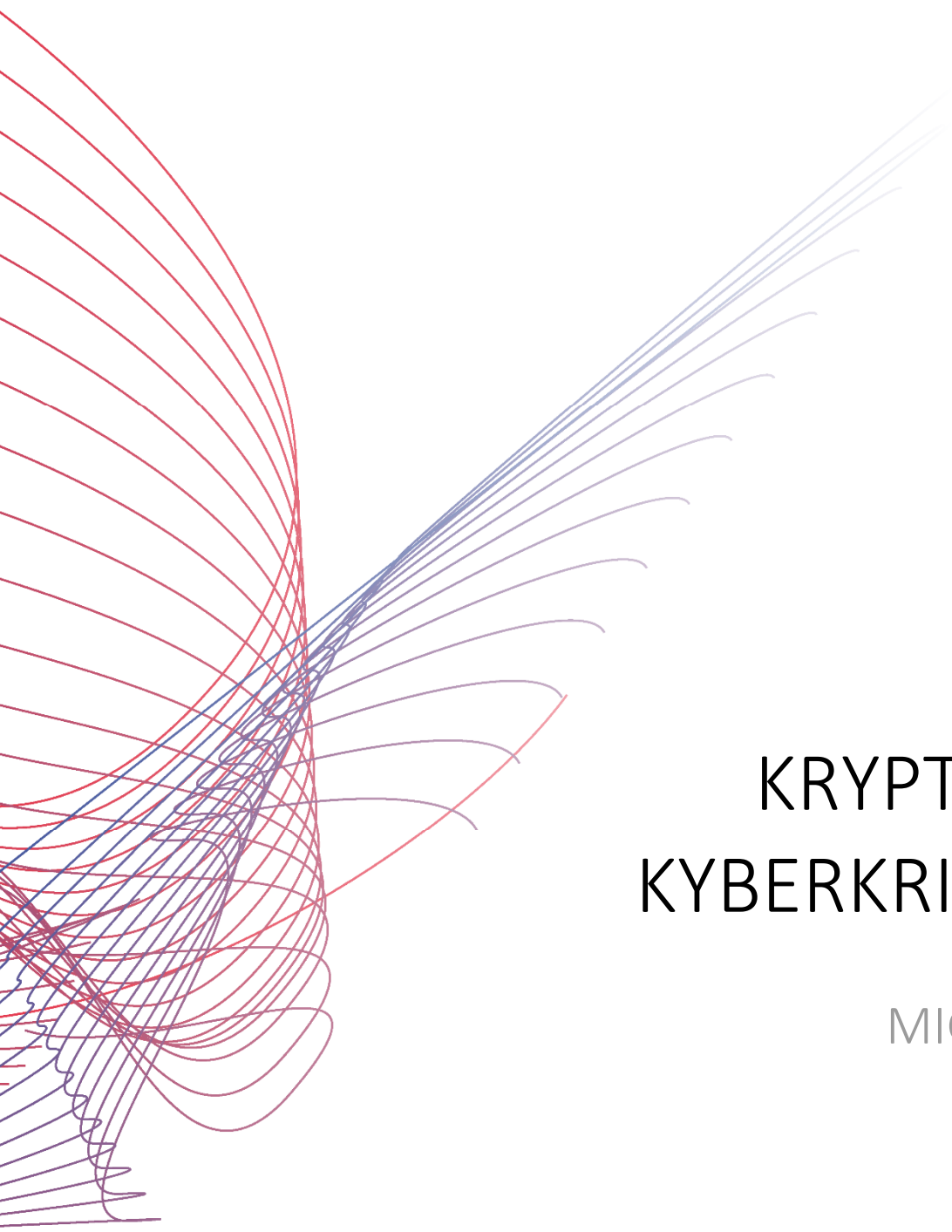
en
cs de
sk es

TECH
pedia



KRYPTOGRAFIA, KYBERKRIMINALITA

MIGUEL SORIANO

Názov: Kryptografia, kyberkriminalita
Autor: Miguel Soriano
Preložil: Martin Broda, Vladimír Hajduk
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktná adresa: Technická 2, Praha 6, Česká republika
Tel.: +420 224352084
Tlač: (iba elektronická)
Počet strán: 39
Edícia (vydanie): 1. vydanie, 2017

ISBN 978-80-01-06205-0

TechPedia
European Virtual Learning Platform for Electrical and Information Engineering
http://www.techpedia.eu

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

VYSVETLIVKY

	Definícia
	Zaujímavosť
	Poznámka
	Príklad
	Zhrnutie
	Výhody
	Nevýhody

ANOTÁCIA

Tento modul predstavuje základné informácie z odboru kryptografie a kyberkriminality.

CIELE

Tento modul poskytuje informácie o kryptografii a kyberkriminalite v ich základnom kontexte, pričom je rozdelený do dvoch častí. Prvá časť kurzu je navrhnutá tak, aby oboznámila študentov s fundamentálnymi možnosťami kryptografie, ktoré ponúka na zaistenie informačnej bezpečnosti. Z toho dôvodu sú v kurze opísané dva základné typy kryptografie a to kryptografia s tajným a kryptografia s verejným kľúčom. Druhá časť kurzu sa venuje konceptu kyberkriminality a klasifikuje rôzne druhy útokov, pričom v závere opisuje možnosti prevencie pred takýmito útokmi.

LITERATÚRA

[1] Bruce Schneier: Applied Cryptography. John Kiley & Sons, Inc., New York, 1994

[2] William Stallings: Cryptography and Network Security. Principles and Practices. Prentice Hall, New Jersey, 2003

[3] Vesna Hassler: Security Fundamentals for E-Commerce. Artech House, Boston, 2001

[4] Rolf Oppliger: Internet and Intranet Security. Artech House, Boston, 2002

[5] Michael Goodrich, Roberto Tamassia: Introduction to Computer Security, 2010

[6] John R. Vacca: Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security), 2009

[7] Jason Andress: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier, 2011

Obsah

1 Kryptografia v základnom kontexte

Kryptografia predstavuje silný matematický nástroj, ktorý slúži na ochranu informácií v počítačových systémoch. Základné operácie kryptografie, šifrovanie a dešifrovanie, využíva mnoho bezpečnostných aplikácií. Citlivé dáta môžu byť vďaka kryptografii bezpečne prenášané prostredníctvom telekomunikačných sietí bez hrozby neoprávneného zachytenia a rozlúštenia obsahu dát. Šifrovanie možno definovať ako proces, po ktorom sa stáva informácia nerozlúštiteľná a zbytočná pre všetkých okrem určených príjemcov správy. Dešifrovanie predstavuje inverzný proces k šifrovaniu. Jedná sa o prevod dát späť do pôvodnej podoby.

Technika kryptografie sa využíva v našom každodennom živote. Napr. pri telefonovaní, platení kreditnou alebo debetnou kartou, výbere peňazí z bankomatu, prihlasovaní sa pomocou hesla do počítačových systémov, atď. Kryptografia umožňuje ukladanie citlivých informácií alebo ich prenos cez nezabezpečené siete (ako napr. Internet) tak, že nikto okrem určeného príjemcu nedokáže prečítať ich obsah. Kryptografia sa stala priemyselným štandardom pre poskytovanie informačnej bezpečnosti, dôvernosti, kontroly prístupu k rôznym zdrojom a elektronickým transakciám. Na druhej strane treba dodať, že kryptografia sama o sebe nie je dostatočný prostriedok na zabezpečenie všetkých potenciálnych hrozieb narušenia informačnej bezpečnosti.

Kryptografický algoritmus, nazývaný tiež šifra, je jednoducho postupnosť určitých procesov, ktoré zahŕňajú šifrovanie a prislúchajúce dešifrovanie. Šifra je matematická operácia špeciálne navrhnutá tak, aby zakryla, resp. znemožnila odhaliť obsah dát. Najúčinnejšie šifrovacie algoritmy pracujú s kombináciou viacerých kľúčov. V prípade použitia rozličných kľúčov môže byť rovnaký otvorený text zmenený na rôzne podoby zašifrovaného textu. Spoľahlivý kryptografický algoritmus musí zabezpečiť, aby nevznikla možnosť získania pôvodného otvoreného textu bez znalosti kľúča. Samozrejme existuje aj metóda tzv. totálnych skúšok, ktorá skúša všetky možné kľúče až kým nenájde ten správny. Štatisticky sa správny kľúč nájde s vysokou pravdepodobnosťou už v prvej polovici všetkých skúšok. Bezpečnosť kryptografického systému je vo všeobecnosti postavená na dvoch veciach: sile kryptografického algoritmu a utajení kľúča.

Počet všetkých možných kľúčov musí byť tak veľký, že je výpočtovo nemožné na základe súčasných prostriedkov odhaliť kľúč v rozumnom čase. Mnoho šifier zvyšuje svoju bezpečnosť vzrastajúcou dĺžkou kľúča. Avšak čím je dĺžka kľúča väčšia, tým je proces výpočtovo náročnejší a teda doba šifrovania a dešifrovania narastá. Preto je dôležité vybrať algoritmus na základe porovnania medzi úrovňou ochrany a výpočtovou náročnosťou algoritmu.

Moderné kryptografické algoritmy môžu byť klasifikované podľa dvoch kritérií: typu kľúča a podľa spôsobu, akým pracujú s dátami.

Podľa typu kľúča sa kryptografické algoritmy delia na:

a) Kryptografia s tajným kľúčom (symetrická kryptografia). Symetrická kryptografia predstavuje kryptografické metódy, v ktorých odosielateľ aj

príjemca používajú rovnaký kľúč na šifrovanie aj dešifrovanie. (Menej známe sú metódy, v ktorých sú jednotlivé kľúče odlišné, ale dajú sa pomerne ľahko odvodiť jeden od druhého). Šifrovací štandard AES (Advanced Encryption Standard) je príkladom široko používaného konvenčného symetrického šifrovacieho systému.

b) Kryptografia s verejným kľúčom (asymetrická kryptografia) využíva dvojicu kľúčov: verejný kľúč na šifrovanie dát a zodpovedajúci súkromný (tajný) kľúč na ich dešifrovanie. Je zrejmé, že medzi obidvoma kľúčmi je matematický vzťah. Matematické operácie sú však také zložité, že je na nich postavená bezpečnosť celého algoritmu. Používateľ alebo časť systému zverejňuje svoj verejný kľúč, pričom súkromný kľúč si ponecháva v bezpečí. Každý, kto získa verejný kľúč môže informáciu šifrovať, avšak k pôvodnej otvorenej správe sa nedostane. Len osoba, ktorá vlastní zodpovedajúci súkromný kľúč môže zašifrované dáta dešifrovať.

Hlavná výhoda kryptografie s verejným kľúčom spočíva v tom, že odosielateľ a príjemca nepotrebujú zdieľať tajný kľúč cez vopred vytvorený zabezpečený kanál. Celá komunikácia vyžaduje len prítomnosť verejného kľúča, ktorý sa môže prenášať aj cez nezabezpečený kanál.

Podľa spôsobu akým algoritmus pracuje s dátami môžu byť šifry klasifikované ako:

a) Blokové šifry pracujú s blokmi dát, s množinou bitov s pevne určenou dĺžkou, s rovnakými operáciami pre všetky bloky. Správa sa rozdelí na menšie bloky, ktoré sa postupne šifrujú. Bloková šifra sa považuje za bezpečnú ak sa všetky bloky otvoreného textu bezpečne transformujú na bloky šifrovaného textu, tzn. že kryptoanalýze by mal odolať každý jeden blok rovnako. Ak sú šifrované rôzne správy rovnakým kľúčom, potom rovnaké bloky dát sa transformujú vždy na rovnaké bloky zašifrovaného textu. Útočník tak môže jednoducho odhaliť opakujúce sa bloky v správe. Z toho dôvodu sa použitie blokovej šifry v takomto režime neodporúča a využívajú sa iné bezpečné režimy.

b) Prúdové šifry transformujú jeden symbol otvoreného textu priamo na jeden symbol zašifrovaného textu. Transformácia je založená na generovaní pseudonáhodnej postupnosti, ktorá predstavuje prúd bitov šifrovacieho kľúča. Tento prúd bitov v spojení s otvoreným textom slúži na zašifrovanie jedného bitu alebo bajtu v jednom časovom okamihu. Takýmto spôsobom sa vytvorí konečný zašifrovaný text.

Základná terminológia:

- Otvorený text je správa, ktorá má byť vysielaná a doručená adresátovi.
- Zašifrovaný text je výstup kryptografického systému, ktorý vznikne zašifrovaním otvoreného textu.
- Šifrovanie je proces zmeny obsahu otvoreného textu za účelom ukrytia prenášanej informácie.

