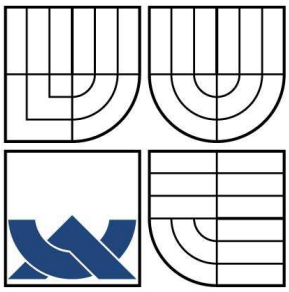
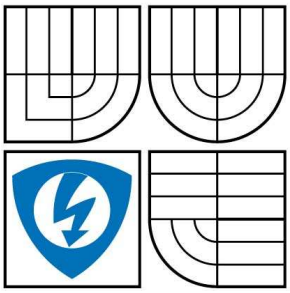


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

DIGITÁLNÍ PODPIS
DIGITAL SIGNATURE

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE **ALEŠ VAVERKA**
AUTHOR

VEDOUCÍ PRÁCE **DOC. ING. VÁCLAV ZEMAN, PH.D.**
SUPERVISOR

BRNO 2008

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma "Digitální podpis" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení
ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.“

V Brně dne 3. 6. 2008 **…....……..**

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce doc. Ing. Václavu Zemanovi, Ph.D. za cenné rady a připomínky při zpracovávání bakalářské práce.

V Brně dne 3. 6. 2008 **.....……..**

(podpis autora)

ANOTACE

Digitálního podpisu, které je námětem této semestrální práce, je v současnosti velmi aktuální. Se stále vzrůstajícími možnostmi internetu a vidinou snižující se četnosti používání papírové dokumentace bylo nutné vyvinout metodu podepisování virtualizovaných dokumentů, která by byla stejně nenapadnutelná a bezpečná jako vlastnoruční podpis. Metoda nese název digitální podpis.

V práci se zaměříme se na vysvětlení základních pojmů souvisejících s digitálním podpisem, vysvětlením základních pojmů s ním souvisejících jako je certifikát, certifikační autorita, autentizace, ale zejména na základní šifrovací algoritmy a aplikace, dále pak na aplikace ve kterých se digitálního podpisu využívá, například poštovní servery či elektronické bankovnictví. V závěru práce se pokusíme zhodnotit přínos digitálního podpisu a jeho nevýhody.

Tato práce si neklade za cíl podat detailní popis procesů šifrování dat, jejím cílem je seznámit přehlednou a srozumitelnou formou širší i nezasvěcenou veřejnost s danou problematikou.

ABSTRACT

Digital signature, the subject of this semester paper, is nowadays very up-to-date. The still rising capabilities of the internet and the vision of lowering the amounts of paper documentation made it necessary to develop a way of signing documents which are transferred through the internet. This is supposed to be equally safe and unassailable as the handwritten signature. This method is called the digital signature.

The paper focuses on the explanation of the essential terms connected to digital signature, such as certificate, certification authority, authentication, but in particular on the elementary cryption algorithms, further on applications that make use of digital signature, e.g. post services and electronic banking. In the final chapter, the positive and negative aspects of the electronic signature are discussed.

This paper is not aspiring to give a detailed description of the processes of data cryption. Its aim is to present an understandable overview of the subject for the public.

OBSAH **str.**

1. ÚVOD

Téma digitálního podpisu, které je obsahem této semestrální práce, je v současnosti a nějaký čas jistě ještě bude tématem aktuálním. Alespoň do doby, než další nové technologie dokážou tento mechanismus popřít, což je ve světe informačních technologií více či méně pravidlem. Nicméně, ve prospěch tvrzení, že téma digitálního podpisu je v současnosti aktuální, mluví neustálý rozmach informačních technologií a zejména používání internetu, který je jedním z hlavních důvodů, proč právě algoritmy digitálního podpisu se staly ne-li nezbytností, tak alespoň užitečnou záležitostí v našem čím dál tím více virtuálním světě.

Máme na mysli hlavně jeho praktické využití v dnešním, na byrokracii založeném, světe. Jak příjemné by bylo moci vyřizovat veškeré formality týkající se například daní apod. z pohodlí domova s nezvratitelnou jistotou, že důvěrné informace, které tímto způsobem odešleme, se nedostanou do nepovolaných rukou.

Dostáváme se k rubu a podstatě celé věci. Aby totiž bylo možné zpracovávat, posílat a považovat za důvěryhodné informace podobného charakteru, je nutné, aby systém podepisování těchto virtualizovaných dokumentů byl stejně nenapadnutelný jako je pouhý vlastnoruční podpis, tzn. aby splňoval nároky na autentizaci, integritu, neodmítnutelnost odpovědnosti. Tímto a mnohým dalším se budeme v práci zabývat.

