (www.postsignum.cz)
- eIdentity (www.eidentity.cz)

Vydání certifikátu je zpoplatněno a částka za jeho vydání se pohybuje v řádu stokorun ročně. Pro ověření totožnosti je obecně nutné dostavit se fyzicky na pobočku certifikační autority a předložit dva doklady totožnosti. v certifikátu je pak uvedeno vaše jméno, příjmení, e-mailové adresa a volitelně další údaje, jako například zaměstnavatel, adresa nebo identifikátor MPSV.

Tyto certifikáty mají nicméně jednu velkou nevýhodu: české certifikační autority nejsou obecně pokládány za důvěryhodné světovými výrobci operačních systémů a prohlížečů a nejsou tedy součástí výchozí instalace. Uživatelům se tedy budou jimi vydané certifikáty jevit jako nedůvěryhodné a doprovázené celou řadou varování.

I.CA a Post Signum jsou alespoň zařazeny do Microsoft Trusted Root programu, což znamená, že jsou jako důvěryhodné chápány na novějších verzích Windows, pokud tato funkce není zakázána, a v programech, které využívají standardní systémové úložiště. Což znamená, že vám budou fungovat jenom někdy a někde – například v Internet Exploreru a Outlooku, ale už ne třeba ve Firefoxu a Thunderbirdu, protože tyto programy standardní systémové úložiště zcela ignorují a s větším či menším úspěchem si vytvářejí vlastní.

Certifikáty zahraničních certifikačních autorit: pro důvěryhodnost bez překážek

Pokud chcete získat certifikát, který bude v běžných programech pokládán automaticky za důvěryhodný, musíte se vydat za hranice. Těmito autoritami vydávané certifikáty ovšem zase nemají speciální postavení z hlediska českého práva.

Pravděpodobně nejznámější světovou certifikační autoritou je VeriSign (www.verisign.com). Nicméně obecně důvěryhodných certifikačních autorit je celá řada. Nabízejí v praxi tytéž služby, ale za výrazně odlišné ceny. Za certifikát s roční platností a prakticky totožnými parametry můžete zaplatit stejně tak dobře deset jako dvě stě dolarů.

Zvláštní zmínku si zaslouží dvě certifikační autority, které vám vydají důvěryhodný certifikát zdarma:

- **InstantSSL by Comodo** vám vydá osobní certifikát pro zabezpečení elektronické pošty zdarma. Jeho nalezení na webu certifikační autority je poněkud obtížné, takže zde je konkrétní odkaz: http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html
- **StartSSL** (www.startssl.com) kromě osobních certifikátů vydává zdarma i základní serverové certifikáty, například pro web servery.

Většina zahraničních komerčních autorit vám vydá základní certifikát pouze na základě ověření e-mailové adresy, případně vlastnictví domény, není nutné dokládat žádné další údaje (a certifikát ani žádné další údaje, jako jméno či adresu, neobsahuje). Vydání certifikátu obvykle trvá desítky minut až hodiny.

Tento typ certifikátu se vám hodí ve chvíli, kdy nemusíte pracovat v režimu českého zákona o elektronickém podpisu (tedy nejste orgánem veřejné moci ani s nimi nehodláte komunikovat) a nevadí vám, že budete muset komunikovat v angličtině. Existují i čeští zprostředkovatelé a přeprodejci, kteří za jistý poplatek odstraní případnou jazykovou bariéru. Zpravidla se jedná o přidruženou výrobu poskytovatelů hostingových služeb nebo registrátorů domén.

Vlastní certifikační autorita? Obvykle špatný nápad

Mohlo by vás napadnout, že pokud máte nějakou uzavřenou skupinu uživatelů (třeba firma a její zákazníci nebo naopak dodavatelé), můžete ušetřit a rozjet si vlastní, soukromou certifikační autoritu.

Téměř nikdy to není dobrý nápad. Nejde o to, že by vydávání certifikátů bylo technicky nějak zvlášť náročné – pomocí nástrojů z Windows SDK nebo OpenSSL to zvládnete za deset minut. Ale provozovat CA se všemi z toho vyplývajícími důsledky a organizačním zajištěním je výrazně složitější a nestojí to za těch pár ušetřených stokorun.