- Dešifrovanie je inverzná operácia k šifrovaniu. Je to proces spätného získania správy vo forme otvoreného textu z jej zašifrovanej podoby (zašifrovaného textu). Tento proces teda transformuje zašifrovaný text na otvorený text.
- Kľúč je slovo, číslo, alebo postupnosť, ktorá sa používa na šifrovanie otvoreného textu alebo dešifrovanie zašifrovaného textu.
- Kryptoanalýza je vedná disciplína, ktorá sa zaoberá metódami na rozkódovanie zašifrovaných správ bez znalosti tajného kľúča.
- Hašovacia funkcia je algoritmus, ktorý transformuje text ľubovoľnej dĺžky na text s fixnou dĺžkou.
- Šifra je kryptografický algoritmus, tzn. matematická funkcia, ktorá sa používa na šifrovanie a dešifrovanie.
- Manažment kľúčov zahŕňa procesy akými sa kľúče vytvárajú, ukladajú, chránia, prenášajú, načítavajú, používajú a ničia.

2 Kryptografia s tajným kľúčom

Proces šifrovania a dešifrovania informácie použitím jedného kľúča je známy pod pojmom kryptografia s tajným kľúčom alebo symetrická kryptografia. V symetrickej kryptografii môžu byť kľúče použité pri šifrovaní a dešifrovaní rovnaké (bežný prípad) alebo je medzi nimi jednoduchý matematický vzťah (menej používané algoritmy). Hlavný nedostatok takéhoto systému spočíva v nutnosti výmeny kľúčov pred samotnou komunikáciou. To súvisí s vytvorením bezpečného komunikačného kanálu pre výmenu kľúčov.

Obidve strany musia chrániť kľúč. Zverejnenie kľúča ktoroukoľvek stranou môže mať za následok ohrozenie informácií.

Proces činnosti kryptografie s verejným kľúčom je nasledovný: Používateľ A chce poslať správu používateľovi B, pričom chce zabezpečiť, aby len používateľ B mohol prečítať obsah správy. Na zaistenie prenosu používateľ A generuje tajný kľúč, šifruje správu a odosiela ju používateľovi B. Používateľ B potrebuje tajný kľúč, aby mohol správu dešifrovať. Používateľ A využije jeden z ponúkaných spôsobov doručenia tajného kľúča adresátovi B. Po tom ako používateľ B príjme tajný kľúč môže dešifrovať správu, čím získa jej pôvodný obsah.

Obr 2.1 Model kryptografie s tajným kľúčom

Každý šifrovací algoritmus musí splniť nasledujúce požiadavky:

- Rozptyl (diffusion): každý bit otvoreného textu ovplyvní mnoho bitov zašifrovaného textu.
- Konfúzia (confusion): je nevyhnutné predísť akémukoľvek vzťahu medzi otvoreným a zašifrovaným textom (špeciálne linearite), na ktorom môžu byť založené známe útoky.
- Zašifrovaný text by mal mať podobu náhodne vyzerajúceho textu a mať dobré štatistické vlastnosti.
- Jednoduchosť (simplicity).
- Efektivita (efficiency): extrémne rýchly na mnohých platformách.

Hlavným problémom symetrickej kryptografie je, že proces prenosu tajného kľúča adresátovi môže spôsobiť bezpečnostné riziko. Prenos tajného kľúča prostredníctvom Internetu (napr. e-mailom) nie je bezpečný. Kľúč odovzdávať verbálnou komunikáciou cez telefónne siete, ktoré môžu byť odpočúvané je takisto riskantné. Podobne klasická pošta predstavuje riziko možného odchytu a sledovania zásielok.

Bezpečnostné riziká kryptografie s tajným kľúčom do značnej miery odstraňuje kryptografia s verejným kľúčom. Symetrická kryptografia sa často používa na šifrovanie dát pri ukladaní na pevné disky. Osoba, ktorá šifruje dáta vlastní kľúč a nevzniká žiaden problém jeho distribúcie.

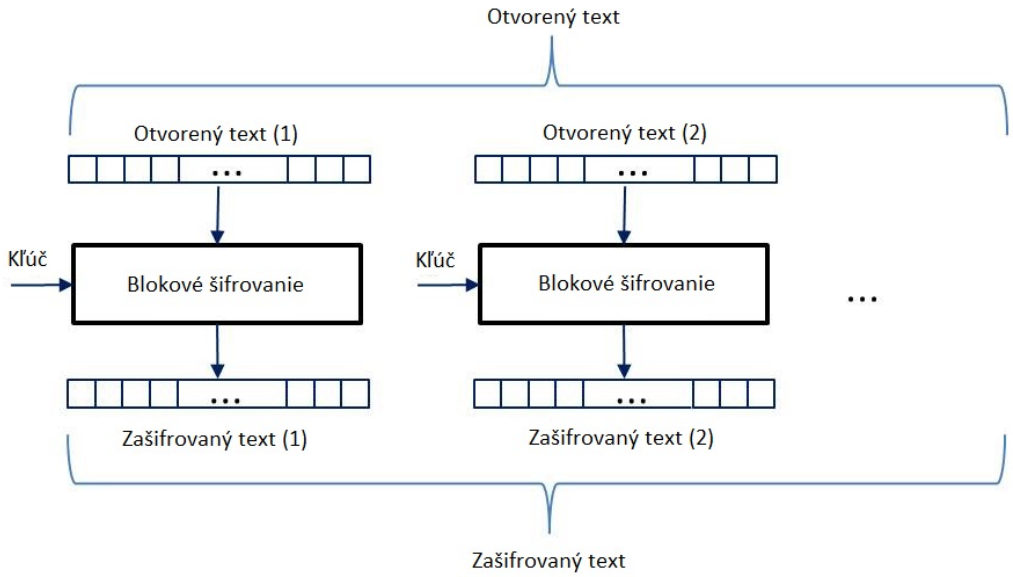
Ako bolo uvedené v predchádzajúcej kapitole, významné delenie v rámci kryptografie s tajným kľúčom je na kryptografiu, ktorá využíva blokové šifry a kryptografiu s prúdovými šiframi. V dnešnej dobe sa tešia obľube hlavne blokové šifry.

2.1 Algoritmy blokových šifier

Blokové šifry transformujú skupiny symbolov otvoreného textu na skupiny symbolov zašifrovaného textu. Takže šifrovanie je realizované blok po bloku otvoreného textu.

Symboly otvoreného textu sa zoskupia po blokoch a šifrovací algoritmus sa aplikuje na každý z nich (za prítomnosti tajného kľúča). Výsledkom šifrovania jedného bloku otvoreného textu je blok zašifrovaného textu o rovnakej veľkosti.

Môže nastať prípad, že veľkosť otvoreného textu nebude celočíselným násobkom veľkosti bloku. V takom prípade je zvyčajne použitá tzv. "padding-scheme" na zaplnenie posledného bloku. V závislosti na prevádzkovom režime šifry však zaplnenie bloku nemusí byť potrebné. Princíp šifrovania a dešifrovania blokovej šifry je zobrazený na nasledujúcom obrázku.



Obr. 2.2 Model blokových šifier

Štruktúra väčšiny blokových šifier pracuje v iteračnom režime. To znamená, že šifrovanie sa vykonáva pomocou viacerých opakovaní jednotlivých procesov. Jedno vystriedanie všetkých procesov sa nazýva runda. Každá runda opakuje sériu operácií za prítomnosti jedinečného kľúča, odvodeného od originálneho vstupného kľúča. Operácie v každej runde zvyčajne pozostávajú zo substitúcie, permutácie a expanzie kľúča. Takéto šifry sa nazývajú Substitučno-permutačné siete (SPN, Stitution-Permutation Networks) alebo Feistelové šifry. Substitúcia je často jedinou nelineárnou časťou mnohých šifier, a preto sa substitučné boxy (S-boxy) vyberajú veľmi starostlivo, aby bola šifra odolná voči prípadným kryptoanalytickým útokom.

Dešifrovanie prebieha obdobným spôsobom. Za prítomnosti rovnakého kľúča, aký bol použitý pri šifrovaní (symetrické šifry) sa rovnaké operácie vykonajú na

zašifrovanom texte, ktorý je na začiatku rozdelený opäť do rovnakých blokov. Výsledkom tohto procesu sú bloky dešifrovaného otvoreného textu.

Typické veľkosti blokov otvoreného a zašifrovaného textu sú 64 alebo 125 bitov.

Výhody blokových šifier:

- vysoký rozptyl,
- odolnosť voči neoprávnenému pozmeňovaniu obsahu, zložitosť vkladania symbolov bez detekcie.

Medzi najpoužívanejšie algoritmy blokových šifier patria:

- Data Encryption Standard (DES),
- Advanced Encryption Standard (AES).

Použitie rovnakého kľúča pri šifrovaní rovnakých častí otvoreného textu sa neodporúča. V takom prípade by sa všetky rovnaké bloky otvoreného textu transformovali na všetky rovnaké bloky zašifrovaného textu. Informácia o znalosti opakovania určitých blokov môže pomôcť kryptoanalýze, a preto existujú viaceré metódy ako tomu predísť. Tieto metódy sa nazývajú režimy blokových šifier.

Režimy blokových šifier

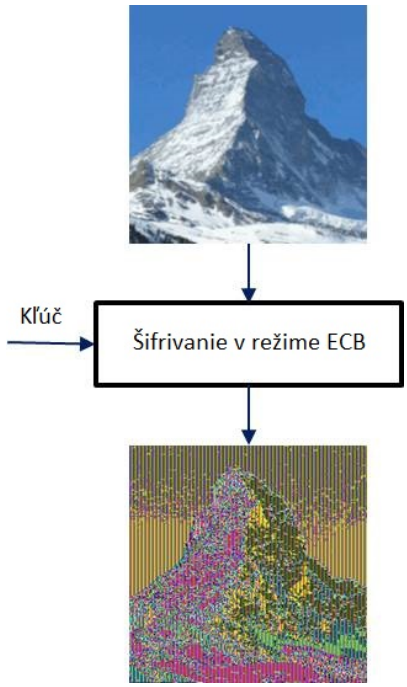
Blokové šifry sa môžu použiť rôznym spôsobom s rozdielnym utajením a vlastnosťami opravy chýb. Výber režimu má vplyv na rýchlosť, bezpečnosť a šírenie chýb daným algoritmom.

Elektronická kódová kniha, resp. režim ECB (Electronic Code Book)

Tento režim predstavuje základný algoritmus blokovej šifry bez akejkoľvek modifikácie. Správa sa rozdelí do blokov a každý blok otvoreného textu je šifrovaný jednotlivo, nezávisle od ostatných. Neexistuje žiadna závislosť medzi blokmi v dôsledku čoho sa tento režim neodporúča. Použitie tohto režimu prináša niekoľko nevýhod:

- Štruktúra otvoreného textu ostáva odkrytá.
- Citlivosť na útok modifikovaním obsahu: reorganizovanie usporiadania blokov alebo opakovanie niektorých blokov môže spôsobiť zmenu obsahu správy.
- Ľubovoľný zašifrovaný text zašifrovaný rovnakým kľúčom môže byť použitý ako zdrojový materiál pre útočníka.

Klasický príklad nevýhody použitia režimu ECB je šifrovanie rastrového obrázku (napr. s príponou .bmp). Aj napriek použitiu silného, bezpečného algoritmu, algoritmus v režime ECB nedokáže efektívne zastrieť obsah správy.

