Bankovní institut vysoká škola Praha

Katedra matematiky, statistiky a informačních technologií

Moderní kryptografické metody

Bakalářská práce

Autor: **Daryna Polevyk**

Informační technologie

Vedoucí práce: **Ing. Vladimír Beneš**

Praha **Duben 2013**

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracovala samostatně pod vedením Ing. Vladimíra Beneše. Veškeré literární prameny a informace, které jsem v práci použila, jsou uvedeny v seznamu literatury.

Svým podpisem stvrzuji, že odevzdaná elektronická podoba práce je identická s její tištěnou verzí, a jsem seznámena se skutečností, že se práce bude archivovat v knihovně BIVŠ a dále bude zpřístupněna třetím osobám prostřednictvím interní databáze elektronických vysokoškolských prací.

V Praze dne 30. 4. 2013 Daryna Polevyk

Poděkování

Ráda bych poděkovala vedoucímu práce Ing. Vladimíru Benešovi nejen za konzultace při vedení práce, ale i za cenné rady a podnětné připomínky.

Anotace práce

Tato práce se v první kapitole věnuje stručným základům kryptografie a kryptoanalýze. Tyto základy jsou důležité pro pochopení struktury a seznamují čtenáře s prací. Druha část je věnována rozdělení moderních kryptografických metod.

Další části popisuji moderní kryptografické metody. Teoretická část obsahuje vysvětlení důležitých pojmů, rozdělení šifer, popis známých algoritmů a použiti moderních kryptografických metod v praxi.

Klíčová slova:

Kryptografie, kryptoanalýza, šifrování, dešifrování, symetrické šifry, asymetrické šifry, digitální podpis, digitální certifikát, DES, RSA, hašovací funkce.

Annotation

The first chapter of this thesis contains brief introduction to the basics of cryptography and cryptanalysis. This is important for understanding of the structure the work on the System is introduced. The second part is devoted to the division of modern cryptographic methods.

Another part describes modern cryptographic methods. The theoretical part contains explanations, important concepts, classification of codes, description of known algorithms, and the use of modern cryptographic methods in practice.

Key words

Cryptography, Cryptanalysis, Encryption, Decryption, Symmetric encryption, Asymmetric encryption, Digital signature, Digital certificate, DES, RSA, The hash function.

Obsah

Úvod

Historie kryptografie - stejného věku jako dějiny lidského jazyka. Navíc původním písmem byl sám šifrovací systém, který v dávných společnostech vlastnilo jen pár vyvolených. Například svaté knihy starověkého Egypta, starověké Indie a jiné. Kryptografie se začala formovat jako nezávislá věda. První kryptografický systém se vyskytl na začátku našeho letopočtu. Caesar ve své korespondenci použil více či méně systematický kód, pojmenovaný podle něj. Během první a druhé světové války došlo k rychlému rozvoji kryptografických systémů. Vývoj výpočetní techniky urychlil zdokonalování kryptografických metod.

Proč je problém použití kryptografických metod v informačních systémech v současné době zvlášť důležitý?

Na druhou stranu vznik nových výkonných počítačů, technologií a neuronové sítě umožňuje rozluštit šifry, které donedávna nebyly prakticky rozluštěné. Problém zajištění potřebné úrovně ochrany informací je velmi složitý, vyžaduje pro jejich řešení nejen souhrn vědeckých, technických a organizačních opatření, ale i využívání specifických nástrojů a metod, vytvoření integrovaného systému organizačních činností a využití specifických nástrojů a metod pro ochranu informací.

Cílem této práce je seznámit zájemce s důležitými pojmy moderní kryptografie, principy známých algoritmů a jejich základními vlastnostmi.

K dosažení tohoto cíle práce pojednává o:

- Obecném pojmu kryptografie a kryptoanalýzy, hlavních úkolech kryptografie.
- Moderních kryptografických metodách a jejich vlastnostech.

1 Kryptologie

1.1 Definice a základní terminy

Kryptologie (angl. cryptology) je samostatná vědní disciplína, která se dělí na kryptografii a kryptoanalýzu. Je vědou o informační celistvosti a zahrnuje tvorbu kryptografických technik (hašovacích funkcí, kryptografických protokolů, kryptoanalytických útoků, kryptografických algoritmů apod.), vymezení podmínek jejich praktického využívání a zkoumání odolnosti kryptografických algoritmů proti kryptoanalytickým útokům. Opírá se rozsáhlý matematický aparát, mimo jiné o propracovanou teorii informace, teorii složitosti, teorii čísel, teorii pravděpodobnosti [11].

Kryptografie se zabývá vyhledáváním a výzkumem matematických metod konverze dat. Oblast zájmu kryptoanalýzy - výzkum možností dešifrování informací bez znalosti klíče. Tato bakalářská práce se obzvlášť zaměřuje na moderní kryptografické metody.

Moderní kryptografie zahrnuje čtyři základní části:

- Symetrické kryptosystémy.
- Asymetrické kryptosystémy.
- Systémy elektronického podpisu.
- Správu klíčů.

Hlavní cíl použití šifrovacích technik - přenos důvěrných informací prostřednictvím komunikačních kanálů (např. e-mail), ověření pravosti přenášených zpráv, ukládání informací (dokumenty, databáze) na datových nosičích, které jsou zakódovány.

Existují různé metody ochrany informace. Například fyzické omezeni přístupu k informací uložením na bezpečné uchování do přísně střežené místnosti. Při ukládání informací je tato metoda užitečná, nicméně když je nutné přenést data prostřednictvím informačního kanálu, je potřeba použít jiný způsob ochrany informace.

Můžete použít jednu ze známých metod skrývání informací:

- Skrýt informace o kanálu pomocí vlastních metod pro přenos zpráv.
- Maskovat přenosový kanál v rámci otevřeného komunikačního kanálu, například skrýt obsah pomocí různých způsobů výměny otevřených zpráv, jejichž význam je předem dohodnut.

Kryptografie umožňuje transformovat informaci takovým způsobem, že její čtení (obnova) je možné pouze se použitím klíče.

Moderní kryptografie je oblast, týkající se řešení problémů informační bezpečnosti, jako je důvěrnost, integrita, autentizace a nepopiratelnost autorství. Dosažení těchto požadavků je hlavním cílem kryptografie.

Zajištění tajnosti - ochrana informací s obeznámeností s jeho obsahem osobami, které nemají přístupová práva.

Zajištění integrity - záruka proti neoprávněným změnám informací. Pro zajištění integrity je potřeba provést jednoduché a spolehlivé testy pro detekci jakékoliv manipulace s daty. Do manipulace s daty patří vkládání, mazání a výměna.

Zajištění autentizace - rozvoj metod identifikace strany a samotné informace v procesu výměny. Při přenosu informací přes komunikační kanál by měl být ověřen zdroj, čas a obsah údajů, doba dodání atd.

Zajištění nepopiratelnosti nebo přiznání autorství – předchází možnosti odmítnutí subjektů od některých spáchaných činů.

1.2 Hlavní cíle kryptografie

Úkolem kryptografie, tj. skryté komunikace, jsou pouze informace, které potřebují ochranu. V takových případech mluvíme o informaci soukromé, tedy takové, která obsahuje tajemství nebo je chráněná. Pro běžné situace tohoto typu byla představena zvláštní koncepce:

- Státní tajemství.
- Vojenské tajemství.
- Obchodní tajemství.
- Právní tajemství.
- Lékařské tajemství atd.

1.3 Kryptologie v současném světě

Během své dlouhé historie až do nedávné doby byla kryptologie k dispozici jen pro omezený počet lidí. Byly to většinou hlavy států a velvyslanců. Jen před několika desítkami let se všechno kardinálně změnilo - informace získala nezávislou obchodní hodnotu a stala se hodně rozšířenou.

Informace se vyrábějí, uchovávají, dopravují, prodávají a nakupují, ale i kradou a dělají falešnými, a proto by měly být chráněny. Moderní společnost se stále více stává informační společností, úspěch jakékoli činnosti silně závisí na vlastnění určitých informací. A čím je tento efekt výraznější, tím větší je potenciální škoda ze zneužívání v informační sféře, a tím větší je potřeba k ochraně informací.

Mezi celou řadu metod pro ochranu dat před neoprávněným přístupem jsou důležitými kryptografické techniky. Na rozdíl od jiných metod jsou založeny pouze na vlastnostech informací a nepoužívají vlastnosti svých fyzických médií, zejména uzly jeho zpracování, přenosu a skladování. Kryptografické techniky budují bariéru mezi chráněnými informacemi

a potenciálním zneužitím. Samozřejmě je kryptografická ochrana určena především pro šifrování dat. Dřív se šifrování provádělo ručně nebo s použitím různých zařízení. Proto rozvoj kryptologie zdržoval problém realizace šifer.

Kryptografický systém pracuje na určité metodice (postupu). Skládá se z:

- Jednoho nebo více šifrovacích algoritmů.
- Klíčů používaných pro šifrování.
- Správy klíčů.
- Výchozího textu.
- Šifrovaného textu.

1.4 Kryptoanalýza

Dešifrování (od řeckého Κρυπτός - skrytý a analýza) – věda o metodách získání počáteční hodnoty zašifrované informace bez přístupu k utajovaným informacím (klíč). Ve většině případů to znamená najít klíč. Termín byl vytvořen americkým šifrantem Williamem F. Friedmanem v roce 1920. Termín "dešifrování" také znamená pokusit se najít chybu v šifrovacím algoritmu nebo protokolu. Přestože hlavní cíl zůstává konstantní v čase, metody kryptoanalýzy se dramaticky změnily. Pokud se dřív kryptoanalýzou zabývali většinou lingvisté, v naší době je osudem "čistých" matematiků. Výsledky dešifrování konkrétního šifrantu se nazývají kryptografickým útokem na šifru. Úspěšný kryptografický útok se nazývá lámání nebo otevření šifry.

Existuje mnoho různých kryptoanalytických metod. Některé z nejdůležitějších jsou uvedeny níže.

