Šifrovanie

Šifrovanie je kryptografické pretváranie údajov, ktorého výsledkom je šifrovaný text.
Takýto text sa tretím osobám javí ako náhodný reťazec znakov, z ktorého nemožno vyčítať užitočnú informáciu.

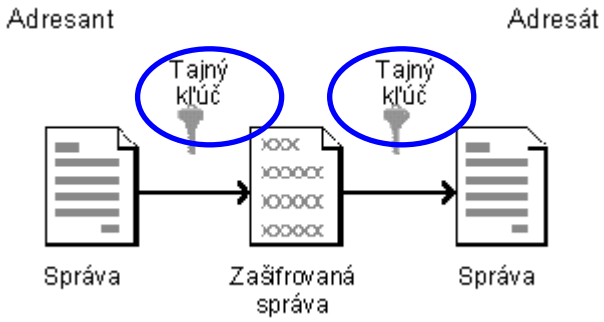
Medzi najznámejšie **kryptografické algoritmy** patria: **DES, RSA, MD5, SHA, IDEA**. Korene kódovania informácií siahajú do hlbokej minulosti ľudských dejín. Až s rozvoj matematiky priniesol vznik pomerne silných kryprografických algoritmov.

Najpoužívanejšími metódami šifrovania sú:

- **symetrické šifrovanie**
- **asymetrické šifrovanie**
- **hashovacie funkcie**

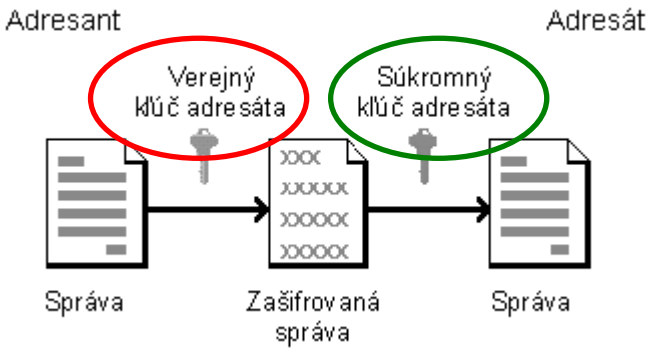
Treba ešte pripomenúť, že dôvodom šifrovania nemusí byť iba snaha utajiť informáciu.

Symetrické šifrovanie



je šifrovacia technika, ktorá **používa ten istý kľúč na šifrovanie aj dešifrovanie.** Vo všeobecnosti kľúč je špeciálne vygenerovaný kód určitej dĺžky znakov. Princíp spočíva v tom, že adresant aj adresát vlastnia rovnaký tajný kľúč, ktorým bola správa adresantom zašifrovaná a ktorou adresát túto správu dešifruje. Medzi prvé symetrické šifrovacie algoritmy patri DES (Data Encryption Standard). Avšak 17 rokov po svojom patentovaní v roku 1976 bol tento hardverový šifrátor prelomený, čo znamenalo smrť tohoto algoritmu. Dnes sa však využíva jeho modifikácia triple DES (3-DES). Za zmienku ešte stojí algoritmus IDEA (Ideal Data Encryption Algorithm) ako náhrada šifry DES . Známe sú ešte symetrické algoritmy ako CAST, Blowfish a RC4.

Asymetrické šifrovanie



je technika šifrovania, ktorá využíva **verejný kľúč** na zašifrovanie správy a **súkromný kľúč** na dešifrovanie správy. Teda používa dva rôzne kľúče - verejný a súkromný. Súkromný kľúč je generovaný na počítači vlastníka a je známy iba jemu, pričom verejný kľúč je distribuovaný všetkým partnerom dotyčného vlastníka, teda je známy verejnosti. Tento pár kľúčov je komplementárny, ale len v tom zmysle, že to, čo sa zašifruje jedným z týchto kľúčov, je možné dešifrovať iba druhým identickým kľúčom z tejto dvojice a naopak.

Najpopulárnejším asymetrickým šifrovacím algoritmom je algoritmus RSA (River-Shamir-Adelman). Algoritmus RSA náhodne vygeneruje veľké prvočíslo (verejný kľúč). Tento kľúč sa použije aplikáciou relatívne zložitých matematických funkcií na odvodenie ďalšieho veľkého prvočísla - súkromného kľúča. Bezpečnosť tohto algoritmu je závislá na tom, že rozklad veľmi veľkých čísiel je extrémne náročný a zaberá množstvo času. Do skupiny reprezentantov asymetrických algoritmov okrem RSA patrí aj DH (Diffie-Hellman) resp. ELGmalova varianta DH algoritmu.