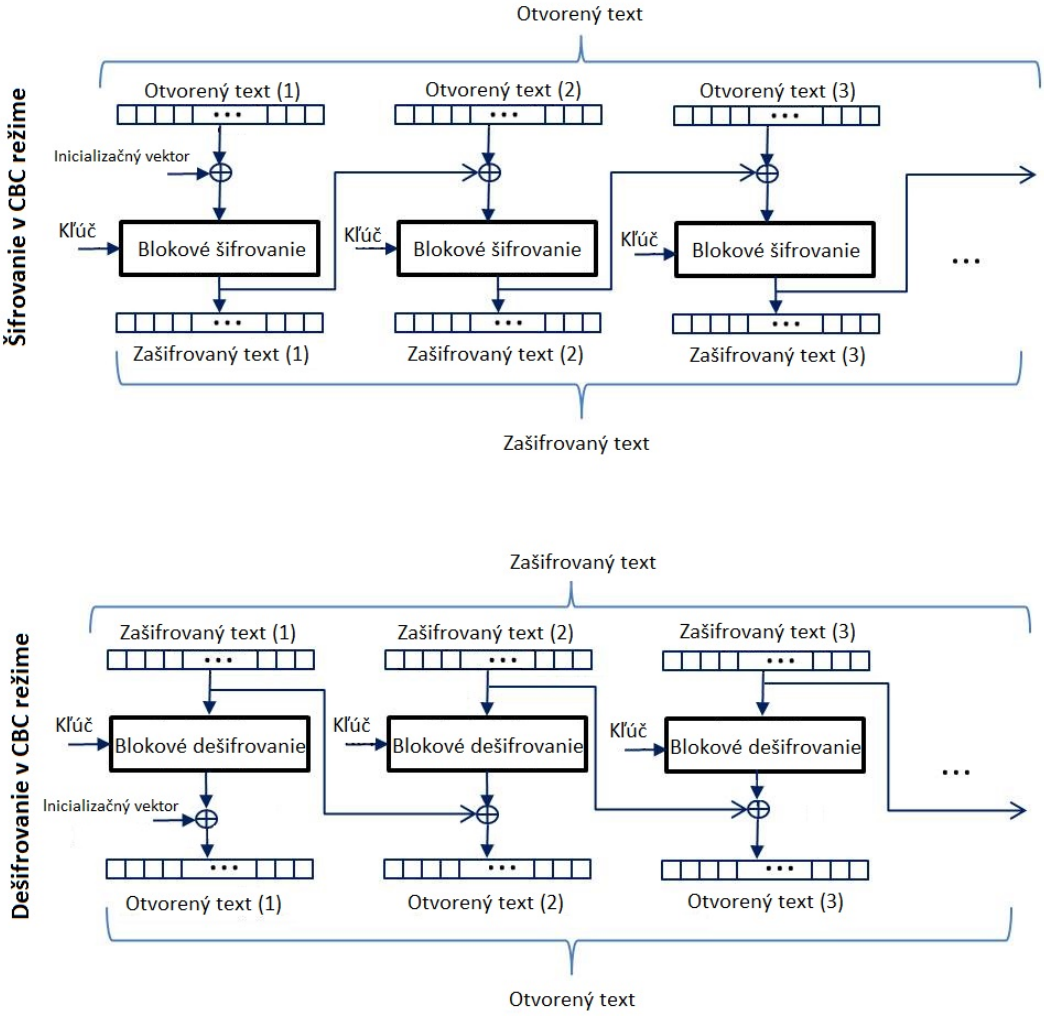


Obr. 2.3 Šifrovanie rastrového obrázka v režime ECB

Zreťazenie zašifrovaného textu, resp. režim CBC (Cipher Block Chaining)

Režim CBC kombinuje ("zreťazuje") bloky otvoreného textu s predchádzajúcimi zašifrovanými blokmi. Na to je potrebný inicializačný vektor IV, ktorý sa podrobí operácii s prvým blokom otvoreného textu.

V procese šifrovania sa použije operácia XOR prvého bloku otvoreného textu a IV ešte pred samotným šifrovaním. Výsledok je následne zašifrovaný a výstupom je prvý blok zašifrovaného textu. Pre nasledujúce bloky je inicializačným vektorom zašifrovaný text predchádzajúceho bloku. Výsledkom zreťazenia je, že blok zašifrovaného textu c_j závisí od bloku otvoreného textu p_j a predchádzajúceho bloku zašifrovaného textu c_{j-1}. Z toho je zrejmé, že blok zašifrovaného textu c_j teda závisí od aktuálneho a všetkých predchádzajúcich blokov otvoreného textu.



Obr. 2.4 Šifrovanie a dešifrovanie v režime CBC

Režim CBC odstraňuje nedostatky ECB, ale prináša dve nevýhody:

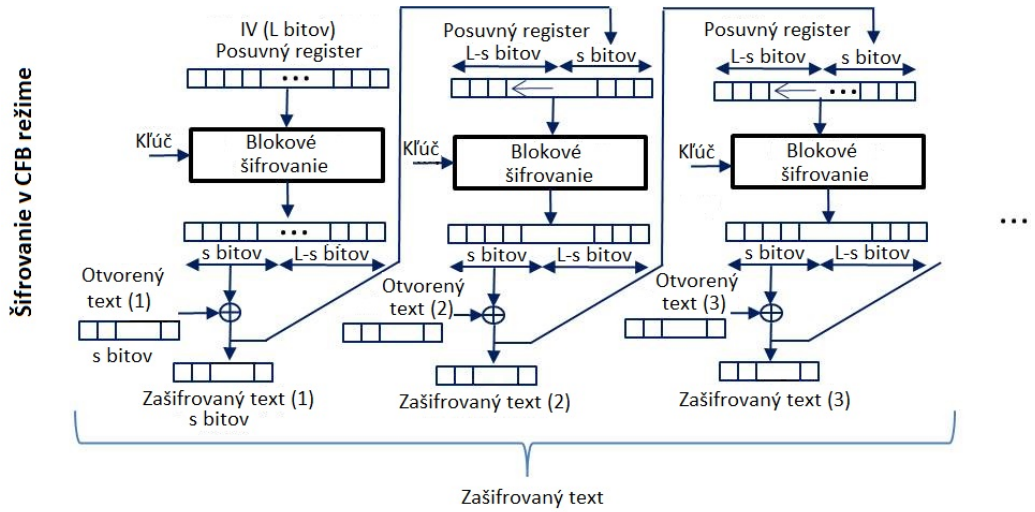
- Nie je možné paralelne šifrovanie: šifrovanie bloku p_{j+1} pred alebo počas šifrovania bloku p_j, pretože blok c_j ešte nie je vytvorený. Na druhej strane, paralelne dešifrovanie je možné. Blok otvoreného textu p_j požaduje bloky c_j a c_{j-1}.

- Šírenie chyby. Chyba len v jednom bite (jednoduchá chyba) počas prenosu bloku c_j sa pri dešifrovaní premietne nielen ako chyba v bloku p_j, ale aj ako chyba v p_{j+1}. Na druhej strane chyba vždy ovplyvní len jeden bit v bloku p_{j+1}. Takýto efekt sa nazýva limitované šírenie chyby (limited error-propagation).

Spätná väzba zo zašifrovaného textu, resp. režim CFB (Cipher Feedback)

CFB je režim utajenia, ktorý je vybavený spätnou väzbu po sebe idúcich blokov zašifrovaného textu do vstupných blokov otvoreného textu. Zašifrovaný text sa vytvorí operáciou XOR medzi blokmi spätnej väzby a blokmi otvoreného textu. Dôležitý parameter v tomto režime je také celé číslo s, že platí $1 \leq s \leq L$, kde L je dĺžka celého bloku.

Prvým vstupným blokom je inicializačný vektor IV. Zjednodušene povedané, proces šifrovania v režime CFB možno brať ako vstup *L* najmenej významových bitov predchádzajúceho IV spojený s *s* bitmi predchádzajúceho bloku zašifrovaného textu, ktorý sa následne šifruje. Výsledný zašifrovaný text vzniká operáciou XOR medzi *s* najvýznamnejšími bitmi bloku po šifrovaní a s bitmi odpovedajúceho bloku otvoreného textu. Tento proces je ilustrovaný na nasledujúcom obrázku.



Obr. 2.5 Šifrovanie v režime CFB

V prípade, že *s*=1, CFB funguje ako prúdová šifra, ktorá šifruje otvorený text bit po bite.

Použitie režimu CFB v paralelnom šifrovaní je podobné ako to bolo v režime CBC. To znamená, že paralelne šifrovanie možné nie je ale dešifrovanie áno.

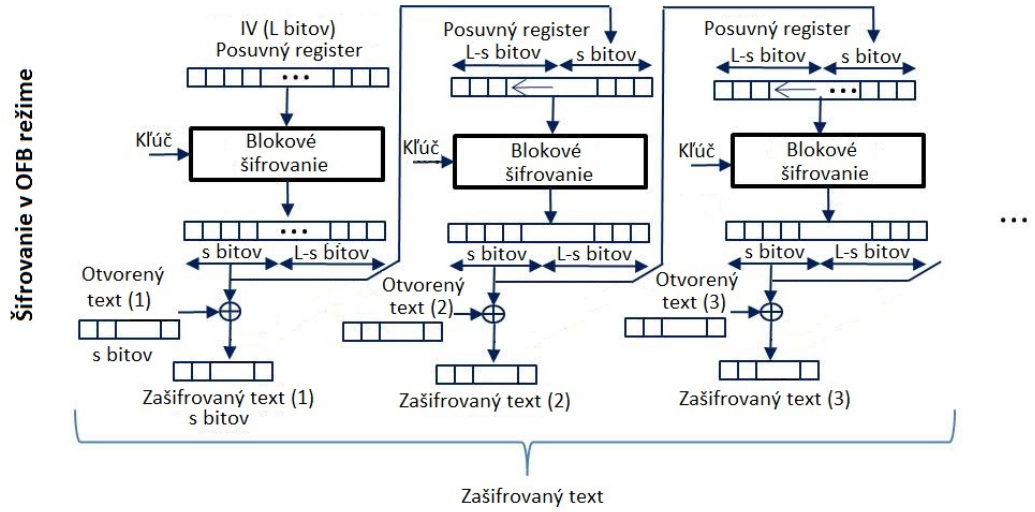
Pokiaľ ide o šírenie chýb, tak jednoduchá chyba v bloku zašifrovaného textu spôsobí chybu v prislúchajúcom bloku dešifrovaného textu ale aj chyby v nasledujúcich dešifrovaných blokoch. Ich počet závisí od počtu bitov spätnej väzby a IV.

Spätná väzba z výstupu, resp. režim OFB (Output Feedback Mode)

Šifra pracujúca v režime OFB pracuje nasledujúcim spôsobom:

Prvým vstupným blokom je inicializačný vektor (IV). Zodpovedajúci vstupný blok je šifrovaný, pričom určitý počet MSB (Most Significant Bits) bitov *s* zašifrovaného bloku sa použije dvoma spôsobmi: ako LSB bity nasledujúceho vstupného bloku a ako sčítanec operácie XOR s *s* bitmi bloku otvoreného textu. Takto sa vytvorí výsledný blok zašifrovaného textu.

OFB je v podstate určitá forma prúdovej šifry. Princíp režimu OFB je ilustrovaný na nasledujúcom obrázku.



Obr. 2.6 Šifrovanie v režime OFB

Je zrejmé, že v tomto režime sa chyby nešíria. Chybne prenesený bit c_j ovplyvní len zodpovedajúci bit dešifrovaného textu p_j.

Hlavnou výhodou tohto režimu je:

+ Ak poznáme IV, je možné vopred vypočítať výstupné bloky ešte pred poznaním otvoreného textu (alebo zašifrovaného textu pri dešifrovaní).

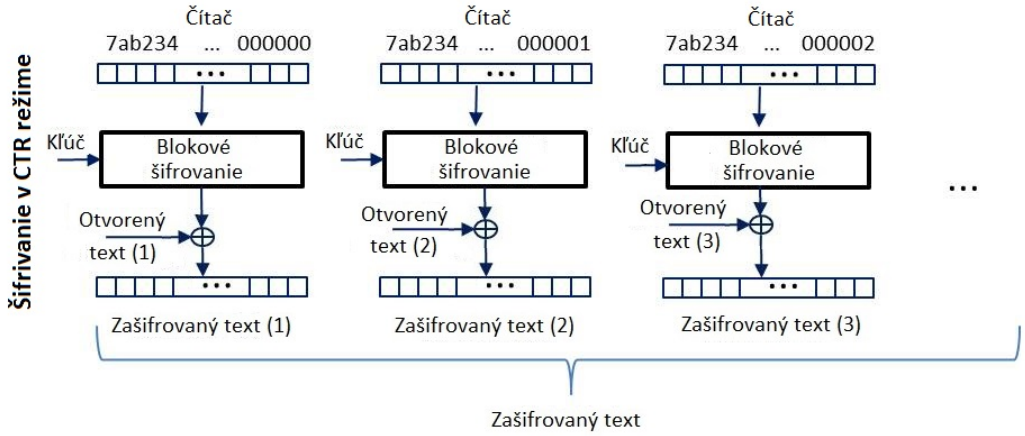
Nevýhody sú nasledovné:

− Šifrovanie ani dešifrovanie nie je možné v paralelnom režime, pretože každý vstupný blok šifrovania závisí od predchádzajúceho zašifrovaného bloku.