Útok se znalostí jenom šifrované informace (ciphertext). To je situace, kdy útočník neví nic o obsahu zprávy a pracuje jen se šifrovaným textem. V praxi lze často hodnověrné předpokládat strukturu textu, protože mnoho příspěvků má standardní záhlaví. Dokonce i obyčejné dopisy a dokumenty, které začínají jednoduchým informací. Často je také možné předpokládat, že určitý údaj obsahuje určité slovo.

Útok se znalostí obsahu šifrování (known-plaintext attack). Útočník ví nebo můžete odhadnout obsah všech nebo části šifrového textu. Hlavním úkolem je rozluštit zbytek zprávy. To může být prováděno buď na základě výpočtu šifrovacího klíče, nebo jej obcházet.

Útok se znalostí zadaného textů (chosen-plaintext attack). Útočník má možnost dostat zašifrovaný dokument, ale neví klíč. Úkolem je najít klíč. Některé metody šifrování, a to zejména RSA, jsou citlivé na tento typ útoku. Při použití těchto algoritmů je třeba pečlivě sledovat, aby útočník nemohl zašifrovat text.

Útok s podstavcem (Man-in-the-middle attack). Útok si klade za cíl výměnu šifrovaných zpráv, a zejména protokol výměny klíčů. Základní myšlenkou je, že když si obě strany vymění klíče pro tajnou komunikaci (například pomocí kódu Diffie-Hellman), je nepřítel představen mezi nimi na lince výměny zpráv. Pak útočník odesílá každé straně klíč. V důsledku toho každá ze stran bude mít různé klíče, z nichž každý je známý útočníkovi. Teď nepřítel může dešifrovat každou zprávu pomoci jeho klíče a potom zašifrovat pomocí jiného klíče před odesláním příjemci. Strany budou mít iluzi tajné korespondence, zatímco ve skutečnosti si nepřítel čte všechny zprávy.

Jeden způsob, jak zabránit tomuto druhu útoku je, že strany při výměně kryptografických klíčů vypočítají hodnoty hašovací funkce protokolu (nebo alespoň hodnotu klíče) a podepíšou zprávu digitálním podpisem a odešlou ho na druhou stranu. Příjemce zkontroluje podpis a hodnotu hašovací funkce, která musí odpovídat vypočtené hodnotě. Tato metoda se používá zejména u systémů Photuris.

Existuje mnoho dalších kryptografických útoků. Nicméně výše uvedené informace jsou pravděpodobně důležité pro rozvoj praktických systémů.

1.5 Kryptografický protokol

Kryptografický protokol (Cryptographic protokol) - abstraktní nebo konkrétní protokol, který obsahuje sadu kryptografických algoritmů. Základem protokolu je soubor pravidel, kterými se řídí používání kryptografických algoritmů a transformace v oblasti informačních procesů.

1.5.1 Funkce kryptografických protokolů

Existují takovéto funkce kryptografických protokolů:

- Ověřování datového původu.
- Autentifikace stran.
- Ochrana osobních údajů.
- Nepopiratelnost s dokladem o přijetí.
- Nepopiratelnost s dokladem zdroje.
- Integrita dat.
- Zajištění integrity spojení bez obnovy.
- Zajistit integritu spojení s obnovou.
- Řízení přístupu.

2 Rozdělení šifer

2.1 Symetrické kryptografie

2.1.1 Definice a princip symetrické kryptografie

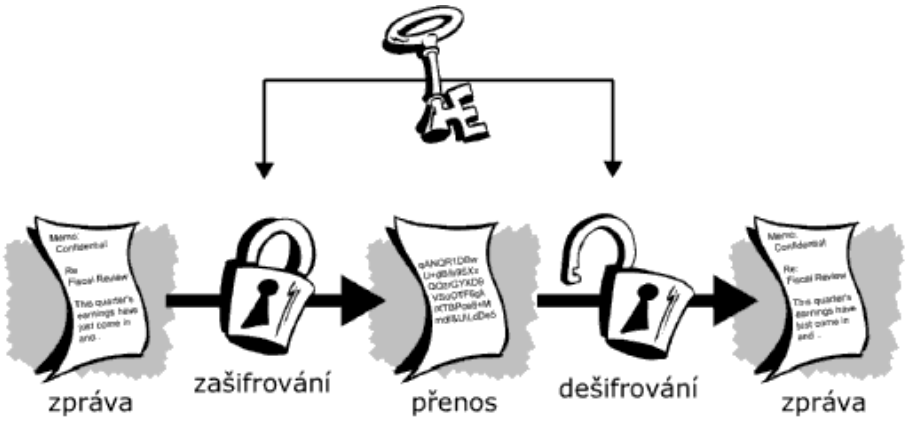
Po dlouhou dobu byl tradičním systémem šifrování vzor se symetrickým klíčem. V tomto režimu je jen jeden klíč, který se používá jak při šifrování, tak při dešifrování informací. Běžné šifrování produkuje s klíčem řadu opatření nad původními daty, procedura dešifrování se provádí pomocí stejného klíče. Dešifrování kódů bez tajného klíče je nemožné.

V praxi se obvykle používají dvě obecné zásady šifrování: disperze a míchání. Disperze se používá pro rozšířeni vlivu ječného znaku otevřeného textu pro mnoho postav šifrového textu: to umožňuje skrýt statistické vlastnosti otevřeného textu. Vývojem této zásady je rozšířit vliv jednoho znaku klíče k mnoha znakům kryptogramu, které pomáhají znemožnit obnovu klíčů po částech.

Míchání se používá při šifrování, které vylučují navrácení vztahu statistických vlastností otevřeného a šifrového textu. Obvyklým způsobem k dosažení dobré disperze je použití kompozitní šifry, která může být provedena ve formě posloupnosti jednoduchých kódů, z nichž každý dělá malý příspěvek ke kumulativní disperzi a míchání. Pro jednoduché šifry se často používají jednoduché náhrady a provedení.

Symetrická kryptografie používá jediného klíče – tajný klíč, který je použit k zašifrování zprávy na straně odesílatele i u příjemce k dešifrování zprávy. Z toho vyplývá nutnost předat před začátkem komunikace nebo v jejím průběhy důvěryhodným kanálem šifrovací klíč spolu s dalšími údaji (např. konkrétní typ algoritmu) druhé straně. Při výměně klíče přes veřejný kanál se využívá asymetrická kryptografie – čímž vzniká chráněný kanál na veřejném kanále. Základní schéma symetrické kryptografie je na obrázku 1.

Obrázek 1 - Šifrování zpráv symetrickou šifrou [12]



2.2 Algoritmy symetrické kryptografie

Současná komerčně dostupná výpočetní technika aplikuje tyto algoritmy téměř v reálném čase. Na druhé straně není nejmodernější výpočetní technika schopna u vhodně zvolené délky klíče dešifrovat data bez znalosti příslušných klíčů, resp. u kratších klíčů (cca 64 bitů) je dešifrovat jen za relativně dlouhé časové období a s velkými finančními náklady. Pomoci matematických metod lze poměrně přesně vyčíslit náklady a čas potřebný k dešifrování dat, které jsou šifrovány definovaným algoritmem [6].

Tabulka 1 - Přehled vybraných blokových algoritmů symetrické kryptografie [3]

Název a základní charakteristika	Typické vlastnosti algoritmu
IDEA (International Data Encryption Algorithm) délka klíče 128 bitů, délka bloku 64 bitů.	Patentovaný, použit společně s RSA v systému PGP, dobrá difúze, pro svou bezpečnost a vysokou rychlost považován za velice kvalitní.
DES Délka klíče 64 bitů (pouze 56 bitů pro	Bývalý kryptograficky standard, vyvinutý firmou IBM v sedmdesátých letech, založen na Feistelových sítích. V roce 1977 se stal

šifrování), délka bloku 64 bitů.	americkou vládní normou pro šifrování, v roce 2000 byl nahrazen standardem AES.
3DES (Triple DES) délka klíče 112 nebo 168 bitů, délka bloku 64 bitů.	Zesílená varianta DES, algoritmus DES je použit třikrát, v prvním a třetím kroku šifruje, v druhém kroku dešifruje. Je výrazně bezpečnější než standardní DES.
Blowfish Proměnná délka klíče (32 – 448 bitů), délka bloku 64 bitů	Navržen autory Adamsem v roce 1993, rychlý šifrovací algoritmus s proměnnou délkou klíče, založen na Feistelových sítích.
ČÁST délka klíče 64 bitů, délka bloku 64 bitů	Navržen autory Adamsem a Tavernsem, velmi podobný algoritmu Blowfish. CAST byl patentován firmou Entrust Technologies, která ho však postoupila pro volné užití.
FEAL (Fast Data Encryption Algorithm) délka klíče 64 bitů, délka bloku 64 bitů.	Navržen v Japonsku v roce 1986, založen na Feistevýh sítích. Původní verze neodolala diferenciální a lineární kryptoanalýze s malým množstvím známých textů. Zesilování zvyšováním počtu kol výpočtu.