Hashovacie funkcie

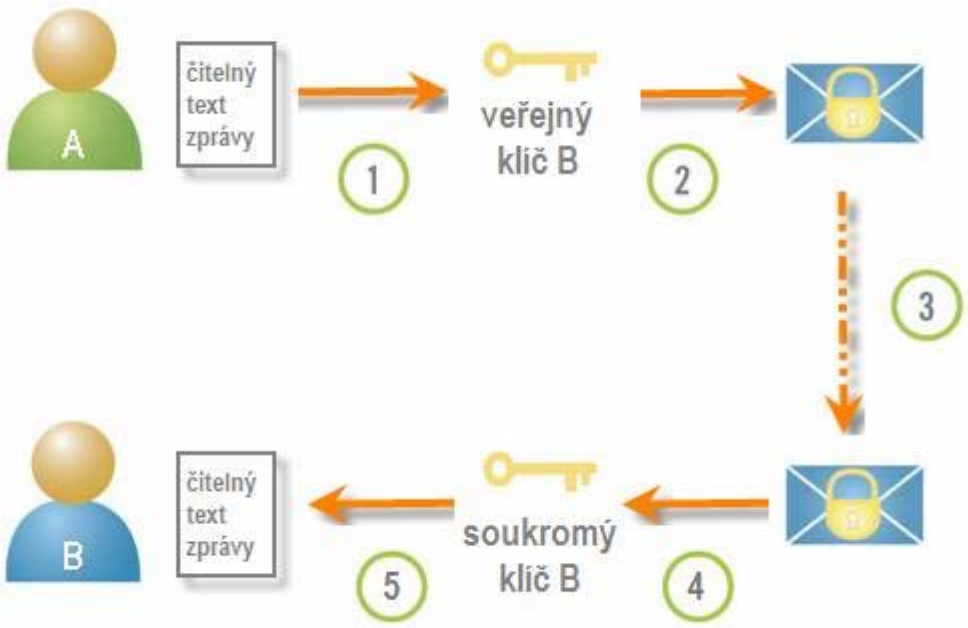
Neoddeliteľnou súčasťou tvorby elektronického podpisu sú hashovacie funkcie, ktoré tvoria základ pre zaručenie autentifikácie a integrity elektronického podpisu.

Hashovacia funkcia je algoritmus, ktorý zo vstupného reťazca znakov vygeneruje iný reťazec pevnej dĺžky znakov, tzv. digitálny odtlačok**. Digitálny odtlačok -fingerprint** je akýsi abstrakt, danej správy.

Je to výsledná hodnota vygenerovaná hashovaciou funkciou, pričom platí, že:

- použitie algoritmu na ten istý vstupný reťazec, vždy dá tú istú hodnotu, tzn. že na danú správu môžeme niekoľkokrát aplikovať hashovaciu funkciu, pričom digitálny odtlačok bude vždy rovnaký.
- je matematicky neuskutočniteľné získať, alebo zrekonštruovať pôvodný reťazec znakov na základe vedomostí výslednej hodnoty, tzn., že z digitálneho odtlačku sa nedá spätne vygenerovať obsah danej správy.
- je matematicky neuskutočniteľné zostaviť dva rôzne vstupné reťazce znakov s rovnakou výslednou hodnotou, tzn., že ak sa zmení obsah danej správy (čo i len 1 znak, 1 bit), zmení sa aj digitálny odtlačok tejto správy.

Elektronický podpis



- **asymetrickým algoritmom zašifrujeme digitálny odtlačok**, pomocou súkromného kľúča adresanta, dostaneme reťazec znakov, ktorý sa nazýva elektronický podpis. Inými slovami povedané,
- **elektronicky podpísať správu znamená, svojím súkromným kľúčom zašifrovať (podpísať) digitálny odtlačok danej správy**

Ak chceme, aby naša správa mala aj dôverný charakter nestačí ju iba podpísať (zašifrovať) svojím súkromným kľúčom, ale naviac celú správu aj s elektronickým podpisom zašifrovať verejným kľúčom adresáta.

Certifikačná autorita

Ako sme si povedali, na vytvorenie podpisu slúži vlastný súkromný kľúč a na zašifrovanie správy, kvôli zachovaniu dôvernosti danej správy, nám slúži verejný kľúč. No nie náš, ale verejný kľúč osoby, ktorej chceme správu poslať.

Asi vám tu napadne nejedna otázka:

Odkiaľ získam tento verejný kľúč, resp. kto mi zaručí, že príslušný verejný kľúč skutočne patrí môjmu partnerovi?

Ak je adresant mne známa osoba a zabezpečili sme si dodanie verejného kľúča (resp. ich výmenu) spoľahlivou cestou (osobne alebo kuriérom), je to v poriadku. No týmto jednoduchým spôsobom to môže fungovať iba medzi známymi. V prípade elektronického podpisu sa však predpokladá, že zmluvy budú uzatvárať osoby, ktoré sa nikdy nestretli a teda nemajú záruky, že verejný kľúč prislúcha naozaj osobe, ktorá sa za jeho držiteľa vydáva.

Práve pre vyriešenie tohto problému je zriadená tzv**. certifikačná autorita**, ktorá potvrdí (zaručí), že daný verejný kľúč skutočne prináleží príslušnej strane.