Keďže neexistuje šírenie chýb, útočník môže riadiť zmeny vykonané na otvorenom texte a pritom vyhodnocovať zmeny zašifrovaného textu.

Čítačový režim, resp. režim CTR (Counter Mode)

Tento režim je založený na šifrovaní množiny vstupných blokov nazývaných čítače. Výsledné bloky zašifrovaného textu sa získajú vykonaním operácie XOR medzi výstupnými blokmi po šifrovaní a blokmi otvoreného textu. Vo všeobecnosti platí, že počiatočné hodnoty čítačov sú odvodené aplikovaním prírastkovej funkcie. Zvyčajne je čítač rozdelený do dvoch častí: číslo správy a číslo bloku v rámci správy. Je pritom nevyhnutné, aby sa hodnota čítača nikdy neopakovala pri použití rovnakého kľúča. Režim CTR je zobrazený na nasledujúcom obrázku.



Obr. 2.7 Šifrovanie v režime CTR

Chyby sa v tomto režime, podobne ako v režime OFB nešíria. Ak sa hodnota bitu v danom bloku vplyvom prenosu zmení, po dešifrovaní to spôsobí len jednoduchú chybu na rovnakom mieste v zodpovedajúcom bloku.

Hlavné výhody režimu CTR:

+

Je možné paralelne šifrovanie aj dešifrovanie. Neexistuje žiadne prepojenie medzi jednotlivými procesmi.

Predspracovanie je možné, tzn. že funkcia šifrovania sa môže vykonať bez prítomnosti otvoreného textu (podobne pri dešifrovaní).

Hlavná nevýhoda:

−

Podobne ako pri režime OFB, útočník môže vykonávať kontrolované zmeny otvoreného textu.

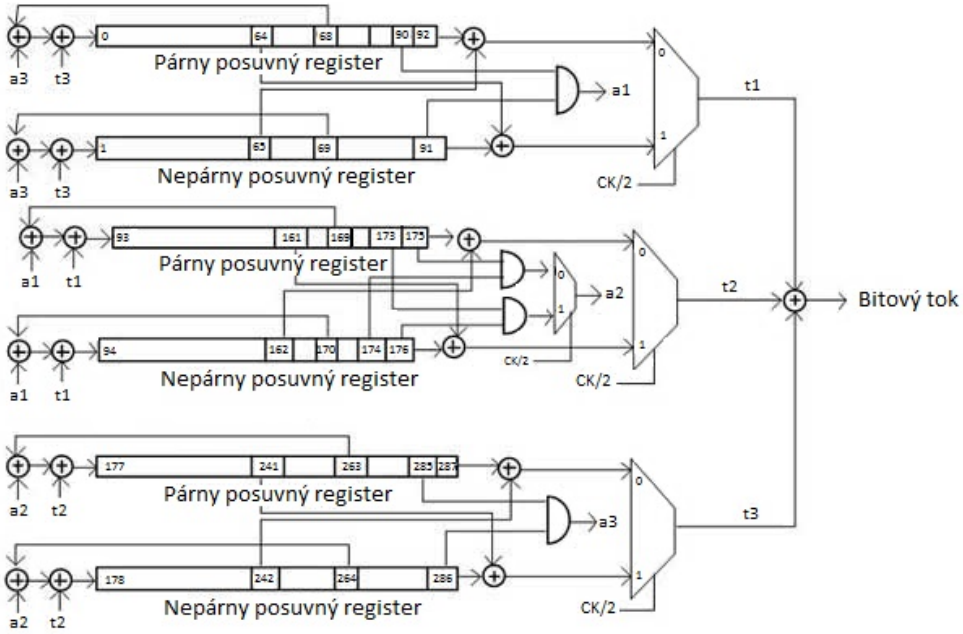
Vyhodnotenie

Režim CBC je najvhodnejší pre šifrovanie bežných súborov alebo paketov. Ak je požadovaná vysoká rýchlosť šifrovania, najlepšou voľbou je režim CTR. V prípade, že chceme zamedziť šíreniu chýb a uvažujeme zašumený prenosový kanál, dobrou voľbou bude OFB režim. A nakoniec, ak počítame s hrozbou mazacieho útoku, použijeme režim CFB a s=8 alebo s=1.

2.2 Algoritmy prúdových šifier

Prúdová šifra je symetrická šifra, ktorá pracuje s časovo premennou transformáciou individuálnych prvkov otvoreného textu. To sa dosiahne určitou operáciou medzi bitmi otvoreného textu a bitmi kľúča. Kľúč je v tomto prípade pseudonáhodná postupnosť (postupnosť, ktorá sa javí útočníkovi ako náhodná). Je produkovaná generátorom, ktorého počiatočný stav je určený tajným kľúčom a verejným parametrom.

Bezpečnosť prúdových šifier je výlučne závislá na pseudonáhodnej postupnosti. Tá musí byť nepredvídateľná, aby sa predišlo úspešným útokom.



Obr. 2.8 Prúdová šifra Trivium

Prúdové šifry sú niekedy menej náročné ako blokové šifry, napr. dĺžka kódu alebo veľkosť čipu. Z toho dôvodu sú atraktívne pre použitie v zariadeniach s obmedzenou veľkosťou, ako napr. mobilné telefóny.

V mnohých oblastiach (napr. internetová bezpečnosť) sú prúdové šifry menej populárne ako blokové šifry. Existuje niekoľko výnimiek. Jednou z týchto výnimiek je prúdová šifra RC4.

Typy prúdových šifier

Na základe vstupných parametrov generuje prúdová šifra pseudonáhodnú postupnosť. V synchrónnej prúdovej šifre je generátor pseudonáhodnej postupnosti

nezávislý od otvoreného alebo zašifrovaného textu. Na druhej strane, prúdová šifra so spätnou väzbou aktualizuje svoj stav na základe predošlých bitov zašifrovaného textu.

Synchrónna prúdová šifra

Synchrónna prúdová šifra je taká prúdová šifra, v ktorej je pseudonáhodná postupnosť generovaná nezávisle na otvorenom alebo zašifrovanom texte. Pseudonáhodná postupnosť je zvyčajne vytváraná generátorom pseudonáhodnej postupnosti. Vstupným parametrom generátora je tajný kľúč celej schémy.

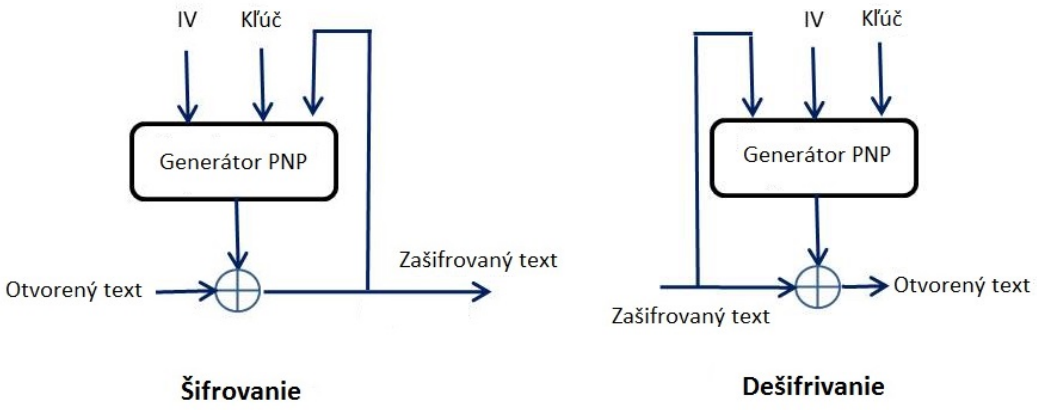
Obr. 2.9 Synchrónna prúdová šifra

Niektoré dôležité vlastnosti synchrónnych prúdových šifier:

- Žiadne šírenie chyby: jednoduchá chyba v c_j ovplyvní len zodpovedajúci prvok otvoreného textu p_j. Prijatá chyba neovplyvní dešifrovanie žiadneho iného prvku.
- Aby sa dosiahlo správne dešifrovanie, odosielateľ aj príjemca potrebujú byť synchronizovaní. Ak sa jeden bit počas prenosu stratí, je potrebná resynchronizácia.

Prúdová šifra so spätnou väzbou

Ak hovoríme o prúdovej šifre so spätnou väzbou resp. asynchrónnej prúdovej šifre, pseudonáhodná postupnosť závisí od tajného kľúča, ale aj od určitého počtu bitov (označme t) zašifrovaného textu (ktoré už boli vytvorené).



Obr. 2.10 Prúdová šifra so spätnou väzbou

Hlavné výhody prúdovej šifry so spätnou väzbou sú nasledovné:

- Spätná väzba: ak sú niektoré bity zašifrovaného textu počas prenosu zmazané alebo zmenené, šifra je schopná automaticky obnoviť správne dešifrovanie po dešifrovaní niekoľkých bitov.
- Limitované šírenie chýb: vplyv jednoduchej chyby je limitovaný. Chyba ovplyvní správne dešifrovanie iba niekoľkých bitov zašifrovaného textu.

3 Kryptografia s verejným kľúčom

Kryptografia s verejným kľúčom bola vyvinutá, aby vyriešila otázku bezpečného prenosu tajného kľúča pri symetrickom šifrovaní. Tento problém sa podarilo vyriešiť použitím dvoch kľúčov namiesto jedného. V tomto procese jeden kľúč slúži na šifrovanie a druhý na dešifrovanie.

Systém je známy ako kryptografia s verejným kľúčom alebo asymetrická kryptografia. Dva kľúče sú známe ako pár kľúčov. V asymetrickej kryptografii je jeden z kľúčov voľne šíriteľný (verejný kľúč). Preto sa táto metóda šifrovania nazýva kryptografia s verejným kľúčom. Druhý kľúč sa nazýva súkromný alebo tajný kľúč. Podľa názvu je zrejmé, že tento kľúč už nie je voľne šíriteľný, ale naopak vlastník ho udržuje v utajení. Vďaka tomu, že medzi kľúčmi jedného páru je určitý matematický vzťah, to čo sa zašifruje verejným kľúčom sa dá dešifrovať len prislúchajúcim súkromným kľúčom a naopak. Je dôležité poukázať na fakt, že odvodiť súkromný kľúč od verejného kľúča je veľmi obtiažne.

Základným nedostatkom kryptografie s verejným kľúčom je, že ak bude mať útočník dostatok času a dostatočný výpočtový výkon, dokáže odvodiť súkromný kľúč od verejného a následne dešifrovať správu. Preto sa volia kľúče o dostatočnej dĺžke (zvyčajne 1024 alebo 2048 bitov). Čím sú použité kľúče dlhšie (dĺžkou sa myslí počet bitov), tým je šifrovací algoritmus odolnejšie voči útokom.

Algoritmy kryptografie s verejným kľúčom sú postavené na matematických problémoch, ktoré v súčasnosti nemajú dostupné riešenie. Pre používateľa je jednoduché vytvoriť pár kľúčov (verejný a súkromný) a použiť ich na šifrovanie a dešifrovanie. Spomínaná obtiažnosť matematických operácií sa ukáže pri pokuse odvodiť súkromný kľúč pri znalosti len príslušného verejného kľúča. Bezpečnosť kryptografie s verejným kľúčom je dosiahnutá týmto spôsobom a sila algoritmu spočíva v uvedenej obtiažnosti. Verejný kľúč teda môže byť zverejnený bez akéhokoľvek bezpečnostného rizika. Bezpečnosť závisí len na utajení súkromného kľúča. Na rozdiel od symetrických šifier, v asymetrickej kryptografii nie je potrebný prvotný bezpečný prenos kľúča medzi komunikujúcimi stranami pred zahájením samotnej komunikácie.

Algoritmy kryptografie s verejným kľúčom sa používajú hlavne na šifrovanie s využitím verejného kľúča a na digitálny podpis. Šifrovanie s využitím verejného kľúča znamená šifrovanie správy za prítomnosti verejného kľúča pričom len osoba, ktorá vlastní príslušný súkromný kľúč má možnosť správu dešifrovať a prečítať. Digitálny podpis je správa, ktorá sa podpíše súkromným kľúčom odosielateľa, pričom môže byť verifikovaná hocikým, kto má prístup k verejnému kľúču odosielateľa. Obidve z týchto aplikácií predstavujú príklady dôvernosti a autorizácie dát s využitím kryptografie s verejným kľúčom.

Asymetrické šifry sú v porovnaní so symetrickými pomalšie. Asymetrické šifry sa často používajú na distribúciu tajného kľúča. Tento tajný kľúč sa následne použije na šifrovanie používateľských dát.

