Šifrovanie informácií

Určite ste sa stretli s problémom, keď potrebujete niekomu predať informáciu a zároveň chcete mať istotu, že nikto iný sa danú informáciu nedozvie. Keď komunikujete s dotyčným medzi "štyrmi" očami nie je problém túto informáciu bezpečne predať (odmyslime si skryté kamery a mikrofóny, prípadne iné "podlé" nástrahy). Problém nastane vtedy, keď komunikačný kanál medzi vami a prijímateľom informácie je verejne prístupný, nie je súkromný alebo utajený, je prítomných viac ľudí, komunikácia je odpočúvaná, využívame prostredníka (poštár, internet, ..), atď. Za takúto nezabezpečenú komunikáciu sa považuje aj komunikácia v internete. Posielanie emailu, odosielanie niektorých údajov cez internet môže byť veľmi jednoducho "odpočúvané".

Teraz prichádza úloha šifrovania - **kryptografie**.

Existuje niekoľko možností, ako zašifrovať správu tak, aby sme "narušiteľovi" čo najviac sťažili úlohu dešifrovania. Z praktického hľadiska môžeme hovoriť o nemožnosti dešifrovania správy. Inými slovami, dešifrovanie správy využitím moderných a rýchlych počítačov môže byť prakticky nerealizovateľné (môže trvať rádovo niekoľko 10^n rokov). Problém dešifrovania môžeme chápať aj ako problém nájdenia kľúča, pomocou ktorého sa správa zašifrovala.

Podľa toho, ako sa využíva **kľúč** (kľúče) hovoríme o kryptografii **symetrickej** a **asymetrickej** (rozdiel je v tom, koľko kľúčov a na čo používame).

Čo teda okrem utajenia obsahu komunikácie prináša kryptografia? Všade (no, všade asi nie) tam, kde od Vás vyžadovali vlastnoručný podpis a v podstate vašu fyzickú prítomnosť, budeme môcť použiť elektronický (digitálny) podpis.

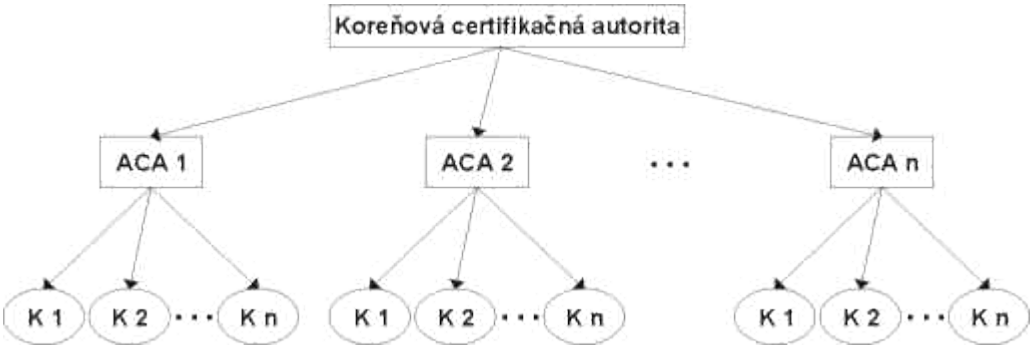
Keď sa vám dostane do rúk dokument podpísaný "klasickým" podpisom a vy nepoznáte podpis príslušnej osoby, len ťažko si overíte jeho pravosť. A aj keby sme dobre poznali podpis tejto osoby, overiť si ho je bežne dostupnými prostriedkami takmer nemožné.

Keď sa vám dostane do rúk dokument podpísaný elektronickým podpisom, v podstate každý, v ktoromkoľvek čase a na ktoromkoľvek mieste Zeme si môže overiť jeho platnosť, t. j. autenticitu dokumentu a identifikáciu autora resp. odosielateľa (ak má príslušné technické vybavenie, čo dnes nie je problém).

Samozrejme na to, aby sme mohli s úradmi, s lekárom, s právnikom alebo s obchodným partnerom týmto spôsobom komunikovať a aby táto komunikácia bola právne akceptovateľná (t. j., aby sme mohli váhu elektronického dokumentu postaviť na úroveň papierového) musíme mať podporu v legislatíve.