2.3 Asymetrická kryptografie

2.3.1 Princip asymetrické kryptografie

V roce 1976 U. Diffi a M. Hellmanom navrhli nový typ šifrovacího systému - systém s veřejným klíčem. V systému veřejného klíče existují dva hlavní klíče - veřejný a soukromý - vybrané tak, aby jejich použití postupného souboru dat ponechávalo pole beze změny. Běžný postup šifrování používá veřejný klíč a pro dešifrování soukromý. Dešifrovací kód bez znalosti tajného klíče není možný, zejména je téměř neřešitelný problém výpočtu tajného klíče od známého veřejného klíče. Hlavní výhodou kryptografie veřejných klíčů je

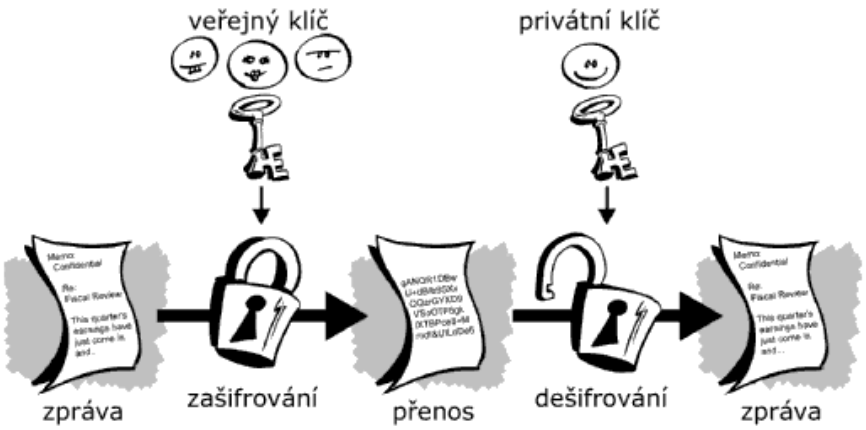
zjednodušený mechanismus pro výměnu klíčů. Při provádění sdělení komunikačním kanálem je přenášen pouze veřejný klíč, který umožňuje to, že lze použít pro tento účel běžné vypouštění, a eliminuje nutnost speciálního bezpečného kanálu pro přenos klíče.

S příchodem systémů s veřejným klíčem se změnilo pojetí ochrany údajů a spolu s ním se funkce kryptografie výrazně zvýšila. V současné době také zahrnuje použití digitálního podpisu (ověřování), udělování licencí, notářské ověření (svědectví), distribuované řízení, hašovací schémata, e-peníze a další. Mezi nejčastější šifrovací funkce veřejného klíče patří digitální podpisy a šifrování. Role digitálních podpisů se v poslední době zvýšila v porovnání s tradičním šifrováním: některé systémy podporují veřejné klíče - digitální podpis, ale nepodporují šifrování.

Oproti symetrické kryptografii se zde používá dvojice klíčů, kterou si vygeneruje uživatel pomocí některého z běžně dostupných programů, a stává se tak jejich jediným majitelem. Pokud nelze prakticky odvodit jeden klíč z druhého klíče, je asymetrická kryptografie označována jako kryptografie s veřejným klíčem [3].

Kryptografie s veřejným klíčem využívá dva různé klíče s různým způsobem jejich použití a je charakteristická tím, že data šifrovaná jedním z klíčů lze v „rozumném čase“ dešifrovat pouze se znalostmi druhého z dvojice klíčů. První z nich – soukromý klíč (tajný klíč) – je bezpečně ukrýván majitelem, zatímco druhy klíč je “věrohodně” zveřejněn nebo přidělen, odtud jeho název – veřejný klíč. Existují dva základní způsoby použití této dvojice klíčů [3].

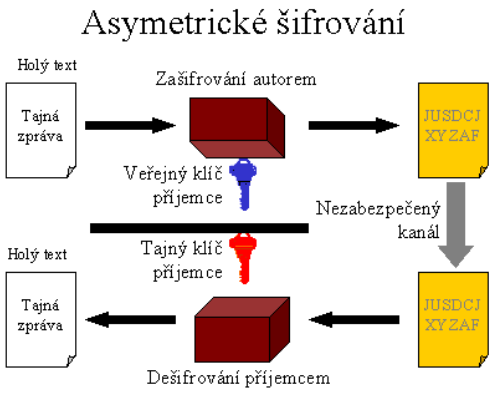
Obrázek 2 - Přenos nešifrované, ale podepsané zprávy [12]



První způsob znázorňuje obr. 2, kde na odesílanou zprávu je použit soukromý klíč odesílatele. Při dešifrování pomocí veřejného klíče odesilatele je pak možné zajistit, že zprávu odeslal právě ten subjekt, jehož veřejným klíčem byla zpráva dešifrována – zpráva nebyla šifrována, ale podepsaná. Za pomoci kryptografie s veřejným klíčem lze takto řešit integritu dat a neodmítnutelnost odpovědnosti na straně odesilatele. Jestliže příjemce pošle podepsané potvrzení o přijetí zprávy, je zajištěna neodmítnutelnost odpovědnosti ze strany příjemce. Není tak ovšem vyřešena otázka důvěrnosti zpráv, tedy nečitelnosti pro neautorizované subjekty, což umožňuje druhý způsob implementace kryptografie s veřejným klíčem [3].

Druhý způsob znázorňuje obr. 3 – na odesílanou zprávu je použit veřejný klíč adresáta. Dešifrování provádí adresát svým soukromým klíčem a zprávu nemůže číst nikdo jiný.

Obrázek 3 - Přenos šifrované, ale nepodepsané zprávy [11].



Tento způsob šifrování používají zejména bezpečnostní protokoly (např. SSL) v první fázi komunikace, kdy se předávají identifikační údaje obou komunikujících stran, a bude použit pro celý zbytek komunikace.

Oba způsoby je také možné zkombinovat, což vytvoří komplexní systém pro utajení i podepsání zprávy. Jinými slovy je tak zajištěna důvěrnost informací, autentizace odesilatele a nepominutelnost odpovědnosti odesílatele.

Nevýhodou kryptografických systémů s veřejným klíčem je jejich pomalost – uvádí se, že asymetrické šifry jsou obvykle 1000 krát pomalejší než šifry symetrické. Proto při řešení konkrétního systému ochrany dat opírajícího se o kryptografické algoritmy je nejlépe kombinovat přístupy symetrické kryptografie s veřejným klíčem v rámci hybridního kryptosystému. Je přitom využívána rychlost symetrických algoritmů na jedné straně a

flexibilita asymetrických šifer na straně druhé. Je také vhodné zvážit, kdy není využití kryptografie s veřejnými klíči nutné – mezi typické případy patří situace, kdy se obě strany osobně setkají k výměně tajných klíčů, resp. v případě prostředí jednoho uživatele [3].

Šifrování veřejným klíčem má mnohem větší prostor klíčů, tj. rozsah možných klíčových hodnot, a proto je méně citlivé na útoky hrubou silou, kdy se zkouší každá možná varianta klíče. Veřejný klíč se snadno šíří, protože nemusí být chráněn před neoprávněným přístupem. Algoritmy pro šifrování pomocí veřejného klíče mohou být použity k vytvoření digitálních podpisů při ověření identity odesílatele dat.

Kryptografický algoritmus s veřejným klíčem je ale extrémně pomalý (v porovnání s šifrovacím algoritmem se soukromým klíčem) a není určen k šifrování velkých objemů dat. Použití veřejného klíče k šifrování je užitečné pouze při přenášení velmi malých datových souborů. Obvykle se šifrování veřejným klíčem používá k šifrování klíče a inicializačního vektoru, které budou použité pro šifrování s privátním klíčem. Po přenosu klíče a vektoru inicializace se používá šifrování soukromým klíčem.

Pro zvýšení účinnosti asymetrické kryptografie se často používají smíšené metody, které implementují různé šifrovací algoritmy. Pokud pro šifrování dat byl vybrán náhodný symetrický algoritmus, používá se symetrický klíč k šifrování zdrojového kódu. Pak používají asymetrický algoritmus z veřejného klíče pro zašifrování symetrického klíče. Pomocí komunikačního kanálu je přenášen text šifrovaný symetrickým klíčem a symetrický klíč je zašifrován pomocí veřejného klíče. Pro dekódování jsou operace prováděny v opačném pořadí: nejprve pro příjemce soukromého klíče je potřeba dešifrovat symetrický klíč a pak použít symetrický klíč.

2.4 El Gamalův systém

Kryptografové neustále hledají efektivnější metody asymetrické kryptografie. V roce 1985 bylo El Gamalem navrženo následující schéma založené na umocňování velkého prvočísla. Pro začátek je potřeba nastavit velké prvočíslo P. Zprávy jsou reprezentovány celými čísly z řady S v intervalech (1, P). Původní protokol zpráv S ve verzi Shamira, jednoho z autorů RSA, vypadá takto: Odesílatel A a příjemce B budou znát pouze P. X generuje náhodné číslo v intervalu (1, R), také B generuje náhodné číslo Y ze stejného intervalu.

V systému El Gamal je vyšší stupeň ochrany, než v algoritmu RSA, což umožňuje téměř o řád zvýšit rychlost šifrování a dešifrování. El Gamal je šifrovací systém založený na tom, že lze snadno vypočítat mocninu celého čísla, stejně jako v operacích s běžnými čísly.

Je však těžké najít exponent, na který je potřeba umocnit dané číslo, aby vysledkem bylo jiné číslo, také zadané. V obecném případě se problém diskrétního logaritmu zdá být těžší než rozklad velkých čísel na prvočinitele, na základě kterých lze předpokládat, že složitost otevření systémů RSA a El Gamal bude podobná. Ale v odolnosti se tyto systémy výrazně liší. Pokud vezmeme v úvahu problém rozkladu libovolného celého čísla o délce 512 bitů na prvočísla a logaritmy celých čísel na 512 bitů, je druhý problém, podle matematiků, mnohem těžší než první. Nicméně je tam jedna vlastnost. Pokud je systém konstruován pomocí algoritmu RSA, šifrant dokázal rozložit veřejný klíč N jedneho z účastníků do dvou prvočísel, možnost zneužití je omezena jen na konkrétního uživatele.

V případě systému konstruovaného algoritmu El Gamal hrozi útok všem účastníkům kryptografické sítě.

Přístup přijatý pro faktorizaci devátého čísla Fermat může výrazně zlepšit způsob diskrétního logaritmu pro některá speciální prvočísla. Ten, kdo nabízí jednoduchý algoritmus pro P El Gamal, má možnost zvolit si speciální číslo, pro které je problém diskrétního logaritmu docela schopný pro běžné počítače.

Je třeba poznamenat, že tento nedostatek algoritmu El Gamal není fatální. Je to dost na to stanovit postup, který zajistí jednoduchý náhodný výběr P v tomto systému. Je třeba poznamenat, že počet zvláštního druhu oslabujících čísel metody El Gamal má velmi malou šanci na jejich výběr a může být ignorován.

