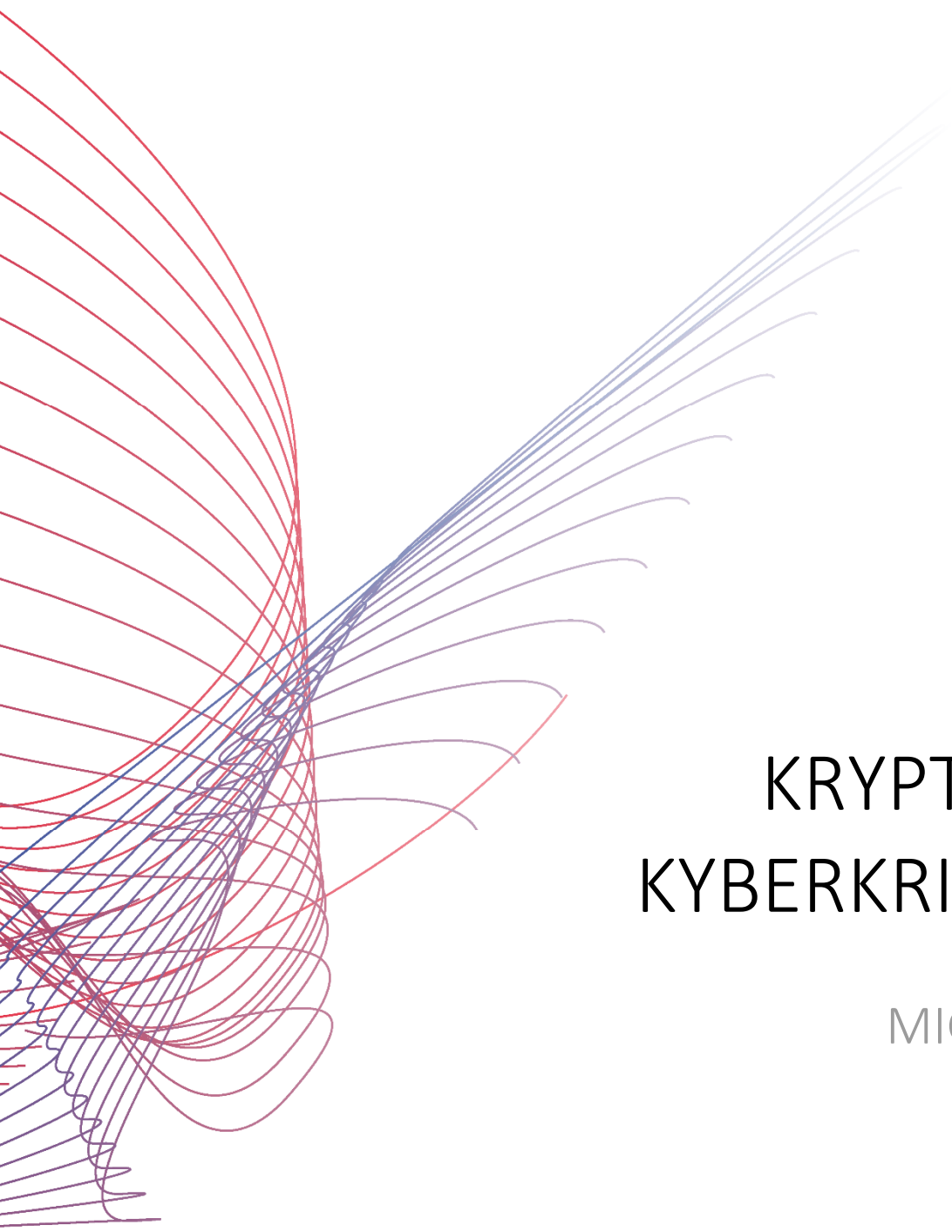
en cs de sk es

TECH pedia



KRYPTOGRAFIE, KYBERKRIMINALITA

MIGUEL SORIANO

Název díla: Kryptografie, kyberkriminalita
Autor: Miguel Soriano
Přeložil: Pavel Bezpalec
Vydalo: České vysoké učení technické v Praze
Fakulta elektrotechnická
Kontaktní adresa: Technická 2, Praha 6
Tel.: +420 224352084
Tisk: (pouze elektronicky)
Počet stran: 39
Edice (vydání): 1. vydání, 2017

ISBN 978-80-01-06201-2

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

Erasmus+

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací odpovídá výlučně autor.
Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Vysvětlivky

	Definice
	Zajímavost
	Poznámka
	Příklad
	Shrnutí
	Výhody
	Nevýhody

ANOTACE

Tento modul obsahuje základní informace z oboru kryptografie a kyberkriminality.

CÍLE

Tento modul poskytuje informace o kryptografii a kyberkriminalitě v jejich základním kontextu. První část kurzu je navržena tak, aby seznámila studenty s fundamentálními možnostmi kryptografie pro zajištění informační bezpečnosti. Z toho důvodu jsou v kurzu popsány dva základní typy kryptografie a to kryptografie s tajným a kryptografie s veřejným klíčem. Druhá část kurzu se věnuje konceptu kyberkriminality a klasifikuje různé druhy útoků. V závěru text popisuje možnosti prevence před takovými útoky.

LITERATURA

[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 Kryptografie v základním kontextu

Kryptografie představuje silný matematický nástroj, který slouží k ochraně informací v počítačových systémech. Základní operace kryptografie, šifrování a dešifrování, využívá mnoho bezpečnostních aplikací. Citlivá data mohou být díky kryptografii bezpečně přenášena prostřednictvím telekomunikačních sítí bez hrozby neoprávněného zachycení a rozluštění obsahu dat. Šifrování je možné definovat jako proces, po kterém se informace stává nerozluštitelná a zbytečná pro všechny kromě určených příjemců zprávy. Dešifrování představuje inverzní proces k šifrování, tedy jedná se o převod dat zpět do své původní podoby.

Technika kryptografie se využívá v našem každodenním životě. Např. při telefonování, platbě kreditní nebo debetní kartou, výběru peněz z bankomatu, přihlašování se pomocí hesla do počítačových systémů, atd. Kryptografie umožňuje ukládání citlivých informací nebo jejich přenos přes nezabezpečené sítě (jako např. internet) tak, že nikdo kromě určeného příjemce nedokáže přečíst jejich obsah. Kryptografie se stala průmyslovým standardem pro poskytování informační bezpečnosti, důvěrnosti, kontroly přístupu k různým zdrojům a elektronickým transakcím. Na druhou stranu je třeba dodat, že kryptografie sama o sebe není dostatečný prostředek na zabezpečení všech potenciálních hrozeb narušení informační bezpečnosti.

Kryptografický algoritmus, nazývaný též šifra, je jednoduchá posloupnost určitých procesů, které zabraňují šifrování a příslušné dešifrování. Šifra je matematická operace speciálně navržená tak, aby zakryla, resp. znemožnila odhalit obsah dat. Nejúčinnější šifrovací algoritmy pracují s kombinací více klíčů. V případě použití různých klíčů může být stejný otevřený text změněn na různé podoby zašifrovaného textu. Spolehlivý kryptografický algoritmus musí zabezpečit, aby nevznikla možnost získání původního otevřeného textu bez znalosti klíče. Samozřejmě existuje též metoda tzv. hrubé síly, která zkouší všechny možné klíče, dokud nenajde ten správný. Statisticky se správný klíč najde s vysokou pravděpodobností již v první polovině všech zkoušek. Bezpečnost kryptografického systému je ve všeobecnosti postavená na dvou věcech: síle kryptografického algoritmu a utajení klíče.

Počet všech možných klíčů musí být tak velký, že je výpočetně nemožné se současnými prostředky odhalit klíč v rozumném čase. Mnoho šifer zvyšuje svoji bezpečnost vzrůstající délkou klíče. Avšak čím je délka klíče větší, tím je proces výpočetně náročnější, a tedy narůstá i doba šifrování a dešifrování. Proto je důležité vybrat algoritmus na základě porovnání mezi stupněm ochrany a výpočetní náročností algoritmu.

Moderní kryptografické algoritmy mohou být klasifikované podle dvou kritérií: typu klíče a podle způsobu, jakým pracují s daty.

Podle typu klíče se kryptografické algoritmy dělí na:

a) Kryptografie s tajným klíčem (symetrická kryptografie). Symetrická kryptografie představuje kryptografické metody, při kterých odesílatel

i příjemce používají stejný klíč na šifrování i dešifrování. (Méně známé jsou metody, při kterých jsou jednotlivé klíče různé, ale dají se poměrně lehce odvodit jeden z druhého). Šifrovací standard AES (Advanced Encryption Standard) je příkladem široce používaného konvenčního symetrického šifrovacího systému.

b) Kryptografie s veřejným klíčem (asymetrická kryptografie) využívá dvojici klíčů: veřejný klíč na šifrování dat a odpovídající soukromý (tajný) klíč na jejich dešifrování. Je zřejmé, že mezi oběma klíči je matematický vztah, nicméně je výpočetně nemožné z privátního klíče odvodit klíč soukromý. Uživatel nebo část systému zveřejňuje svůj veřejný klíč, přičemž soukromý klíč si ponechává v bezpečí. Každý, kdo získá veřejný klíč, může informaci šifrovat, avšak k původní otevřené zprávě se nedostane. Jen osoba, která vlastní odpovídající soukromý klíč může zašifrovaná data dešifrovat.

Hlavní výhoda kryptografie s veřejným klíčem spočívá v tom, že odesílatel a příjemce nepotřebují sdílet tajný klíč přes předem vytvořený zabezpečený kanál; celá komunikace vyžaduje jen přítomnost veřejného klíče, který se může přenášet i přes nezabezpečený kanál.

Podle způsobu, jakým pracuje algoritmus s daty, mohou být šifry klasifikovány jako:

a) Blokové šifry, které pracují s bloky dat, množinou bitů s pevně danou délkou, se stejnými operacemi pro všechny bloky. Zpráva se rozdělí na menší bloky, které se postupně šifrují. Bloková šifra se považuje za bezpečnou, jestliže se všechny bloky otevřeného textu bezpečně transformují na bloky šifrovaného textu; kryptoanalýze by měl odolat každý blok stejně. Avšak jsou-li šifrovány různé zprávy stejným klíčem, potom stejné bloky dat se transformují vždy na stejné bloky zašifrovaného textu. Útočník může tak jednoduše odhalit opakující se bloky ve zprávě. Z toho důvodu se použití blokové šifry v takovém režimu nedoporučuje, přičemž se využívají jiné, bezpečné režimy.

b) Proudové šifry transformují jeden symbol otevřeného textu přímo na jeden symbol zašifrovaného textu. Transformace je založená na generování pseudonáhodné posloupnosti, která představuje proud bitů šifrovacího klíče. Tento proud bitů ve spojení s otevřeným textem slouží k zašifrování jednoho bitu nebo bajtu v jednom časovém okamžiku. Takovým způsobem se vytvoří konečný zašifrovaný text.

Základní terminologie:

- Otevřený text je zpráva, která má být vyslána a doručena adresátovi.
- Zašifrovaný text je výstup kryptografického systému, který vznikne zašifrováním otevřeného textu.
- Šifrování je proces změny obsahu otevřeného textu za účelem skrytí přenášené informace.

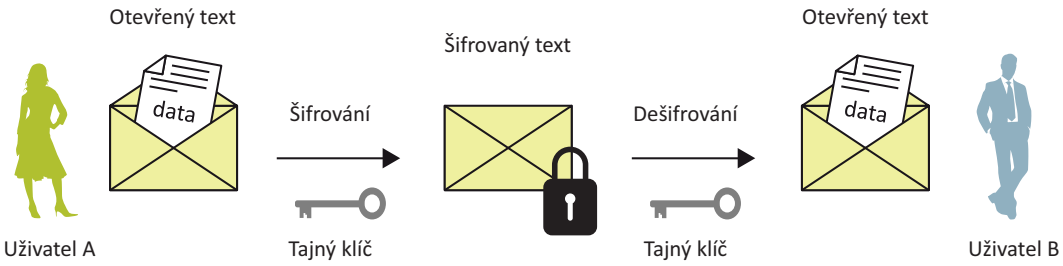
- Dešifrování je inverzní operace k šifrování; je to proces zpětného získání zprávy ve formě otevřeného textu z její zašifrované podoby (zašifrovaného textu). Tento proces teda transformuje zašifrovaný text na otevřený text.
- Klíč je slovo, číslo, nebo posloupnost, která se používá na šifrování otevřeného textu nebo dešifrování zašifrovaného textu.
- Kryptoanalýza je vědní disciplína, která se zaobírá metodami pro rozkódování zašifrovaných zpráv bez znalosti tajného klíče.
- Hash funkce je algoritmus, který transformuje text o libovolné délce na text s fixní délkou.
- Šifra je kryptografický algoritmus, tzn. matematická funkce, která se používá na šifrování a dešifrování.
- Správa klíčů zahrnuje procesy, jakými se klíče vytvářejí, ukládají, chrání, přenáší, čtou, zapisují, používají a ničí.