Podľa potreby a povahy dokumentu je možné voliť primeranú úroveň bezpečnosti. Tento stav je zakotvený aj v legislatíve, podľa ktorej je elektronický podpis akceptovaný aj v súdnom konaní. Je treba zdôrazniť, že dôkazová sila elektronického podpisu je závislá od jeho bezpečnostnej charakteristiky. Dôveryhodnosť elektronického podpisu je zabezpečovaná tzv. pyramídou dôvery, umožňujúcej spoľahlivé overenie odosielateľa dokumentu (PKI, Public Key Infrastructure). Na jej vrchole je koreňová certifikačná autorita, ktorú spravuje NBÚ.

Stred pyramídy je tvorený akreditovanými certifikačnými autoritami a základňa pyramídy je tvorená klientmi, vlastníkmi kvalifikovaných certifikátov.



Zákon o elektronickom podpise bol schválený 15. marca 2002 zákonom č. 215/2002. Okrem koreňovej certifikačnej autority do "hry" vstupuje ďalší subjekt, certifikačná autorita. Certifikačná autorita vystupuje v úlohe "notára", ktorý overuje elektronický podpis a garantuje komu patrí a dokedy platí. Akreditáciu na poskytovane týchto služieb (služieb certifikačnej autority) dáva koreňová certifikačná autorita, ktorú spravuje NBÚ (http://www.nbusr.sk).

Symetrická kryptografia

V symetrických šifrách používame jeden kľúč aj na šifrovanie aj na dešifrovanie správy. Tento kľúč je tajný a poznať ho majú len osoby, ktoré navzájom pomocou tejto šifry komunikujú. Správa, ktorá sa zašifruje tajným kľúčom sa dá dešifrovať opäť použitím toho istého tajného kľúča.

Medzi najjednoduchšie symetrické šifry patria zámeny písmen. Šípka smerom dole ukazuje smer šifrovania a šípka smerom hore ukazuje smer dešifrovania.

pôvodná správa:	tajna sprava	pôvodná správa:
smer šifrovania ↓	kľúč: a b c d e f g h i j k l m n o p q r s t u v w x y z w k l c x y z f g h i j a b o p q r s t u v d e m n	smer dešifrovania ↑
zašifrovaná správa	twhbwnsprwuw	zašifrovaná správa

Ďalšou možnosťou sú posuny v abecede. Predpokladajme, že budeme posúvať abecedu o štyri znaky (mimochodom toto je šifra, ktorú používal aj Julius Caesar).

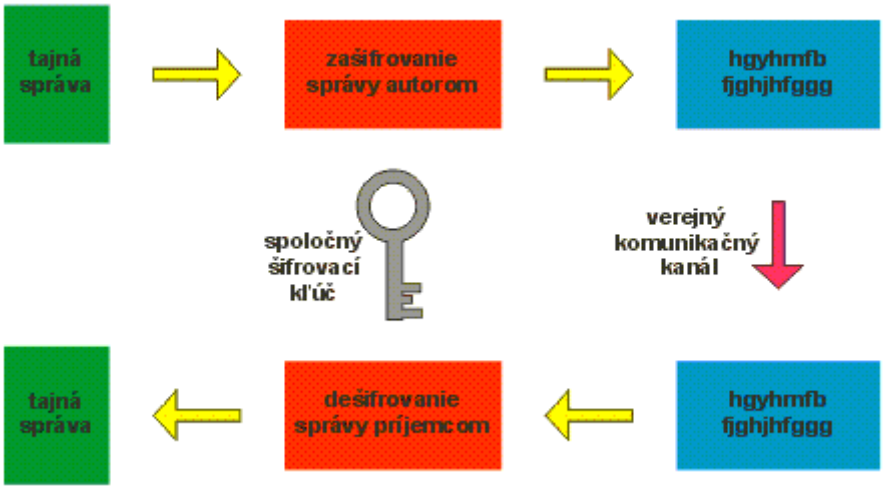
pôvodná správa:	tajna sprava	pôvodná správa:
smer šifrovania ↓	kľúč: posuň písmená v abecede o 4 znaky	↑ smer dešifrovania
zašifrovaná správa	xenredwtveze	zašifrovaná správa