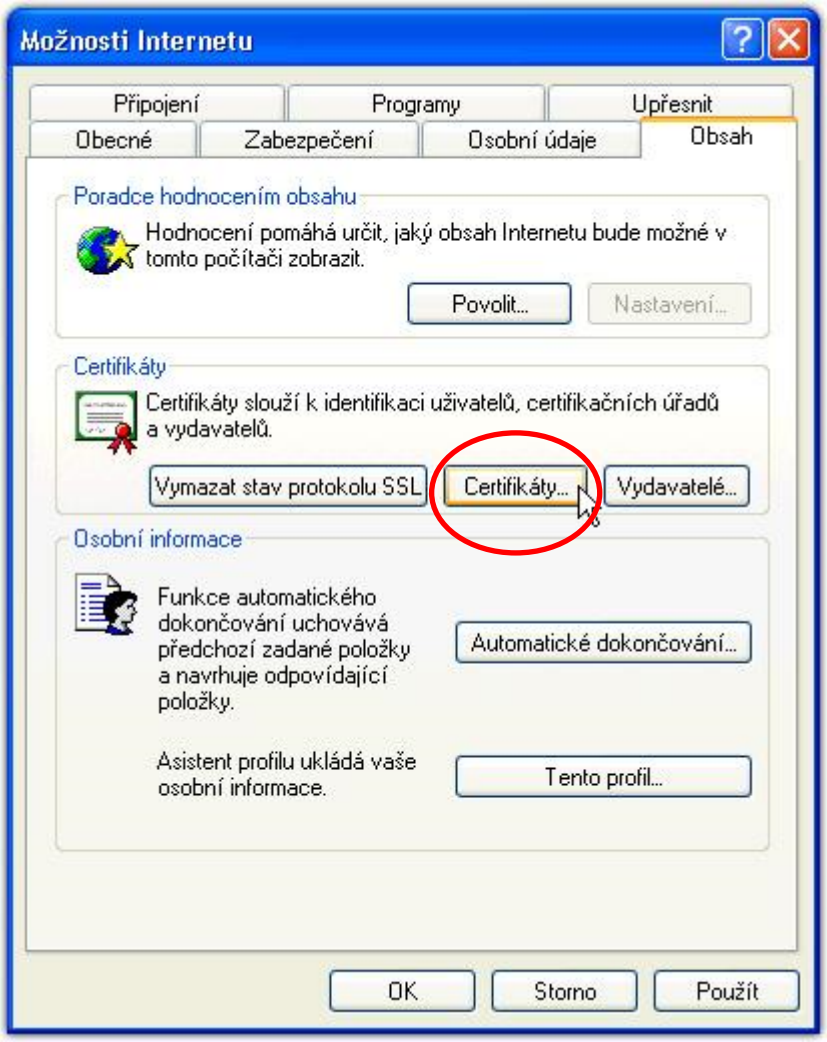
Vstupuje tu tretí nezávislý a dôveryhodný subjekt.

Keby sme hľadali podobnosť v bežnom živote, mohli by sme certifikačnú autoritu prirovnať k notárskemu úradu.

Certifikačná autorita **nie je fyzická osoba ani predmet**. **Je to skôr systém, prevádzkovaný firmou alebo štátnou inštitúciou.** Tento **systém zahŕňa** okrem patričného **programového a technického vybavenia aj bezpečné uloženie vlastného súkromného kľúča, poistenie pre prípad jeho odcudzenia, súbor pravidiel na vydávanie certifikátov iným subjektom a iné náležitosti.** Úrovňou ochrany a bezpečnostnej politiky certifikačnej autority je daná jej dôveryhodnosť.

Hlavnou úlohou certifikačnej autority je vydávanie certifikátov používaných na identifikáciu majiteľa verejného šifrovacieho kľúča.

Certifikát



je elektronický dokument podpísaný súkromným kľúčom certifikačnej autority, ktorý obsahuje verejný kľúč majiteľa certifikátu (presnejšie povedané môže obsahovať svoj vlastný pár kľúčov - jeden súkromný, ktorý sa používa na vytváranie elektronického podpisu a druhý, verejný, ktorý sa používa na šifrovanie údajov pri komunikácii s druhou stranou) a ďalšie údaje týkajúce sa certifikátu ako aj jeho držiteľa

- **sériové číslo certifikátu**
- **meno majiteľa**
- **typ certifikátu**

(pre obchodníkov, servery, platobné portály a pod.), meno certifikačnej autority, dobu platnosti certifikátu.

Certifikát je teda akýmsi elektronickým preukazom totožnosti, v paralele s bežným životom občiansky preukaz.

V skutočnosti je to dátová štruktúra (reťazec bitov), pomocou ktorej sa zverejňujú údaje o užívateľovi a hlavne užívateľov verejný kľúč.

Certifikáty sa vydávajú spravidla na dobu pol roka. Po tejto dobe strácajú svoju platnosť. Certifikát sa môže zneplatniť aj skôr, napríklad v prípade vyzradenia, či straty súkromného kľúča užívateľa. Tento zneplatnený certifikát sa potom zverejní na zozname zneplatnených certifikátov, tzv. CRL zoznam (Certificate Revocation List). Udržiavanie a publikovanie zneplatnených ako aj vydaných certifikátov patrí medzi základné povinnosti certifikačnej autority. Môže byť diskutabilné, či pojem certifikačná autorita je úplne slovensky správny, možno by sa skôr hodil pojem poskytovateľ certifikačných služieb. Výraz "poskytovateľ certifikačných služieb" je definovaný v Direktíve o elektronickom podpise (právna norma Európskeho parlamentu) ako aj v nemeckom a francúzskom práve. Naša právna norma nepoužíva tento europeizovaný výraz, ale americký výraz "certifikačná autorita".