2 Kryptografie s tajným klíčem

Proces šifrování a dešifrování informace použitím jednoho klíče je znám pod pojmem kryptografie s tajným klíčem nebo symetrická kryptografie. V symetrické kryptografii mohou být klíče použity pro šifrování a dešifrování stejně (běžný případ), nebo je mezi nimi jednoduchý matematický vztah (méně používané algoritmy). Hlavní nedostatek takového systému spočívá v nutnosti výměny klíčů před samotnou komunikací. To souvisí s vytvořením bezpečného komunikačního kanálu pro výměnu klíčů.

Obě strany musí chránit klíč; zveřejnění klíče kteroukoli stranou může mít za následek ohrožení informací.

Proces činnosti kryptografie s veřejným klíčem je následující: Uživatel A chce poslat zprávu uživateli B, přičemž chce zabezpečit, aby jen uživatel B mohl přečíst obsah zprávy. Pro zajištění přenosu uživatel A generuje tajný klíč, šifruje zprávu a odesílá ji uživateli B. Uživatel B potřebuje tajný klíč, aby mohl zprávu dešifrovat. Uživatel A využije jeden z nabízených způsobů doručení tajného klíče adresátovi B. Po té, co uživatel B přijme tajný klíč, může dešifrovat zprávu, čímž získá její původní obsah.



Obr. 2.1 Model kryptografie s tajným klíčem

Každý šifrovací algoritmus musí splnit následující požadavky:

- Rozptyl (diffusion): každý bit otevřeného textu ovlivní mnoho bitů zašifrovaného textu.
- Konfuze (confusion): je nevyhnutelné předejít jakémukoli vztahu mezi otevřeným a zašifrovaným textem (speciálně linearitě), na kterých mohou být založeny známé útoky.
- Zašifrovaný text by měl mít podobu náhodně vypadajícího textu a mít dobré statistické vlastnosti.
- Jednoduchost (simplicity).
- Efektivita (efficiency): extrémně rychlý na různých platformách.

Hlavním problémem symetrické kryptografie je, že proces přenosu tajného klíče adresátovi může způsobit bezpečnostní riziko. Přenos tajného klíče prostřednictvím internetu (např. e-mailem) není bezpečný. Klíč předávaný verbální komunikací přes telefonní sítě, které mohou být odposlouchány je taktéž riskantní. Podobně klasická pošta podstupuje riziko možného odchytu a sledování zásilek.

Bezpečnostní rizika kryptografie s tajným klíčem do značné míry odstraňuje kryptografie s veřejným klíčem. Symetrická kryptografie se často používá na šifrování dat při ukládání na pevné disky. Osoba, která šifruje data vlastní klíč a nevzniká žádný problém s jeho distribucí.

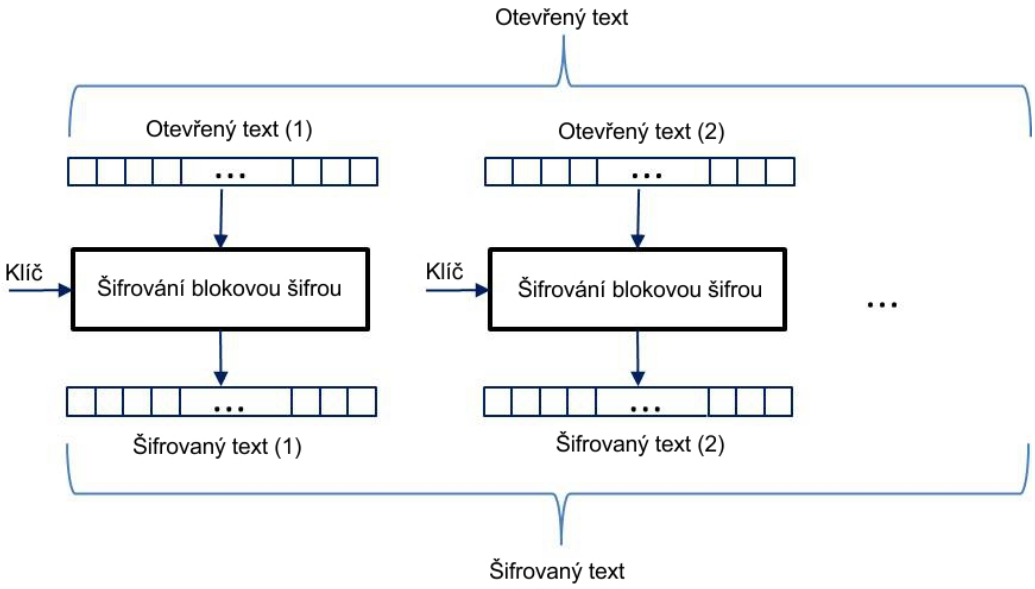
Jako bylo uvedeno v předcházející kapitole, významné dělení v rámci kryptografie s tajným klíčem je na kryptografii, která využívá blokové šifry a kryptografii s proudovými šiframi. V dnešní době se těší oblibě hlavně blokové šifry.

2.1 Algoritmy blokových šifier

Blokové šifry transformují skupinu symbolů otevřeného textu na skupiny symbolů zašifrovaného textu. Takže jde o šifrování realizované blok po bloku otevřeného textu.

Symboly otevřeného textu se seskupí do bloků a šifrovací algoritmus se aplikuje na každý z nich (za přítomnosti tajného klíče). Výsledkem šifrování jednoho bloku otevřeného textu je blok zašifrovaného textu o stejné velikosti.

Může nastat případ, že velikost otevřeného textu nebude celočíselným násobkem velikosti bloku. V takovém případě se obvykle používá tzv. "padding-scheme" pro zaplnění posledního bloku. V závislosti na provozním režimu šifry nemusí být zaplnění bloku potřeba. Princip šifrování a dešifrování blokové šifry je zobrazen na následujícím obrázku.



Obr. 2.2 Model blokových šifer

Většina blokových šifer pracuje v iteračním režimu. To znamená, že šifrování se vykonává pomocí více opakování jednotlivých procesů. Jedno vystřídání všech procesů se nazývá runda. Každá runda opakuje sérii operací za přítomnosti jedinečného klíče, odvozeného z originálního vstupního klíče. Operace v každé rundě obvykle sestávají z: substituce, permutace a expanze klíče. Takovéto šifry se nazývají Substitučně-permutační sítě (SPN, Substitution-Permutation Networks) nebo Feistelovy šifry. Substituce je často jedinou nelineární částí mnoha šifer, a proto se substituční boxy (S-boxy) vybírají velmi starostlivě, aby byla šifra odolná proti případným kryptoanalytickým útokům.

Dešifrování probíhá obdobným způsobem. Za přítomnosti stejného klíče, který byl použit při šifrování (symetrické šifry) se stejné operace vykonají na zašifrovaném

textu, který je na začátku rozdělen opět do stejných bloků. Výsledkem tohoto procesu jsou bloky dešifrovaného otevřeného textu.

Typické velkosti bloků otevřeného a zašifrovaného textu jsou 64 nebo 128 bitů.

Výhody blokových šifer:

- vysoký rozptyl,
- odolnost vůči neoprávněnému pozměňování obsahu: složitost vkládání symbolů bez detekce.

Mezi nejpoužívanější algoritmy blokových šifer patří:

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

Použití stejného klíče při šifrování stejných částí otevřeného textu se nedoporučuje. V takovém případě by se všechny stejné bloky otevřeného textu transformovaly na všechny stejné bloky zašifrovaného textu. Informace o znalosti opakování určitých bloků může dopomoci kryptoanalýze, a proto existují víceré metody jako tomu předejít. Tyto metody se nazývají režimy blokových šifer.

Režimy blokových šifer

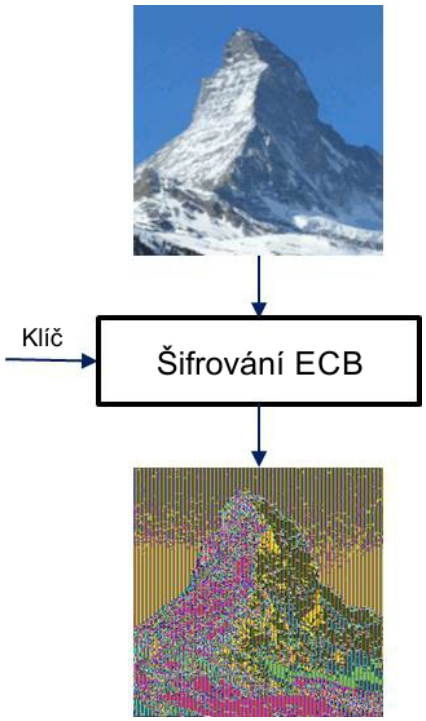
Blokové šifry se mohou použít různým způsobem s rozdílným utajením a vlastnostmi opravy chyb. Výběr režimu má vliv na rychlost, bezpečnost a šíření chyb daným algoritmem.

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

Tento režim představuje základní algoritmus blokové šifry bez jakékoli modifikace. Zpráva se rozdělí do bloků a každý blok otevřeného textu je šifrován jednotlivě, nezávisle na ostatních. Tedy neexistuje žádná závislost mezi bloky, v důsledku čeho se tento režim nedoporučuje. Použití tohoto režimu přináší několik nevýhod:

- Struktura otevřeného textu zůstává odkrytá.
- Citlivost na útok modifikováním obsahu: reorganizování uspořádání bloků nebo opakování některých bloků může způsobit změnu obsahu zprávy.
- Libovolný zašifrovaný text zašifrovaný stejným klíčem může být použit jako zdrojový materiál pro útočníka.

Klasický příklad nevýhody použití režimu ECB je šifrování rastrového obrázku (např. s příponou .bmp). I přes použití silného, bezpečného algoritmu, algoritmus v režimu ECB nedokáže efektivně zastínit obsah zprávy.