V predchádzajúcich prípadoch sa šifra dá "jednoducho" prelomiť. Keďže meníme písmeno za písmeno, stačí ak poznáme relatívne početnosti (zoberieme reprezentatívnu vzorku jazyka a zistíme koľko percent všetkých znakov tvorí písmeno "a", koľko "b" atď.) výskytov jednotlivých znakov v danom jazyku.
Posuny v abecede teda môžeme prepracovať a vyrobiť "tvrdšiu" šifru. Jednotlivé písmená budeme posúvať vždy o iný počet znakov. Napr.: "1|3|2" znamená toto. Vstupnú správu rozdelíme na trojice písmen. Prvé písmeno v trojici posunieme o 1, druhé o 3 a tretie písmeno o 2. Prelomiť takúto šifru môže byť riadne tvrdý oriešok. Navyše jej sila rastie so zložitosťou kľúča.

pôvodná správa:	tajna sprava taj | na | spr | ava	pôvodná správa:
smer šifrovania ↓	kľúč: posuň podľa 1|3|2	↑ smer dešifrovania
zašifrovaná správa	udl | odb | tst | byc udlodbtstbyc	zašifrovaná správa

Uvedené šifry majú jednu nevýhodu. Ak poznáme pôvodnú správu a šifrovanú verziu tej istej správy, vieme si vyrobiť kľúč. Postup je totiž v princípe známy.
To sa dá spraviť napr. takto: Alica a Boris komunikujú a používajú niektorú z vyššie uvedených šifier. Cyril, ktorý chce ich vzájomnú komunikáciu odpočúvať, dá Borisovi správu a požiada ho, aby ju poslal Alici použitím tajného kľúča. Boris tak spraví. Cyril odchytí zašifrovanú správu, takže má aj originál aj šifrovanú správu. No a môže začať pracovať na prelomení šifry.
Ak chcete poznať aj ďalšie šifry, pozrite si "Šifrovanie pre deti".
V skutočnosti existujú šifry, ktoré používajú omnoho komplikovanejšie postupy. Napríklad pri dĺžke kľúča 128 b (znakov) môže dešifrovanie trvať až 10^{39} rokov!!

Princíp symetrickej šifry je nasledovný:



Výhody	Nevýhody
• šifrovanie a dešifrovanie je veľmi rýchle • používajú sa na šifrovanie dát, ktoré sa nikam neposielajú, aby si ich nemohol nikto prečítať (dáta na disku, súbory, ..)	• problém je oboznámiť druhú stranu s šifrovacím kľúčom tak, aby sa o ňom nikto iný nedozvedel • počet kľúčov: ak by napr. 500 zamestnancov jednej firmy chcelo komunikovať medzi sebou, a každá dvojica by mala svoj tajný kľúč, potrebovali by 124750 kľúčov

Asymetrická kryptografia

Asymetrická kryptografia predstavuje iný spôsob šifrovania. Rozdiel spočíva v tom, že každý účastník má šifrovacie kľúče dva, súkromný a verejný. Oba kľúče vytvárajú dvojicu.

Súkromný kľúč sa používa (majiteľom) na dešifrovanie došlých správ a podpisovanie odosielaných správ. Verejný kľúč sa používa (ostatnými) na šifrovanie odosielaných správ a overenie autentičnosti (podpisu) došlých správ.