Zaměříme se na digitální podpis jako takový, vysvětlení základních pojmů s ním souvisejících, na základní šifrovací algoritmy a aplikace, ve kterých se digitálního podpisu využívá. V závěru práce se pokusíme zhodnotit přínos digitálního podpisu a jeho nevýhody.

2. STRUČNÁ HISTORIE KRYPTOGRAFIE

Téma a nutnost šifrování nejrůznějších typů zpráv byli lidstvu vlastní odnepaměti. Mezi nejznámější historické způsoby šifrování bychom mohli zařadit např. Caesarovu šifru (50 př.n.l.), tabulku záměn, různé druhy aditivních šifer mezi nimiž např. Vigenerovu šifru ze 16. st. či Vernamovu šifru ze století 20. Posledně jmenovaná je dodnes považována za nerozluštitelnou, o čemž svědčí důkazy matematika C. E. Shannona ze čtyřicátých let. Dále jmenujme např. Cardanovu mřížku, či dnes už chronologicky známou Morseovu abecedu či stenografii, která je považována za starší sestru dnešní kryptografie.

Nabízí se otázka „Co měly tyto šifrovací metody a systémy navzdory různé úrovni složitosti společného?“ Rozumí se samo sebou, že účelem šifrování, neboli převádění informací do nečitelné podoby za pomoci nejrůznějších matematických a jiných kódů a principů, bylo uchránit tyto informace před nepovolanými třetími osobami. V historických dobách byly nejčastějším motivem takového počínání nejrůznější politické, vládní a potažmo vojenské důvody, které ale našly své uplatnění i ve 20.st. - vzpomeňme např. šifrovací stroj ENIGMA, využíván převážně za druhé světové války.

Současným a stále častějším motivem šifrování se stala s vývojem informačních technologií nutnost chránit zprávu samotnou ne coby tajný text sloužící k ofenzivním účelům ale chránit ji i coby autentický text a tím i jejího autora, tzn. zamezit jejímu případnému narušení či přivlastnění třetí osobou, narušení její integrity, což by mohlo mít pro autora významné následky.

Se stoupajícími možnostmi internetu a s vidinou snižující se četnosti používání papírové dokumentace bylo tedy nutné vyvinout metody, které by takovouto bezpečnost přenosu informací a identitu autora zaručovaly. Společným jmenovatelem pro tyto současné šifrovací algoritmy, využívané v informačních technologiích, je **DIGITÁLNÍ PODPIS**.

Než se ale podíváme blíže na jednotlivé algoritmy šifrování, které se využívají v digitálním podpisu, je nutné podotknout, že v praxi je často digitální podpis zaměňován s termínem elektronický podpis a naopak, což může být zavádějící. Jaký je tedy mezi nimi rozdíl, je-li nějaký?

Termíny digitální a elektronický podpis jsou často používány jako synonyma. Zatímco v Evropě je zaužíván spíše druhý výraz a byl takto 1. října 2000 i legalizován zákonem č.227/2000 Sbírky, v USA se naopak užívá termínu digitální podpis.

Jistý rozdíl zde nicméně existuje. Digitální podpis je jakýsi datový soubor vygenerovaný na kryptografickém základě připojený k vlastnímu souboru dat, *zatímco za elektronický podpis se v širším významu považuje i prosté nešifrované uvedení identifikačních údajů (například jména a adresy, názvu a sídla, rodného nebo jiného identifikačního čísla atd.) na konci textu v elektronické (digitální) podobě, které zaručuje identifikaci (tedy jednoznačné určení) označené osoby, avšak nikoliv* ***integritu*** *podepsaného dokumentu ani* ***autentizaci*** *podepsaného. V české legislativě však byl význam pojmu z důvodu rozdílných výkladů dodatečně zúžen, aniž by byl plně vyjasněn, takže nyní je stěží rozeznatelný rozdíl mezi termínem elektronický podpis a zaručený elektronický podpis.* [8]

Jinak řečeno, elektronický podpis je vlastně informace, která se připojuje k elektronickým datům, aby identifikovala odesílatele příjemci. Největším problémem je ověřitelnost takového elektronického podpisu. Proto byl vytvořen tzv. digitální podpis, který umožňuje jednoznačnou identifikaci osoby. *Digitální podpis je v podstatě spojením klasického elektronického podpisu s certifikátem zajišťujícím identitu člověka*.[12]

Elektronický podpis je tedy spíše všeobecný termín zahrnující veškeré formy prokazování totožnosti elektronickou formou. Může se jednat třeba i o snímání otisků či otisk struktury oční duhovky. Naproti tomu digitální podpis je realizován na základě šifrování záznamu v digitální podobě.