Existuje několik výjimek:

1. Autority pro vývoj a testování. Kde nezáleží na bezpečnosti a poskytovaných službách, prostě potřebujete mít možnost dělat si, co potřebujete a zkoušet.
2. Technické infrastruktury, které certifikáty a certifikační autority interně využívají, třeba některá rozsáhlejší nasazení Microsoft Active Directory.
3. Opravdu velké firmy, kde se předpokládá vydání řádově více než 5000 certifikátů.

Pokud spadáte do dvou posledně zmiňovaných kategorií, může být užitečné o vlastní CA uvažovat, nicméně v takovém případě potřebujete znát o hodně více, než kolik se dozvíte z této knížky.

Časová razítka pro střednědobou udržitelnost

V minulých dílech jsme si představili algoritmy pro vytváření elektronického podpisu. a zmínili jsme se i o certifikátech, které umožňují šifrovací klíče propojit s reálnou osobou a stanovit také různá omezení pro jejich použití. Jedním z typických omezení je časová platnost. Každý vydaný certifikát obsahuje též informaci o době, od kdy do kdy je platný. U běžných certifikátů je zpravidla jeden rok. Proč je zde toto omezení?

V první řadě z důvodu bezpečnosti. S dobou, po kterou je certifikát používán a se vzrůstajícím objemem dat stoupá jeho hodnota, nebo chcete-li velikost průšvihu, ke kterému dojde v případě jeho kompromitace. Zároveň klesá jeho bezpečnost. Potenciální útočník má k dispozici více materiálu pro kryptoanalýzu (což může být pro některé typy útoků velmi podstatné). Kromě toho, s postupujícím vývojem výpočetní techniky se v čase zvyšuje její výkon.

Podle Mooreova zákona (který platí již od sedmdesátých let minulého století) se počet tranzistorů v čipu zdvojnásobí každé dva roky. Spolu s dalšími vylepšeními to znamená, že hrubý výpočetní výkon procesoru se zdvojnásobuje každých zhruba osmnáct měsíců. Musíme tedy být připraveni dle potřeby prodlužovat délku klíčů v asymetrických algoritmech, případně přijímat další opatření, které zajistí, že naše kryptosystémy budou nadále bezpečné.

Časové omezení platnosti certifikátu je jedním z nástrojů, jak podpořit obměnu klíčů a jejich výměnu za bezpečnější. No a s trochou jedovatosti můžeme dodat, že také zajišťuje zdravé cash flow certifikačním autoritám, neboť zajišťuje opakovaný business.

Kdy byl dokument podepsán?

Při ověřování elektronického podpisu musíme brát v úvahu časové hledisko. Je podstatné, kdy byl dokument podepsán, protože platnost podpisového certifikátu musíme posuzovat k tomuto okamžiku. Nejedná se přitom jenom o předem danou omezenou platnost certifikátu, ale také o jeho možné předčasné zneplatnění (revokaci).

Pokud je certifikát platný od 1. 1. 2011 do 31. 12. 2011, při ověřování v současnosti je již neplatný, protože vypršel. Nicméně pokud dokážeme prokázat, že podpis vznikl například 6. 6. 2011, je podpis nadále platný, neboť vznikl v době původní platnosti certifikátu. Stejně tak, pokud uživatel certifikát řekněme 5. 5. 2011 zneplatnil (revokoval), bude podpis vytvořený po tomto datu neplatný, z důvodu právě oné revokace.

Časová razítka

Problémem ovšem zůstává, jak prokázat, kdy byl elektronický podpis vytvořen. Nebo, pojmeme-li problém šířeji, jak prokázat, že určitá datová zpráva existovala v konkrétním čase. Zde přicházejí ke slovu časová razítka (timestamps) a autority pro vydávání časových razítek (timestamping authority, TSA).

Autorita pro vydávání časových razítek je nezávislá třetí strana, které důvěřujeme. Má tedy logickou pozici podobnou, jako certifikační autorita – a v praxi jsou také TSA obvykle „přidruženou výrobou“ certifikačních autorit, včetně všech třech českých akreditovaných, o nichž byla řeč v minulém pokračování.

Kromě toho, že je TSA nezávislá a důvěryhodná, disponuje též kvalitními hodinami s definovanou přesností, typicky nějakou formou synchronizovanými s časovým etalonem.

Potřebujeme-li opatřit zprávu časovým razítkem, spočítáme její hash a tento hash pošleme autoritě pro vydávání časových razítek. Autorita tedy nezná obsah razítkovaného dokumentu, jenom jeho hash. Autorita k tomuto hashi přidá údaj o aktuálním čase, celé to elektronicky podepíše svým klíčem a vrátí žadateli.