Postup pri získaní certifikátu

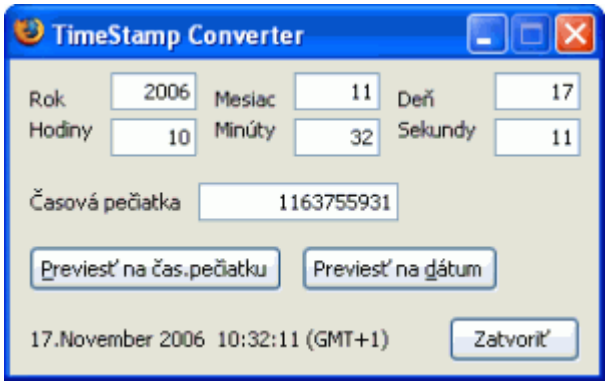
- podanie žiadosti
- zaplatení poplatku
- certifikačná autorita overí našu žiadosť a totožnosť.

Vydanie certifikátu spolu s vlastným párom kľúčov, pričom súkromný kľúč si musíme uchovať v čo najväčšej tajnosti (disketa, čipová karta, token*) a verejný kľúč môžeme zverejniť

Časová pečiatka

Právna norma zavádza pojem časová pečiatka. **Používa sa v prípade, keď je dôležité určiť, kedy sa s daným dokumentom niečo robilo**. Bude to mať význam napríklad pri presnom určení termínu podania daňového priznania. **Časová pečiatka sa vytvorí pripojením časového údaja k elektronickému dokumentu nezávislou treťou stranou (môže byť aj certifikačná autorita).**

- je to len potvrdenie, že nejaký dokument existoval v čase
- **certifikačná autorita** môže vydať aj tzv. **certifikát transakcie**, ktorý potvrdzuje, že sa daná transakcia uskutočnila a tým sa znemožňuje popretie tejto transakcie v budúcnosti.



- je jedinečný identifikačný kód, ktorý je vygenerovaný a poslaný zo servera na klientsky softvér pre identifikáciu interakcií zasadnutí a ktoré klient spravidla ukladá ako HTTP cookie
- Bezpečnostnostný token (známy aj ako hardvérový token, autentizačný token alebo kryptografické token), fyzické zariadenia, ktoré u autorizovaného užívateľa počítačových služieb je uvedený na pomoc pri overovaní
- prístup token, systém objekt predstavujúce predmetom kontroly prístupu operácie

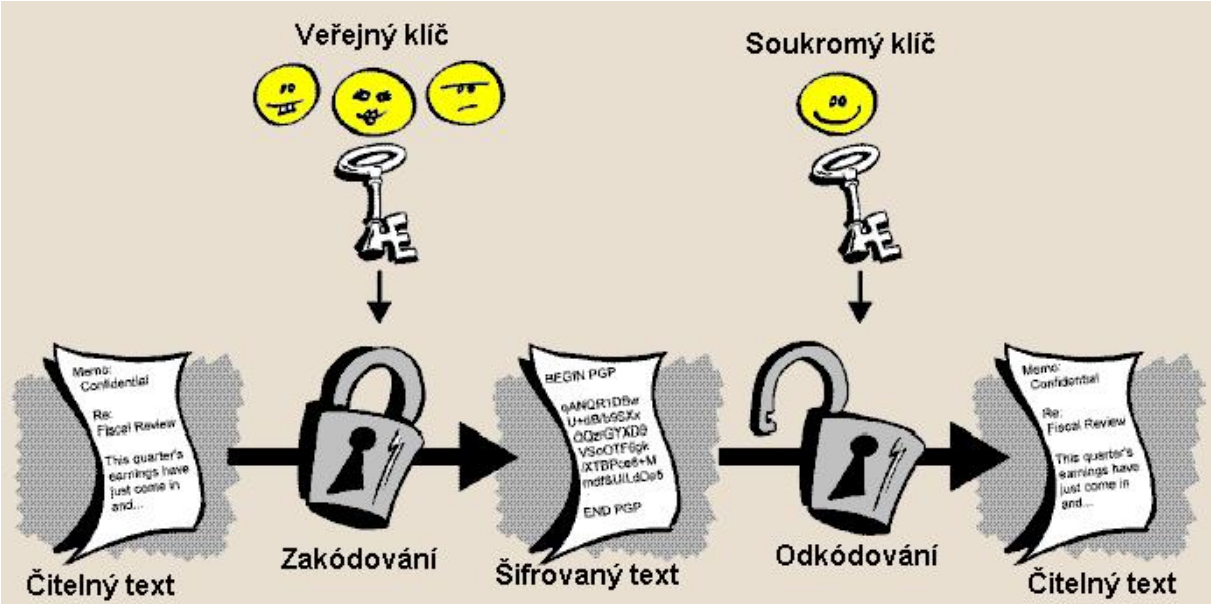
- Token Ring, lokálne siete, technológie, v ktorých virtuálny objekt známy ako token prechádza medzi zariadeniami v sieti, ich povolenie na komunikáciu

- tokeny, niekedy nazývaný "kódexy", sa niekedy používa ako spôsob obmedzovania webových stránok registračné číslo pre účely.