Manažment kľúčov je omnoho jednoduchší v kryptografii s verejným kľúčom v porovnaní so symetrickými šiframi. Existuje však chybná predstava, že manažment kľúčov pomocou kryptografie s verejným kľúčom je jednoduchý.

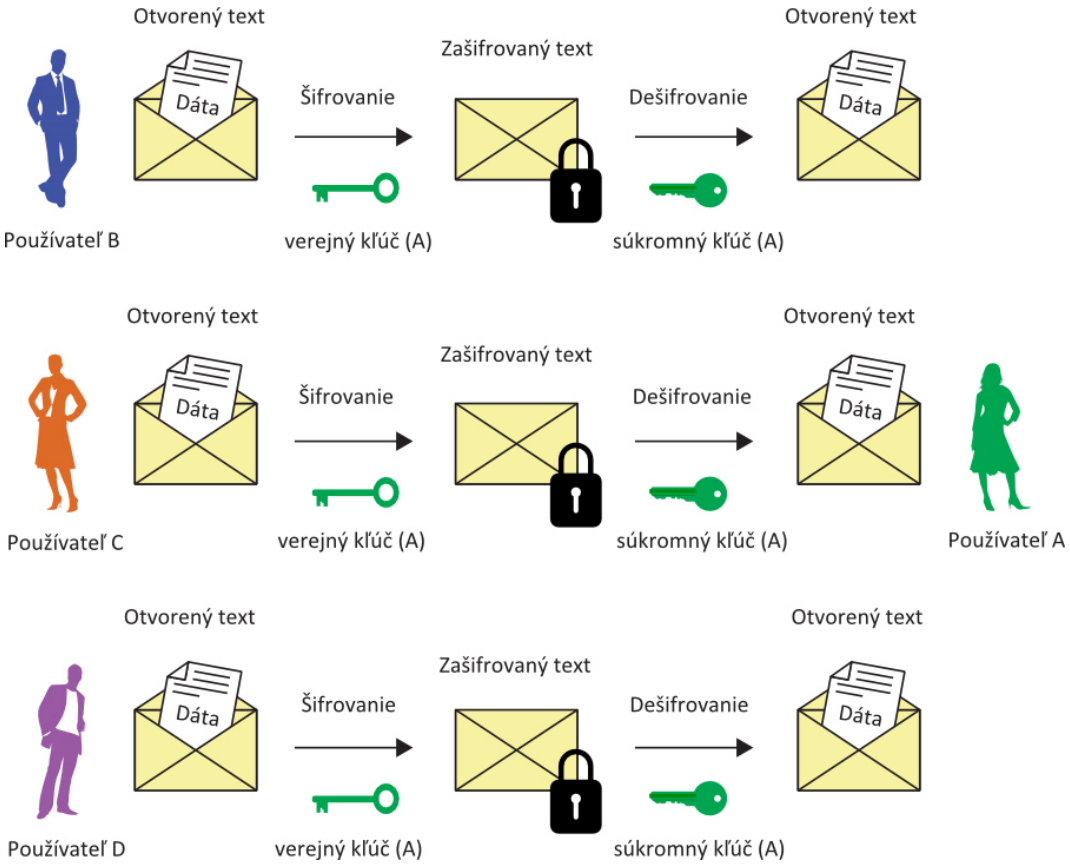
Navyše niektorí používatelia si nesprávne myslia, že kryptografia s verejným kľúčom je bezpečnejšia v porovnaní s kryptografiou s tajným kľúčom. V skutočnosti bezpečnosť ktoréhokoľvek systému závisí od dĺžky kľúča a potrebnej výpočtovej zložitosti vynaloženej na prelomenie šifry.

Najznámejší algoritmus kryptografie s verejným kľúčom je ***RSA***.

3.1 Systém kryptografie s verejným kľúčom

Použitie kryptografie s verejným kľúčom na poskytnutie dôvernosti

Poďme si ukázať príklad, kde Používateľ_B chce odoslať správu Používateľovi_A. Používateľ B zašifruje správu verejným kľúčom Používateľa_A a Používateľ_A dešifruje prijatú správu použitím svojho súkromného kľúča. Keďže medzi verejným a súkromným kľúčom jedného páru je istý matematický vzťah, len súkromný kľúč Používateľa_A dokáže dešifrovať prijatú správu. Ak teda niektorý iný používateľ zachytí zašifrované dáta, nedokáže ich bez daného súkromného kľúča dešifrovať. Táto metóda neposkytuje žiadnu autentifikáciu, či odosielateľ správy bol Používateľ_B, pretože verejný kľúč Používateľa_A je verejne známy. Tento systém však poskytuje garanciu toho, že iba Používateľ_A dokáže správu dešifrovať.

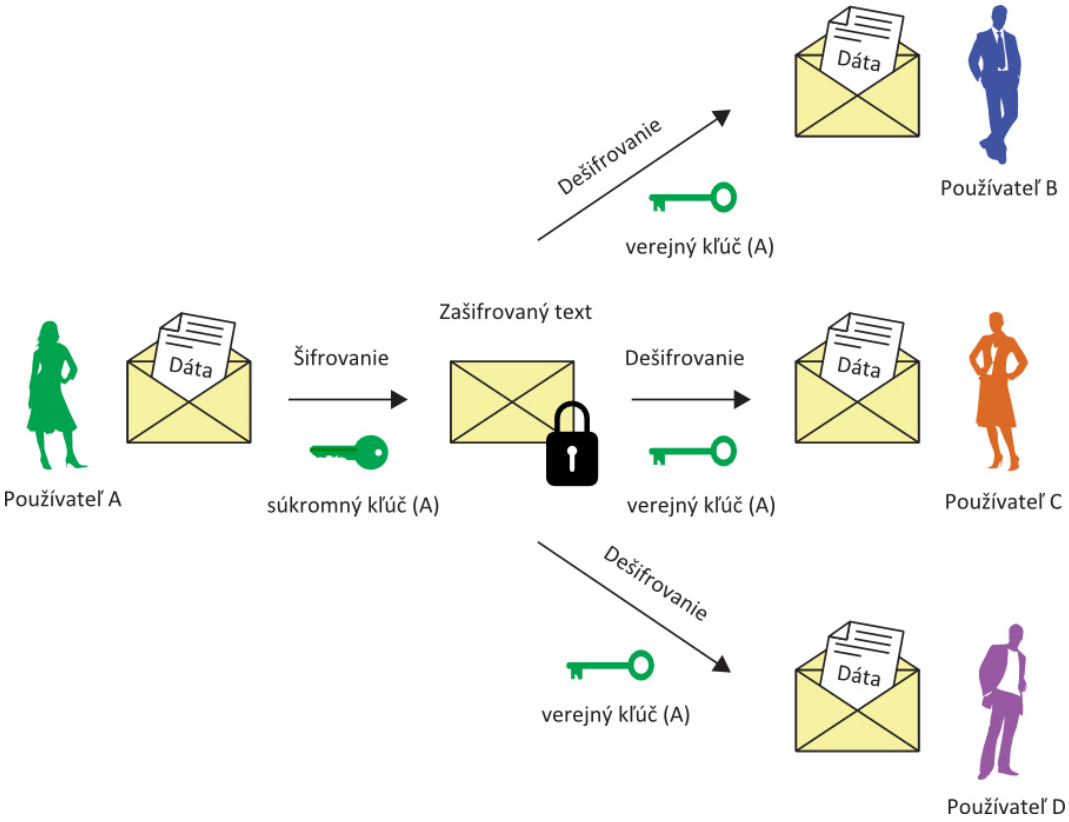


Obr. 3.1 Model kryptografie s verejným kľúčom (poskytnutie dôvernosti obsahu dát)

Táto metóda veľmi jasne ukazuje, že dáta ktoré používateľ odosiela adresátovi, môžu byť zašifrované len verejným kľúčom adresáta a dešifrované jeho súkromným kľúčom, ktorý vlastní iba on. Teda správa môže byť prenesená bezpečne. Odosielateľ a adresát si nemusia vymeniť svoje tajné kľúče ako v algoritmoch symetrických šifier. Celá komunikácia vyžaduje iba verejné kľúče a súkromné kľúče nemusia byť vôbec prenášané alebo zdieľané.

Použitie kryptografie s verejným kľúčom na poskytnutie autentifikácie zdroja informácie (overenia pravosti)

Za účelom autentifikácie musí Používateľ_A zašifrovať správu svojím súkromným kľúčom a Používateľ_B ju dešifruje verejným kľúčom Používateľa_A. Táto metóda poskytuje autentifikáciu zdroja informácie. Neposkytuje dôvernosť informácií, pretože verejný kľúč Používateľa_A je voľne dostupný. Každý, kto ho vlastní môže danú zašifrovanú správu dešifrovať.



Obr. 3.2 Model kryptografie s verejným kľúčom (poskytnutie autentifikácie zdroja dát)

Použitie kryptografie s verejným kľúčom za účelom poskytnutia autentifikácie a dôvernosti

Ak systém vyžaduje zabezpečenie dôvernosti aj autentifikáciu zdroja, Používateľ_B musí zašifrovať otvorený text najprv svojím súkromným kľúčom. Zabezpečí tak autentifikáciu zdroja. Následne Používateľ_B použije verejný kľúč Používateľa_A pri šifrovaní správy. Týmto sa zase zabezpečí dôvernosť komunikácie.

Nevýhoda tohto systému spočíva v dĺžke trvania celého procesu šifrovania a dešifrovania.

4 Hybridný systém: Kombinácia symetrického a asymetrického šifrovania

Nevýhoda ***kryptografie s verejným kľúčom*** (asymetrických šifier) v porovnaní so symetrickými šiframi spočíva vo výraznom ***predĺžení času šifrovania a dešifrovania***. Dôvodom je dĺžka použitého kľúča, ktorá je 1024 až 4094 bitov. ***Symetrické šifry*** sú výrazne ***rýchlejšie***. Používajú dĺžku kľúča 40 až 256 bitov. Na druhej strane, kryptografia s tajným kľúčom musí riešiť problém bezpečného distribuovania kľúča. Obidve tieto techniky môžu byť spoločne použité na vytvorenie dokonalejších metód šifrovania.

Hybridný kryptografický systém používa asymetrické šifry na bezpečný prenos tajného kľúča symetrických šifier. Tajná správa je potom zašifrovaná prijatým tajným kľúčom a následne poslaná príjemcovi. Týmto sa dosiahne bezpečná distribúcia tajného kľúča a kompenzácia nevýhody symetrického šifrovania. Na kódovanie každej odoslanej správy sa používa nový tajný kľúč. Z tohto dôvodu sa niekedy nazýva aj kľúč relácie. To znamená, že ak bude daný kľúč relácie odcudzený (zachytený nepovolanou osobou), útočník bude schopný dešifrovať len správu zašifrovanú týmto kľúčom relácie. Ak by chcel dešifrovať aj ostatné správy, musel by sa zmocniť aj kľúčov ostatných relácií.

Odosielaná správa sa zašifruje kľúčom relácie, ktorý sa následne zašifruje verejným kľúčom príjemcu. Potom je už správa pripravená na odoslanie. Príjemca použije svoj súkromný kľúč na dešifrovanie kľúča relácie a následne použije kľúč relácie na dešifrovanie správy. Mnoho aplikácií využíva takýto systém.