Časové razítko je tedy datová struktura, která obsahuje hash zprávy, časový údaj a elektronický podpis (plus nějaká další metadata, která nejsou pro náš příklad podstatná). Je to vyjádření, přeložitelné do lidského jazyka asi jako „já, důvěryhodná autorita, tímto prohlašuji, že jsem viděla hash XXX dne toho a toho v tolik a tolik hodin“.

Jsme-li schopni úspěšně ověřit časové razítko (tedy ověřit podpis na něm a ověřit hash s hashem dokumentu), jsme schopni zafixovat zprávu v čase a říci, že existovala nejpozději v daném čase a že od té doby nebyla modifikována.

Ani časová razítka nejsou na věky

Ani časová razítka ovšem neplatí věčně. i ona sama jsou založena na asymetrické kryptografii, certifikátech a principech zmíněných dříve. Pravda, certifikáty použité při jejich vydávání jsou obvykle platné déle, než ty běžné koncové (řádově 5-10 let), nicméně jednoho dne vyprší. a co potom?

Pokud hrozí, že bude nutné prokazovat platnost podpisu po delší době, než jaká je platnost časového razítka, budete muset dokument celý (i se stávajícím razítkem) „přerazítkovat“, a to ještě v době platnosti původního časového razítka. Tímto způsobem lze prodlužovat platnost a ověřitelnost elektronického podpisu na věky věkův – s tím, že s každým prodloužením zaplatíte za nové časové razítko.

Existují různé systémy, které se snaží tento proces automatizovat a občas i zlevňovat tím, že více či méně sofistikovaným způsobem propojují jednotlivé dokumenty mezi sebou. Tím snižují počet potřebných razítek, za která je nezbytné platit. *(Full disclosure: jsem spoluautorem jednoho takového systému, jmenuje se InfoStream a najdete ho na www.infostream.cz.)*

Pomocí návazných časových razítek lze zajistit – s trochou snahy a nákladů – střednědobou platnost digitálně podepsaných dokumentů, řekněme v horizontu 5-10 let, což je postačující například z hlediska promlčecí lhůty pro většinu právních sporů.

Pokud byste chtěli nebo potřebovali zajistit důvěryhodnost elektronicky podepsaných dokumentů na ještě delší dobu, na desítky či stovky let, bude váš úkol mnohem náročnější. Dlouhodobá archivace digitálních dat je jedním z největších problémů současné aplikované kryptografie a dost dynamicky se rozvíjí. Řešení teoreticky existuje celá řada, ale s jejich standardizací a praktickou implementací už je to mnohem horší. Na dlouhodobou úschovu není navíc připravena ani legislativa. Na úrovni mezinárodní jsou jakési náznaky, v rámci ČR nejsou ani ty, protože s pádem Topolánkovy vlády se elektronizace státní správy v podstatě zastavila a zájem o eGovernment vyprchal. To implementátory zanechává v dosti nepříjemné situaci, v níž neexistují jednoznačná a správná řešení.

Závěr

V úvodním dílu jsme se seznámili s některými základními pojmy a také si představili takzvaný Kerckhoffsův princip. Auguste Kerckhoffs byl holandský kryptolog, který koncem 19. století sepsal šest pravidel pro návrh šifrovacích systémů[7].

Většinu z nich v dnešní době spokojeně porušujeme, protože jsou poplatná době svého vzniku. Příkladně dnes již můžeme beztrestně hřešit proti pravidlu, že zašifrovaná data musejí být schopná telegrafického přenosu.

Nicméně druhé pravidlo, které též nazýváme „Kerckhoffsův princip“, je platné trvale. Zní: „Šifrovací systém sám nesmí představovat tajemství a nesmí představovat problém, padne-li do rukou nepřítele.“ v dobách studené války americká NSA navrhovala šifry s ideovým předpokladem, že exemplář číslo jedna každého nového zařízení bude okamžitě doručen do Kremlu.

Kryptografické algoritmy musejí být otevřené širokému zkoumání. Všechny dnes běžně používané algoritmy jsou otevřené a jsou dnes a denně předmětem zkoumání špičkovými odborníky, což napomáhá odhalování jejich slabin. Bezpečnost každého systému pak závisí na použitém klíči, nikoliv na tajemném šifrovacím algoritmu.