2.5 Porovnaní kryptografických systémů

Výhody a nevýhody kryptografických systémů (včetně porovnání se symetrickými kryptosystémy) s veřejným klíčem jsou shrnuty v tab. 2 [3].

Tabulka 2 - Porovnání výhod a nevýhod kryptografie s veřejným klíčem a symetrické kryptografie [3].

Přednosti kryptografie s veřejným klíčem	Nevýhody kryptografie s veřejným klíčem
Soukromé klíče nemusí být přenášeny ani předávány – snadná správa klíčů (včetně jejich výměny). Kromě šifrování může být využita také pro digitální podpis (soukromým klíčem šifrování, podpis dešifrován veřejným klíčem) Veřejný šifrovací klíč může být uveřejněn. Prověřování digitálních podpisů pomocí veřejných klíčů nenarušuje odpovědnost uživatele za ochranu svého vlastního soukromého klíče. Tato skutečnost je často nazývána nepopiratelnost zodpovědnosti za zprávu. Výrazně jednodušší management klíčů.	Při šifrování i dešifrování je výrazně pomalejší než symetrická kryptografie. Může se stát náchylnou k falšování zpráv i tehdy, když soukromé klíče uživatelů nejsou dostupné pro útočníky. Jsou realizovatelné útoky se znalostí dvojic otevřený text – šifrovaný text, resp. útoky proti omezenému množství otevřených textů. Podstatně větší délka klíče pro dosažení stejné úrovně bezpečnosti.

3 Standard DES

3.1 Princip standardu DES

DES (zkratka z angl. Data Encryption Standard) byl v USA po dobu 25 let standardem Federal Information Processing Standard pro blokové symetrické šifrovací algoritmy. DES byl od roku 1977 velice sledován a donedávna byl nejznámějším a nejrozšířenějším symetrickým algoritmem ve světě. DES nikdy nesloužil pro utajování velmi citlivých dat (vojenství, tajné vládní informace) a byl určen pouze pro civilní sektor.

Norma se používá v několika režimech:

ECB (Electronic Code Book) – vhodný pro krátké zprávy nebo pro šifrování klíče. Nedoporučuje se k šifrování delších zpráv, na rozdíl od modů šifrování s různě implementovanou zpětnou vazbou.

CBC (Cipher Block Chaining) – výstupní blok šifrovaného textu je použit jako výstup a současně je sčítán mod 2 s dalším vstupním blokem otevřeného textu. Tento druh provozu je vhodný pro šifrování zprav.

CFB (Cipher FeedBack mode) – nejprve je zašifrován náhodný blok a ten se modulo 2 sečte s prvním blokem otevřeného textu.

OFB (Output FeedBack mode) – šifrovaný text se využívá pro vytvoření zpětné vazby na otevřený text.

Přijetí standardního šifrování DES ovlivnilo použití šifry v komerčních systémech. Zavedení tohoto standardu je skvělým příkladem sjednocení a standardizace systému ochrany. Příkladem systematického přístupu k vytvoření jednotného rozsáhlého informačního systému bezpečnosti je směrnice ministerstva financí z roku 1984, podle které všechny veřejné a soukromé organizace podnikající s vládou USA musí zavést postup pro šifrování DES.

Takže algoritmus DES je hlavním mechanismem, který je využíván v soukromých a veřejných institucích Spojených států v oblasti ochrany informací. Současně Národní bezpečnostní agentura, která je znalcem kryptografických algoritmů, vyvíjí nové algoritmy pro šifrování dat pro masy.

3.2 Základní vlastnosti DES

Využívá bloky o velikosti 64 bitů, pro šifrování používá klíč dlouhý 56 bitů, 8 bitů klíče dává celkem variant šifrování. Původně byl DES navrhován s klíčem délky 112 bitů, což by zajistilo jeho dostatečnou bezpečnost proti útoku hrubou silou.

Je založen na Feistelovských sítích, sestaven z 16 kol výpočtu, byl speciálně vyvinut s ohledem na hardwarovou implementaci.

Postup šifrování (viz obr. 4 a obr. 5):

1. Vstupní permutace 64bitového bloku otevřeného textu bez použití klíče.

2. Rozdělení bloku na dva 32bitové subbloky L a R (levá a pravá strana).

3. V 16 kolech výpočtu se opakuje výpočet.

4. Sloučí se levá a pravá strana a provede se koncová permutace.

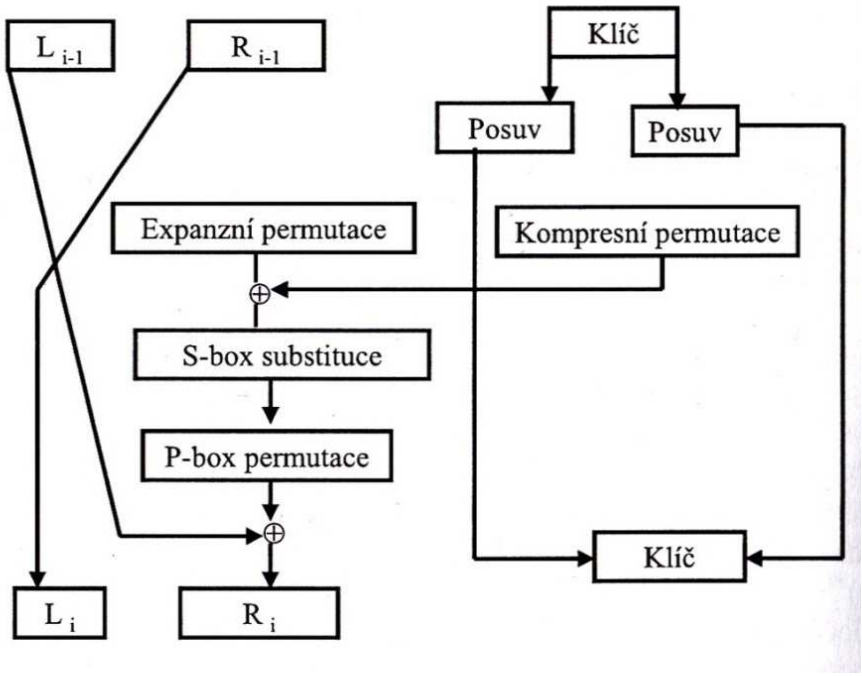
Počáteční a koncová permutace nemá vliv na bezpečnost, souvisí se způsobem jeho implementace.

Vhodnými způsoby prolomení algoritmu DES jsou diferenciální a lineární kryptoanalýza vzhledem k nedostatečné délce klíče i útoku hrubou silou, což bylo několikrát úspěšně ověřeno na paralelních počítačích pro délku klíče 40 bitů a 56 bitů – např. společným úsilím uživatelů internetu.

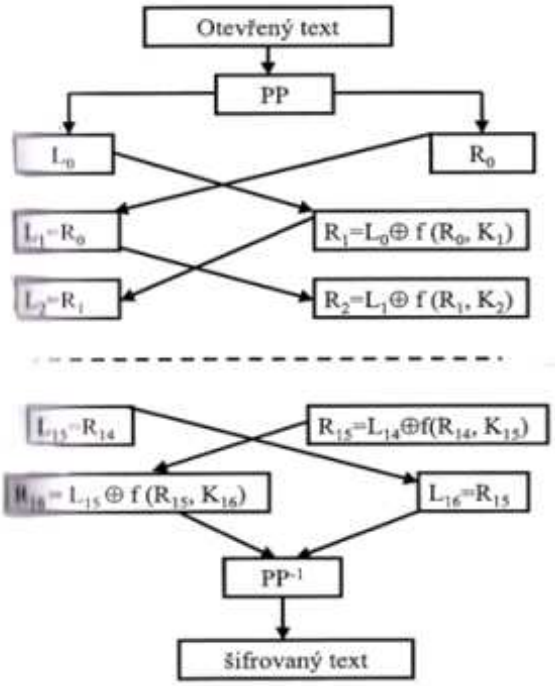
Je-li DES používán ke komunikaci, je třeba měnit často klíče a věnovat speciální pozornost správě klíčů.

Při šifrování souborů na pevném disku neměnit často DES klíče, použít master DES klíč pro zašifrování seznamu DES klíčů.

Obrázek 4 - Jedno kolo výpočtu algoritmu DES [3]



Obrázek 5 - Schéma šifrování algoritmem DES [3]



3.2.1 Hlavní výhody algoritmu DES

Výhody algoritmu DES jsou:

- Používají pouze jeden klíč s délkou 56 bitů.
- Pro šifrování zprávy pomocí ječného balíčku a pro dešifrování můžete použít jakýkoli jiný.
- Relativní jednoduchost algoritmu poskytuje vysokorychlostní zpracování dat.
- Vysoká odolnost algoritmu.
- Proces šifrování a dešifrování.

DES šifruje 64bitové bloky dat pomocí 56bitového klíče. Dešifrování DES je operace opačná a funguje přes opakování kryptografických operací v opačném pořadí.

Proces šifrování vychází z permutací bitů 64-bit bloku, šestnácti cyklech šifrování a nakonec obrácení permutace bitů.

3.3 Šifra AES

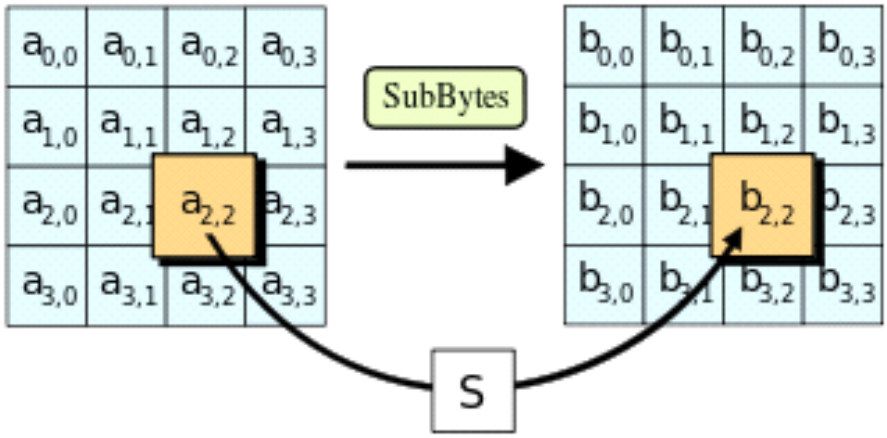
Šifrovací algoritmus AES (Advanced Encryption Standard) patři do standardního symetrického šifru USA. Tento šifrovací standard AES byl vybrán, aby nahradil v otevřeném výběrovém řízení, kde se všechny zúčastněné organizace a jednotlivci mohou učit a komentovat algoritmy.