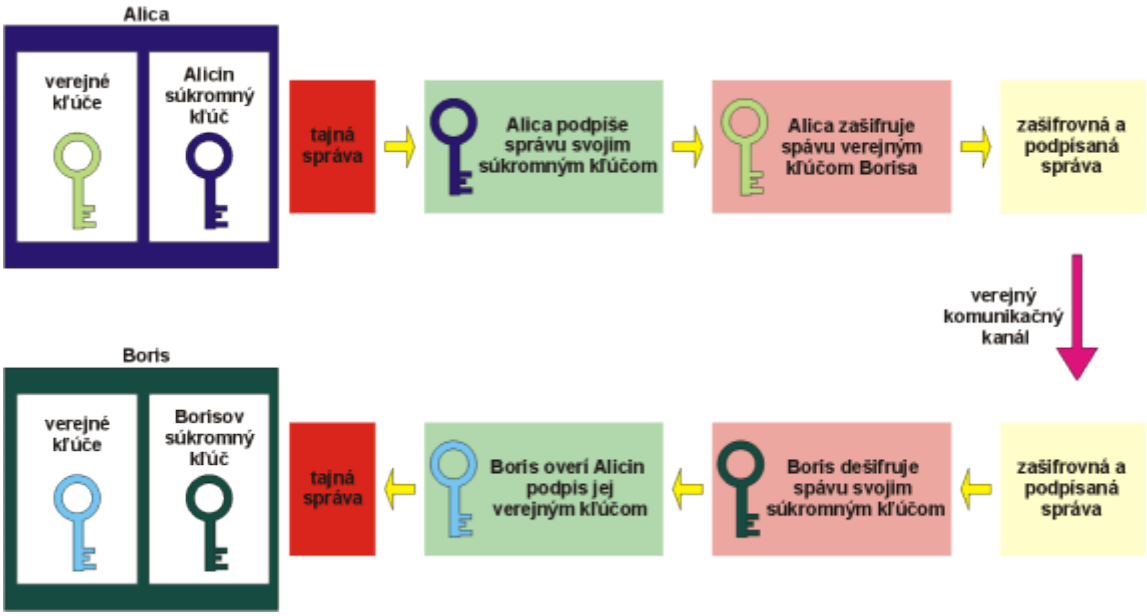
Podpisovanie správy prebieha nasledovne. Z textu odosielanej správy sa pomocou špeciálnej funkcie (nazýva sa hašovacia) vytvorí otlačok správy. Je to reťazec znakov pevnej dĺžky. Pri zmene čo i len jedného znaku v našej správe dostaneme úplne iný otlačok správy. Otlačok môžeme chápať aj ako kontrolný súčet správy, takže ak sa správa cestou niekde zmení, príjemca to okamžite zistí. Je prakticky nemožné vyrobiť správu k existujúcemu otlačku, alebo zmeniť správu tak, aby otlačok vyhovoval. Tento reťazec sa potom pomocou súkromného kľúča podpíše (zašifruje) a pripojí na koniec odosielanej správy (systémy používajúce asymetrické šifrovanie celý proces robia automaticky, takže prax je "omnoho jednoduchšia" ako teória). Aby si správu nikto (teda okrem príjemcu) nemohol prečítať, veko možeme zašifrovať verejným kľúčom príjemcu.

Schematicky môžeme takúto šifrovanú komunikáciu popísať nasledovne. Dvaja účastníci asymetricky šifrovanej komunikácie sú Alica a Boris. Každý z nich má svoju dvojicu kľúčov, svoj súkromný a svoj verejný kľúč. Súkromný kľúč si každý pozorne stráži aby sa k nemu nedostal nikto iný, naopak verejný kľúč sa zverejní tak, aby sa k nemu mohlo dostať čo najviac ľudí.

Takže ak chcú spolu komunikovať, musia si navzájom vymeniť svoje verejné kľúče.

	súkromný	verejný
Alica		
Boris		

Samotná komunikácia vyzerá nasledovne:



Správu nemusíme šifrovať aj podpisovať súčasne. Potom to vyzerá nasledovne:

Alica poslala čistú správu	=> Boris nemá istotu, že správu poslala Alica a navyše si ju cestou mohol niekto iný prečítať alebo zmeniť (takto sa bežne komunikuje emailom)
Alica správu podpísala svojim súkromným kľúčom	=> Boris má istotu, že správu poslala Alica, ale cestou si mohol správu niekto iný prečítať
Alica zašifrovala správu Borisovým verejným kľúčom	=> Správu môže dešifrovať len Boris, ale nemá istotu, že správu poslala Alica
Alica zašifrovala správu Borisovým verejným kľúčom a podpísala ju svojim súkromným kľúčom	=> Správu môže dešifrovať len Boris a navyše má istotu, že správu poslala Alica

Na záver ..