Historie ukázala, že většina tajených, proprietárních algoritmů obsahuje zásadní chyby. Patřičně odstrašujícím příkladem je třeba Content Scramble System (CSS) použitý pro ochranu obsahu na DVD nebo proprietární šifrování používané v RFID kartách MIFARE Classic. Obojí dokážeme prolamovat v reálném čase. Pokud někdo tají, jaké algoritmy používá, historická zkušenost praví, že nejspíš ví proč, a měli bychom se před jeho produkty mít na pozoru.

Symetrické šifrovací algoritmy

Ve druhém dílu jsme si představili symetrické šifrovací algoritmy a zejména pak současný standard Advanced Encryption System (AES). Symetrické šifry používají tentýž klíč pro šifrování i dešifrování dat. Klíč má obvykle velikost ve stovkách bitů (AES 128-256) a je tvořen náhodnými daty – čím náhodnějšími, tím lépe, ovšem získat náhodná data není tak jednoduché.

Symetrické algoritmy používáme typicky v případě, že data nikam neposíláme – například u šifrování dat na pevných nebo přenosných discích. Druhou možností je, že máme možnost bezpečně přenést symetrický klíč, například tak, že ho zašifrujeme asymetricky a obě základní šifrovací metody tak zkombinujeme.

Asymetrické šifry

Třetí díl se zabýval asymetrickými šiframi, najmě pak algoritmem RSA. Asymetrické algoritmy se vyznačují tím, že mají klíče dva: tajný a veřejný. Tajný klíč slouží k dešifrování dat a vytváření elektronického podpisu a je nutné jej bedlivě střežit. k tomu se používají i speciální hardwarová zařízení, jako čipové karty nebo autentizační tokeny. Veřejný klíč slouží k šifrování dat a ověření elektronického podpisu a tajit jej není třeba a ani to není možné, naopak musíme být schopni jej předat každému, s kým chceme bezpečně komunikovat.

[7] http://en.wikipedia.org/wiki/Auguste_Kerckhoffs

Hashovací algoritmy

Pomocí hashovacích algoritmů, jako je například MD5, SHA-1, SHA-2 nebo horká novinka SHA-3, můžeme z libovolných dat spočítat „výtah“, nebo chcete-li „otisk“. Jakýsi „kontrolní součet“, pomocí kterého lze snadno zjistit, zda se data shodují nebo ne, aniž bychom je museli porovnávat bit po bitu.

Hashovací algoritmy nám samy o sobě proti záměrnému útoku nepomohou, ale jsou důležitou součástí rozsáhlejších kryptosystémů. Dokážeme pomocí nich například ověřit pravost klíče nebo elektronického podpisu.

Elektronický podpis

Elektronický podpis neslouží k utajení obsahu zprávy. Lze pomocí něj prokázat, že zpráva nebyla oproti originálu změněna. Změně nelze zabránit, ale přijde se na ni. Obvykle používáme elektronické podpisy na bázi asymetrického algoritmu RSA.

S použitím dalších technických i organizačně-právních opatření lze také jednoznačně identifikovat osobu, která podpis vytvořila a například tak vyjádřila souhlas s obsahem podepisovaného dokumentu.

Alice, Bob, Eva a tajemství certifikátů

Na příkladu ukázkových osob Alice, Boba a nepřátelské Evy jsme si předvedli funkci certifikátů a certifikačních autorit. Pro bezpečnost (šifer i podpisů) je totiž nutné mít jistotu, že klíč patří skutečně tomu, komu předpokládáme. Lze to sice zajistit i bez autorit, ale v praxi obvykle spoléháme právě na ně, protože přímé vzájemné ověření klíčů je nepraktické a v řadě případů dokonce nemožné.

Seznámili jsme se s pojmem „certifikát“, což je vlastně veřejný klíč, doplněný metadaty a to celé podepsané certifikační autoritou. Představili jsme si také obvyklé typy certifikačních autorit z pohledu běžné praxe i českého práva a snad se mi podařilo vás odradit od nápadu vytvořit si vlastní.

Časová razítka pro střednědobou udržitelnost

Zejména u elektronických podpisů je nutné sledovat i časové hledisko. Certifikáty mají časově omezenou platnost a navíc je lze zneplatnit (revokovat) i před jejím vypršením. Z hlediska střednědobého uchovávání digitálně podepsaných dokumentů tedy musíme vědět nejenom kdo, ale také kdy podpis vytvořil.