Soutěž o nahrazení DES byla vyhlášena v roce 1997 Národním institutem standardů a technologie (NIST - National Institute of Standards and Technology). Kde bylo prezentováno 15 algoritmů, které byly vyvinuty dobře známými organizacemi v oblasti kryptografie (RSA Security, přehozy atd.). Výsledky soutěže byly vyhlášeny v říjnu 2000: a vítězem byl vyhlášen algoritmus Rijndael, vyvinutý Vincentém Ridzhmenem a Joanem Daemenem.

Algoritmus Rijndael se nepodobá většině známých symetrických algoritmů, je to struktura, která s nazývá "sítě Feistele". Zvlaštnost sítě Feistele je, že vstupní hodnota je rozdělena do

dvou nebo více dílčích bloků, z nichž některé se v každém kole zpracovávají podle určitého pravidla, pak překrývá neobdělávané bloky (viz obr. 6).

Obrázek 6 - sítě Feistele [6]



Rijndaelův algoritmus je blok dat ve formě dvourozměrného souboru bajtů velikosti 4x4, 4x6 nebo 4X8 (přijatelné mají pevnou velikost bloku šifrovaných dat). Všechny operace se provádí z jednotlivých bajtů souboru, jakož i nezávislými sloupci a řádky.

Rijndaelův algoritmus provádí čtyři transformace: BS (ByteSub) - tabulkové nahrazení každého bytového pole, SR (ShiftRow) - posun řádků pole. V této operaci se první řádek nemění a zbývající byte je cyklicky posunut doleva o stanovený počet bajtů, v závislosti na velikosti pole. Například pole velikosti 4x4 linek 2, 3 a 4, se posune o 1, 2 nebo 3 bajty.

4 Standard RSA

První zmínka o kryptosystému RSA se objevuje v roce 1978 v článku autorů Rivesta,Shamira a Adlemana, jejich iniciály daly název systému. Jedná se o původně patentovanou šifru. Po sedmnácti letech patent vypršel a RSA se stal hodně používaným algoritmem v oblasti bezpečných komunikaci.

Zcela běžně se dnes používá například v bankomatech, v mobilních telefonech nebo pro elektronické podpisy. Na základě využívání RSA vznikla i známá americká společnost RSA Data Security Inc. Bezpečnost RSA je založena na náročnosti řešení úlohy faktorizace – je obtížné rozložit velmi velká čísla (z nichž každé je součinem dvou velkých prvočísel). Navíc míru této bezpečnosti lze prakticky libovolně zvyšovat volbou velikosti klíčů – tedy velikosti prvočísel, která jej tvoří [3].

Algoritmus RSA je jeden ze systémů asymetrické kryptografie, jehož bezpečnost je založena na složitosti výpočtu rozkladu čísla na prvočinitele, avšak při špatné volbě použitých parametrů se bezpečnost může snižovat. V této kapitole jsou podány informace o tom, jak RSA funguje a o doporučeních na volbu klíčů, modulu i exponentů.

V případě RSA jde o šifru asymetrickou, což znamená, že k zašifrování a dešifrování zprávy je použit jiný klíč. Klíč, kterým je zpráva šifrována, je nazýván klíčem veřejným a klíč, který se používá k dešifrování zprávy, je klíč soukromý (privátní), dvojice těchto klíčů se pak nazývá klíčový pár.

Šifra RSA funguje tím způsobem, že každý uživatel má svůj unikátní pár klíčů, ten veřejný klíč je volně dostupný, takže může kdokoliv zprávu tímto klíčem zašifrovat, ale pouze uživatel, který vlastní příslušný soukromý klíč, může zprávu dešifrovat, je to právě tento veřejný klíč, který je spolu s identifikačními údaji vkládán do digitálního certifikátu.

Aby však certifikát opravdu věrohodně identifikoval daného uživatele, je k jeho vydávání využíváno nezávislé třetí strany. Tou je certifikační autorita.

4.1 Princip RSA

Celý algoritmus je tady založen na obtížnosti faktorizace velkých čísel. Oba klíče se odvozují jako součin dvou velkých prvočísel.

$$N = p.q$$

Poté se zvolí šifrovací klíč e tak, aby čísla e a (p-1).(q-1) byla čísla nesoudělná. A pomocí Eulerova rozšířeného algoritmu vypočteme dešifrovací klíč d, pro který platí.

$$e.d = 1(\mathrm{mod}(p-1)(q-1))$$

V tuto chvíli již čísla p a q pro další postup nepotřebujeme. Také je potřeba rozdělit zprávu na bloky, které budou kratší než n.

Pomocí tohoto algoritmů je možné šifrovat a dešifrovat.

Šifrovat: $c = m^e . mod\ n$

Dešifrování: $m = c^d . mod\ n$

4.1.1 Vlastnosti RSA

Číslo n by mělo být větší než 129 míst, protože současná technologie nedokáže rozložit více jak 129timístní dekadický modul.

Pokud by se někdo pokoušel prolomit algoritmus pomocí útoku hrubou silou, tak tato metoda je ještě méně efektivní než se pokusit faktorizovat číslo n.

RSA je však asi 1000 krát pomalejší než DES při hardwarové realizaci a 100krát pomalejší než při softwarové realizaci [1].

Algoritmus se dá urychlit vhodnou volbou hodnoty e. Nejpoužívanější jsou hodnoty 3, 17, 65537. Číslo 65537 totiž obsahuje v binárním vyjádření pouze 2 jedničky, čímž se urychluje výpočet [5].

4.1.2 Bezpečnost RSA

Bezpečnost kryptosystémů RSA závisí zcela na problému nacházeni činitele pro velká čísla. Technicky je toto tvrzení nepravdivé. Nikdy nebylo prokázáno matematicky, že je potřeba rozšířit na činitele n, aby se našlo m. Je zřejmé, že existuje úplně jiný způsob dešifrování RSA. Nicméně tato nová metoda umožňuje dostat d, které může být také použito pro nacházení činitele.

Zde je také možné dešifrovat RSA pomoci hodnoty (p-1) (q-1). Tento útok je snazší než nacházení činitele n.

Nejzřejmějším způsobem je nacházení činitele n. Každý útočník muže získat veřejný klíč e a modul n. Cílem je nalézt dešifrovací klíč d, oponent musí rozložit činitele n. Ted' je zřejmé, že číslo pro odhadnutí musí obsahovat 129 desetinná místa. Proto musí být n větší než tato hodnota.

Samozřejmě může kryptoanalytik projít všechna možná d, než vybere správnou hodnotu. Ale není to efektivní.

Čas od času se objevuje, že byl nalezen jednoduchý způsob, jak otevřít RSA, ale zatím žádné z těchto sdělení nebylo potvrzeno. Například v roce 1993 v návrhu článku Williama Payna byla zveřejněna metoda, která je založena na teoréme Fermat. Bohužel tato metoda je pomalejší než faktoringová.

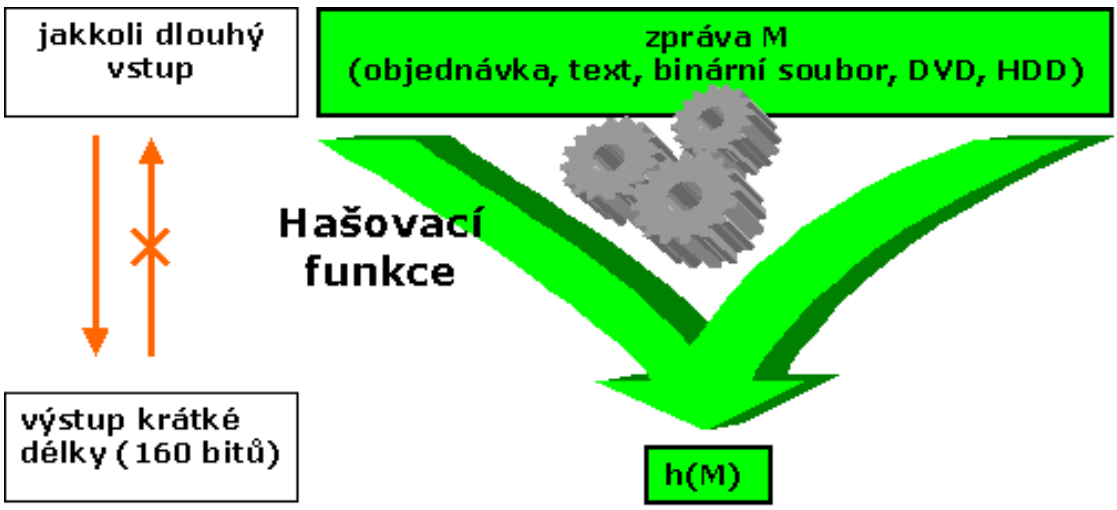
5 Hašovací funkce

5.1 Koncepce hašovací funkce

Aplikace asymetrických algoritmů je výrazně pomalejší než užití algoritmů symetrických, což je dáno matematickou podstatou asymetrických algoritmů. Proto se mnohdy při tvorbě digitálního podpisu nešifruje soukromým klíčem odesílatele celá zprava, ale nejprve se na data použije jednosměrná hašovací funkce. Hašovací funkce vrací jednoznačnou hodnotu pevné délky. Haš si lze představit jako zhuštěnou hodnotu dlouhé zprávy. Opačný proces je nemožný. Výpočet haš-hodnoty zprávy je velmi rychlý. Při digitálním podepisování se nejprve vypočte haš-hodnota zprávy, která bývá výrazně kratší než podepisovaná zpráva, a ta se zašifruje některým asymetrickým algoritmem s použitím soukromého klíče. Výsledkem je takzvaný digitální podpis, který je potom odeslán jako příloha zprávy nebo v samostatném bloku. Výhodou digitálního je, že splňuje stejná bezpečnostní kritéria jako podpis celého dokumentu, provedení však trvá nesrovnatelně kratší dobu [3].