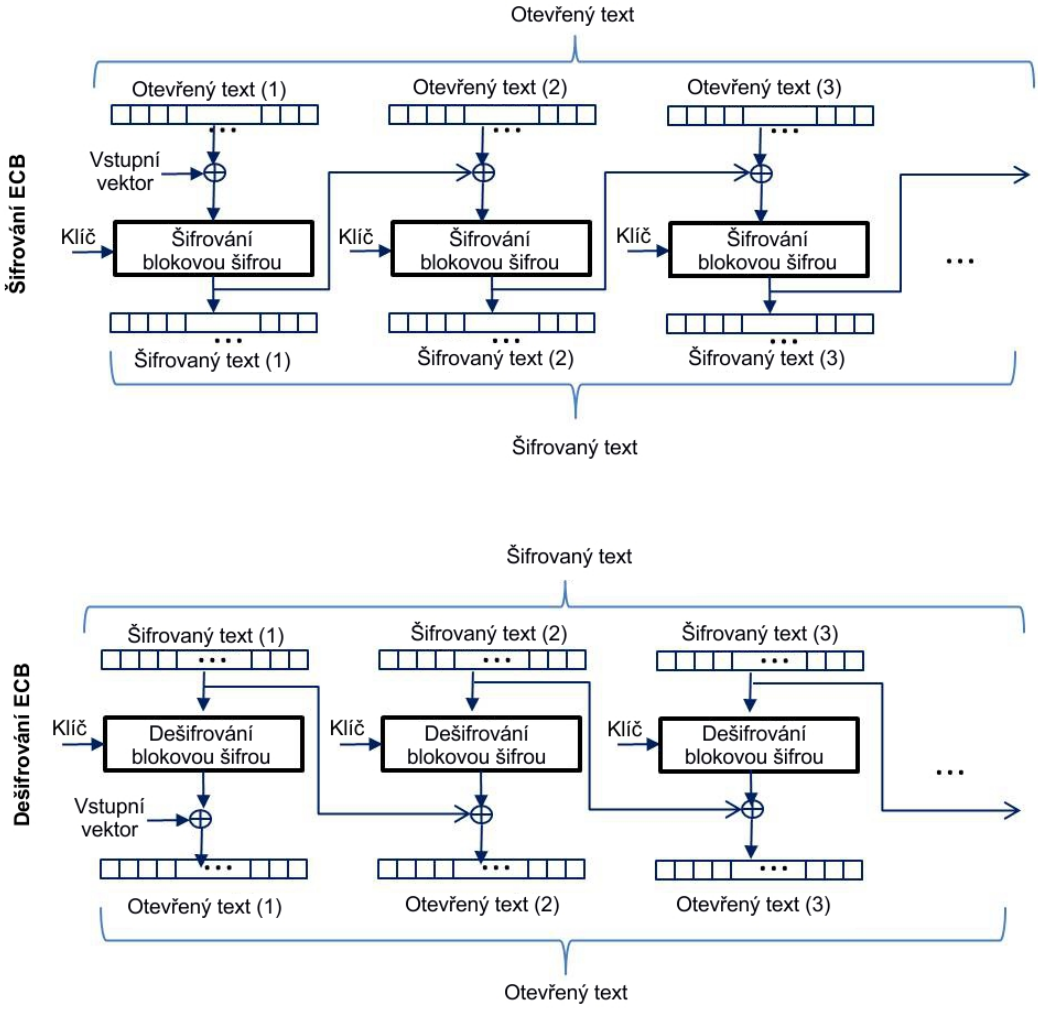


Obr. 2.3 Šifrování rastrového obrázku v režimu ECB

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

Režim CBC kombinuje (“řetězí”) bloky otevřeného textu s předcházejícími zašifrovanými bloky. Na to je potřeba inicializační vektor IV, který se podrobí operaci s prvním blokem otevřeného textu.

V procesu šifrování se použije operace XOR prvního bloku otevřeného textu a IV ještě před samotným šifrováním. Výsledek je následně zašifrován a výstupem je první blok zašifrovaného textu. Pro následující bloky je inicializačním vektorem zašifrovaný text předcházejícího bloku. Výsledkem zřetězení je, že blok zašifrovaného textu c_j je závislý na bloku otevřeného textu p_j a předcházejícího bloku zašifrovaného textu c_{j-1}. Z toho je zřejmé, že blok zašifrovaného textu c_j teda závisí na aktuálním a všech předcházejících blocích otevřeného textu.



Obr. 2.4 Šifrování a dešifrování v režimu CBC

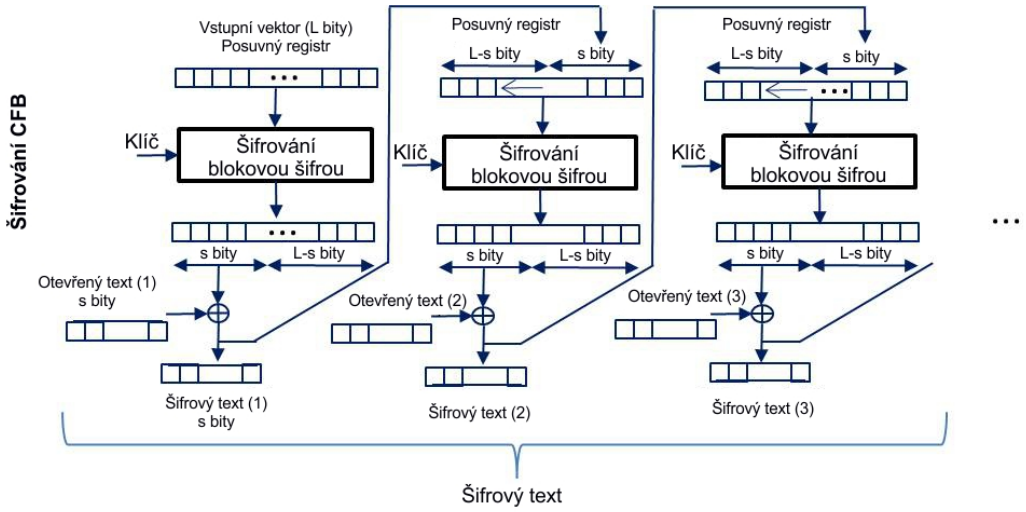
Režim CBC odstraňuje nedostatky ECB, ale přináší dvě nevýhody:

- Není možné paralelní šifrování: šifrování bloku p_{j+1} před nebo během šifrování bloku p_j, protože blok cj ještě není vytvořen. Na druhé straně, paralelní dešifrování možné je; blok otevřeného textu p_j požaduje bloky c_j a c_{j-1}.
- Šíření chyby. Chyba jen v jednom bitu (jednoduchá chyba) se během přenosu bloku c_j při dešifrování promítne nejen jako chyba v bloku p_j, ale i jako chyba v p_{j+1}. Na druhé straně chyba vždy ovlivní jen jeden bit v bloku p_{j+1}. Tento efekt se nazývá limitované šíření chyby (limited error-propagation).

Zpětná vazba ze zašifrovaného textu, resp. režim CFB (Cipher Feedback)

CFB je režim utajení, který je vybaven zpětnou vazbou po sobě jdoucích bloků zašifrovaného textu do vstupních bloků otevřeného textu. Zašifrovaný text se vytvoří operací XOR mezi bloky zpětné vazby a bloky otevřeného textu. Důležitým parametrem v tomto režimu je také celé číslo s, pro které platí $1 \leq s \leq L$, kde L je délka celého bloku.

Prvním vstupním blokem je inicializační vektor IV. Jednoduše řečeno, proces šifrování v režimu CFB je možno brát jako vstup *L* nejméně významných bitů předcházejícího IV spojený s *s* bity předcházejícího bloku zašifrovaného textu, který se následně šifruje. Výsledný zašifrovaný text vzniká operací XOR mezi *s* nejvýznamnějšími bity bloku po šifrování a *s* bity odpovídajícího bloku otevřeného textu. Tento proces je zobrazen na následujícím obrázku.



Obr. 2.5 Šifrování v režimu CFB

V případě, že *s*=1, CFB funguje jako proudová šifra, která šifruje otevřený text bit po bitu.

Použití režimu CFB v paralelním šifrování je podobné jako to bylo v režimu CBC. To znamená, že paralelní šifrování možné není, přičemž dešifrování ano.

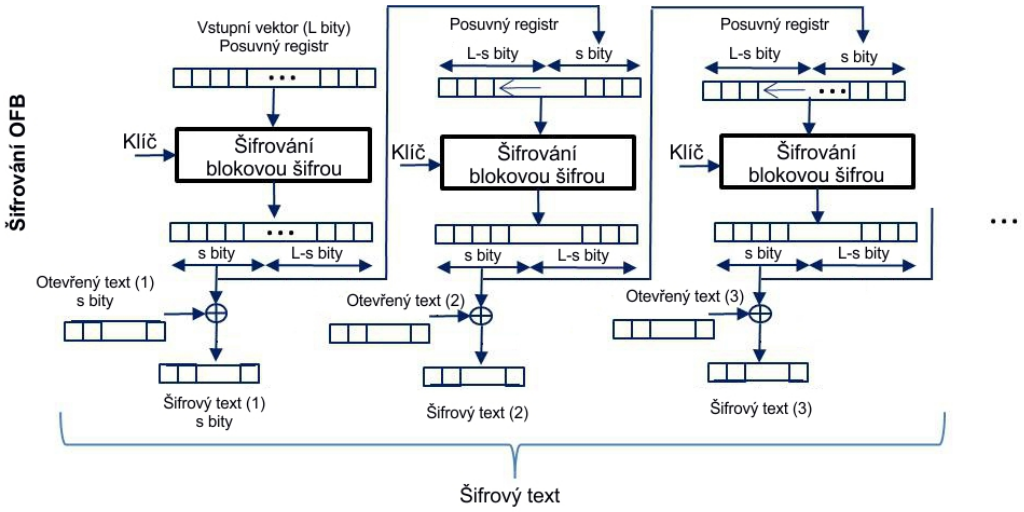
Pokud jde o šíření chyb, jednoduchá chyba v bloku zašifrovaného textu způsobí chybu v příslušném bloku dešifrovaného textu, ale i chyby v následujících dešifrovaných blocích. Jejich počet závisí na počtu bitů zpětné vazby a IV.

Zpětná vazba z výstupu, resp. režim OFB (Output Feedback Mode)

Šifra v režimu OFB pracuje následujícím způsobem:

Prvním vstupním blokem je inicializační vektor (IV). Odpovídající vstupní blok je šifrován, přičemž určitý počet MSB (Most Significant Bits) bitů *s* zašifrovaného bloku se použije dvěma způsoby: jako LSB bity následujícího vstupního bloku a jako sčítanec operace XOR s *s* bity bloku otevřeného textu. Takto se vytvoří výsledný blok zašifrovaného textu.

OFB je v podstatě určitá forma proudové šifry. Princip režimu OFB je zobrazen na následujícím obrázku.



Obr. 2.6 Šifrování v režimu OFB

Je zřejmé, že v tomto režimu se chyby nešíří. Chybně přenesený bit c_j ovlivní jen odpovídající bit dešifrovaného textu p_j.

Hlavní výhodou tohoto režimu je:

+ Známe-li IV, je možno předem vypočítat výstupní bloky ještě před poznáním otevřeného textu (nebo zašifrovaného textu při dešifrování).

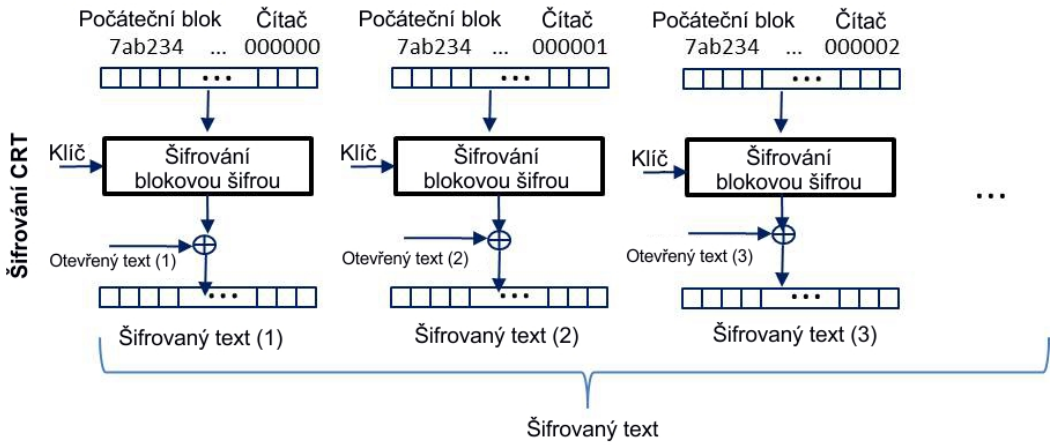
Nevýhody jsou následující:

− Ani šifrování ani dešifrování není možné v paralelním režimu, protože každý vstupní blok závisí na předcházejícím zašifrovaném bloku.

Vzhledem k tomu, že neexistuje šíření chyb, může útočník řídit změny vykonané na otevřeném textu a přitom vyhodnocovat změny zašifrovaného textu.

Čítačový režim, resp. režim CTR (Counter Mode)

Tento režim je založen na šifrování množiny vstupních bloků nazývaných čítače. Výsledné bloky zašifrovaného textu se získají vykonáním operace XOR mezi výstupními bloky po šifrování a bloky otevřeného textu. Ve všeobecnosti platí, že po inicializaci čítače jsou následující hodnoty čítače odvozeny aplikováním přírůstkové funkce. Obvykle je čítač rozdělen do dvou částí: číslo zprávy a číslo bloku v rámci zprávy. Je přitom nevyhnutelné, aby se hodnota čítače nikdy neopakovala při použití stejného klíče. Režim CTR je zobrazen na následujícím obrázku.