K řešení tohoto problému slouží časová razítka, která vydávají speciální důvěryhodné instituce zvané „autority pro vydávání časových razítek“ (timestamping authority – TSA), většinou se jedná o přidruženou výrobu certifikačních autorit. Této autoritě předložíme hash dokumentu, ona jej doplní aktuálním časem a podepíše vlastním klíčem. Bohužel, i platnost certifikátu časového razítka jednoho dne vyprší a chceme-li provozovat dlouhodobou archivaci, je nutné dokumenty pravidelně přerazítkovávat.

Odkazy na další zdroje

V tomto krátkém materiálu jsem se snažil představit obor, který se pro mnoho lidí stal předmětem celoživotního studia. v zájmu stručnosti a přístupnosti co nejširší veřejnosti jsem se tedy dopustil velkého množství různých nepřesností, zjednodušení a spoustu věcí jsem zcela záměrně vypustil. Účelem mých článků bylo představit nejzákladnější principy a také ve čtenářích vzbudit zájem a zvědavost.

Pokud jste po přečtení všech dílů skončili s větším množstvím otázek, než s jakými jste číst začínali, moje práce byla úspěšná. Chcete-li najít odpovědi, následují odkazy na další zdroje v českém a anglickém jazyce.

Simon Singh: The Code Book

Beletristický a i pro laika srozumitelně napsaný průvodce kryptografií od starověkého Egypta po kvantovou kryptografii. Doporučuji pro každého, kdo se o téma chce zajímat v širším kontextu, nebo spíše pro zábavu. Oficiální stránku knihy najdete na http://simonsingh.net/books/the-code-book/.

Kniha vyšla v letech 2003 a 2009 v nakladatelství Argo i v českém překladu pod názvem Kniha kódů a šifer. Český překlad nicméně nepovažuji za příliš povedený a stačí-li vám na to jazykové znalosti, doporučuji spíše anglický originál, který je k dispozici i jako elektronická kniha.

Wikipedie

Kvalita wikipedistických článků na toto téma je – zejména v anglické Wikipedii – dosti vysoká a tento zdroj tedy lze vřele doporučit. Kromě hledání konkrétních pojmů lze jako dobrý startovací bod doporučit i portál Kryptografie: http://en.wikipedia.org/wiki/Portal:Cryptography.

Velký průvodce infrastrukturou PKI a technologií elektronického podpisu

Původní česká kniha Libora Dostálka, Marty Vohnoutové a Miroslava Knotka (vydal Computer Press v roce 2009) je podle mého názoru nejlepším českým zdrojem na toto téma. Kniha se zabírá praktičtějšími aspekty implementace, je to odborná literatura, ne beletrie. Povinná četba pro programátory a správce IT.

Kurzy na Stanford University

V rámci projektu Coursera nabízí Stanford University zdarma online kurzy Cryptography i a II. Pokud dáte přednost video prezentaci a interaktivním cvičením, je toto vhodný zdroj pro vás. Další informace najdete na https://www.coursera.org/course/crypto a https://www.coursera.org/course/crypto2. v rámci projektu Coursera najdete i další kurzy, které se kryptografie týkají, zejména jejího matematického pozadí. (Za tip v komentáři děkuji čtenáři s přezdívkou Indian.)

Bruce Schneier: Applied Cryptography, Practical Cryptography

Klasickou dvojici představují knihy Bruce Schneiera Applied Cryptography (Aplikovaná kryptografie) a Practical Cryptography (Praktická kryptografie, s N. Fergusonem). Zde se jedná již o podstatně komplikovanější četbu. Není mi známo, že by tyto knihy byly kdy přeloženy do češtiny a nejspíše ani nikdy nebudou. Další informace a zajímavé postřehy najdete i na stránkách autora, http://www.schneier.com/.

CryptoWorld

Český elektronický občasník, věnovaný kryptografii. Webové stránky naleznete na adrese http://crypto-world.info/, je také možno přihlásit se k e-mailovému odběru „sešitů“.

SecPublica.cz

Každá liška chválí svůj ocas, takže na závěr uvedu svůj vlastní projekt SecPublica. Jeho heslem je „Securitas – Res Publica“, tedy „bezpečnost – věc veřejná“. Jeho cílem je snažit se propagovat bezpečnostní témata srozumitelným způsobem. Funguje převážně jako rozcestník na články, které jsem publikoval jinde, ale obsahuje i stále se rozšiřující kolekci praktických video návodů (screencastů). Publikována je série o šifrování a digitálním podepisování e-mailů, pracuje se na sérii o šifrování disků.