Hašovací funkce byla původně označením pro funkci, která libovolně velkému vstupu přiřazovala krátký hašovací kód o pevně definované délce.

Obrázek 7 - Hašovací funkce [5]



5.2 Základní vlastnosti

Hašovací funkce je jednosměrná matematická funkce, jejíž vstupem je blok proměnné délky a výstupem je blok pevné délky (obvykle 128 či 160 bitů). Výstup se nazývá haš. Na rozdíl od šifrování je tady hašování jednosměrnou funkcí – výsledek výpočtu je jednoznačným obrazem originálu, ale dochází k redukci množství původní informace, a originál proto nelze rekonstruovat. Hašovací funkce se využívají jako součet protokolů pro digitální podpisy, jsou součástí kryptografických protokolů, certifikátů, běžné je využití při bezpečném uložení a při kontrole hesel v operačních systémech. Příklady praktického použití: autentizace knihy (autorského díla), ukládání hesel na serveru v podobě hašovaných bloků (pouze porovnání po vložení hesla, heslo není principiálně dostupné ani správci sítě), hašování příchozí zprávy před jejím podpisem soukromým klíčem [11].

Vlastnosti hašovací funkce:

- Pro delší texty komprese souboru, jednosměrnost operace. Tím, že zkrátí proměnný obsah zprávy na haš o konstantní délce, umožní podstatně urychlit proces šifrování i dešifrování.
- Pro libovolnou změnu v původním dokumentu se tato změna projeví i v haš-hodnotě – tím je spolehlivě detekováno zachování integrity dokumentu.
- Pro dva odlišné dokumenty nesmí existovat stejná haš-hodnota – požadavkem je vyloučení kolizí. Tento teoretický předpoklad není v praxi dosažitelný na 100 %, ale pravděpodobnost shody dvou haš-hodnot pro dva odlišné dokumenty musí být minimalizována a je dána délkou haše.

5.3 Formální popis hašovací funkce

Hašovací funkce je matematická funkce, která převádí vstupní posloupnost D bytů jakékoliv délky na posloupnost konstantní délky R bitů.

$$H: D \rightarrow R, \text{ kde } D>R$$

Existence kolizí plyne z pojmu hašovací funkce, tyká se dvojice vstupních dat (x, y), $x \neq y$ tak že $h(x) = h(y)$. Znamená to, že dvojice různých vstupních dat může mít stejnou haš.

Kolize jsou nežádoucí, ale nelze se jim vyhnout, možná jenom snižovat pravděpodobnost výskytu. Hlavním cílem je dosáhnout nejvyšší pravděpodobnosti, že dvojice zpráv se stejnou haší je totožná.

Pro eliminaci kolize by hašovací funkce musela být stejné délky jako vstupní data. Tím by ztratila efektivita v kompresi další zpracování.

5.4 Hašování hesel

Metoda hašování hesel umožňuje uživatelům ukládat ne 128 bajtů a smysluplný výraz, slovo nebo řetězec znaků, který se nazývá heslo. Skutečně při vývoji jakéhokoliv šifrovacího algoritmu je třeba poznamenat, že u koncového uživatele systému je člověk, ne automatický systém. To vyvolává otázku, zda je opravdu pohodlné pro osobu si pamatovat 128bitový klíč (32 hexadecimálních číslic). Ve skutečnosti limit na hranici zapamatovatelnosti je 8,12 znaků. A proto pokud přinutíme uživatele k použití takového klíče, tak jej téměř nutíme k tomu, aby si klíč poznamenal na kus papíru nebo uložil v elektronické formě, například jako text. To samozřejmě výrazně snižuje bezpečnost systému.

Hašovací funkce v tomto případě se nazývá matematické nebo algoritmické transformace daného bloku dat, který má následující vlastnosti:

- Hašovací funkce má nekonečnou doménu.
- Hašovací funkce má konečný rozsah.
- Hašovací funkce je nevratná.

Tyto vlastnosti umožňují použít pro vstup haš. funkce hesla, která jsou textové řetězce libovolné délky v každém národním jazyce. Omezení rozsahu funkčního rozsahu 0, …, 2N-1, kde N - délka klíče v bitech.

5.5 Využiti hašovacích funkcí

Hašovací funkce je použita pro ověření integrity. Pod slovem integrita rozumíme celistvost dat. Ověřená integrita znamená, že přijata zpráva musí být shodná se zprávou, která byla odeslaná.

S tímto pojmem souvisí korekční a detekční kódy. Smyslem detekčních kódů je odhalení chyby v přenosu informací. Často je používaná technika, kde se používá vypočet kontrolního součtů zpráv, který je poslán s původní zprávou. Na druhé straně je vypočítán z příchozí zprávy kontrolní součet a je porovnán s původním. Jestli se ten součet liší, integrita je narušena. Korekční kód mají také takové vlastnosti, které umožnuji ten kód opravit.

Cyklický redundantní součet je speciální hašovací funkce, která je často používaná pro detekcí chyb během přenosu dat. Jde o velmi rozšířený způsob realizace kontrolního součtu kvůli své dobré matematické vlastnosti a jednoduchosti.

Kontrolní součet je odesilán společně s informací a slouží k ověření, jesti při přenosu nebo uchování mohlo dojít k chybě. Pak je zase nezávisle spočítán. Pokud jsou kontrolní součty odlíšné, je jasné, že při přenosu došlo k chybě. Jestli jsou shodné, znamená to, že k chybě ndošlo. Také je možné chyby opravovat.

Jako přiklad může sloužit použití kontrolního součtu ve statistických výkazeh nebo v daňovém přiznání, kde je předávána řada čísel a kontrolním součtem je součet všech těchto čisel. Cyklický redundantní součet je možné použít pro zajišťování chyb, které vznikly v důsledku selhání techniky. Pro odhalení záměrné změny dat počítačovými piráty je slabý.

6 Digitální certifikát

Digitální certifikát je digitálně podepsaný veřejný šifrovací klíč, který slouží k ověření identity protistrany při navazování zabezpečené komunikace. Certifikát má formu souboru s pevnou strukturou, která je popsána normou X.509. Každý digitální certifikát tedy obsahuje následující údaje:

- Verze.
- Sériové číslo (volitelný).
- Identifikační údaje autority vydávající certifikát.
- Platnost od – do.
- Jméno subjektu, pro který se certifikát vydává.
- Veřejný RSA klíč subjektu (viz následující kapitola).
- Další informace (od X.509 v3 a výše).

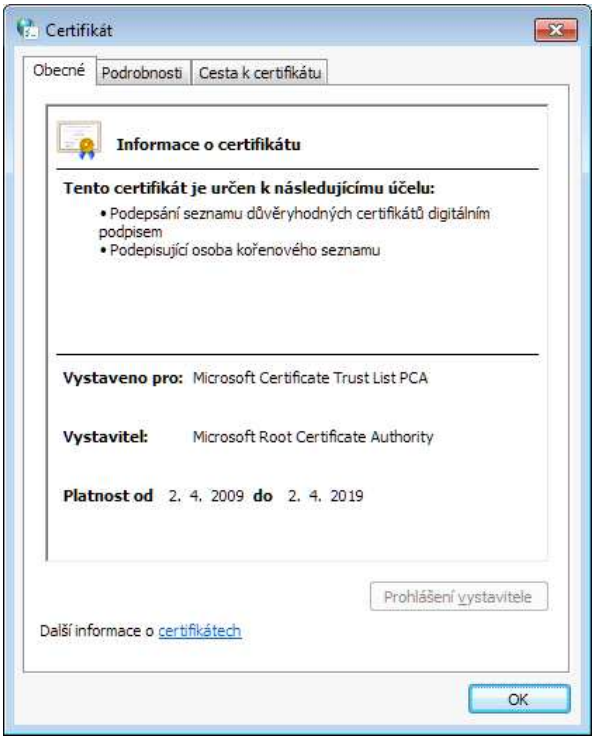
6.1 Certifikační autorita

Certifikační autoritou je subjekt, který ověřuje pravdivost poskytovaných údajů pro vydání certifikátu. Princip komunikace uživatelů s touto třetí stranou popisuje obr. 9. Pro certifikační autoritu je nejdůležitější důvěra, což znamená, že certifikáty, které vydává, musí mít vždy pravdivé údaje, proto musí pečovat o svoji důvěryhodnost. Stejně jako v mnoha jiných prostředích i toto je jen tak silné, jako jeho nejslabší článek, pokud je autoritou vydán certifikát s neplatnými údaji, její důvěryhodnost upadá.

Certifikáty, které jsou frekventovaně využívané, mohou být integrovány do webových prohlížečů, viz obr. 8.