K tomu, aby digitální podpis mohl dostát třem základním požadavkům a sice: požadavku autentizace a integrity a neodmítnutelnosti odpovědnosti je zapotřebí nejen samotné šifry a klíčů k jejímu ověření, ale také certifikátu pro možnost přesné identifikace autora textu.

V neposlední řadě je také nutno zdůraznit, že často dochází ke slučování termínů digitální podpis a asymetrické šifrování. My se pokusíme ukázat, že i jiné typy šifrování, mezi nimiž např. symetrické či hashové, mají své opodstatnění a stejně tak spadají pod označení digitálního podpisu.

Základní dělení šifer digitálního podpisu tedy představují šifry symetrické, asymetrické a hashové. Podívejme se tedy nyní blíže na toto dělení algoritmů, jejich podstatu a principy používání.

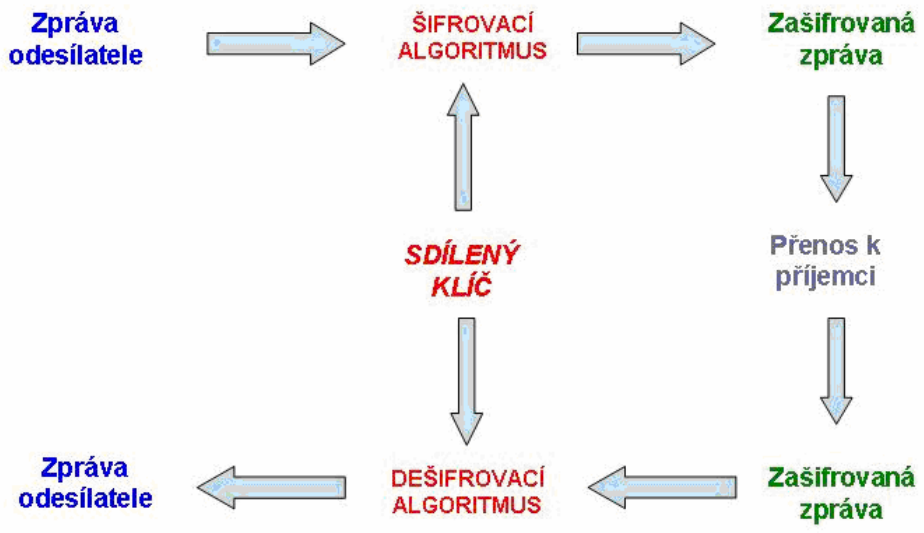
3. DRUHY ŠIFROVACÍCH ALGORITMŮ

3.1 Symetrické šifrování

Pojem symetrický šifrovací systém, nebo také konvenční šifrování, označuje základní způsob moderního šifrování. Principem tohoto systému je, že odesílatel vygeneruje klíč, pomocí kterého zašifruje svou zprávu. Tuto pak pošle veřejným kanálem příjemci, který ji pomocí stejného klíče dešifruje. Problém může nastat při procesu předání klíče příjemci, kdy vzniká nebezpečí úniku tajných informací, pokud neoprávněná osoba získá zmíněný klíč posílaný tajným kanálem.

Výhodou tohoto systému šifrování je nízká výpočetní náročnost a tím pádem velká rychlost šifrování a dešifrování, algoritmy pro šifrování s veřejným klíčem, o kterých pojednáváme v následující kapitole, mohou být i desettisíckrát pomalejší. Značnou nevýhodou je pak právě fakt, že k šifrování i dešifrování je zapotřebí téhož klíče, tzn. jediného tajného klíče. Tento způsob šifrování není vhodný pro digitální (elektronické) podepisování dokumentů.

Na následujícím obrázku můžeme sledovat zjednodušený princip symetrického šifrování.



Obr. 1: Princip symetrického šifrování

Symetrické šifry dělíme na dvě základní kategorie:

- *blokové šifry* – jedná se o rozšířenější způsob šifrování, kdy se výchozí data rozdělí na jednotlivá bitová slova, která se pak doplní bitovou šifrou (klíčem). V současné době je nejčastější šifrování pomocí 128 bitů. Mezi blokové šifry patří např. následující algoritmy – AES, Blowfish, DES, 3DES, GOST, CAST, IDEA, RC2, RC5, atd.
- *proudové šifry* – oproti předchozímu se jedná o šifrování bit po bitu a dešifrování probíhá stejným postupem. Mezi proudové šifry patří např. následující algoritmy – FISH, RC4, atd.