Obr. 2.7 Šifrování v režimu CTR

Chyby se v tomto režimu, podobně jako v režimu OFB nešíří. Jestliže se hodnota bitu v daném bloku vlivem přenosu změní, po dešifrování to způsobí jen jednoduchou chybu na stejném místě v zodpovídajícím bloku.

Hlavní výhody režimu CTR:

+

Je možné paralelní šifrování i dešifrování. Neexistuje žádné propojení mezi jednotlivými procesy.

Předzpracování není možné, funkce šifrování se může vykonat bez přítomnosti otevřeného textu (podobně při dešifrování).

Hlavní nevýhoda:

−

Podobně jako u režimu OFB může útočník vykonávat kontrolované změny otevřeného textu.

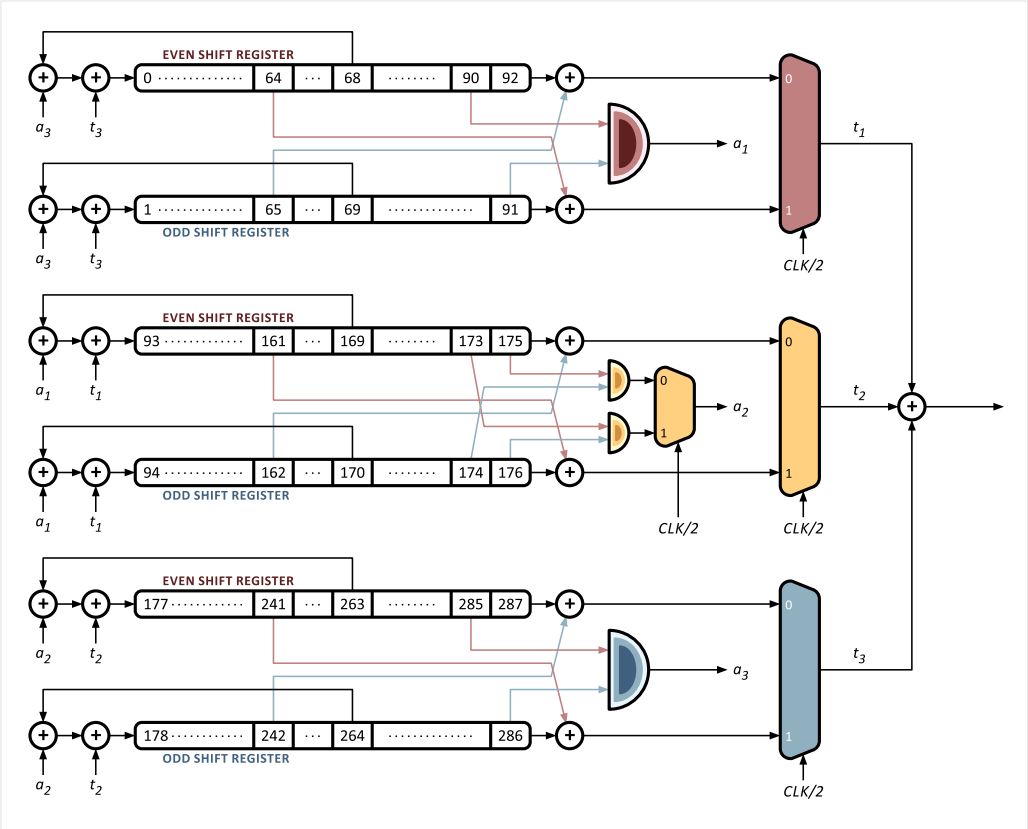
Vyhodnocení

Režim CBC je nejvhodnější pro šifrování běžných souborů nebo paketů. Je-li požadována vysoká rychlost šifrování, je nejlepší volbou režim CTR. V případě, že chceme zamezit šíření chyb a uvažujeme zašuměný přenosový kanál, dobrou volbou bude OFB režim. A nakonec, počítáme-li s hrozbou mazacího útoku, použijeme režim CFB a s=8 nebo s=1.

2.2 Algoritmy proudových šifer

Proudová šifra je symetrická šifra, která pracuje s časově proměnnou transformací individuálních prvků otevřeného textu. Toho se dosáhne matematickou operací mezi bity otevřeného textu a bity klíče. Klíč je v tomto případě pseudonáhodná posloupnost (posloupnost, která se jeví útočníkovi jako náhodná) produkovaná konečným automatem, jehož počáteční stav je určený tajným klíčem a veřejným parametrem.

Bezpečnost proudových šifer je výlučně závislá na pseudonáhodné postupnosti. Ta musí být nepředvídatelná, aby se předešlo úspěšným útokům.



Obr. 2.8 Proudová šifra Trivium

Proudové šifry někdy požadují méně zdrojů jak blokové šifry, např. délka kódu, nebo velikost čipu. Z tohoto důvodu jsou atraktívní pro použití v zařízeních s omezenou velikostí, jako např. mobilní telefony.

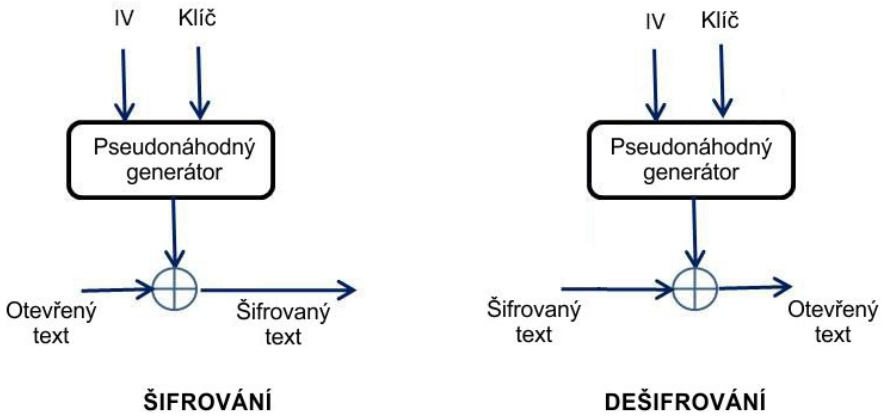
V mnoha oblastech (např. internetová bezpečnost) jsou proudové šifry méně populární než blokové šifry. Existuje však několik výjimek. Jednou z nich je proudová šifra RC4.

Typy proudových šifer

Proudová šifra generuje následující prvky proudu dat na základě interního stavu. V synchronní proudové šifře je mechanismus aktualizace vnitřního stavu aktualizován nezávisle na otevřeném nebo zašifrovaném textu. Naopak proudová šifra se zpětnou vazbou aktualizuje svůj stav na základě předešlých bitů zašifrovaného textu.

Synchronní proudová šifra

Synchronní proudová šifra je taková proudová šifra, v které je pseudo-náhodná posloupnost generovaná nezávisle na otevřeném nebo zašifrovaném textu. Pseudo-náhodná posloupnost je obvykle vytvářená generátorem pseudo-náhodné postupnosti. Vstupním parametrem generátoru je tajný klíč celého schématu.



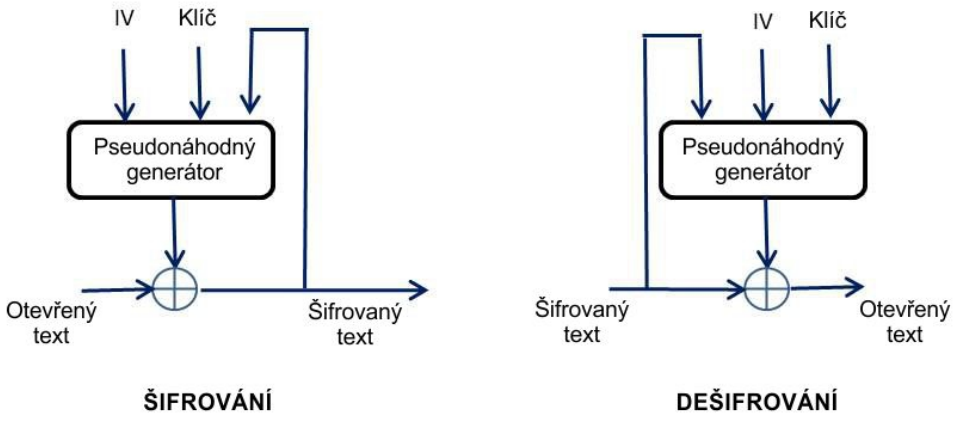
Obr. 2.9 Synchronní proudová šifra

Některé důležité vlastnosti synchronních proudových šifer:

- Žádné šíření chyby: jednoduchá chyba v c_j ovlivní jen odpovídající prvek otevřeného textu p_j. Přijatá chyba neovlivní dešifrování žádného jiného prvku.
- Aby se dosáhlo správného dešifrování, potřebují být odesílatel i příjemce synchronizováni. Jakmile se ztratí jeden bit v průběhu přenosu, je potřeba resynchronizace.

Proudová šifra se zpětnou vazbou

Hovoříme-li o proudové šifře se zpětnou vazbou, resp. asynchronní proudové šifře, závisí pseudo-náhodná posloupnost na tajném klíči, ale i na určitém počtu bitů (označme t) zašifrovaného textu (které už byly vytvořeny).



Obr. 2.10 Proudová šifra se zpětnou vazbou

Hlavní výhody proudové šifry se zpětnou vazbou jsou následující:

- Zpětná vazba: jsou-li smazány či změněny některé bity zašifrovaného textu během přenosu, je šifra schopna automaticky obnovit správné dešifrování po dešifrování několika znaků.
- Omezené šíření chyb: vliv osamocené chyby je omezený. Tato chyba ovlivní správné dešifrování pouze po několik znaků zašifrovaného textu.

3 Kryptografie s veřejným klíčem

Kryptografie s veřejným klíčem byla vyvinuta proto, aby vyřešila otázku bezpečného přenosu tajného klíče při symetrickém šifrování. Tento problém se podařilo vyřešit použitím dvou klíčů místo jednoho. V tomto procesu jeden klíč slouží na šifrování a druhý na dešifrování.

Tento systém je známý jako kryptografie s veřejným klíčem nebo asymetrická kryptografie. Tyto dva klíče jsou známy jako pár klíčů. V asymetrické kryptografii je jeden z klíčů volně šiřitelný (veřejný klíč). Proto se tato metoda šifrování nazývá kryptografie s veřejným klíčem. Druhý klíč se nazývá soukromý nebo tajný klíč. Podle názvu je zřejmé, že tento klíč už není volně šiřitelný, ale naopak, vlastník ho udržuje v utajení. Díky tomu, že mezi klíči jednoho páru je určitý matematický vztah, je možné data, která se zašifrují veřejným klíčem, dešifrovat jen příslušným soukromým klíčem a naopak. Je důležité poukázat na fakt, že odvodit soukromý klíč od veřejného klíče je velmi obtížné.

Základním nedostatkem kryptografie s veřejným klíčem je, že bude-li mít útočník dostatek času a dostatečný výpočetní výkon, dokáže odvodit soukromý klíč od veřejného a následně dešifrovat zprávu. Kvůli tomu se volí klíče o dostatečné délce (obvykle 1024 nebo 2048 bitů). Čím jsou použité klíče delší (délkou se myslí počet bitů), tým je šifrovací algoritmus odolnější vůči útokům.

Algoritmy kryptografie s veřejným klíčem jsou postaveny na matematických problémech, které v současnosti nemají dostupné řešení. Pro uživatele je jednoduché vytvořit pár klíčů (veřejný a soukromý) a použít je na šifrování a dešifrování. Zmiňovaná obtížnost matematických úkonů se ukáže při pokusu odvodit soukromý klíč při znalosti jen příslušného veřejného klíče. Bezpečnost kryptografie s veřejný m klíčem je zajištěna tímto způsobem; síla algoritmu spočívá v uvedené obtížnosti. Veřejný klíč tedy může být zveřejněný bez jakéhokoli bezpečnostního rizika. Bezpečnost závisí jen na utajení soukromého klíče. Na rozdíl od symetrických šifer není v asymetrické kryptografii potřeba prvotní bezpečný přenos klíče mezi komunikujícími stranami před zahájením samotné komunikace.