Slovník základných pojmov

Adresant - odosielateľ, ten ktorý správu odosiela.
Adresát - prijímateľ, ten ktorý správu prijíma.
Asymetrické šifrovanie - technika šifrovania, ktorá využíva jeden kľúč na zašifrovanie správy a druhý kľúč na jeho dešifrovanie.
Autentifikácia - proces overovania informácií o totožnosti, vlastníctve a oprávnení.
Certifikát - elektronický doklad totožnosti majiteľa certifikátu.
Certifikát transakcie - potvrdenie, že daná transakcia sa naozaj uskutočnila a tým znemožňuje popretie tejto transakcie v budúcnosti.
Certifikačná autorita - dôveryhodný orgán, ktorý vyhotovuje a zrušuje certifikáty.
Časová pečiatka - zápis, ktorý určuje dátum a čas podpísania elektronického dok.
Dešifrovanie - proces, ktorým sa pretvára šifrovaný text do pôvodnej podoby.
Digitálny odtlačok - abstrakt, hodnota alebo výsledok vytvorený hashovacou funkciou a je pevnej dĺžky.
Elektronický podpis - technika, spôsob, ktorým sa podpisujú elektronické dokum.
Hashovacia funkcia - algoritmus, ktorý zo vstupného reťazca znakov vyprodukuje iný reťazec znakov.
Integrita- proces, ktorým sa zabezpečuje súdržnosť údajov, proti zmenám a zničeniu.
Kľúč- špeciálne vygenerovaný kód určitej dĺžky znakov.
Kryptografia - odbor v kryptológii, ktorý sa zaoberá vývojom šifier a techník šifrovania.
Nepopierateľnosť- princíp v elektronickej komunikácii, ktorý chráni jedného účastníka komunikácie pred falošným tvrdením druhého účastníka, že komunikácia sa neuskutočnila.
Súkromný kľúč - jeden z párov kľúčov v systéme asymetrického šifrovania, ktorý by mal byť vždy utajený a známy len majiteľovi. Majiteľ ho používa najmä na vytvorenie elektronického podpisu.
Symetrické šifrovanie - šifrovacia technika, ktorá používa ten istý kľúč na šifrovanie aj dešifrovanie.
Šifrovanie- kryptografické pretváranie údajov, ktorého výsledkom je šifrovaný text.
Verejný kľúč - jeden z páru kľúčov, ktorý sa používa v systéme asymetrického šifrovania

Dekryptovanie a enkryptovanie



Typy kryptosystémov

- na úrovni súborového systému

Tieto systémy kryptujú (a dekryptujú) na **úrovni drivera** pre konkrétny typ súborového systému. Typickými implementáciami su **PGPdisk, Secure File System (SFS), Linux CryptoAPI, ScramDisk. Tieto kryptovače kryptujú obsah celého súborového systému a ich hlavnou výhodou je, že sú transparentné pre koncového užívateľa - všetko je buď kryuptované, alebo nie.**

- na úrovni súborov

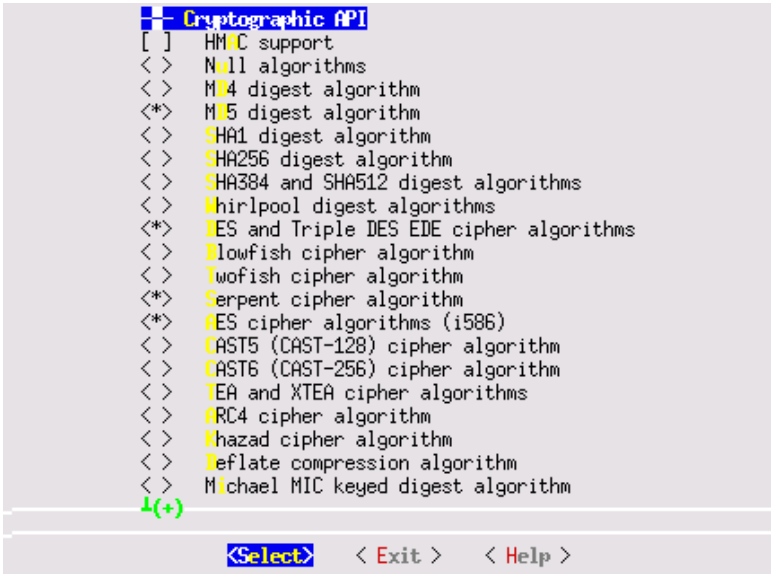
Kryptovače tohto druhu **pracujú na aplikačnej alebo prezentačnej vrstve a umožňujú skutočné kryptovanie medzi dvoma koncovými bodmi (medzi dvoma aplikáciami)**.
Obyčajne potrebujú aby samotná aplikácia dopredu vedela, že sa bude pristupovať ku kryptovaným dátam a teda aplikácie, ktoré nie sú na kryptovanie dát pripravené, nebudú vedieť s dátami pracovať. **Príkladom je PGP: ak máte kryptovaný súbor, musíte mať v editore PGP plugin, alebo musíte dáta rozkrypovať mimo aplikácie.**
Implementácie tohto typu sú vhodné v prostredí, kde je počet kryptovaných súborv malý a človek rozhoduje o použití kryptovania. Tieto systémy sa však vôbec nehodia na masové nasadenie pre kryptovanie množstva adresárov a súborov.