Základné kroky tejto metódy sú:

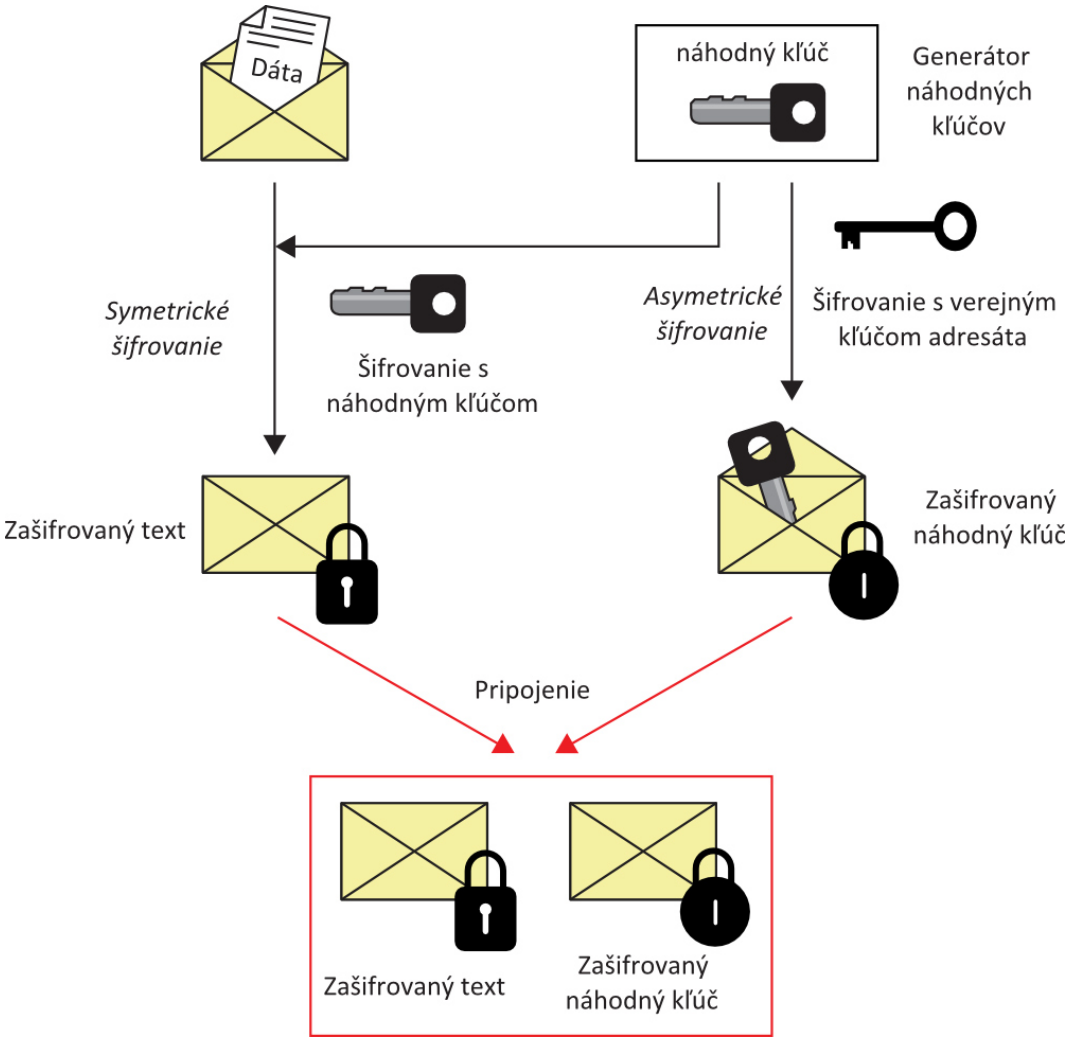
1. Šifrovanie otvoreného textu pomocou symetrickej šifry a náhodného kľúča.

2. Šifrovanie tohto náhodného kľúča verejným kľúčom príjemcu pomocou asymetrického šifrovania. Následne sa pošle zašifrovaný náhodný kľúč príjemcovi. Príjemca teraz môže dešifrovať náhodný kľúč pomocou svojho súkromného kľúča.

3. Nakoniec sa zašlú konkrétne zašifrované dáta. Tieto zašifrované dáta môžu byť dešifrované pomocou kľúča, ktorý bol zašifrovaný verejným kľúčom príjemcu.

Hybridné techniky šifrovania majú rozsiahle využitie. Napríklad pri *Secure Shell* (**SHH**) na zabezpečenie komunikácie medzi klientom a serverom a pri **PGP** (*Pretty good privacy*) na posielanie správ. Najväčšie využitie je pri *Transport Layer Security* (**TLS**), ktoré je najrozšírenejšie pri webových prehliadačoch a webových serveroch na udržanie zabezpečenia komunikácie medzi kanálmi.

Nasledujúci obrázok ilustruje spomínaný proces.



Obr. 4.1 Model hybridného šifrovacieho systému (poskytnutie dôvernosti dát)

5 Hašovacia funkcia

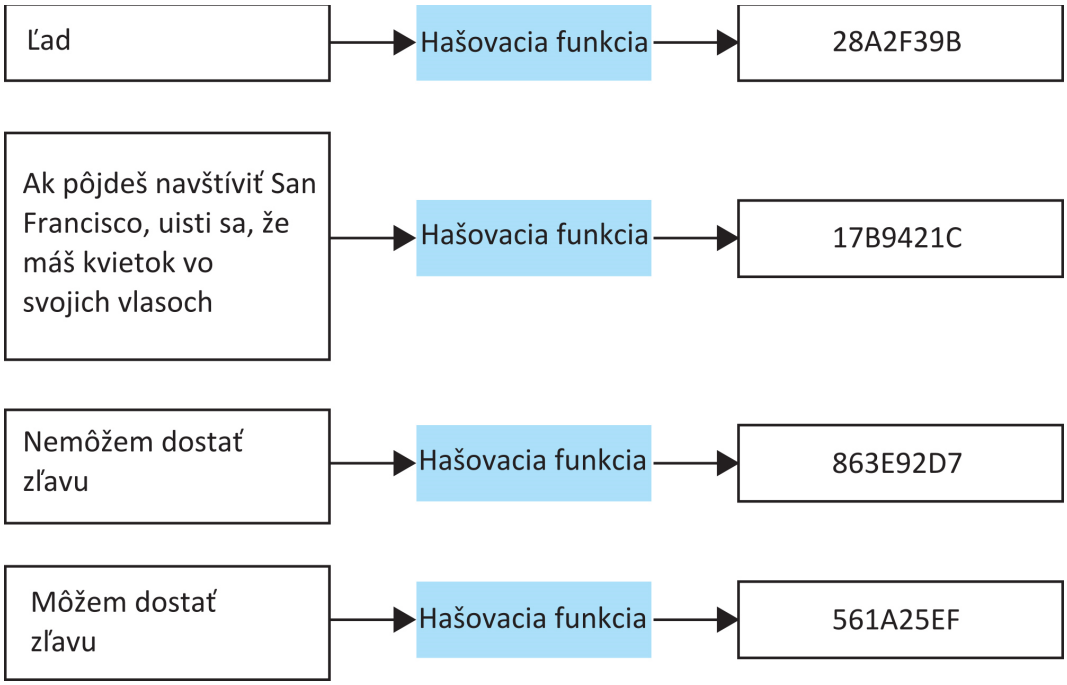
Termín hašovacia funkcia pochádza z počítačovej oblasti, kde označuje funkciu zmenšenia reťazca akéhokoľvek vstupu do reťazca pevnej dĺžky. Akákoľvek zmena vstupných dát spôsobí (s veľkou pravdepodobnosťou) zmenu hodnoty hašovacej funkcie (hašovacieho kódu). Hašovacie funkcie práve s touto vlastnosťou majú vo všeobecnosti rôzne použitie. Ak ich využijeme v kryptografii, tak sa tieto hašovacie funkcie volia tiež v závislosti od niektorých ďalších parametrov. Kryptografické hašovacie funkcie sa používajú na ochranu integrity správ (aby sa ochránil pôvod informácie), ale taktiež aj ako ochrana pred hrozbou odmietnutia (threat of repudiation) a na zabezpečenie hesiel. Na rozdiel od symetrického a asymetrického šifrovania, hašovacia funkcia nepoužíva žiadny kľúč.

Základné požiadavky na hašovaciu funkciu v kryptografii sú:

- vstup s ľubovoľnou dĺžkou,
- výstup s pevnou dĺžkou,
- jednoduchosť výpočtu hašovacieho kódu pre akúkoľvek správu,
- hašovacia funkcia je jednosmerná a z daného hašovaciaho kódu je výpočtovo nemožné dopracovať sa k pôvodnej správe,
- nie je možné akokoľvek zmeniť správu bez zmeny hašovacieho kódu,
- odolnosť voči kolíziám v sieti znamená, že nie je možné nájsť dve rôzne správy ktoré majú rovnaký hašovací kód.

Hašovací kód určuje stručnejšie vyjadrenie pôvodnej dlhšej správy alebo dokumentu. Môže sa zdať, že takéto zhrnutie správy je podobné „digitálnemu odtlačku prsta“ rozsiahlejšieho dokumentu.

Hlavná úloha hašovacej funkcie v kryptografii je v oblasti poskytovania digitálnych podpisov. Navyše hašovací kód môže byť odhalený bez toho, aby sa odhalil dokument z ktorého je odvodený.



Obr. 5.1 Hašovacia funkcia

6 Digitálny podpis

Digitálne podpisy sú jednou z najvýznamnejších prác založených na vývoji kryptografie s verejným kľúčom a poskytujú zabezpečenie, ktoré by bolo zložité implementovať nejakým iným spôsobom. Digitálny podpis je elektronický podpis, ktorý slúži k autentifikácii identity človeka, ktorý posiela správu alebo človeka podpisujúceho dokument s možnosťou zabezpečenia integrity obsahu. Digitálne podpisy sa jednoducho preposielajú a nemôžu byť falšované neoprávnenou osobou.

Digitálne podpisu sú založené na vlastnoručných podpisoch, ktoré sa používajú na určenie vlastníckych práv alebo na potvrdenie daného obsahu správy.

Vlastnoručné podpisy musia disponovať nasledujúcimi vlastnosti:

- ***Podpis je bezpečný*** – podpis by nemal byť napodobňovaný a prípadný pokus o falšovanie podpisu by mal byť ľahko zistený.
- ***Podpis uľahčuje autentifikáciu*** – podpis jednoznačne identifikuje majiteľa, ktorý dokument podpísal bez obmedzenia a vedome.
- ***Podpis je neprenosný*** – podpis je súčasťou dokumentu a neoprávnený vlastník nie je schopný previesť podpis na iný dokument.
- ***Dokument, ktorý je podpísaný nie je možné zmeniť*** – dokument nemôže byť zmenený a upravený po jeho podpísaní.
- ***Podpis nesmie byť odmietnutý*** – majiteľ podpisu nemôže poprieť schválenie podpísaného dokumentu.

V skutočnosti žiadna z týchto vlastností nemôže byť splnená vlastnoručným podpisom. Zároveň všetky tieto vymenované vlastnosti by mali spĺňať digitálne podpisy. Na druhej strane sa taktiež môžu vyskytnúť rôzne problémy spájajúce sa s praktickou realizáciou digitálnych podpisov. Digitálne súbory môžu byť ľahko kopírované čo môže spôsobiť to, že časť dokumentu sa prenesie do iného dokumentu. Z toho vyplýva, že podpísaný dokument môže byť jednoducho upravovaný.

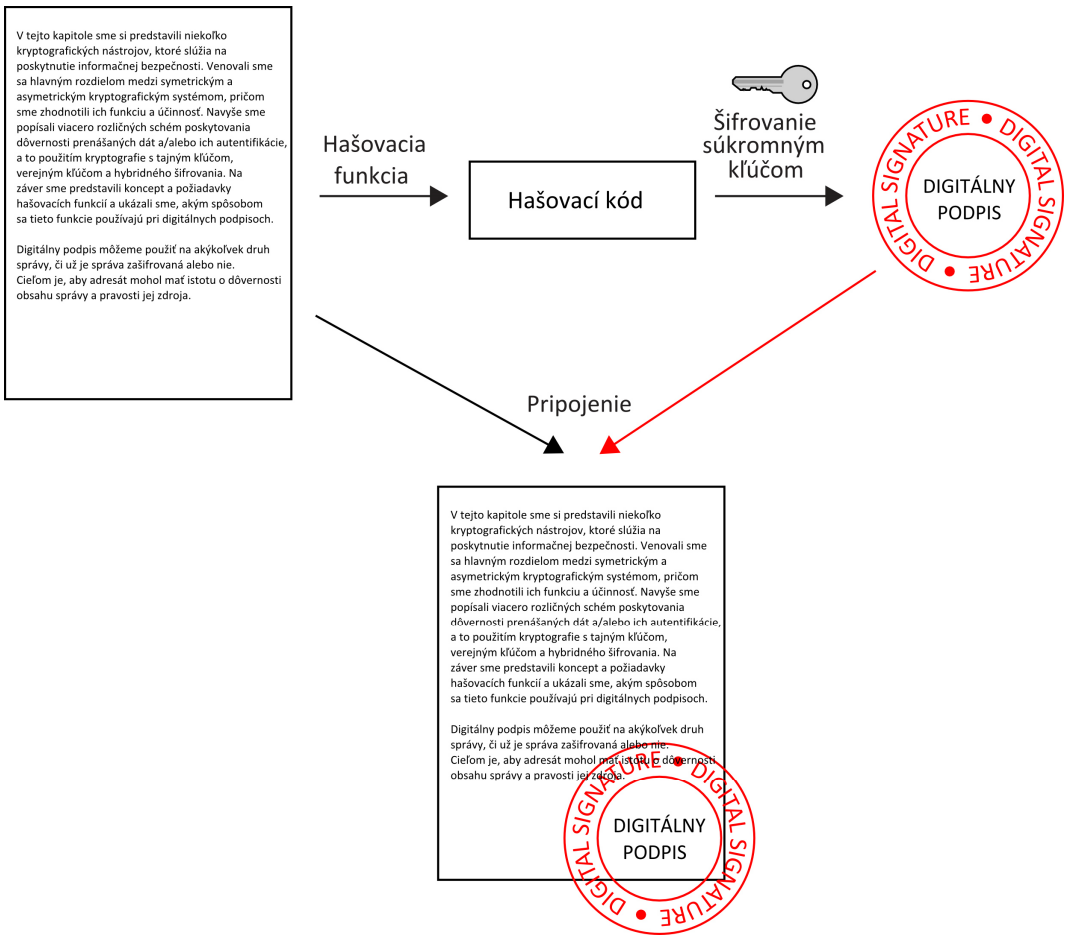
Pre digitálny podpis môžeme formulovať tieto požiadavky:

- Podpis musí mať formu bitovej postupnosti, ktorá ***závisí od podpisovanej správy***.
- Podpis ***musí obsahovať niektoré jedinečné informácie odosielateľa***, aby sa predišlo falšovaniu a popieraniu pravosti.
- ***Realizácia*** digitálneho podpisu musí byť pomerne ***jednoduchá***.
- ***Falšovanie*** digitálneho podpisu musí byť ***výpočtovo nemožné*** tým, že výsledkom útoku bude odlišná správa pre existujúci digitálny podpis alebo falošný digitálny podpis pre danú správu.
- Praktická úschova kópie digitálneho podpisu v pamäti.