Algoritmy kryptografie s veřejným klíčem se používají hlavně na šifrování s využitím veřejného klíče a pro zajištění digitálního podpisu. Šifrování s využitím veřejného klíče znamená šifrování zprávy za přítomnosti veřejného klíče, přičemž jen osoba, která vlastní příslušný soukromý klíč má možnost zprávu dešifrovat a přečíst. Digitální podpis je zpráva, která se podepíše soukromým klíčem odesílatele, přičemž může být verifikovaná kýmkoli, kdo má přístup k veřejnému klíči odesílatele. Obě z těchto aplikací představují příklady důvěrnosti a autorizace dat s využitím kryptografie s veřejným klíčem.

Asymetrické šifry jsou v porovnání se symetrickými pomalejší. Často se ale asymetrické šifry používají na distribuci tajného klíče. Tento tajný klíč se následně použije na šifrování uživatelských dat.

Vzhledem k tomu, že v kryptografii s veřejným klíčem je správa klíčů mnohem jednodušší, je tu v porovnání se symetrickými šiframi mylná představa toho, že správa klíčů pomocí kryptografie s veřejným klíčem je jednoduchá. Navíc si někteří

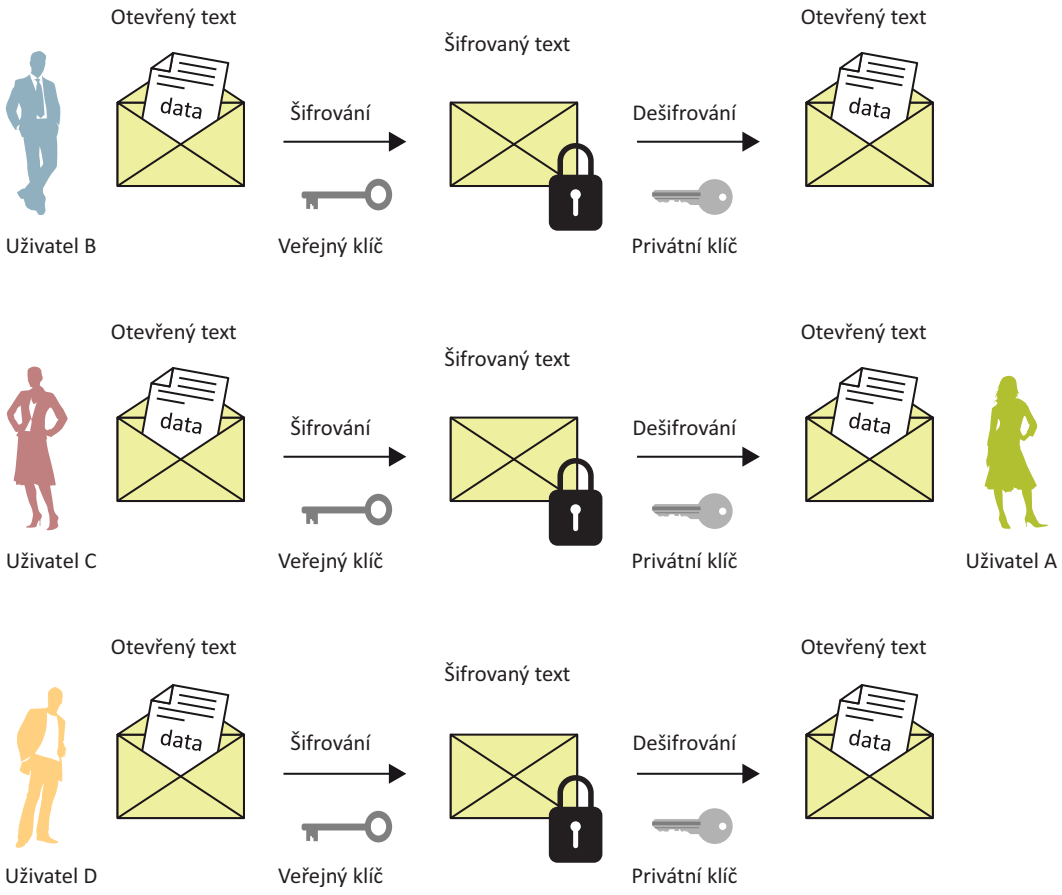
uživatelé mylně myslí, že kryptografie s veřejným klíčem je bezpečnější v porovnání s kryptografií s tajným klíčem. Ve skutečnosti závisí bezpečnost kteréhokoli systému na délce klíče a potřebné výpočetní složitosti vynaložené na prolomení šifry.

Nejznámější algoritmus kryptografie s veřejným klíčem je ***RSA***.

3.1 Systém kryptografie s veřejným klíčem

Použití kryptografie s veřejným klíčem na poskytnutí důvěrnosti

Pojďme si ukázat příklad, v němž Uživatel_B chce odeslat zprávu Uživateli_A. Uživatel_B zašifruje zprávu veřejným klíčem Uživatele_A a Uživatel_A dešifruje přijatou zprávu použitím svého soukromého klíče. Vzhledem k tomu, že mezi veřejným a soukromým klíčem jednoho páru je jistý matematický vztah, jen soukromý klíč Uživatele_A dokáže dešifrovat přijatou zprávu. Zachytí-li některý jiný uživatel zašifrovaná data, nedokáže je bez daného soukromého klíče dešifrovat. Tato metoda neposkytuje žádnou autentifikaci, zda odesílatelem zprávy byl Uživatel_B, protože veřejný klíč Uživatele_A je veřejně známý. Avšak tento systém poskytuje garanci toho, že pouze Uživatel_A dokáže zprávu dešifrovat.

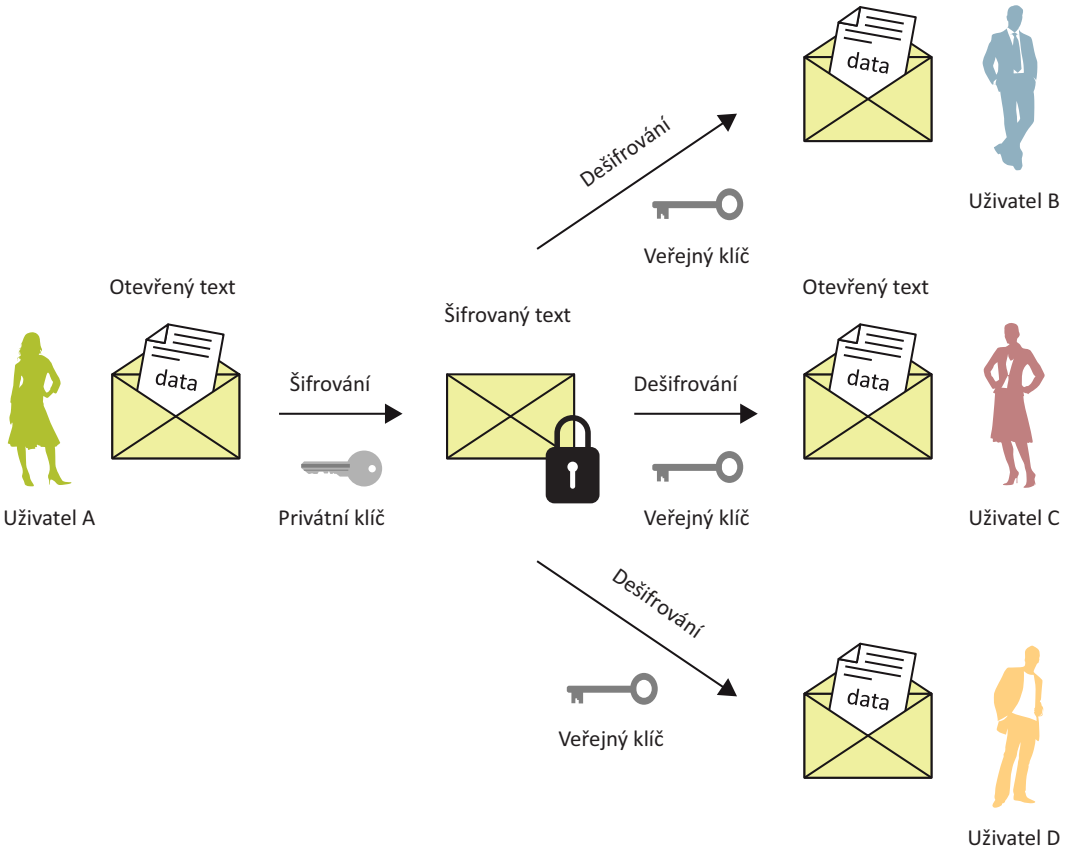


Obr. 3.1 Model kryptografie s veřejným klíčem (poskytnutí důvěrnosti obsahu dat)

Tato metoda velmi jasně ukazuje, že data, která uživatel odesílá adresátovi, mohou být zašifrovaná jen veřejným klíčem adresáta a dešifrovaná jeho soukromým klíčem, který vlastní pouze on. Zpráva tedy může být přenesena bezpečně. Odesílatel a adresát si nemusí vyměňovat svoje tajné klíče, jako je to v algoritmech symetrických šifer. Celá komunikace vyžaduje pouze veřejné klíče, a tak soukromé klíče nemusí být vůbec přenášeny nebo sdíleny.

Použití kryptografie s veřejným klíčem na poskytnutí autentifikace zdroje informace (ověření pravosti)

Za účelem autentifikace musí Uživatel_A zašifrovat zprávu svým soukromým klíčem a Uživatel_B ji dešifruje veřejným klíčem Uživatele_A. Tato metoda poskytuje autentifikaci zdroje informace, ale neposkytuje důvěrnost informací, protože veřejný klíč Uživatele_A je volně dostupný a každý, kdo jej vlastní může danou zašifrovanou zprávu dešifrovat.



Obr. 3.2 Model kryptografie s veřejným klíčem (poskytnutí autentifikace zdroje dat)

Použití kryptografie s veřejným klíčem za účelem poskytnutí autentifikace a důvěrnosti

Vyžaduje-li systém zabezpečení důvěrnosti i autentifikaci zdroje, musí Uživatel_B zašifrovat otevřený text nejprve svým soukromým klíčem, což zabezpečí autentifikaci zdroje. Následně Uživatel_B použije veřejný klíč Uživatele_A pro šifrování zprávy. Tím se zabezpečí důvěrnost komunikace.

Nevýhoda tohoto systému spočívá v délce trvání celého procesu šifrování a dešifrování.

4 Hybridní systém: Kombinace symetrického a asymetrického šifrování

Nevýhodou ***kryptografie s veřejným klíčem*** (asymetrických šifer) v porovnání se symetrickými šiframi spočívá ve výrazném ***prodloužení času šifrování a dešifrování***. Důvodem je délka použitého klíče, která je 1024 až 4094 bitů. Na druhé straně jsou ***symetrické šifry*** výrazně ***rychlejší***. Používají délku klíče 40 až 256 bitů. Kryptografie s tajným klíčem musí řešit problém bezpečné distribuce klíče. Obě tyto techniky mohou být společně použity na vytvoření dokonalejších metod šifrování.

Hybridní kryptografický systém používá asymetrické šifry na bezpečný přenos tajného klíče symetrických šifer. Tajná zpráva je potom zašifrovaná přijatým tajným klíčem a následně zaslána příjemci. Tím se dosáhne bezpečné distribuce tajného klíče a kompenzují se nevýhody symetrického šifrování. Na kódování každé odeslané zprávy se používá nový tajný klíč. Z tohoto důvodu se někdy nazývá i klíč relace. To znamená, že bude-li daný klíč relace odcizen (zachycen nepovolanou osobou), útočník bude schopen dešifrovat jen zprávu zašifrovanou tímto klíčem relace. Jestliže by chtěl dešifrovat i ostatní zprávy, musel by se zmocnit i klíčů ostatních relací.

Odesílaná zpráva se zašifruje klíčem relace, který se následně zašifruje veřejným klíčem příjemce. Potom je už zpráva připravena na odeslání. Příjemce použije svůj soukromý klíč na dešifrování klíče relace a následně použije klíč relace na dešifrování zprávy. Mnoho aplikací využívá takovýto systém.