- na úrovni adresárov

Tieto systému **umožňujú kryptovanie na úrovni adresátov a súborov v nich, pričom na kryptovanie používajú kľúč.** Medzi známe implementácie patrí Cryptographic File System (CFS) navrhnutý Mattom Blazeom, Transparent Cryptographic File System (TCFS), ktorý je implementovaný na Linux e a **BSD, ďalej CryptFS ako aj EFS pod Windows 2000.**

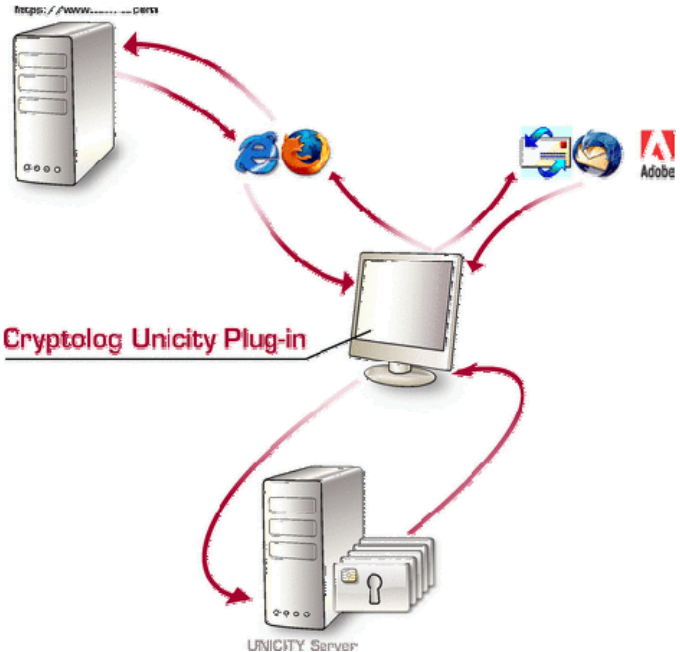
Návrh kryptosystému – CryptFS

Ide o kryptosystém, ktorý kryptuje celý súborový systém. Využíva modulárnu štruktúru, ktorú si UNIXové deriváty osvojili v poslednom čase. **Linux, Solaris a iné používajú dátovú štruktúru vnode (virtual inode),** ktorá reprezentuje objekt z ľubovoľného (virtuálneho) súborového systému. Užívateľský proces, ktorý číta zo súboru, pristupuje skrze jadro najskôr k vnodu a až potom pristupuje k inodu pre konkrétny filesystém. Implementácia vnodov je "štósovateľná", takže podobne ako kempingové stoličky sa dajú na seba vkladať jednotlivé volania a moduly. CryptFS vkladá svoje volanie tak, ako je to naznačené na nasledujúcom obrázku. Akekoľvek dáta ktoré sú zapisované resp. čítané, prechádzajú v jadre cez vloženú kryptovaciu úroveň a su kryptované resp. dekryptované, takže na disku je vždy krypotovaná reprezentácia dát. Samozrejme, že implementácia vyžaduje istú mieru manažmentu, takže existujú nástroje na primontovanie a odmontovanie CryptoFS, čo môže urobiť len root. Každý používateľ tohoto CryptoFS má možnosť manažovať svoje kľúče. Kryptovanie a dekryptovanie. je viazané nielen na UID užívateľa ale aj na groupID procesu, takže nikto (ani root) nemá možnosť užívateľské dáta čítať, lebo nemá možnosť vytvoriť proces s už existujúcim group id. (iba ak by to bol veľmi skúsený r00t).