Asymetrické šifrovanie má aj svoje nevýhody. Je niekoľkonásobne pomalšie ako symetrické (čo v prípade šifrovania emailov nie je tragické). Ďalej si musíme byť 100% (slovom sto percentne) istý pravosťou verejných kľúčov našich "priateľov". Čo ak niekto na verejné miesto podstrčil falošný verejný kľúč a správy zašifrované týmto kľúčom "odchytí", dešifruje, prečíta, zašifruje pravým verejným kľúčom príjemcu a pošle na jeho adresu? Ale to nám môže zaručiť certifikačná autorita.

Malý slovník pojmov:

asymetrická kryptografia	Public Key Cryptography	spôsob šifrovania, kde sa na šifrovanie používa verejný kľúč a na dešifrovanie súkromný kľúč
certifikačná autorita	Certificate Authority, CA	• dôveryhodná autorita, ktorá generuje certifikáty a zoznamy zrušených certifikátov (komponent infraštruktúry PKI) • jedna alebo viac dôveryhodných individualít, ktoré sú oprávnené potvrdzovať pravosť kľúča
dešifrovať	Decrypt	prevádzať zašifrované dáta do pôvodného tvaru
digitálny (elektronický) podpis	Digital Signature	• menšie množstvo dát automaticky pripojených k správe na základe ktorých sa dá overiť totožnosť autora • Jedinečná digitálna identifikácia entity, ktorá sa využíva na autentifikáciu zdroja, integrity dát a nepopierateľnosť. Digitálny podpis využíva súkromný kľúč, ktorému zodpovedá príslušný verejný kľúč, matematickú funkciu známu ako „message digest“ a princípy asymetrickej kryptografie.
doba platnosti	Expired	doba (dátum) po ktorej sa stane kľúč neplatný
kľúč (šifrovací, dešifrovací)	Key (Encrypt, Decrypt)	číslo, ktoré je použité ako základ pre šifrovanie postup šifrovania, dešifrovania súbor pravidiel v rámci daného šifrovacieho systému nutný k zašifrovaniu (dešifrovaniu) danej správy
kryptografia	Cryptography	obor zaoberajúci sa kódovaním/šifrovaním dát (zakódovaním/šifrovaním aj rozkódovaním/dešifrovaním)
otlačok prsta	Fingerprint	• kontrolný súčet obsahu kľúča

		• tzv. hash verejného kľúča. Hash je matematická funkcia, ktorá vytvára „skratku“ dát (message digest). Z dát rôznej veľkosti vytvorí skrátenú správu fixnej veľkosti. Zo správy nie je možné spätne získať pôvodné dáta. Akákoľvek zmena vstupných dát sa preukáže tým, že sa vytvorí iný message digest.
otlačok správy	Message Digest	postupnosť znakov pevnej dĺžky, je výsledkom hašovacej funkcie, ktorej argumentom je správa
overiť	Verify	proces overenie správnosti vykonanej činnosti (podpisu),
pár kľúčov	Keypair	dvojica kľúčov, jeden je verejný a druhý súkromný
PGP veľmi dobré súkromie	PGP	Pretty Good Privacy nástroj na kvalitné šifrovanie emailov, súborov a sieťovej komunikácie
registračná autorita	RA	Komponent infraštruktúry PKI, používaný na posúvanie schválených žiadostí o vydanie certifikátu do CA.
samorozšifrovateľný	SDA Self-Decrypting Archives	zašifrované dáta ktoré možno dešifrovať bez použitia externého dešifrovacieho programu
súkromný kľúč	Private Key	kľúč na podpisovanie a dešifrovanie pri asymetrickej kryptografii
symetrická kryptografia	Conventional Cryptography	spôsob šifrovania, kde sa na šifrovanie a dešifrovanie používa ten istý kľúč
šifrovať	Encrypt	postup vedúci k takej zmene podoby zdrojových dát, že sa bez znalosti šifrovacieho kľúča nedajú previesť do pôvodnej podoby
verejný kľúč	Public Key	kľúč na overovanie a šifrovanie pri asymetrickej kryptografii
vyčistiť	Wipe	odstrániť zvyšky zmazaných súborov z disku
zneplatniť	Revoke	proces zneplatnenia kľúča

Zdroj: Mgr. Ján Guniš: Úvod do kryptografie