Digitálny podpis môže byť použitý s akýmkoľvek druhom správy, či je šifrovaná alebo nie. Jednoducho tak, že príjemca si môže byť istý identitou odosielateľa a tým, že správa dorazila neporušená.

Existuje niekoľko možných schém pre digitálny podpis. Jedna z najpoužívanejších je založená na báze hašovacích funkcií. V tom prípade, ak používateľ chce podpísať dokument musí dodržiavať tieto kroky:

1. Výpočet hašovacieho kódu dokumentu, ktorý má byť podpísaný.
2. Odosielateľ zašifruje hašovací kód svojím súkromným kľúčom, čím dosiahne digitálny podpis (využitie asymetrického šifrovania).
3. Pripojenie digitálneho podpisu k dokumentu.

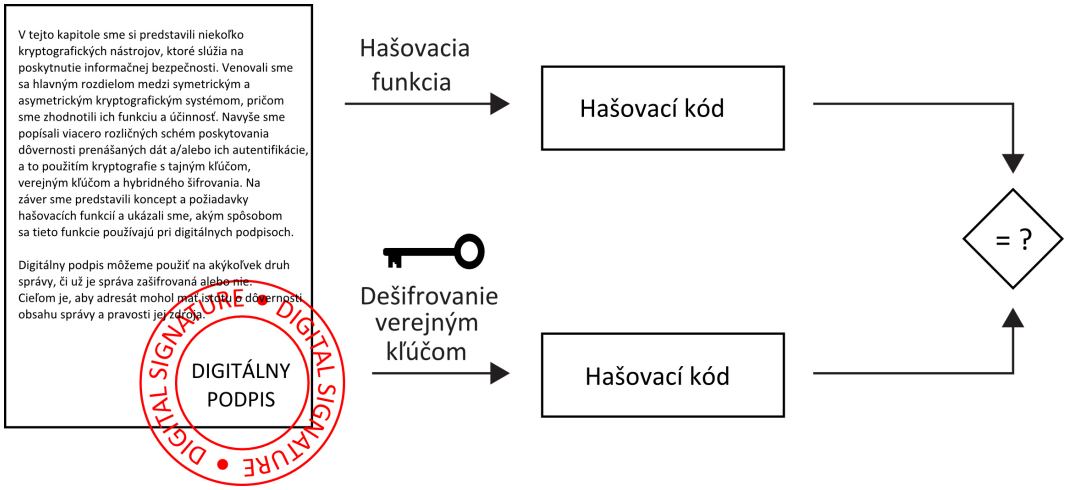


Obr. 6.1 Digitálny podpis na báze hašovacích funkcií

Adresát môže následne overiť pravosť tohto digitálneho podpisu pomocou týchto krokov:

1. Výpočet hašovacieho kódu dokumentu (okrem digitálneho podpisu).
2. Pomocou verejného kľúča odosielateľa príjemca dešifruje digitálny podpis, čím získa hašovací kód vypočítaný odosielateľom.

3. Porovnanie získaných výsledkov v dvoch predchádzajúcich krokoch.



Obr. 6.2 Proces verifikácie dát digitálnym podpisom na báze hašovacích funkcií

V prípade, že hašovacie kódy získané v dvoch krokoch sú rovnaké prijímateľ bude vedieť, že podpísane dáta neboli zmenené.

7 Distribúcia kľúčov. Digitálna certifikácia

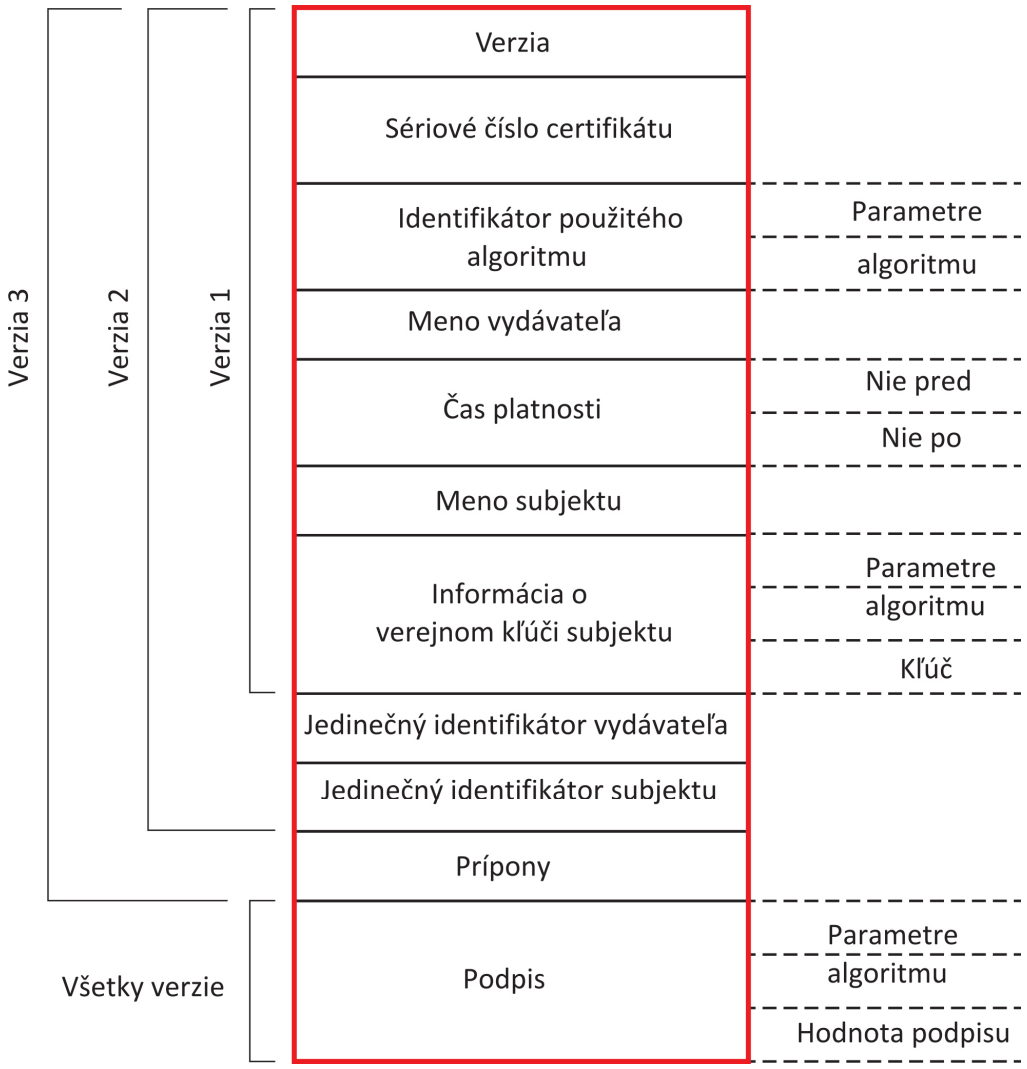
Digitálne podpisy predstavujú jeden z hlavných využití kryptografie s verejným kľúčom. Vhodne implementovaný digitálny podpis dáva dôvod sa domnievať, že aj správa, ktorá bola odoslaná cez nezabezpečený kanál bola odoslaná požadovaným odosielateľom. V mnohých ohľadoch sú digitálne podpisy ekvivalentné k tradičným vlastnoručným podpisom. Správne implementované digitálne podpisy je ťažšie sfalšovať ako ich vlastnoručné ekvivalenty. Za účelom overenia digitálneho podpisu musí mať príjemca znalosť verejného kľúča odosielateľa. Z tohto dôvodu je nevyhnutné použiť určitý mechanizmus distribúcie kľúčov.

Najúčinnejší prístup riešenia daného problému je založený na využití tzv. digitálnych certifikátov, ktoré umožňujú realizáciu výmeny kľúčov (distribúciu kľúčov).

Digitálny certifikát je elektronický dokument, ktorý sa využíva na identifikáciu jednotlivcov, serverov, spoločností a pod. a spája túto identitu s príslušným verejným kľúčom. Zahŕňa digitálny podpis, ***ktorý spája verejný kľúč s identitou*** – informácie ako napríklad meno osoby alebo organizácie, ich adresy a tak ďalej. Pomocou certifikátov sa dá overiť, či verejné kľúče patria konkrétnym osobám. Certifikáty pomáhajú brániť používaniu falošných verejných kľúčov. Iba verejný kľúč overený digitálnym certifikátom bude spolupracovať so zodpovedajúcim súkromným kľúčom entity, ktorá je identifikovaná certifikátom.

Digitálny certifikát je dátová štruktúra, ktorá obsahuje verejný kľúč nejakého subjektu alebo držiteľa certifikátu, identifikačné údaje držiteľa certifikátu, časovú pečiatku spojenú s platnosťou udeleného certifikátu a ďalšie údaje od certifikačnej autority. Táto štruktúra je podpísaná privátnym kľúčom *certifikačnej autority* (**CA**) a každý používateľ je schopný overiť pravosť obsahu certifikátu pomocou verejného kľúča certifikačnej autority. Certifikačné autority sú subjekty, ktoré vydávajú certifikáty a overenia identít.

Nasledujúci obrázok znázorňuje štruktúru digitálneho certifikátu.



Obr. 7.1 Štruktúra digitálneho certifikátu

8 Kyberkriminalita: Úvod

Kyberkriminalita alebo počítačová kriminalita predstavuje akúkoľvek trestnú činnosť zahŕňajúcu počítače a počítačové siete. Môže to siahať od rôznych podvodov až k nevyžiadaným e-mailom (spam). Tieto prípady kriminality zahŕňajú útoky na počítačové dáta a systémy, krádeže identity, distribúciu fotiek detskej pornografie, internetové aukčné podvody, infiltráciu on-line finančných služieb, zavádzanie vírusov, „botnetov“ a rôzne e-mailové podvody, ako je napr. „phishing“.

Jedným z najlepších spôsobov ako sa vyhnúť tomu, aby sme sa stali obeťou počítačovej kriminality, je využitie systému, ktorý používa jednotný systém softvérového a hardvérového zabezpečenia pre overenie všetkých informácií, ktoré sú odoslané alebo prístupné cez Internet.

Počítačová kriminalita je definovaná ako: „Trestný čin, ktorý je vedome spáchaný voči jednotlivcom alebo skupinám osôb so zámerom poškodiť povesť obete alebo spôsobiť jej fyzické alebo psychické poškodenie priamo alebo nepriamo s využitím moderných telekomunikačných sietí ako je Internet a mobilné telefóny (SMS / MMS).“ Tieto trestné činy môžu ohroziť bezpečnosť a ekonomiku štátu. S týmito trestnými činmi súvisí aj napr. porušovanie autorských práv či šírenie detskej pornografie. Taktiež sem patria hrozby úniku citlivých informácií.