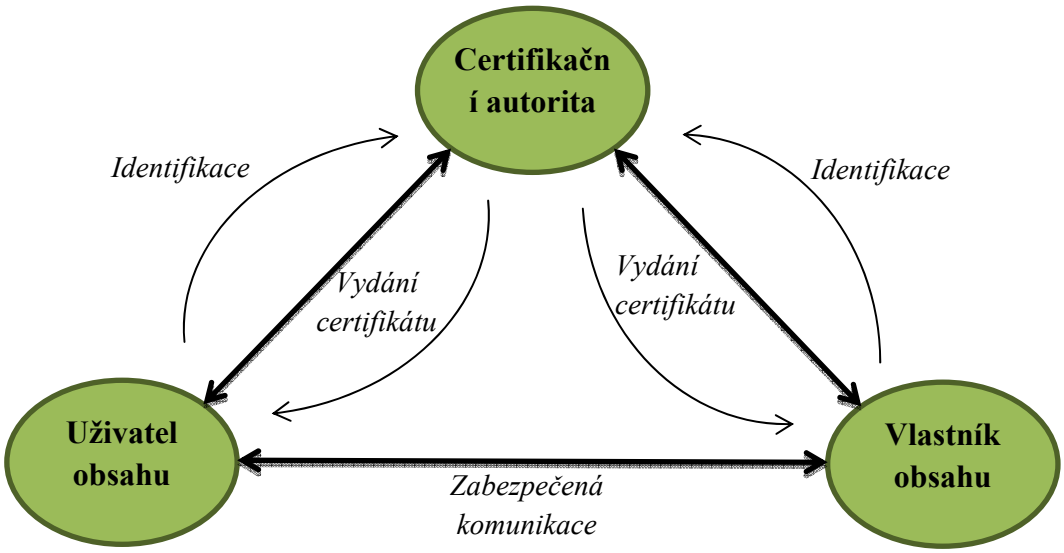
Obrázek 8 - Příklad certifikátu z webového prohlížeče

Zdroj: vlastní úprava



Obrázek 9 - Princip využití certifikační autority pro zabezpečenou komunikaci

Zdroj: vlastní úprava



7 Digitální podpis

7.1 Popis principu digitálního podpisu

Velkou výhodou asymetrické kryptografie je, že umožňuje implementaci digitálního podpisu. Digitální podpis slouží ke stejnému účelu jako běžný ruční podpis. Ruční podpis však lze jednoduše padělat. Digitální podpis je mnohem kvalitnější a jeho padělání je téměř nemožné [5].

Elektronický podpis může mít následující funkce:

- Důkaz o zdroji dokumentu. V závislosti na podrobnostech vymezení dokument může být podepsán, jako je "autor", "změny", "časové razítko" atd.
- Ochrana před změnami v dokumentu. Pro náhodné nebo úmyslné změny dokumentu (nebo podpis) změní haš, podpis se tedy stává neplatným.
- Aby se vytvořil platný podpis, vlastník musí znát soukromý klíč, který je znám pouze jemu, proto vlastník nemůže odmítnout svůj podpis k dokumentu.
- Firmy a obchodní organizace v poskytování finančních výkazů veřejných institucí v elektronické podobě;

Digitální podpis zajišťuje:

- Autenticitu – důkaz, že odesílatel dokument skutečně podepsal. Jde o potvrzení totožnosti.
- Integritu zprávy – po podpisu již nelze dokument upravovat.
- Jednorázovost použití – podpis nelze aplikovat na jiný dokument.
- Neodmítnutelnost zodpovědnosti – odesílatel se nemůže zbavit zodpovědnosti za dokument, který je podepsán jeho jménem. Podpis má právní závaznost a může sloužit jako důkaz v právním sporu [6].

7.2 Definice digitálního podpisu

Digitální podpis je mechanismus, kterým se zajišťuje důkaz nepopiratelnosti dat (správnosti dokumentů). Digitální podpis je binární číslo, jehož délka bývá až 4096 bitů. Jeho vypočet nebo ověření nelze provádět ručně, protože jde o složité matematické operace. Digitální podpis vzniká matematickým spojením 2 čísel. První číslo je část dokumentu získaná matematickým výpočtem a označuje se jako haš dokumentu. Druhé číslo se nazývá souhrnný elektronický klíč. Takto vzniklá digitální podpis se pak připojí k dokumentu [6].

Stejně jako v reálném světě ruční podpis identifikuje jeho autora, digitální podpis jednoznačně označuje uživatele ve světě elektronickém. Digitální podpis se používá k podepisování dokumentů, a lze tím jednoznačně určit, zda byl obsah dokumentu po jeho podpisu změněn.

Postup podepisování dokumentu probíhá stejně jako při šifrování zprávy jen s tím rozdílem, že se k zašifrování použije privátní šifrovací klíč, tento zašifrovaný dokument se připojí k originálnímu nezašifrovanému, díky digitálnímu certifikátu může být veřejným klíčem v něm uchovaný dokument dešifrován a porovnán s originálem, pokud se shoduje, je jisté, že po své cestě mezi odesílatelem a příjemcem nebyl dokument změněn.

Šifrování je však časově náročný proces, proto se nešifruje celý dokument, nýbrž se vytvoří otisk, což je vlastně zjednodušeně řečeno zmenšená část dokumentu. Otisk neboli haš je vytvářen hašovací funkcí, mezi neznámější algoritmy patří například MD5 (message-digest algoritm) nebo SHA (secure hash algorithm).

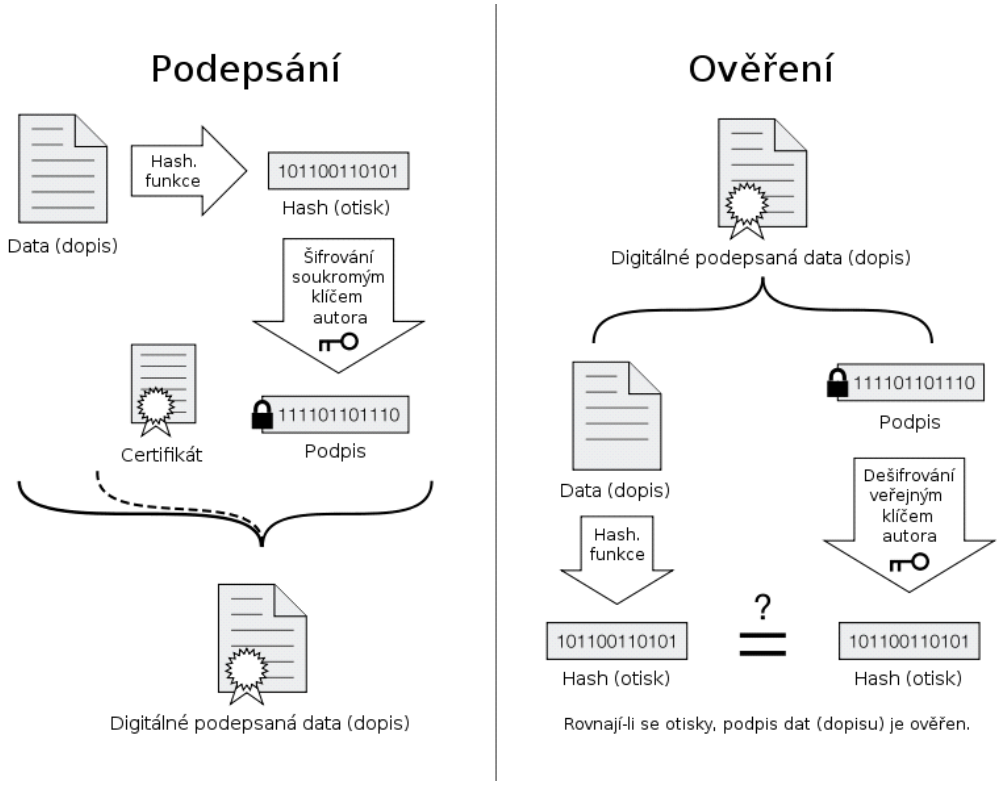
Přestože je otisk méně obsáhlý než samotný dokument, jeho hlavní výhodou je, že se v něm projeví jakákoliv změna v dokumentu, ať už je sebemenší.

7.3 Vytvářeni digitálního podpisu

Digitální podpis se vytváří ve dvou krocích - obr. 10:

Spočítá se otisk z dokumentu. Výsledný otisk se šifruje soukromým klíčem uživatele, který podpis vytváří. Soukromý klíčem šifrovaný otisk ze zprávy se nazývá digitální podpis zprávy.

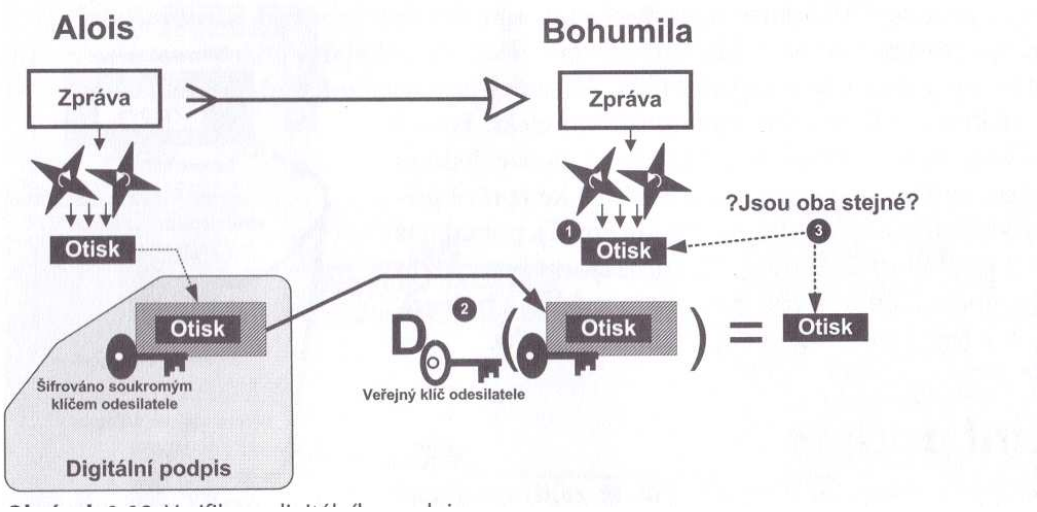
Obrázek 10 - Podepsání a ověření elektronického podpisu [4]



Na obr. 11 je pak znázorněno ověřování (verifikace) digitálního podpisu. To se provádí ve třech krocích:

- Příjemce samostatně spočte otisk z přijaté zprávy.
- Příjemce dešifruje přijatý digitální podpis veřejným klíčem odesilatele.
- Příjemce porovná výsledek získaný z bodu 1 s výsledkem získaným z bodu 2. Pokud jsou stejné, pak mohl digitální podpis vytvořit pouze ten, kdo vlastní soukromý klíč odesilatele – tedy odesilatel. A navíc tato skutečnost prokazuje, že zpráva nebyla během přenosu pozměněna.