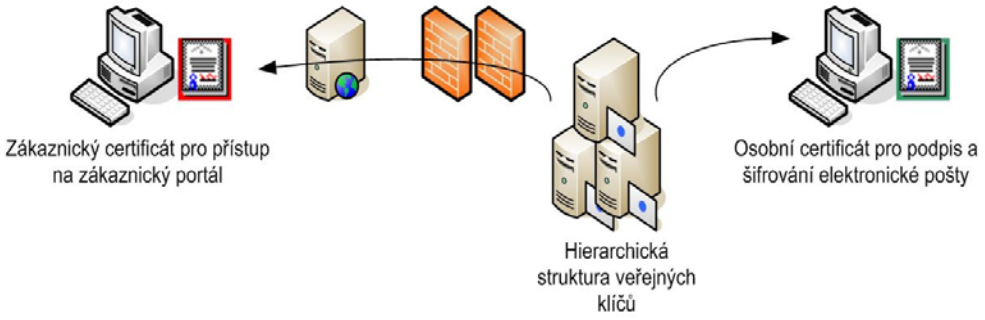


Linux CryptoAPI

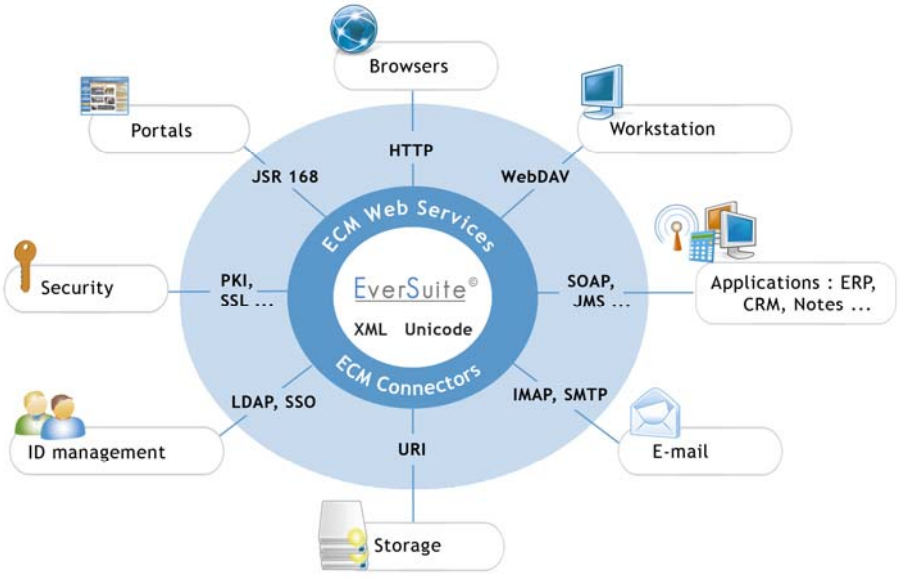
Linux Crypto API **nie je úplne presne kryptovanie súborového systému. Poskytuje len možnosť súborový systém kryptovať.** Toto API bolo pôvodne obsiahnuté v kernelint patchi, ktorý bol určený pre jadrá série 2.2. V sérii 2.4 sa toto API prirodzene vyvynulo do univerzálneho kryptoAPI pre kernel-land funkcie.



EFS pod Windows 2000



EFS je implementované pomocou PKI schémy. Samotné dáta sú kryptované rýchlym symetrickým algoritmom, ktorý je náhodne generovaný. **Tento kľúč sa volá file encryption key a po zakryptovaní samotných dát v súbore je následne zakryptovaný verejným PKI kľúčom užívateľa, ktorý sa získa z X.509v3 certifikátu užívateľa.** Privatna časť uživateľského PKI kľúča sa použije na rozkryptovanie file encryption key ak chce užívateľ neskôr pristúpiť k dátam.



Implementácie EFS podporuje symetrické algoritmy chránené heslom.

EFS v súčasnosti podporuje DESx kryptovací algoritmus, ktorý je založený na 128 bitovým kryptovacom kľúči a v budúcnosti sa plánuje podpora viacerých kryptovacích algoritmov.

$$2^{-\frac{n}{2}}\ \left(|0\rangle + e^{2\pi i\,[0.x_n]}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i\,[0.x_{n-1}x_n]}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i\,[0.x_1x_2\ldots x_n]}|1\rangle\right).$$

Morzeová abeceda

Namiesto písmen používa bodky a čiarky (krátke a dlhé signály). **Cieľom Morseovej abecedy nie je správu utajiť, ale iba efektívne sprostredkovať**.

- **Písmeno** Zápis *Pomocné slovo*
- **A** . - **Akát**
- **B** - . . . **Blýskavice**
- **C** - . - . **Cílovníci**
- **D** - . . **Dálava**
- **E** . **Erb**
- **F** . . - . **Filipíny**
- **G** - - . **Grónská zem**
- **H** . . . . **Hrachovina**
- **CH** - - - - **Chvátám k vám sám**
- **I** . . **Ibis**
- **J** . - - - ***Jasmín bílý***
- **K** - . - ***Krákorá***
- **L** . - . . ***Lupíneček***
- **M** - - ***Mává***
- **N** - . ***Nástup***
- **O** - - - ***Ó náš pán***
- **P** . - - . ***Papírníci***
- **Q** - - . - ***Kvílí orkán***
- **R** . - . ***Rarášek***
- **S** . . . ***Sobota***
- **T** - ***Trám***
- **U** . . - ***Uličník***
- **V** . . . - ***Vyučený***
- **W** . - - ***Wagón klád***
- **X** - . . - ***Xénokratés***
- **Y** - . - - ***Ygar mává***
- **Z** - - . . ***Známá země***

Číslice v Morseově abecedě

když jsem si probrali základní abecedu, tak si ji doplníme o číslice, ty se hodí téměř vždy.

- **Číslo** Zápis
- **1** . - - - -
- **2** . . - - -
- **3** . . . - -

- **4** . . . . -
- **5** . . . . .
- **6** - . . . .
- **7** - - . . .
- **8** - - - . .
- **9** - - - - .
- **0** - - - - -

Morseova abeceda - další znaky

Ono nemusíme je dopodrobna umět, ale pro nějaké vypečenější texty, logické hry, šifry se určitě bude hodit i znát tyto znaky. Včetně zavinače.

- **Znak** Zápis
- **.** . - . - . -
- **,** - - . . - -
- **;** - . - . - .
- **!** - - . . . -
- **?** . . - - . .
- **:** - - - . . .
- **-** - . . . . -
- **=** - . . . -
- **"** . - .. - .
- **()** - . - - . -
- **@** . - - . - .

