Téma: Šifrovanie

Veľmi zjednodušene môžeme povedať, že šifrovanie je zapisovanie textu v takej podobe, aby mu nepovolaný čitateľ nemal šancu porozumieť. Najčastejšie sa šifrovanie v jeho rôznych podobách používa pri komunikácii: jeden človek má informáciu, ktorú potrebuje poslať inému; nechce však, aby si ju mohol cestou prečítať ktokoľvek ďalší.
Kryptografia: vedná oblasť zaoberajúca sa ukrývaním obsahu textu pred nepovolanými osobami.
Kryptoanalýza: vedná oblasť zaoberajúcu sa štúdiom metód, ktoré môže útočník použiť pri snahe získať zo zašifrovaného textu ukryté informácie.
Steganografia: vedná oblasť, ktorá sa zaoberá utajovaním samotného prenosu správ.

Kryptografia v historických dobách

Prvé zachované snahy o šifrovanie textu pochádzajú zo starého Egypta a z Mezopotámie. Zväčša išlo o jednoduchú zámenu symbolov textu, tzv. substitúciu: každý symbol pôvodného, tzv. otvoreného textu je konzistentne nahradený iným symbolom, čím vzniká šifrový text, nečitateľný pre nezasväteného. Napríklad sa zachovali prípady, kedy „pisár“ použil pozmenené formy hieroglyfov – je však možné, že pri spomínaných nápisoch na hrobkách nešlo ani tak o snahu ukryť text pred čitateľom, ako o dramatický efekt. Treba si však uvedomiť, že nie len v tejto dobe, ale ešte aj dlho potom bolo už samotné napísanie textu akousi formou šifrovania – drvivá väčšina ľudí totiž nevedela čítať, a tak bol obsah správy pred nimi ukrytý. Často krát samotný posol prenášajúci správu nevedel čítať a významu správy nerozumel. Jednoduché substitučné šifry ostávajú v obľube ešte dlhé storočia. Známym príkladom je **hebrejská šifra atbaš**, ktorej názov popisuje samotný postup šifrovania: prvé písmeno abecedy sa nahradí posledným, druhé predposledným, a tak ďalej. Pri použití dnešnej anglickej abecedy by sme namiesto každého A písali Z, namiesto každého B by bolo Y, namiesto C by sme použili W a tak ďalej. Napríklad zo slova ZABA dostali zašifrované slovo AZYZ. (Za povšimnutie stojí, že na dešifrovanie sa pri tejto šifre použije ten istý postup ako na šifrovanie.)

Úloha: Šifrou atbaš sme zašifrovali krátky text. Tu je výsledok: KLPOZW QV FPIBGB KLW HPZOLF. Viete zistiť znenie zašifrovanej správy? (Pomôcka: Použitá je anglická 26-znaková abeceda – tá, ktorú nájdete na klávesnici.)

Asi najznámejšou z týchto jednoduchých šifier je **Cézarova šifra**, ktorú používal Gaius Július Cézar v správach posielaných svojim vojvodcom: každé písmeno správy posunul v abecede o tri miesta. (Samotný Cézar aj jeho nasledovníci občas používali aj iné posuny ako o tri, v súčasnosti sa preto pojem „Cézarova šifra“ bežne používa aj v prenesenom význame na označenie ľubovoľného posunu abecedy.) V časoch antického Grécka sa prvýkrát objavuje použitie mechanickej šifrovacej pomôcky: Išlo o drevený kolík, v gréčtine nazývaný **skytalé** (pozri obr.). Na ten sa navinul prúžok pergamenu a po riadkoch sa naň napísala správa. Po rozvinutí zostala na pergamene nezmyselná postupnosť písmen. Príjemca potom zobral rovnako hrubý kolík a znova naň pergamen navinul, čím sa písmená správy správne zarovnali do riadkov

Spolu s rozvojom rôznych metód šifrovania samozrejme prichádza aj k snahe nepovolaných osôb šifrovaný text rozlúštiť. Výsledkom týchto snáh je dnes vedná oblasť nazývaná **kryptoanalýza**. Jednou

z prvých písomných zmienok je text z deviateho storočia nášho letopočtu, ktorého autorom bol Al-Kindí. V tomto texte popisuje viacero metód lúštenia šifrových textov. Okrem iného ide o prvú písomnú zmienku o metóde nazývanej frekvenčná analýza: Útočník (teda nepriateľ, ktorý odchytil zašifrovanú správu a snaží sa ju dešifrovať) si spočíta, ktoré znaky sa v správe ako často vyskytujú, a potom pri lúštení použije predpoklad, že často sa vyskytujúce znaky zodpovedajú najbežnejším písmenám.

Úloha: Našli ste papierik s textom VCVQ URTCXC UC FC NCJMQ QFUKHTQXCV. Ide o šifru podobnú Cézarovej, ale odosielateľ použil iný posun v abecede, nie o tri znaky. Viete určiť, aký posun si zvolil, a tento text rozšifrovať? (Opäť je použitá 26-písmenová abeceda z klávesnice. Zašifrovaný text je v slovenčine. Napovieme, že najčastejšie písmeno v slovenskom texte je A. Aké je najčastejšie písmeno v šifrovom texte? A aký posun by tomu zodpovedal?)