Základní kroky této metody jsou:

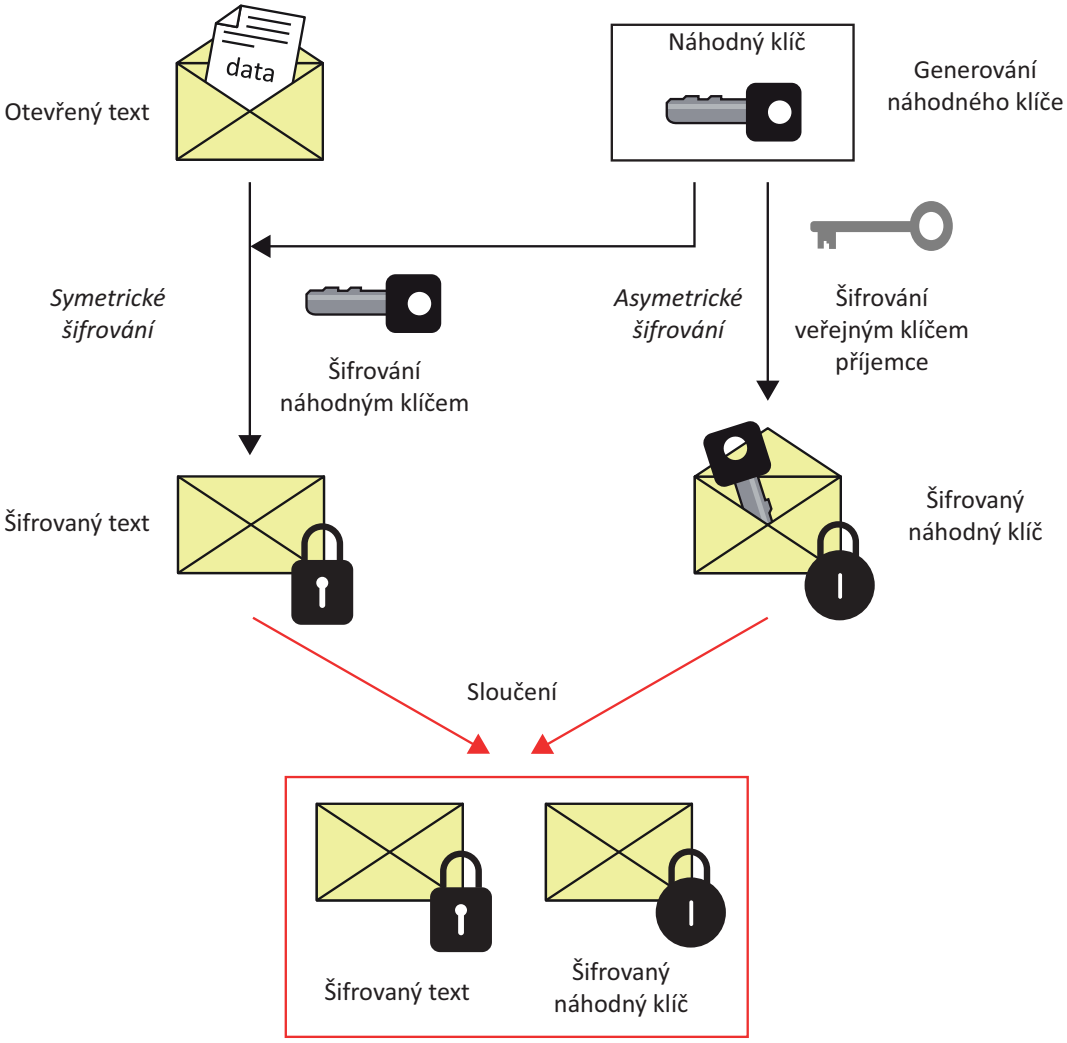
1. Šifrování otevřeného textu pomocí symetrické šifry a náhodného klíče.

2. Šifrování tohoto náhodného klíče veřejným klíčem příjemce pomocí asymetrického šifrování. Následně se pošle zašifrovaný náhodný klíč příjemci. Příjemce může nyní dešifrovat náhodný klíč pomocí svého soukromého klíče.

3. Následně se zašlou konkrétně zašifrovaná data. Tato zašifrovaná data mohou být dešifrovaná pomocí klíče, který byl zašifrován veřejným klíčem příjemce.

Hybridní techniky šifrování mají rozsáhlé využití. Například u ***Secure Shell (SSH)*** na zabezpečení komunikace mezi klientem a serverem a u ***PGP (Pretty Good Privacy)*** na zasílání zpráv. Největší využití je u ***Transport Layer Security (TLS)***, které je nejrozšířenější ve webových prohlížečích a webových serverech na udržování zabezpečení komunikace mezi kanály.

Následující obrázek ilustruje zmíněný proces.



Obr. 4.1 Model hybridního šifrovacího systému (poskytnutí důvěrnosti dat)

5 Hash funkce

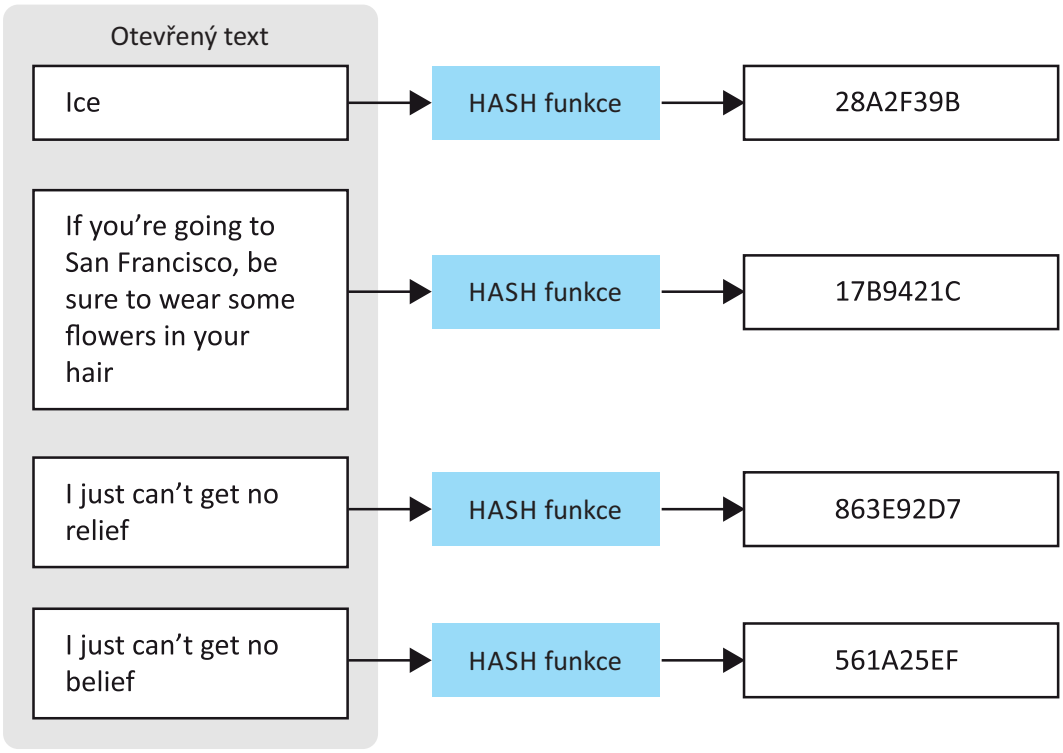
Termín hash funkce pochází z počítačové oblasti, kde označuje funkci zmenšení řetězce jakéhokoli vstupu do řetězce pevné délky. Jakákoli změna vstupních dat způsobí (s velkou pravděpodobností) změnu hodnoty hash funkce (hash kódu). Hash funkce právě s touto vlastností mají ve všeobecnosti různé použití. V kryptografii se používají hash funkce kvůli některým dalším parametrům. Kryptografické hash funkce se používají na ochranu integrity zpráv (aby se ochránil původ informace), ale taktéž jako ochrana před hrozbou odmítnutí (threat of repudiation) a zabezpečení hesel. Na rozdíl od symetrického a asymetrického šifrování, nepoužívá hash funkce žádný klíč.

Základní požadavky na hash funkci v kryptografii jsou:

- vstup s libovolnou délkou,
- výstup s pevnou délkou,
- jednoduchost výpočtu hash kódu pro jakoukoli zprávu,
- hash funkce je jednosměrná. To znamená, že z daného hash kódu je výpočetně nemožné dopracovat se k původní zprávě,
- není možné jakkoli změnit zprávu beze změny hash kódu,
- Odolnost vůči kolizím v síti. To znamená, že není možné nalézt dvě různé zprávy, které mají stejný hash kód.

Hash kód určuje stručnější vyjádření původní delší zprávy nebo dokumentu. Může se zdát, že takovéto shrnutí zprávy je podobné „digitálnímu otisku prstu“ rozsáhlejšího dokumentu.

Hlavní úloha hash funkce v kryptografii je v oblasti poskytování digitálních podpisů. Navíc může být hash kód odhalen bez toho, aby se odhalil dokument, ze kterého je odvozen.



Obr. 5.1 Hash funkce

6 Digitální podpis

Digitální podpisy jsou jedním z nejvýznamnějších prací založených na vývoji kryptografie s veřejným klíčem a poskytují zabezpečení, které by bylo složité implementovat nějakým jiným způsobem. Digitální podpis je elektronický podpis, který slouží k autentifikaci identity člověka, který posílá zprávu nebo člověka podpisujícího dokument s možností zabezpečení integrity obsahu. Digitální podpisy se jednoduše přeposílají a nemůžou být falšované neoprávněnou osobou.

Digitální podpisy jsou založeny na vlastnoručních podpisech, které se používají na určení vlastnických práv nebo na potvrzení daného obsahu zprávy.

Vlastnoruční podpisy musí disponovat následujícími vlastnosti:

- ***Podpis je bezpečný*** – podpis by neměl být napodobitelný a případný pokus o falšování podpisu by měl být lehce zjistitelný.
- ***Podpis ulehčuje autentifikaci*** – podpis jednoznačně identifikuje majitele, který dokument podepsal bez omezení a vědomě.
- ***Podpis je nepřenosný*** – podpis je součástí dokumentu a neoprávněný vlastník není schopen převést podpis na jiný dokument.
- ***Dokument, který je podepsaný není možné změnit*** – dokument nemůže být změněn a upraven po jeho podepsání.
- ***Podpis nesmí být odmítnut*** – majitel podpisu nemůže popřít schválení podepsaného dokumentu.

Ve skutečnosti žádná z těchto vlastností nemůže být splněná vlastnoručními podpisy. Zároveň by měly všechny tyto vyjmenované vlastnosti splňovat digitální podpisy. Na druhé straně se taktéž mohou vyskytnout různé problémy s praktickou realizací digitálních podpisů. Digitální soubory mohou být lehce kopírované, což může způsobit to, že část dokumentu se přenese do jiného dokumentu. Z toho vyplývá, že podepsaný dokument může být jednoduše měnitelný.