Morseova abeceda - speciální texty

Můžeme napsat pomocí písmenek, ale když už na to je nějaká zkratka tak proč ji nevyužít?

- **Znak** Zápis
- **Zač. vysílání** - . - . - . - .
- **Jsem připraven** . - - .
- **Rozumím** - - - - . -
- **Nerozumím** . . . . . .
- **Pomaleji** - . - . - ..
- **Omyl** . / . / . / . / . / . / . / .
- **Čekej** . - . . .
- **Opakuji** . . / . . / . . / . . / . .
- **Konec vysílání** . . . - . -
- **Zlomková čára** - . . - .
- **SOS** . . . / - - - / . . .

Osobně jsem tato slovní spojeni nepoužíval, ale třeba Vám k nečemu budou. Spíše jen pro ucelený přehled v problematice Morzeovy abecedy.

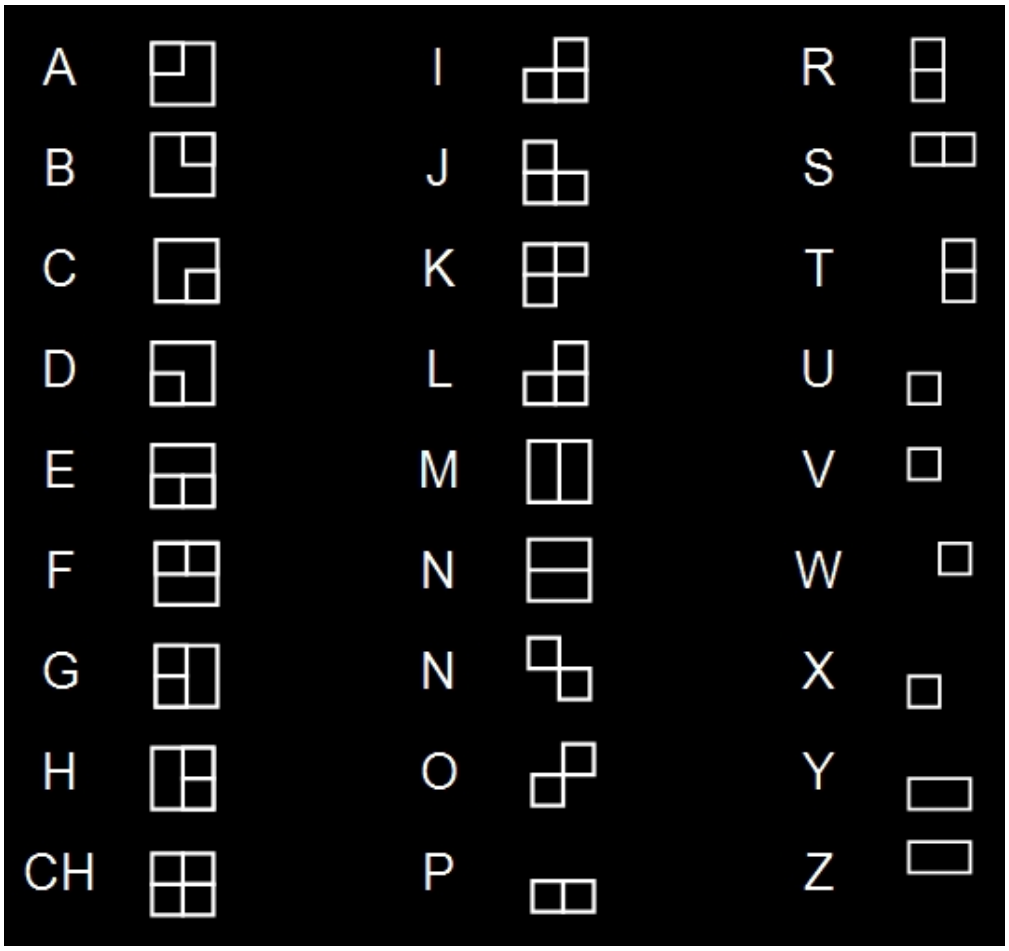
OBRÁZKOVÁ ŠIFRA

Úvod

Obrázkové šifry jsou velice jednoduchí a můžeme si je vytvořit k obrazu svému. Z toho vyplívá, že pravděpodobnost stejné šifry je nulová. Každý si může zvolit různé obrázky ať už čtverečky či kolečka, jejich uspořádaní, či barvu. Fantazii se žádné meze nekladou.

Případně může kombinovat ještě s jinou šifrou jako je posunutí písmenek atd. Viz další články o šifrách.

Ukážka



Jedna z možnosti jak obrázková šifra může vypadat.

Šifrovanie

No a již můžeme nějaký text zakodovat. To se v jednoduchosti rovede tak, že každé písmenko se nahradí daným obrázkem. Kdo obrázky nemá k dispozici bude dlouho tento text dešifrovat.

Bezpečnost šifry

Pokud napíšte, ale rozsáhlý text, tak se podle počtu znaku dá uršit, kterému znaku odpovída jaké písmeno. Přeci jen v češtině se nějaká písmenka vyskytuji často (E,A), jako jednopísmené předložky a spojky mohou být také jen určitá písmena atd. Ale pro nějakou táborovou hru je tato šifra jednoduchá rychlá zajimavá.