Zjavným vylepšením Cézarovej šifry je všeobecná substitučná šifra: každé písmeno bolo konzistentne nahradené iným symbolom, napríklad namiesto A srdiečko, namiesto B trojuholník, a tak ďalej. Samozrejme, nové symboly mohli byť opäť písmená, len v inom poradí – autor správy mohol namiesto každého A písať C, namiesto každého B písať W, namiesto každého C písať Q atď. Substitučná šifra sa dá ľahko rozlúštiť práve použitím frekvenčnej analýzy. Kvôli svojej jednoduchosti sú však substitučné šifry obľúbené dodnes, často sa používajú napríklad pri rôznych hrách. Stretneme sa s nimi aj v krásnej literatúre, napríklad v poviedke Zlatý chrobák od Edgara Allana Poea (1843) a v poviedke Tancujúce figúrky od Sira Arthura Conana Doyla (1903).

V šestnástom storočí už prichádzajú k slovu aj iné metódy šifrovania. Giovanni Battista Bellaso v roku 1553 prvýkrát popisuje šifru používajúcu periodické heslo. V neskorších rokoch sa objav tejto šifry omylom pripíše inému kryptografovi: Blaisovi Vigenèrovi, podľa neho je dnes táto šifra známa ako **Vigenèrova šifr**a. Princíp je opäť veľmi jednoduchý – dostatočne jednoduchý na to, aby sa šifrovať dalo len pomocou pera a papiera. Odosielateľ a adresát sa dohodnú na spoločnom hesle, napríklad „JAHODA“. Toto heslo, presnejšie spoločnú tajnú informáciu zdieľanú odosielateľom a adresátom, v kryptografii označujeme tiež pojmom kľúč. Šifrovanie teraz prebehne nasledovne: Odosielateľ si napíše text, ktorý chce poslať. Pod každé jeho písmeno napíše jedno písmeno hesla. Celé to teda môže vyzerať napríklad nasledovne:

STRETNEME SA O POLNOCI

JAHODAJAH OD A JAHODAJ

V každom stĺpci teraz máme dve písmená. Tieto „sčítame“ (ako keby to boli čísla, teda napríklad v anglickej abecede by mohlo byť A=1, B=2, ..., Z=26), a tým dostaneme jedno písmeno šifrového textu.

Príklad: S=19, J=10, teda S+J=19+10=29. Keďţe 26=Z, 27 je opäť A, 28 je B a 29 je C. Dostávame teda, že vo vyššie uvedenom príklade by prvým písmenom šifrového textu bolo C. Ďalej dostávame T+A=20+1=21=U, R+H=18+8=26=Z, E+O=5+15=20=T, atď. Výsledný šifrový text: CUZTXOONM HE P ZPTCSDS. Všimnite si, že na rozdiel od substitučnej šifry sa tu môže stať, že rôzne písmená otvoreného textu sa zašifrujú na rovnaké písmená. Pekne to vidieť na dvoch po sebe idúcich O v prvom slove šifrového textu.

Úloha: Heslom PES sme zašifrovali jedno slovenské slovo. Dostali sme takto šifrový text HJOEQNSNT. Viete ho dešifrovať?

Vigenerova šifra pôsobila natoľko neprelomiteľne, že si vyslúžila pomenovanie nevylúštiteľná šifra. Opak je však pravdou, jej rozlúštenie je len o trošku ťažšie ako rozlúštenie Cezarovej šifry. Napriek

tomu je efektívny postup jej lúštenia prvýkrát verejne publikovaný až v roku 1863, teda vyše tristo rokov po jej objave.

Steganografia

Jednou samostatnou oblasťou kryptológie je steganografia, veda o tom, ako informácie ukrývať. Oproti klasickému šifrovaniu je tu jeden veľmi podstatný rozdiel: Pri posielaní šifrovanej správy je nepriateľovi jasné, že autor a adresát spolu komunikujú, nevie však zistiť obsah tejto komunikácie. Pri steganografii je hlavným cieľom utajiť, že k akejkoľvek komunikácii došlo. Ľudovo môžeme povedať, že sa snažíme prenášané informácie ukryť na miesto, kde by ich nik nehľadal. Prvé pokusy ukrývania správ, ktoré môžeme zahrnúť do oblasti steganografie, sa datujú do antických dôb, napríklad sa dochovali prípady, kedy odosielateľ napísal text na drevenú dosku, tú potom pokryl voskom (čím správu ukryl) a do vosku napísal inú, nevinnú správu. Do steganografie tiež patria napríklad rôzne „neviditeľné“ atramenty, či vtipné triky typu „do obálky vložím falošný list, skutočnú správu napíšem na obálku a prelepím ju známkou“. Asi prvú steganografickú metódu fungujúcu čisto v textovej podobe vymýšľa začiatkom 17. storočia Francis Bacon. Spočíva v tom, že autor použil dva rôzne atribúty písma (napríklad v tlačenej podobe mohlo ísť o dva rôzne rezy písma). Do textu sa potom tajná správa ukryje tak, že každá pätica znakov otvoreného textu kóduje jeden znak textu ukrytého systémom podobným dvojkovej sústave. Aj v súčasnosti má steganografia mnoho praktických využití. Jedným z nich je boj s cenzúrou. Vo viacerých krajinách je preto stále nelegálne používať šifrovanie. Zatiaľ čo použitie šifry môže disidenta rovno dostať do väzenia, v prípade úspešného použitia steganografie je pred nepovolanými utajené, že vôbec nejaká komunikácia prebehla. Iným, menej dramatickým využitím, je podpisovanie elektronických diel (tzv. digitálna vodotlač), ktorá autorovi umožní dokázať, že práve on je autorom dotyčného diela.