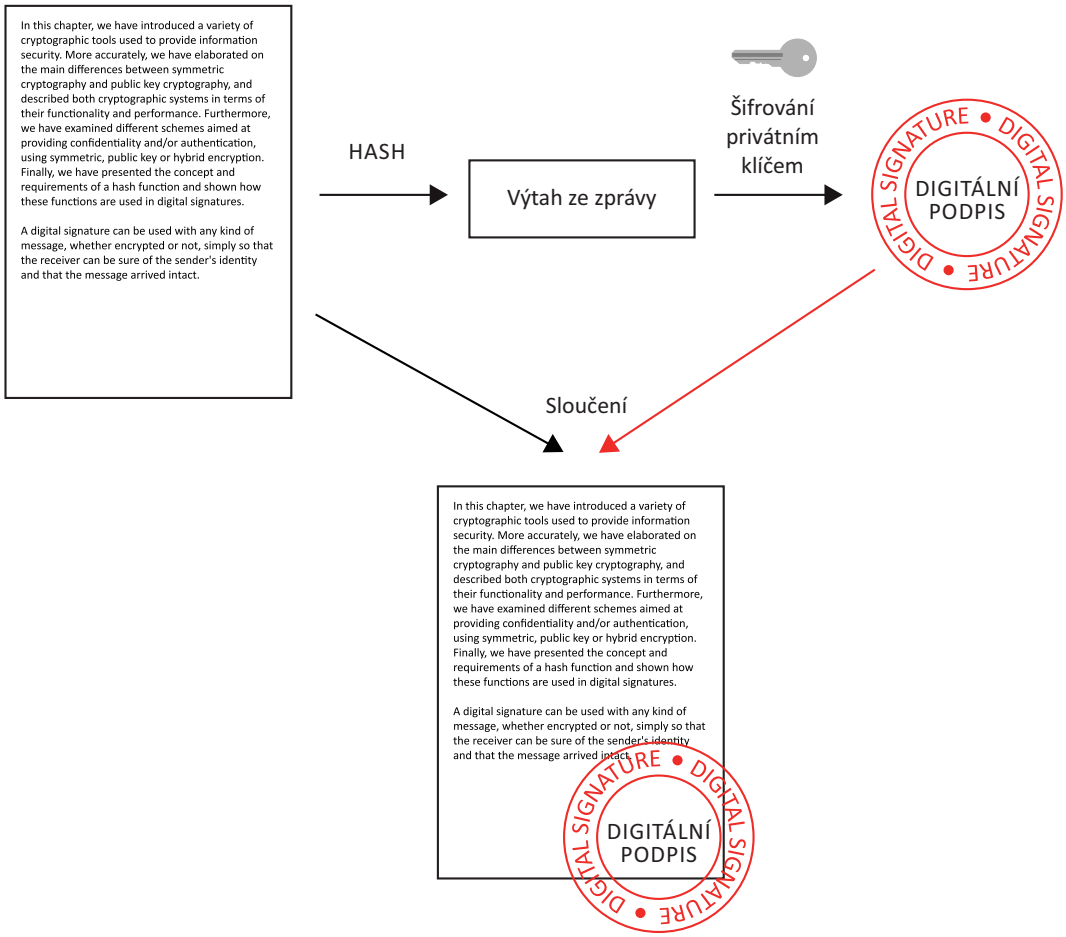
Pro digitální podpis můžeme formulovat tyto požadavky:

- Podpis musí mít formu bitové postupnosti, která ***závisí na podepisované zprávě***.
- Podpis ***musí obsahovat některé jedinečné informace odesílatele,*** aby se předešlo falšování a popírání pravosti.
- ***Realizace*** digitálního podpisu musí být poměrně ***jednoduchá***.
- ***Falšování*** digitálního podpisu musí být ***výpočetně neproveditelné***. Falšováním se vytvoří buď nová zpráva pro existující digitální podpis, nebo falešný digitální podpis pro existující zprávu.
- Praktická úschova kopie digitálního podpisu v paměti.

Digitální podpis může být použit s jakýmkoli druhem zprávy, ať je šifrovaná nebo ne, jednoduše tak, že příjemce si může být jist identitou odesílatele a že zpráva dorazila neporušená.

Existuje několik možných schémat pro digitální podpis. Jedno z nejpoužívanějších je založeno na hash funkci. V tomto případě, hodlá-li uživatel podepsat dokument, musí dodržovat tyto kroky:

1. Výpočet hash kódu dokumentu, který má být podepsán.
2. Odesílatel zašifruje hash kód svým soukromým klíčem, čímž vytvoří digitální podpis (využití asymetrického šifrování).
3. Připojení digitálního podpisu k dokumentu.

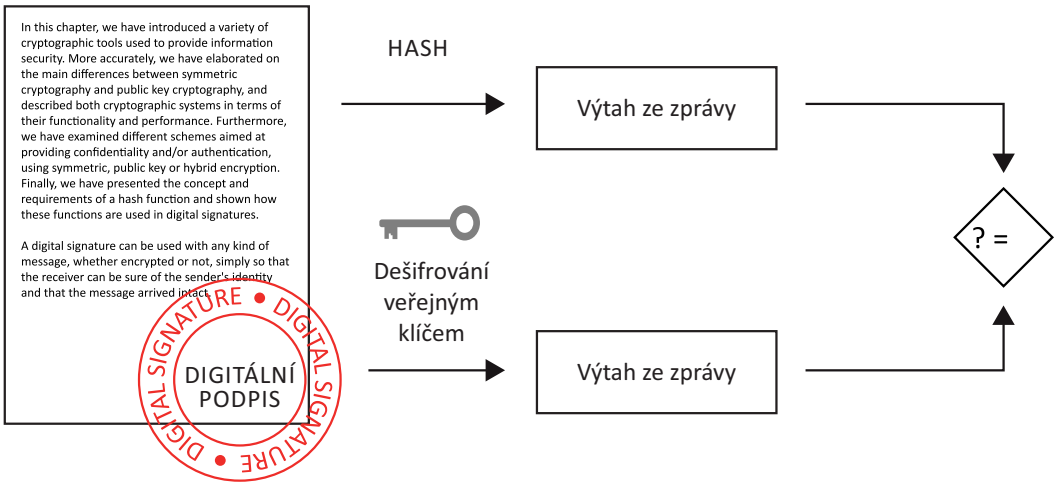


Obr. 6.1 Digitální podpis na základě hash funkce

Adresát může následně ověřit pravost tohoto digitálního podpisu pomocí těchto kroků:

1. Výpočet hash kódu dokumentu (kromě digitálního podpisu).
2. Pomocí veřejného klíče odesílatele příjemce dešifruje digitální podpis, čímž získá hash kód vypočtený odesílatelem.

3. Porovnání výsledků získaných ze dvou předcházejících kroků.



Obr. 6.2 Proces verifikace dat digitálním podpisem na základě hash funkce

V případě, že hash kódy získané ve dvou krocích jsou stejné, příjemce bude vědět, že podepsaná data nebyla změněna.

7 Distribuce klíčů. Digitální certifikace

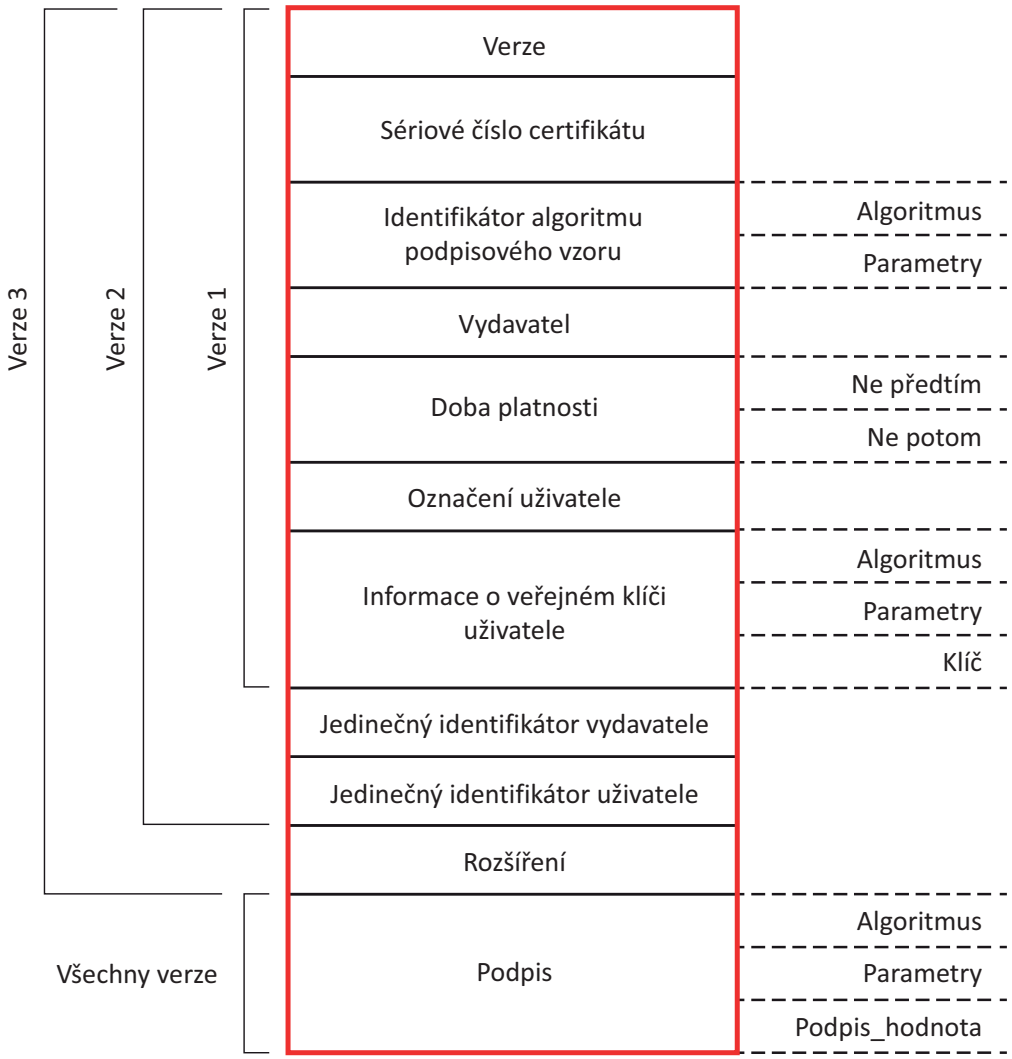
Digitální podpisy představují jedno z hlavních využití kryptografie s veřejným klíčem. Vhodně implementovaný digitální podpis dává důvod se domnívat, že i zpráva, která byla odeslaná přes nezabezpečený kanál, byla odeslaná požadovaným odesílatelem. V mnohých ohledech jsou digitální podpisy ekvivalentní tradičnímu vlastnoručnímu podpisu, avšak je těžší zfalšovat správně implementované digitální podpisy než jejich vlastnoruční ekvivalenty. Za účelem ověření digitálního podpisu musí mít příjemce znalost veřejného klíče odesílatele. Z tohoto důvodu je nevyhnutné použít určitý mechanismus distribuce klíčů.

Nejúčinnější přístup řešení daného problému je založen na využití tzv. digitálních certifikátů, které umožňují realizaci výměny klíčů (distribuci klíčů).

Digitální certifikát je elektronický dokument, který se využívá pro identifikaci jednotlivců, serverů, společností apod., a spojuje tuto identitu s příslušným veřejným klíčem. To zahrnuje digitální podpis, ***který spojuje veřejný klíč s identitou*** – informace, jako například jméno osoby nebo organizace, jejich adresy, atd. Pomocí certifikátů se dá ověřit, zda veřejné klíče patří konkrétním osobám. Certifikáty pomáhají bránit v používání falešných veřejných klíčů. Pouze veřejný klíč ověřený digitálním certifikátem bude spolupracovat s odpovídajícím soukromým klíčem entity, která je identifikovaná certifikátem.

Digitální certifikát je datová struktura, která obsahuje veřejný klíč nějakého subjektu nebo držitele certifikátu, jakož i identifikační údaje držitele certifikátu, časové razítko spojené s platností uděleného certifikátu a další údaje certifikační autority. Tato struktura je podepsaná privátním klíčem ***certifikační autority (CA)*** a každý uživatel je schopen ověřit pravost obsahu certifikátu pomocí veřejného klíče certifikační autority. Certifikační autority jsou subjekty, které vydávají certifikáty a ověření identit.

Následující obrázek znázorňuje strukturu digitálního certifikátu:



Obr. 7.1 Struktura digitálního certifikátu

8 Kyberkriminalita: Úvod

Kyberkriminalita nebo počítačová kriminalita představuje jakoukoli trestnou činnost zahrnující počítače a počítačové sítě. Může to sahat od různých podvodů až k nevyžádaným e-mailům (spam). Tyto případy kriminality zahrnují útoky na počítačová data a systémy, krádeže identity, distribuci fotek dětské pornografie, internetové aukční podvody, infiltraci on-line finančních služeb, jako i zavádění virů, „botnetů“ a různé e-mailové podvody, jako je např. „phishing“.