Je dôležité si uvedomiť, že rozpoznať každý útok počítačovej kriminality je pred samotným ovplyvnením cieľových subjektov nemožné. Z tohto dôvodu je veľmi dôležité sa zamerať na kybernetickú bezpečnosť, ktorá kladie dôraz na včasné odhalenie a riešenie problému.

Účinný postup reakcie na rôzne incidenty zahŕňa nasledujúce kroky:

- Identifikácia hrozieb, ktoré postihli infraštruktúru.
- Obmedzenie dopadov hrozby. Prevencia v rámci určitej časti infraštruktúry.
- Vyšetrovanie, ktorého cieľom je identifikovať postihnuté systémy a spôsob, akým daný útok prenikol do počítačových systémov.
- Sanácia/obnovenie navrátením IT infraštruktúry späť do on-line režimu. Vyšetrovanie je ukončené.
- Odoslanie a zdieľanie informácií o riešenom probléme vyššiemu manažmentu a zdieľanie údajov o incidente prostredníctvom špecializovaných platforiem, ktoré umožňujú rýchle zdieľanie dát ďalším spoločnostiam.

Žiaľ, popísaný postup je zriedkavo dodržiavaný. Až doteraz boli ochrana a riešenie hrozieb výlučne manuálnym (ľudským) procesom, ktorý zlyhával na ľudskom faktore. Ľudia nereagovali, čím bolo riešenie problémov neefektívne.

9 Techniky útokov

Bezpečnostné útoky možno charakterizovať ako rôzne druhy systematických aktivít zameraných na zníženie alebo poškodenie bezpečnosti. Z tohto pohľadu môže byť útok definovaný ako systematická hrozba generovaná subjektom úmyselným a inteligentným spôsobom. Počítačové siete môžu byť vystavené mnohým rizikám ako napríklad:

- Sociálne inžinierstvo, kde sa niekto pokúsi získať prístup prostredníctvom sociálnych prostriedkov (predstierať, že je oprávnený používateľ systému alebo správca, podvádzať ľudí odhaľovaním tajomstva, atď.).

- Vojenské vytáčanie, kde niekto používa počítačový softvér a modem na vyhľadávanie stolových počítačov, ktoré sú vybavené modemami a ktoré na vytáčanie reagujú a odpovedajú. Poskytujú potenciálnu cestu do podnikovej siete.

- Útoky odmietnutie služby, vrátane všetkých typov útokov, ktoré majú infiltrovať počítače alebo siete takým spôsobom, že legitímni používatelia počítačov alebo siete ich nebudú schopní použiť.

- Útoky na báze protokolov, ktoré využívajú známe (alebo neznáme) slabé stránky sieťových služieb.

- Hostiteľské útoky, ktoré napádajú zraniteľné miesta v niektorých operačných systémoch alebo to ako je systém nastavený a ako sa spravuje.

- Hádanie hesla. Heslá sú sekvencie znakov zvyčajne spojené s používateľským menom, ktoré poskytujú mechanizmus na identifikáciu a autentifikáciu konkrétneho používateľa. Samotní používatelia si môžu zvoliť heslá takmer vo všetkých počítačoch. To kladie bremeno zabezpečenia na koncových používateľov, ktorí buď nevedia alebo sa nestarajú o vhodné bezpečnostné postupy. Vo všeobecnosti platí, že heslá ktoré sa jednoducho pamätajú sú slabé a je pomerne jednoduché ich uhádnuť. Útočníci majú niekoľko možností na uhádnutie hesiel a na ich prelomenie.

- Odpočúvanie každého druhu, vrátane odcudzenia e-mailových správ, súborov, hesiel a iných informácií prostredníctvom odpočúvania sieťového pripojenia.

Bezpečnostné útoky možno rozdeliť do týchto dvoch kategórií:

- pasívne útoky,

- aktívne útoky.

9.1 Pasívne útoky

Pasívne útoky sa pokúšajú zistiť alebo využiť rôzne informácie zo systému, ale nemajú snahu o určitý zásah do systémových prostriedkov. Pasívny útok je taký útok, v ktorom útočník komunikačný kanál iba sleduje. Pasívny útočník ohrozuje iba dôvernosť dát.

Pasívne útoky sa zameriavajú na odpočúvanie alebo sledovanie komunikačného prenosu. Cieľom je získať informáciu, ktorá sa prenáša.

Pasívne útoky delíme do dvoch základných tried:

- Odpočúvanie. Všeobecne platí, že väčšina sieťovej komunikácie prebieha v nezabezpečenej forme. To umožňuje útočníkovi, ktorý získal prístup do siete „počúvať“, resp. sledovať komunikáciu medzi dvoma stranami. Odpočúvanie siete je všeobecne najväčší bezpečnostný problém, ktorému musia administrátori v podnikoch čeliť. Bez zabezpečenia prenášaných informácií kryptografickými systémami je hrozba odpočúvania veľmi veľká.

- Analýza prevádzky. V tomto prípade nejde len o pozorovanie správ, ale aj ich zachytenie a podrobenie analýze. Cieľom analýzy je získať akékoľvek informácie zo zachytenej prevádzky. Analýza prevádzky môže byť účinná aj v prípade, že správy sú zašifrované a nemožno ich dešifrovať. Všeobecne platí, že čím väčší je počet pozorovaných (zachytených) správ, tým sa zvyšuje aj možnosť odhalenia ich významu.

9.2 Aktívne útoky

Aktívne útoky slúžia na zmenu systémových prostriedkov alebo ovplyvňujú ich prevádzku. Tento typ útoku sa používa, ak útočník chce zmazať, pridať alebo pozmeniť prenášaný signál. Aktívny útočník ohrozuje integritu a autentifikáciu dát, podobne ako aj ich dôvernosť.

Aktívne útoky zahŕňajú niekoľko modifikácií a môžu byť rozdelené do šiestich kategórií:

- Maškaráda (masquerade). Je to typ útoku v ktorom útočník predstiera, že je autorizovaný používateľ, aby získal prístup k systému alebo vyšším právomociam.

- Opakovanie (replay). V tomto type útoku je originálny prenos podvodne opakovaný alebo oneskorený. To sa vykoná útočníkom, ktorý zachytí originálny prenos dát a znovu dáta odošle (pravdepodobne ako časť útoku maškaráda).

- Modifikácia obsahu správy. Útočník odstráni správu zo sieťovej prevádzky, upraví jej obsah a znova ju vráti.

- Človek v strede (*Man in the Middle* (**MitM**)). Pri tomto druhu útoku útočník zachytáva komunikáciu medzi dvoma zúčastnenými stranami, zvyčajne medzi koncovým používateľom a webovou stránkou za účelom zneužitia informácie na predstieranie oprávnenej osoby alebo iný typ útoku.

- Odopretie služby (*Denial of Service* (**DoS**)) a distribuované odopretie služby (*Distributed Denial of Service* (**DDoS**)). Útok odopretia služby je útok, v ktorom je používateľ (alebo organizácia) zbavený konkrétnej poskytovanej služby, ktorú má za normálnych okolností poskytovanú. V útoku distribuované odopretie služby veľký počet spreneverených systémov (niekedy nazývaných „botnet [http://searchsecurity.techtarget.com/definition/botnet] “) útočí na jeden cieľ.

- Pokročilá pretrvávajúca hrozba (*Advanced Persistent Threat* (**APT**)). Je to sieťový útok, v ktorom neautorizovaná osoba získa prístup k sieti, kde ostáva bez povšimnutia dlhú dobu. Zámerom APT útoku je ukradnúť dáta radšej ako spôsobiť výpadok siete alebo organizácie. APT útoky sa používajú na získavanie veľmi cenných informácií ako napr. v sekcii národnej obrany, výroby a finančného sektora.

10 Prevencia

Prevencia proti počítačovej kriminalite môže byť priama – ak sa vyzbrojení len trochou technickej podpory dokážeme vyhnúť mnohým útokom. Všeobecne platí, že on-line útočníci sa snažia zarobiť peniaze tak rýchlo a ľahko ako je to len možné. Čím viac im sťažíme ich prácu, tým väčšia je pravdepodobnosť, že sa stiahnu a presunú na ľahší cieľ. Pravdepodobne najlepšou obranou je byť koncovým používateľom. Čím menej rizika na seba berieme, tým nižšia je pravdepodobnosť, že budeme obeťou počítačového útoku. Nižšie uvedené typy poskytujú základné informácie o tom ako zabrániť on-line podvodom.

- Udržiavajte počítačový systém s najnovšími aktualizáciami. Ak sa objaví chyba, predajcovia zvyčajne poskytujú aktualizácie softvéru. Jedným z najlepších spôsobov, ako udržať útočníkov v bezpečnej vzdialenosti od zariadenia, je použiť aktualizáciu softvéru hneď ako je dispozícii. Väčšina produktových dokumentácií ponúka spôsob ako získať nové aktualizácie. Niektoré aplikácie skontrolujú dostupné aktualizácie automaticky. V opačnom prípade je nevyhnutná manuálna kontrola ich dostupnosti. V každom prípade tým, že pravidelne aktualizujeme softvér počítača, zablokujeme útočníkom možnosť využiť softvérové chyby (zraniteľnosti), ktoré by inak mohli využiť na vniknutie do systému. To, že udržiavame softvér počítača aktualizovaný, nezaručuje ochranu pred všetkými útokmi ale sťažuje prácu hackerov, blokuje mnoho základných a automatických útokov a môže odradiť menej rozhodnutého útočníka.

- Uistite sa, že je počítač správne nakonfigurovaný. Inštalácia systému hneď po vybalení z krabice a ponechanie ho s predvolenou konfiguráciou je pravdepodobne jednou z najčastejších chýb, ktoré ľudia robia pri nastavovaní siete. Ak je počítač nainštalovaný, je dôležité venovať pozornosť nielen tomu aby systém fungoval, ale zamerať sa na to, aby fungoval správne. Predvolená konfigurácia má často štandardnú správu účtov a hesiel, čo vedia útočníci po celom svete. Konfigurácia internetových aplikácií ako webový prehliadač a e-mailový softvér je jednou z najdôležitejších oblastí, na ktoré sa musíte zamerať.

- Zvoľte si silné heslá a udržujte ich v bezpečí. Heslá sú často použité v systéme ako jediná ochrana. Používateľské ID je iba meno a neprechádza verifikáciou, pričom heslo je spojené s ID používateľa a funguje ako identifikátor. Brány a systémy detekcie prelomenia systému neznamenajú nič, ak sú vaše heslá nezabezpečené. Silné heslo je to, ktoré sa nenachádza v žiadnom slovníku. Taktiež to znamená heslo, ktoré nie je jednoduché odcudziť.

- Chráňte počítač bezpečnostným softvérom. Niekoľko typov bezpečnostného softvéru vrátane ochrannej brány a antivírusu sú nevyhnutné pre základnú ochranu v reálnom čase. Ochranná brána je softvérový alebo hardvérový produkt, ktorý zobrazuje informácie prichádzajúce a opúšťajúce počítač tak aby zabezpečil, že neexistuje žiadny neoprávnený prístup k počítaču a týmto spôsobom poskytuje prvú líniu obrany. Ďalšou líniou obrany je mnohokrát antivírusový softvér, počítačový program, ktorý môže byť použitý na skenovanie súborov, identifikáciu a odstránenie počítačových vírusov a ďalšieho škodlivého softvéru (malwaru). Presnejšie povedané vírus je

program, ktorý sa môže replikovať sám a je určený na šírenie sa z jedného počítača do druhého. Robí veci tak, aby o tom koncový používateľ nevedel a/alebo s danými zmenami nesúhlasil. Malware je širší pojem, skratka pre škodlivý softvér, pričom existuje veľa rôznych foriem vrátane vírusov, trójskych koňov, keyloggerrov, červov, adwarov, spywarov.

- Chráňte svoje osobné údaje. Autorizácia používateľa sa stáva veľkým problémom bezhotovostných transakcií a bankových služieb. V kyberkriminalite sa útočníci snažia o nelegálny prístup k dátam o osobnom bankovom účte, kreditnej karte, debetnej karte a k ďalším citlivým informáciám používateľa, ktoré chcú útočníci využiť na svoje finančné obohatenie. To môže viesť k značným finančným stratám a dokonca aj „pošpiniť“ úverovú históriu obete. Preto je pri zdieľaní osobných informácií ako je meno, adresa, telefónne číslo a e-mailová adresa, nutná opatrnosť. Avšak ak chcete využiť rad služieb poskytovaných on-line, budete musieť poskytnúť svoje osobné údaje za účelom fakturácie a dodania zakúpeného tovaru.