Moderná kryptografia a bezpečnosť šifier

Hľadanie absolútne bezpečnej šifry Ako sme sa dozvedeli v našom stručnom prehľade histórie šifrovania, základný princíp šifrovania bol spočiatku v tom, že tajomstvom bola samotná metóda, ktorou sa z otvoreného textu stával šifrový text. Dnes by sme povedali, že nutnou požiadavkou na bezpečnosť šifry bolo utajenie samotného šifrovacieho algoritmu. Takéto šifrovanie však malo obrovskú nevýhodu: len čo sa tento algoritmus prezradil, šifra sa okamžite stala úplne nepoužiteľnou. A prax ukázala, že každý algoritmus sa skôr či neskôr prezradí. Už v Cézarovom prípade sa to stalo, a to pravdepodobne vtedy, keď sa Cicero pridal k jeho odporcom.

V renesančnej Európe potom prišlo k významnému posunu v prístupe k šifrovaniu: oddelil sa od seba šifrovací algoritmus, ktorý bol často krát známy mnohým ľuďom, a kľúč – tajná informácia, ktorú zdieľali len odosielateľ a adresát, a ktorá mala len tomu správnemu adresátovi umožniť prečítanie zašifrovanej správy.

V roku 1917 si Gilbert Vernam dal patentovať vynález, ktorý ku ďalekopisu pripojil vopred pripravený kľúč na diernej páske. Potom vždy, keď odosielateľ zadal písmeno správy, prečítal ďalekopis ďalšie písmeno kľúča a z nich pomocou vhodnej jednoduchej operácie vypočítal zašifrované písmeno, ktoré potom odoslal.

Uvedieme jeden príklad, ako sa v súčasnosti môže používať Vernamova šifra. Pri návšteve rodnej krajiny sa veľvyslanec zastaví na ministerstve zahraničných vecí. Tam im počítačový program vygeneruje niekoľko gigabajtov (pseudo)náhodných znakov. Túto postupnosť napália na dve DVD. Jedno z týchto dvoch identických DVD zostane zatvorené v trezore na ministerstve, druhé si veľvyslanec zoberie so sebou do sveta. A následne vždy, keď potrebujú spolu bezpečne komunikovať, zoberie odosielateľ z DVD toľko znakov, ako dlhú správu posiela, a použije ich ako kľúč na jej

zašifrovanie. Kým sú obe DVD bezpečne utajené pred svetom, majú komunikujúce strany úplnú istotu, že nik nepovolaný ich šifrovanú komunikáciu nedokáže rozlúštiť.

Princíp asymetrického šifrovania

Ďalší zlomový okamih kryptografie prišiel v roku 1976, kedy Diffie a Hellmann prišli s prevratným nápadom: asymetrickým šifrovaním. Tento ich nápad totiž riešil problém, ktorým dovtedy trpeli úplne všetky šifrovacie systémy: potrebu vopred sa stretnúť. Staré šifrovacie systémy boli založené na myšlienke, že sa odosielateľ a adresát vopred dohodnú na šifrovacom systéme. V neskorších rokoch mohol síce byť šifrovací systém verejne známy, ale aj tak sa odosielateľ a adresát potrebovali vopred dohodnúť na kľúči, ktorý nik iný nepoznal. Čo však, ak sa ocitnem v situácii, keď zrazu potrebujem niekomu novému poslať utajenú správu? Spoločný kľúč dohodnutý, samozrejme, nemáme a dohodnúť sa na nejakom nemáme možnosť. Čo v takejto situácii? (Uvedomte si, že by sme sa mohli stretnúť, či inak si dohodnúť kľúč, tak by som mu rovno mohol oznámiť tú správu, a nepotrebovali by sme sa dohadovať.)