Obrázek 11 - Verifikace digitálního podpisu [1]



Digitální podpis provádí důkaz pravosti na základě vlastnictví soukromého klíče. Je tedy nutné, abychom si své soukromé klíče dobře střežili. Ztráta soukromého klíče je pak obdobná jako výměna podobizny v občanském průkazu či záměna otisků prstů v evidenci zločinců.

Na rozdíl od šifrování použije digitální podpis klíč odesilatele. Ten algoritmus umožnuje nejprve dešifrovat soukromý klíč a pak šifrovat veřejným klíčem, tj. že operace šifrování a dešifrování jsou zaměnitelné. Algoritmem, který takovouto záměnu umožnuje, je právě algoritmus RSA [1].

7.4 Vlastnosti digitálního podpisu

- Autenticita.

Autenticita znamená, že lze ověřit identitu subjektu, kterému patří elektronický podpis. Autenticita je realizována pomocí přenosu důvěry.

- Integrita.

Pomocí integrity lze prokázat, že od vytvoření elektronického podpisu nedošlo k žádné změně v podepsaném dokumentu, tj. že dokument (podepsaný soubor) není úmyslně či neúmyslně poškozen.

- Nepopiratelnost.

Nepopiratelnost znamená, že autor nemůže tvrdit, že elektronický podpis příslušný k dokumentu nevytvořil. Důvodem je fakt, že pro vytvoření elektronického podpisu je potřeba privátní klíč, který je těsně svázán s veřejným klíčem, pomocí kterého dochází k matematickému ověření elektronického podpisu. Bez přístupu k privátnímu klíči nelze elektronický podpis vytvořit a ověření elektronického podpisu může být provedeno jen veřejným klíčem, který k němu patří.

- Časové ukotvení.

Elektronický podpis může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu. Časové razítko vydává důvěryhodná třetí strana, a protože je součástí elektronického podpisu, lze ji ověřit stejným postupem jako elektronicky podepsaný dokument [6].

7.5 Bezpečnost digitálního podpisu

Na bezpečnost digitálního podpisu má vliv použitá podepisovací a ověřovací metoda, bezpečnost implementace algoritmu v konkrétní aplikaci, spolehlivost oprávněné osoby (jak udržuje svůj soukromý klíč v tajnosti). Protože zaručený elektronický podpis je vázán na konkrétní fyzickou osobu, lze předpokládat, že každý si bude svůj soukromý klíč chránit, podobně jako PIN ke kartě do bankomatu, jinak bude nést důsledky za zneužití svého podpisu [3].

Hlavní rizika digitálního podpisu:

- Krádež privátního klíče.

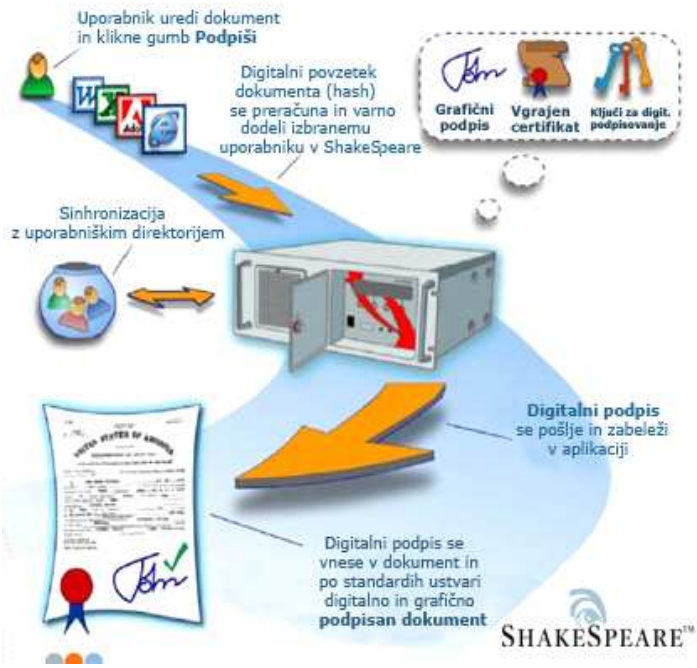
- Vydavatel digitálního certifikátu neoprávněně zkopíruje informace pro podepisování, jinak tajný klíč může byt předán třetí osobě.
- Odhadnuti šifrovacího algoritmu (může být pouze v případech špatné provedeného vlastního algoritmu).
- Padělání veřejného klíče odesilatele, narušení jednoznačnosti vazby veřejného klíče na danou osobu.

7.6 Elektronický podpis v praxi

V následujícím textu si ukážeme, k čemu může být využít zaručený podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.

Ministerstvo financí umožňuje občanovi, který disponuje uznávaným elektronickým podpisem podat přiznání k některým daním elektronickou formou.

Obrázek 12 - Elektronický podpis v praxi [12]



Dále ministerstvo dovoluje podat elektronickou cestou oznámení o nezdaněných vyplacených částkách fyzickým osobám a podat obecnou písemnost [9].

Instituce velikosti zdravotních pojišťoven si mohou dovolit zřídit elektronickou podatelnu nebo portál pro komunikaci se svými smluvními partnery – zdravotnickými zařízeními a případně klienty – pojištěnci. Této možnosti využilo zatím sedm našich pojišťoven. Využití systému klienty umožnila zatím pouze Hutnická zaměstnanecká pojišťovna.

Všeobecná zdravotní pojišťovna, naše největší, má přístup povolen pouze pro zdravotnická zařízení a zaměstnavatele. Česká národní zdravotní pojišťovna, Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví, Revírní bratrská pokladna, Zaměstnanecká pojišťovna Škoda a Zdravotní pojišťovna Metal-Aliance provozují systém, který je rovněž určen jen zdravotnickým zařízením a zaměstnavatelům. Mezi běžnou funkcionalitu těchto systémů patří možnost elektronického vyúčtování zdravotní péče, které využívají zdravotnická zařízení a hromadné oznámení zaměstnavatele společně se zasíláním přehledu o platbě pojistného, které slouží zaměstnavatelům [9].

Pokud jsou oba komunikující subjekty držiteli certifikátu, mohou použít své veřejné klíče k zašifrování zprávy.

Šifruje se veřejným klíčem příjemce. Není vhodné používat stejný klíč pro více účelů, jelikož to usnadňuje případný útok. Podepsání zaručí druhé straně jistotu odesilatele. Hlavní možností, jak využít elektronický podpis, je podepisování dokumentů. Takto je možné podepisovat hlavně dokumenty ve formátu pdf, dokumenty vytvořené v prostředí MS Office a přílohy k elektronické poště.

Závěr

Současná kryptografie je nejdůležitější součástí informačních systémů začínající od e-mailu, přístupu k internetu a e-bankovnictví. Šifrování zajišťuje odpovědnost, transparentnost, přesnost a důvěrnost. Snaží se zabránit podvodům v oblasti e-commerce a poskytuje platné finanční transakce. Kryptografie pomáhá vytvořit svou identitu, ale také poskytuje anonymitu.

V teto bakalářské práce jsem popsala stručný přehled hlavních metod moderní kryptografie. Popsala jsem klasické moderní metody šifrování. Samozřejmě že existují i jiné kryptografické metody symetrických systémů (LOKI, NewDES, IDEA, SKIPJAK ITD) a asymetrických systémů (LUC, Rabin), ale princip činnosti zůstává stejným. Neměla jsem za cíl zde popsat všechny známé kryptografické metody.

Výsledkem práce byly ty nejznámější z asymetrických a symetrických šifrovacích metod.

Seznam použité literatury

Tištěná literatura

[1] DOSTÁTEK, Libor, VOHNOUTOVÁ, Marta, KNOTEK, Miroslav. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu, 2. Aktualizované vydání. Computer Press, a.s., Brno, 2009. ISBN 978-80-251-2619-6.

[2] POŽÁR, Josef. Informační bezpečnost. [s.l.] : Aleš Čeněk - vydavatelství a nakladatelství, 2005. 311 s. ISBN 80-86898-35-5.

[3] ZELENKA, J., ČAPEK, J., FRANCEK, J. a JANÁKOVÁ, H. Ochrana dat. Kryptologie. 1 vyd. Hradec Králové : Gaudeamus, 2003. ISBN 80-7041-737-4.

Elektronické zdroje

[4] Citace. In: Wikipedia: the free encyclopedia [online]: Elektronický podpis, [cit. 9. 3. 2013]. Dostupný z:
http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis

[5] KLÍMA, Vlastimil: Hašovací funkce, principy, příklady a kolize, [cit. 7-11-2005], Dostupný z:
http://cryptography.hyperlink.cz/2005/cryptofest_2005.htm#_Toc98987052

[6] Citace. In: Wikipedia: the free encyclopedia [online]: Advanced Encryption Standard, [cit 9. 3. 2013]. Dostupný z:
http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard

[7] Citace. In: Wikipedia: the free encyclopedia [online]: Cryptographic hash function, [cit 9. 3. 2013]. Dostupný z:
http://en.wikipedia.org/wiki/Cryptographic_hash_function

[8] BERÁNEK, Marek, LÍPA, Tomáš, PODZIMEK, Ondřej: Elektronický podpis. [cit. 13-12-2008], Dostupný z: http://kryptologie.uhk.cz/54.htm

[9] STEGURA, Tomáš. Teorie a praxe elektronického podpisu. . Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra systémové analýzy. 2004 Dostupné z: < http://www.vkc.cz/pdf/stegura-2004_ep_bak-prace.pdf>..

[10] Jak funguje digitální podpis [cit. 23-10-2002], Dostupný z: http://interval.cz/clanky/jak-funguje-digitalni-podpis/

[11] ELEKTRONICKÝ PODPIS, [cit. 25-3-2008]
Dostupný z: http://sandbox.cz/~varvara/El_podpis/index.html

[12] KRYPTOGRAFIE: Moderní metody šifrování, Redakce PCT , [cit. 19-7-2005].
Dostupný z: http://pctuning.tyden.cz/index.php?option=com_content

Seznam použitých tabulek a obrázků