Jedním z nejlepších způsobů jak se vyhnout tomu, abychom se stali obětí počítačové kriminality, je využití systému, který používá jednotný systém softwarového a hardwarového zabezpečení pro ověření všech informací, které jsou odeslány nebo přístupny přes internet.

Počítačová kriminalita je definovaná jako: „Trestný čin, který je vědomě spáchán vůči jednotlivcům nebo skupinám osob se záměrem poškodit pověst oběti nebo způsobit jí fyzické nebo psychické poškození přímo nebo nepřímo, s využitím moderních telekomunikačních sítí, jako je internet a mobilní telefony (SMS / MMS).“ Tyto trestné činy mohou ohrozit bezpečnost a ekonomiku státu. S těmito trestnými činy souvisí též např. porušování autorských práv či šíření dětské pornografie. Taktéž sem patří hrozby úniku citlivých informací.

Je důležité si uvědomit, že rozpoznat každý útok počítačové kriminality je před samotným ovlivněním cílových subjektů nemožné. Z tohoto důvodu je velmi důležité se zaměřit na kybernetickou bezpečnost, která klade důraz na včasné odhalení a řešení problému.

Účinný postup reakce na různé incidenty zahrnuje následující kroky:

- Identifikace hrozeb, které postihly infrastrukturu.
- Omezení dopadů hrozby. Prevence v rámci určité části infrastruktury.
- Vyšetřování, jehož cílem je identifikovat postižené systémy a způsob, jakým daný útok pronikl do počítačových systémů.
- Sanace/obnovení navrácením IT infrastruktury zpět do on-line režimu po ukončení vyšetřování.
- Report a sdílení informací o řešeném problému vyššímu vedení a sdílení údajů o incidentu prostřednictvím specializovaných platforem, které umožňují rychlé sdílení dat dalším společnostem.

Bohužel, popsaný postup je zřídkakdy dodržován. Až doposud byla ochrana a řešení hrozeb výlučně manuálním (lidským) procesem, který selhával na lidském faktoru. Lidé nereagovali, a tím bylo řešení problémů neefektivní.

9 Techniky útoků

Bezpečnostní útoky je možno charakterizovat jako různé druhy systematických aktivit zaměřených na snížení nebo poškození bezpečnosti. Z tohoto pohledu může být útok definován jako systematická hrozba generovaná úmyslným a inteligentním způsobem. Počítačové sítě mohou být vystaveny mnoha rizikům, jako například:

- Sociální inženýrství, při kterém se někdo pokusí získat přístup prostřednictvím sociálních prostředků (předstírat, že je oprávněný uživatel systému nebo správce, klamat lidi, aby odhalili tajemství, atd.).
- War-dialing, při kterém se používá počítačový software a modem na vyhledávání stolních počítačů vybavených modemy, které na volání odpoví a tím poskytnou potenciální cestu do podnikové sítě.
- Útoky odmítnutí služby, včetně všech typů útoků, které mají infiltrovat počítače nebo sítě tak, že oprávněný uživatel počítače nebo sítě jej nebude moci použít.
- Útoky na protokoly, které využívají známé (nebo dosud neznámé) slabé stránky síťových služeb.
- Hostitelské útoky, které napadají zranitelná místa v některých operačních systémech, nebo činnosti, jak je systém nastaven a spravován.
- Hádání hesla; hesla jsou sekvence znaků, obvykle spojené s uživatelským jménem, které poskytuji mechanismus pro identifikaci a autentifikaci konkrétního uživatele. Téměř ve všech počítačích si mohou uživatelé sami zvolit hesla. To klade břemeno zabezpečení na koncové uživatele, kteří buď nevědí, nebo se nestarají o vhodné bezpečnostní postupy. Ve všeobecnosti platí, že hesla která se jednoduše pamatují, jsou slabá a je poměrně jednoduché je uhádnou. Útočníci mají několik možností na uhádnutí hesel a na jejich prolomení.
- Odposlouchávání všeho druhu, včetně odcizení e-mailových zpráv, souborů, hesel a jiných informací prostřednictvím odposlouchávání síťového připojení.

Bezpečnostní útoky je možno rozdělit do dvou kategorií:

- pasívní útoky,
- aktívní útoky.

9.1 Pasívní útoky

Pasívní útoky se pokoušejí zjistit nebo využít různé informace ze systému, ale nemají snahu o určitý zásah do systémových prostředků. Pasivní útok je takový útok, při kterém útočník pouze sleduje komunikační kanál. Pasívní útočník ohrožuje pouze důvěrnost dat.

Pasívní útoky se zaměřují na odposlouchávání nebo sledování komunikačního přenosu. Cílem je získat informaci, která se přenáší.

Pasívní útoky dělíme do dvou základních tříd:

- Odposlech. Všeobecně platí, že většina síťové komunikace probíhá v nezabezpečené formě, která umožňuje útočníkovi, jenž získal přístup do sítě „poslouchá“, resp. sledovat komunikaci mezi dvěma stranami. Odposlouchávání sítě je všeobecně největší bezpečnostní problém, kterému musí administrátoři ve firmách čelit. Bez zabezpečení přenášených informací kryptografickými systémy, je hrozba odposlouchávání velmi velká.

- Analýza provozu. V tomto případě nejde jen o pozorování zpráv, ale též jejich zachycení a podrobení analýze. Cílem analýzy je získat jakékoli informace ze zachyceného provozu. Analýza provozu může být účinná i v případě, že zprávy jsou zašifrované a není možno je dešifrovat. Všeobecně platí, že čím větší je počet pozorovaných (zachycených) zpráv, tím se zvyšuje i možnost odhalení jejich významu.

9.2 Aktívní útoky

Aktívní útoky slouží ke změně systémových prostředků nebo ovlivňují jejich provoz. Tento typ útoku se používá, hodlá-li útočník smazat, přidat nebo pozměnit přenášená data. Aktívní útočník ohrožuje integritu a autentizaci dat, podobně jako i jejich důvěrnost.

Aktívní útoky mohou být rozděleny do šesti kategorií:

- Maškaráda (masquerade). Je to typ útoku, při kterém útočník předstírá, že je autorizovaný uživatel, aby získal přístup k systému nebo vyšším pravomocem.

- Opakování (replay). Při tomto typu útoku je platný datový přenos zlomyslně nebo podvodně opakován nebo zpožděn. Toto realizuje útočník, který zachytí originální přenos dat a znovu data odešle (pravděpodobně jako součást útoku typu maškaráda).

- Modifikace obsahu zprávy. Útočník vyjme zprávu ze síťového provozu, upraví její obsah a vrátí ji zpět.

- Člověk uprostřed (Man in the Middle (MitM)). Při tomto druhu útoku zachytává útočník komunikaci mezi dvěma zúčastněnými stranami, obvykle mezi koncovým uživatelem a webovým serverem, za účelem zneužití informací (předstírání oprávněné osoby nebo součást jiného typu útoku).

- Odmítnutí služby (Denial of Service (DoS)) a distribuované odmítnutí služby (Distributed Denial of Service (DDoS)). Útok odmítnutí služby je útok, při kterém je uživatel nebo organizace zbaven konkrétní poskytované služby, kterou za normálních okolností poskytovanou má. Při útoku distribuované odmítnutí služby je využit velký počet zpronevěřených systémů (někdy nazývaných „botnet [http://searchsecurity.techtarget.com/definition/botnet] “) útočících na jeden cíl.

- Pokročilá přetrvávající hrozba (Advanced Persistent Threat (APT)). Je to síťový útok, při kterém neautorizovaná osoba získá přístup k síti a zůstává tam bez povšimnutí dlouhou dobu. Záměrem útoku APT bývá spíše ukradnout data než způsobit výpadek sítě nebo organizace. Útoky APT se používají na získávání velmi cenných informací, jako např. ze sekce národní obrany, výroby a finančního sektoru.

10 Prevence

Prevence proti počítačové kriminalitě může být přímá – jestliže se dokážeme vyhnout mnohým útokům vyzbrojeni jen malou technickou podporou. Všeobecně platí, že on-line útočníci se snaží vydělat peníze tak rychle a lehce jak je to jen možné. Čím více jim ztížíme jejich práci, tím větší je pravděpodobnost, že se stáhnou a přesunou se na lehčí cíl. Pravděpodobně nejlepší obranou je být koncovým uživatelem. Čím méně rizika na sebe bereme, tím nižší je pravděpodobnost, že budeme obětí počítačového útoku. Níže uvedené typy prevence poskytují základní informace o tom, jako zabránit on-line podvodům.

- Udržujte počítačový systém s nejnovějšími aktualizacemi. Objeví-li se chyba, prodejci obvykle poskytují aktualizaci software. Jedním z nejlepších způsobů jak udržet útočníky v bezpečné vzdálenosti od zařízení, je použít aktualizaci software jakmile je dispozici. Většina dokumentací k produktům nabízí způsob, jakým získat nové aktualizace. Některé aplikace kontrolují dostupné aktualizace automaticky, v opačném případě je nevyhnutelná manuální kontrola jejich dostupnosti. V každém případě tím, že pravidelně aktualizujeme software počítače, blokujeme útočníkům možnost využít softwarové chyby (zranitelnosti), které by jinak mohly využít na průnik do systému. To, že udržujeme software počítače aktualizovaný, nezaručuje ochranu před všemi útoky, ale stěžuje to práci hackerům, blokuje mnoho základních a automatických útoků a může odradit méně rozhodnutého útočníka.

- Ujistěte se, že je počítač správně nakonfigurován. Instalace systému hned po vybalení z krabice a nechání ho s továrním nastavením je pravděpodobně jednou z nejčastějších chyb, které lidé dělají při nastavování sítě. Jakmile je počítač nainstalován, je důležité věnovat pozornost nejen tomu, aby systém fungoval, ale zaměřit se na to, aby fungoval správně. Tovární nastavení má často standardní správu účtů a hesel, což znají útočníci po celém světě. Konfigurace internetových aplikací, jako webový prohlížeč a e-mailový software je jednou z nejdůležitějších oblastí, na které se musíte zaměřit.

- Zvolte si silná hesla a udržujte je v bezpečí. Hesla jsou často použity v systému jako jediná ochrana. Uživatelské ID je jen jméno a neprochází verifikací, přičemž heslo je spojeno s ID uživatele a funguje jako identifikátor. Brány a systémy detekce prolomení systému neznamenají nic, jsou-li vaše hesla nezabezpečená. Silné heslo je to, které se nenachází v žádném slovníku. Taktéž to znamená heslo, které není jednoduché odcizit.

- Chraňte počítač bezpečnostním softwarem. Několik typů bezpečnostního software, včetně firewallu a antiviru jsou nevyhnutné pro základní ochranu v reálném čase. Firewall je softwarový nebo hardwarový produkt, který filtruje informace přicházející a opouštějící počítač tak, aby zabezpečil, že neexistuje žádný neoprávněný přístup k počítači a tímto způsobem poskytuje první linii obrany. Další linií obrany je mnohdy antivirový software, počítačový program, který může být použit na skenování souborů, identifikaci a odstranění počítačových virů a dalšího škodlivého software (malware). Virus je program, který se může sám replikovat a je určen k šíření sebe sama z jednoho počítače na jiný. Provádí své činnosti tak, aby o tom koncový uživatel nevěděl a/nebo

s danými změnami nesouhlasil. Malware je širší pojem, zkratka pro škodlivý software, přičemž existuje v mnoha různých formách, čítaje viry, trójské koně, keyloggery, červy, adware, spyware.

- Chraňte svoje osobní údaje. Autorizace uživatele se stává velkým problémem bezhotovostních transakcí a bankovních služeb. Při této kyberkriminalitě se útočníci snaží o nelegální přístup k datům o osobním bankovním účtu, kreditní kartě, debetní kartě a k dalším citlivým informacím uživatele, které chtějí útočníci využít na své finanční obohacení. To může vést ke značným finančním ztrátám a dokonce i „pošpinit“ kreditní historii oběti. Proto je při sdílení osobních informací, jako je jméno, adresa, telefonní číslo a e-mailová adresa, nutná opatrnost. Avšak chcete-li využít řady služeb poskytovaných on-line, budete muset poskytnout své osobní údaje za účelem fakturace a dodání zakoupeného zboží.