Jedno možné riešenie tejto zdanlivo neriešiteľnej situácie si môžeme priblížiť vtipnou logickou úlohou: Známy archeológ Indiana Jones našiel prastarú truhlicu plnú artefaktov. Chcel by ju poslať svojmu otcovi do Anglicka. Ako to však spraviť? Ak ju pošle nezamknutú, po ceste ju určite niekto vykradne. Ale ak ju pošle poriadne zamknutú, nedostane sa k jej obsahu ani jeho otec. Mohol by samozrejme poslať zamknutú truhlicu a nejakou inou cestou aj kľúč od nej, čo ak ho však niekto sledoval a odchytí na pošte aj truhlicu, aj kľúč? Indiana Jones vymyslel nasledovné riešenie: Kúpi si poriadny zámok a zamkne truhlicu. Kľúč si nechá, truhlicu pošle svojmu otcovi. Ten ju síce nevie otvoriť, vie však spraviť niečo iné: aj on si kúpi zámok a tiež ním truhlicu zamkne. (Pozri obrázok nižšie.) Dvakrát zamknutú truhlicu, teda stále bezpečne zatvorenú, odošle späť svojmu synovi. Keď Indiana Jones dostane truhlicu späť, zoberie svoj kľúč, odomkne svoj zámok a odstráni ho z truhlice. Zostane mu truhlica, ktorá je naďalej zamknutá – teraz už však len zámkom jeho otca. Truhlicu teraz Indiana Jones opäť pošle svojmu otcovi. No a keď ju ten dostane, odomkne svoj zámok a má pred sebou otvorenú truhlicu plnú artefaktov.

Príklad s truhlicou nám teda ukazuje jeden veľmi dôležitý poznatok: v niektorých situáciách môže existovať spôsob bezpečnej komunikácie, ktorý nebude potrebovať žiadne vopred zdieľané spoločné tajomstvo! A práve takéto úvahy umožnili neskôr objav asymetrickej kryptografie.

Šifra RSA

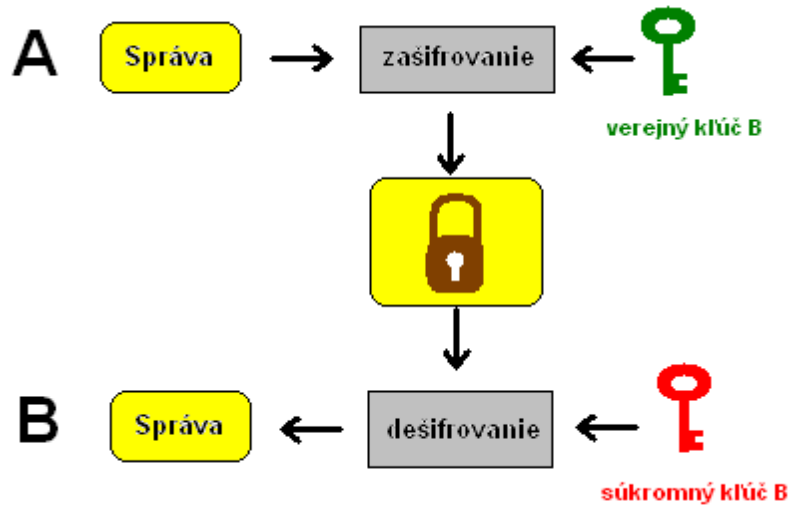
Už rok po Diffieho a Hellmannovom nápade, v roku 1978, prišli Rivest, Shamir a Adleman s prakticky použiteľnou realizáciou takejto šifry. Šifra RSA (nazvaná podľa prvých písmen ich priezvisk) sa v praxi používa odvtedy až dodnes. Táto šifra je založená na veľmi jednoduchom pozorovaní. Viete vypočítať, koľko je 479-krát 521? Určite. S kusom papiera a perom túto úlohu zvládne za minútu aj bežný základoškolák. No viete povedať, aké dve prvočísla treba vynásobiť, aby sme dostali výsledok 252 179? Asi by trvalo dosť dlho, kým by ste sa prepracovalik odpovedi – ak by ste ju vôbec v rozumnom čase našli.

Každý človek, ktorý chce prijímať správy šifrované pomocou RSA, si musí vygenerovať svoj kľúč. Toto spraví tak, že si zvolí dve prvočísla a . (V praxi majú tieto prvočísla medzi sto a tisíc cifier. A, samozrejme, človek ručne nerobí nič, všetko sa udeje vnútri v počítači.) Tieto prvočísla si zapamätá,

on musí byť jediný, kto ich pozná. Hovoríme, že tieto prvočísla tvoria jeho súkromný kľúč. Ďalej vypočíta ich súčin a ten zverejní. Tejto hodnote hovoríme verejný kľúč.

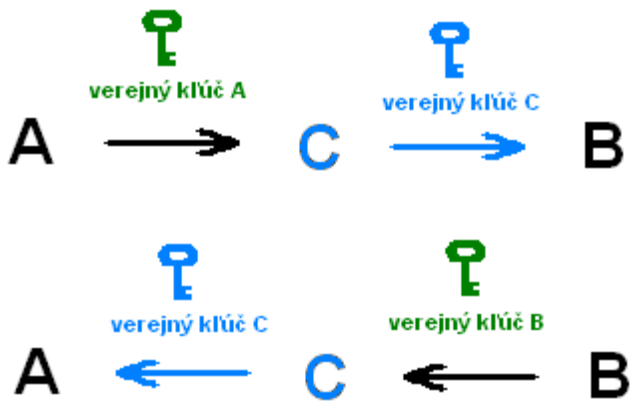
Verejný kľúč, ako už naznačuje jeho názov, môže poznať každý. Existujú dokonca stránky, ktoré slúžia ako „telefónny zoznam“: podľa e-mailovej adresy adresáta tam nájdete jeho verejný kľúč. (Presnejšie, vhodný program ho tam nájde za vás.) Prínos Rivesta, Shamira a Adlemana bol v tom, že vymysleli algoritmy na šifrovanie a dešifrovanie, ktoré majú nasledovnú dôležitú vlastnosť: Na šifrovanie stačí poznať verejný kľúč, na dešifrovanie je nutné poznať súkromný kľúč. Dôležité je uvedomiť si, že zverejnenie verejného kľúča nijak neohrozuje bezpečnosť šifry. Ak nepriateľ pozná verejný kľúč, nemá ako zistiť z neho súkromný kľúč: číslo n je totiž také obrovské, že na nájdenie p a q by aj najlepší známy program potreboval miliardy rokov.

Pokiaľ používateľ A chce odoslať používateľovi B zašifrovanú správu, použije na zašifrovanie verejný kľúč používateľa B. Takto zašifrovanú správu odošle používateľovi B. Používateľ B potom k dešifrovaniu správy použije svoj súkromný kľúč. Neoprávnenej osobe k dešifrovaniu správy nestačí znalosť verejného kľúča, algoritmu a ani prenášanej zakódovanej správy, pretože jej chýba súkromný kľúč.

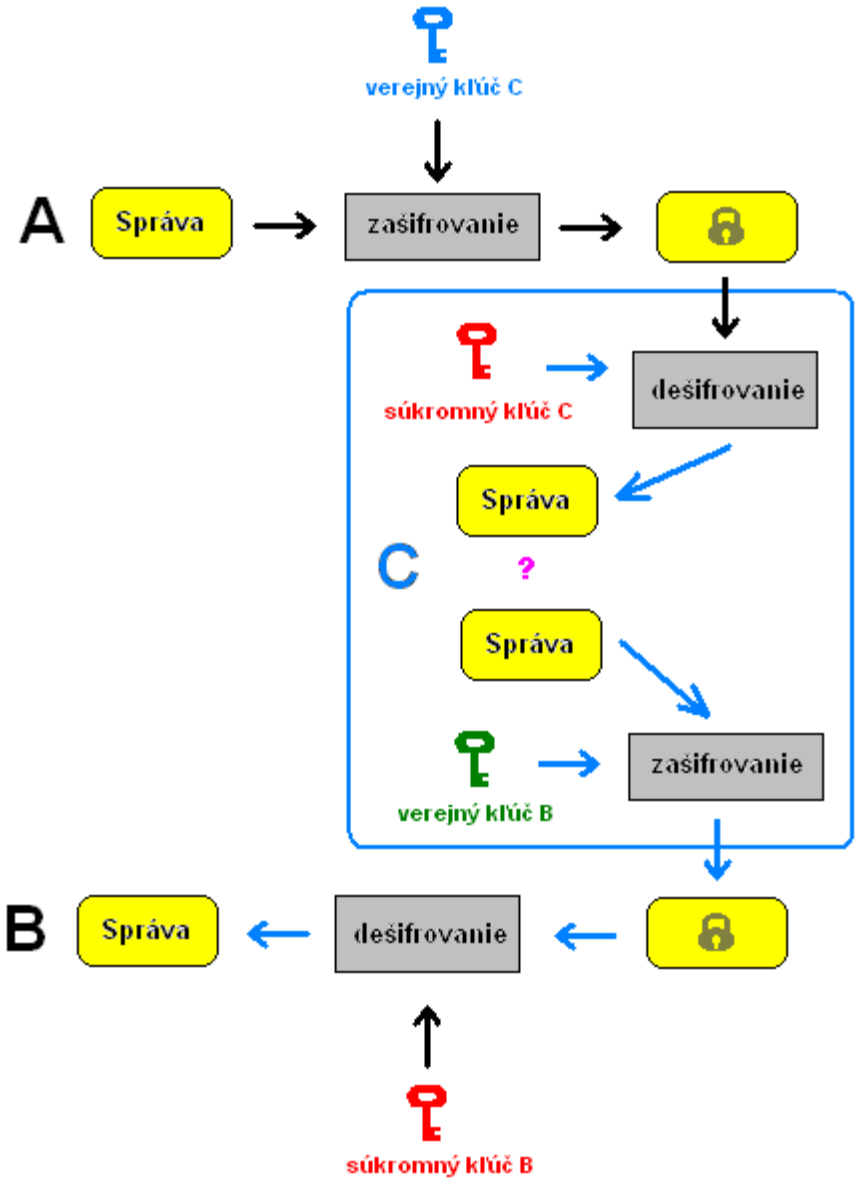


Digitálny certifikát a certifikačná autorita

Samotné šifrovanie z predchádzajúcej kapitoly síce ochráni komunikáciu pred odpočúvaním, ale bez overenia autentickosti verejných kľúčov sa komunikujúce strany môžu stať obeťou tzv. útoku **Man in the middle** (z angličtiny *človek uprostred*). Podstatou tohto útoku je snaha útočníka odpočúvať komunikáciu tak, že sa stane jej aktívnym prostredníkom. Pri počiatočnej vzájomnej výmene verejných kľúčov získa verejné kľúče účastníkov odpočúvanej komunikácie a podsunie im namiesto nich svoj verejný kľúč:



Následnú šifrovanú komunikáciu preposiela cez seba ako sprostredkovateľ, pričom pôvodnú správu dokáže nielen prečítať, ale môže túto správu aj pozmeniť:



Predstavme si napríklad, že Alica má v elektronickej forme vyplnené daňové priznanie. Chcela by ho podpísať, a tak potvrdiť údaje v ňom uvedené. Ako to spraví? Tak, že zoberie dotyčný súbor a odšifruje ho pomocou svojho súkromného kľúča. Výsledkom tejto operácie je reťazec predstavujúci jej podpis. Ten Alica pripojí k samotnému dokumentu. Keď chce Karol overiť pravosť tohto podpisu, môže zobrať Alicin verejný kľúč, pomocou neho zašifrovať jej podpis a overiť, že sa výsledok rovná pôvodnému dokumentu.

Prečo to celé funguje? Pretože Karol vie, že Alica je jediná, kto vie pomocou jej kľúča aj dešifrovať – a teda dotyčný podpis musela vyrobiť ona, nik iný na to nemá dostatok informácií.

Ak by Alica teraz chcela takto podpísané daňové priznanie z pohodlia svojho domova podať, nefungovalo by to. Chýba totiž jeden dôležitý článok: prepojenie medzi verejným kľúčom (súborom získateľným kdesi na internete) a Alicou ako fyzickou osobou. Štát nemá prečo len tak uveriť, že Alicin verejný kľúč je zrovnal tento a nie jeden zo sta iných.

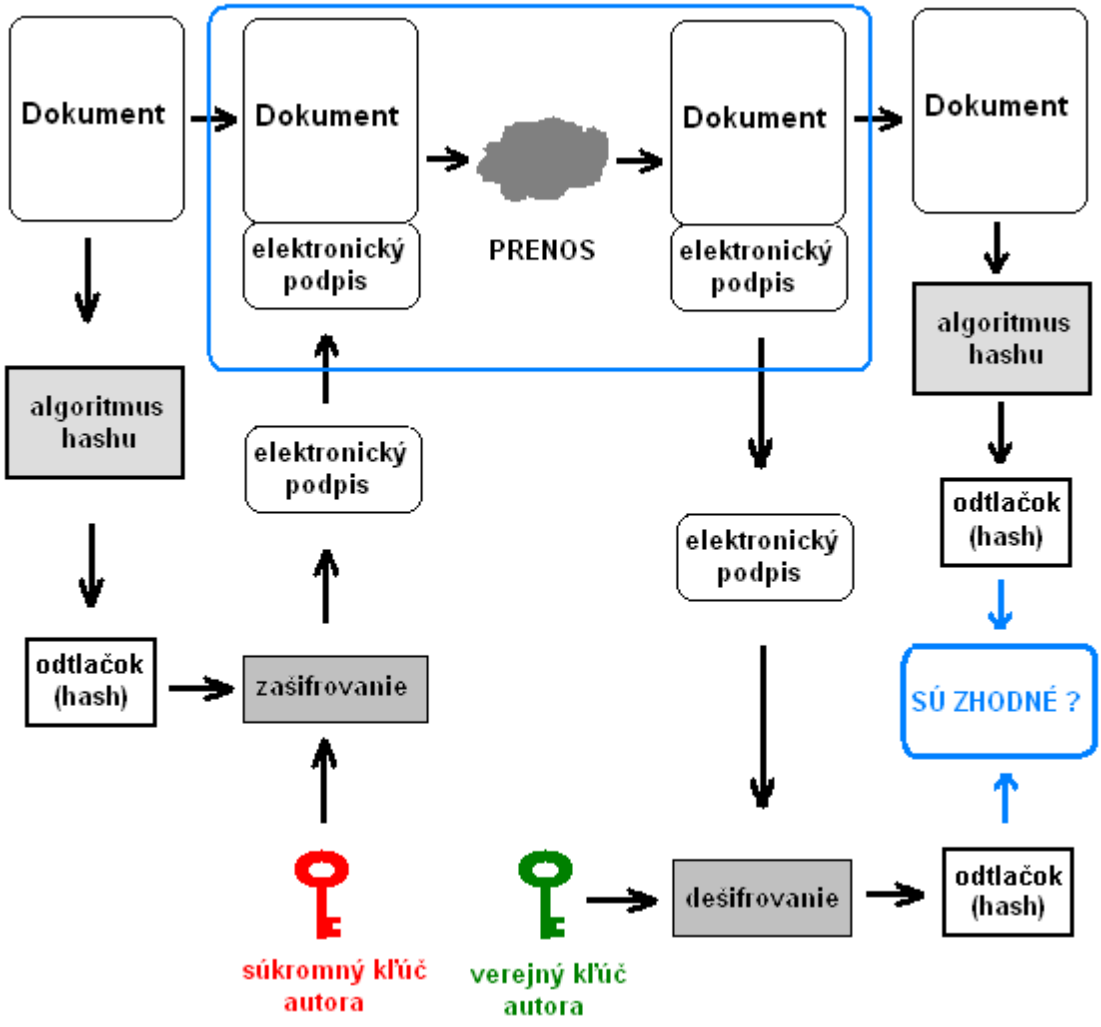
Aj na toto sa však myslelo. U nás na Slovensku túto problematiku rieši Zákon 215/2002 Z.z. o elektronickom podpise. Tento definuje tzv. **zaručený elektronický podpis**, ktorý má, zjednodušene povedané, rovnakú právnu váhu ako fyzický podpis na klasickom dokumente. Ako vieme takýto podpis vyrobiť? Chýbajúci medzičlánok – záruku korešpondencie medzi verejným kľúčom a fyzickou

osobou – zabezpečujú inštitúcie nazývané **akreditované certifikačné autority**. Celý proces si môžeme jednoducho popísať nasledovne:

Alica zoberie svoj občiansky preukaz a navštívi niektorú akreditovanú certifikačnú autoritu (CA).(V zmysle zákona kvalifikovaný certifikát, ktorý je potrebný pre zaručený elektronický podpis, môže vydať iba certifikačná autorita akreditovaná NBÚ (Národný bezpečnostný úrad). Aktuálny zoznam akreditovaných certifikačných autorít pre zaručený elektronický podpis nájdeme na stránkach NBÚ (www.nbusr.sk).)

- Pracovník CA si overí jej totožnosť a následne jej vygeneruje súkromný a verejný kľúč.
- Ku kľúču jej navyše vydá certifikát, teda potvrdenie, že ide naozaj o Alicin kľúč. (Tento certifikát je vlastne elektronický dokument obsahujúci potrebné údaje a podpísaný kľúčom dotyčnej certifikačnej autority.)
- Od tejto chvíle vie Alica vyrábať zaručených elektronických podpisov, koľko len chce. Ku podpísanému dokumentu následne priloží aj certifikát, ktorý príjemcovi umožní overiť totožnosť odosielateľa.

Elektronický podpis funguje nasledujúcim spôsobom: z obsahu dokumentu sa vytvorí tzv. odtlačok (hash) – krátky (typicky niekoľko stoviek bitov) výťah vytvorený pomocou špecializovaných algoritmov (hašovacie funkcie) a takto získaný odtlačok sa následne zašifruje súkromným kľúčom autora. Zašifrovaný odtlačok predstavuje elektronický podpis, ktorý sa k podpisovanému dokumentu priloží. Pri overovaní podpisu sa z dokumentu opäť vytvorí rovnakým algoritmom nový odtlačok a z priloženého elektronického podpisu sa pomocou verejného kľúča autora dešifruje pôvodný odtlačok dokumentu. Novozískaný odtlačok sa porovná s dešifrovaným odtlačkom, a ak sú identické, tak sa týmto zaručila integrita podpísaného dokumentu. Úspešným dešifrovaním elektronického podpisu konkrétnym verejným kľúčom je jednoznačne určený autor podpisu.

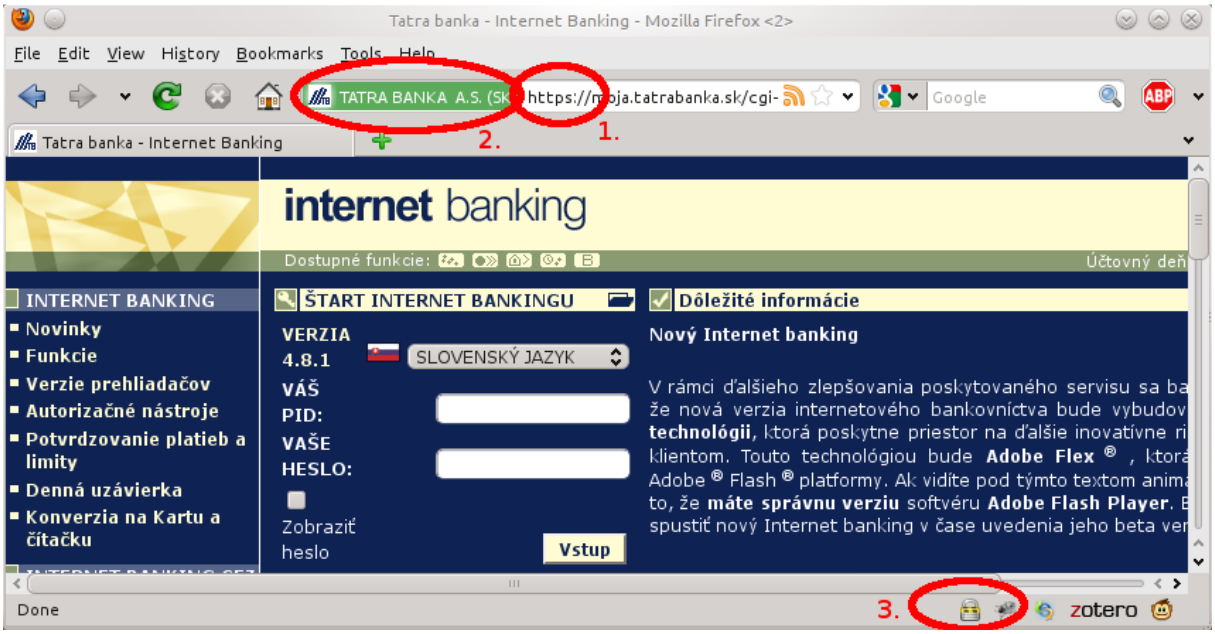


Je dôležité, aby súkromný kľúč ostal vždy súkromným, teda utajeným. V prípade straty alebo odcudzenia súkromného kľúča je dôležité okamžite zrušiť certifikát k príslušnému verejnému kľúču (predčasne ukončiť jeho platnosť). Certifikát na požiadanie vydáva, obnovuje a taktiež zneplatňuje certifikačná autorita. Vydaný certifikát k verejnému kľúču má definovanú dobu platnosti, zvyčajne jeden rok.

Praktické aplikácie kryptografie

Máloktorý používateľ počítača si uvedomuje, že keď si prezeráte webstránky, skoro všetky údaje posielané medzi vaším počítačom a servermi sa prenášajú (pomocou protokolu HTTP) v nešifrovanej podobe. Hocikto teda môže túto komunikáciu odpočúvať. Sú však situácie, kedy toto nechceme: napríklad také čítanie súkromnej elektronickej pošty, alebo platenie pomocou kreditnej karty. Na tieto účely bol vymyslený protokol HTTPS („S“ ako „secure“, presnejšie ide o kombináciu protokolov HTTP a SSL/TLS). Pri tomto protokole komunikácia prebieha v zašifrovanej podobe. Dôveryhodné webstránky, ako napríklad internet banking vašej banky, vás pri návšteve zväčša automaticky presmerujú na HTTPS verziu prihlasovacej stránky. To, že na stránku pristupujete prostredníctvom šifrovanej komunikácie, spoznáte ľahko priamo v prehliadači. V prvom rade podľa protokolu uvedeného v URL adrese stránky: tá nebude začínať znakmi „http://“, ale znakmi „https://“. Väčšina prehliadačov tiež zobrazí ikonku zámku, ak je obsah prenášaný šifrovane.

Samotné zabezpečenie komunikácie však ešte nestačí – ako vieme, že tá webstránka skutočne patrí našej banke, a nie nejakému zlodejovi? Tu, podobne ako pri zaručených elektronických podpisoch, musia prísť k slovu certifikáty. Niekto dostatočne dôveryhodný (certifikačná autorita) vydal banke certifikát potvrdzujúci jej totožnosť. A práve týmto certifikátom sa webserver banky potom preukáže vášmu prehliadaču. Prehliadač si overí, že certifikát banky je podpísaný certifikačnou autoritou, ktorej dôveruje, a výsledkom je to, čo vidíme na obrázku označené číslom 2: v adrese sa objaví farebne zvýraznená informácia o tom, že bol úspešne overený certifikát stránky, a tiež to, kto je jeho vlastníkom. Ak teda všetko prebehlo ako sme očakávali, môžeme pokojne zadať naše prihlasovacie údaje – máme dostatočnú dôveru, že ich skutočne posielame našej banke.



Ak overenie certifikátu neprebehlo úspešne, prehliadač vás presmeruje na stránku podobnú tej na obrázku. Ak sa vám toto zrazu stane pri prihlasovaní sa na stránku, ktorá „dovtedy fungovala“, je veľmi pravdepodobné, že ste práve obeťou nejakého útoku. V takomto prípade rozhodne nič neodsúhlasujte a nikam nepíšte svoje heslo. Pokúste sa pripojiť ešte raz, ideálne tak, že priamo zadáte adresu do prehliadača. V prípade neúspechu kontaktujte správcu stránky (teda napríklad svoju banku). Niekedy sa môže stať, že takéto varovanie uvidíte aj na legitímnej stránke. Uznávanou certifikačnou autoritou podpísané certifikáty sú totiž drahé, a tak webstránky prevádzkované neziskovými inštitúciami často takéto certifikáty nemajú.

Aby fungovalo HTTPs spojenie na ne, vygenerujú si teda certifikát samy. To však vedie k varovaniu ukázanému na obrázku: prehliadač nás upozorňuje, že síce mu stránka ukázala certifikát, ale nepodarilo sa mu overiť jeho pravosť. Ak pristupujete na takúto webstránku, skontrolujte si, či jej certifikát obsahuje správne údaje.