Symetrický šifrovací systém využívá nejrůznější typy šifrovacích algoritmů. Mezi nejznámější algoritmy dnes patří: AES (Advanced Electronic Signature), DES (Data Encryption Standard), 3DES, IDEA (International Data Encryption Algorithm), RCx , Blowfish, Twofish, Serpen, aj. Některé z nich jsou schematizovány v následující tabulce, kde můžeme porovnat jejich základní parametry z hlediska praktického využití. Následně se s jednotlivými algoritmy seznámíme detailněji.

TYPY ALGORITMŮ	**délka klíče (bit)**	**bezpečnost (v současnosti)**	**výhody**	**nevýhody**
DES	56	nedostačuje	rychlý	malá délka klíče
3DES	112 - 168	bezpečnější verze DES	kompatibilní s DES	pomalejší než AES
IDEA	128	bezpečný klíč	rychlejší než DES	patentovaný
BlowFish	32 – 448 (obvykle 128)	bezpečný	proměnlivá délka klíče, rychlý, žádný patent, dodnes neprolomena	
CAST	40-128	bezpečný	proměnlivá délka klíče,	
AES	128 - 256	bezpečný	proměnlivá délka klíče,	

Tab. 1: Porovnání symetrických algoritmů

3.1.1 Typy algoritmů symetrického šifrování

DES (Data Encryption Standard)

Jedná se o šifrovací algoritmus vyvinutý společností IBM v 70. letech 20. století. Na začátku 70. let zadalo ministerstvo obchodu USA soutěž o vytvoření nového šifrovacího standardu pro zabezpečení ochrany tajných dat v oblasti výpočetní techniky. Tuto soutěž vyhrála společnost IBM, která pro vytvoření nového algoritmu použila svůj stávající algoritmus „Lucifer“, který pouze zdokonalila. Nový algoritmus používá klíč o délce 56 bitů. Tento algoritmus se stal na konci 70. let šifrovacím standardem pro zabezpečení neutajovaných dat v civilním a vládním sektoru v USA.

Již od začátku jeho používání se vedly debaty o jeho bezpečnosti kvůli malé délce šifrovacího klíče. Toto se potvrdilo v roce 1997, kdy agentura RSA vypsala kryptoanalytickou soutěž, ve které bylo úkolem rozluštit text se známým začátkem a s délkou šifrovacího klíče 56 bitů. Toto se povedlo „hrubým útokem“ (vyzkoušením všech možných kombinací klíče) za necelých pět měsíců týmu DES Challenge vedeným Rocke Versenem, kdy se tímto potvrdila nízká bezpečnost tohoto algoritmu.

3DES (TripleDES)

Jedná se o bezpečnější variantu systému DES. Jeho výhodou je přímá návaznost na algoritmus DES při vyšší bezpečnosti. Rozdíl proti algoritmu DES spočívá v tom, že šifrovaná data projdou algoritmem třikrát. Tím se zvýší jak délka klíče, tak i bezpečnost šifrovaných dat. I přes trojité šifrování zůstává tento systém stále rychlým.

IDEA (International Data Encryption Algorithm)

Tento šifrovací algoritmus vznikl jako evropská alternativa k algoritmu DES. Jeho první popis je datován v roce 1991, kdy jej navrhli ve Švýcarsku J.L. Massey a Xuejia Lai.

Je sice patentován v mnoha zemích (patent vyprší v letech 2010-2011), přesto je ale volně dostupný i pro veřejnost. Tento algoritmus pracuje s klíčem o délce 128 bitů a je považován za nejlepší a nejbezpečnější algoritmus dostupný veřejnosti. Na přelomu století se již ale nedoporučoval díky vyšší dostupnosti rychlejších algoritmů, pokrokům v kryptografii a také díky problémům s patentem.

BlowFish

Tato šifra byla poprvé popsána v roce 1994 B. Schneiderem. Jedná se o šifru, která pracuje s klíčem o délce od 32 do 448 bitů. Nejobvyklejší délkou klíče je velikost 128 bitů. Tato šifra je volně šiřitelná a i přes tuto skutečnost není stále známý jakýkoli případ jejího prolomení.

AES (Advanced Encryption Standard)

Jedná se o algoritmus vyvinutý na zakázku americké vlády na konci 90. let minulého století pro potřebu šifrování svých tajných dokumentů. Algoritmus AES využívá klíče o velikosti 128, 192 nebo 256 bitů. V současnosti se jedná o nejrozšířenější a nejpopulárnější šifrovací algoritmus, u kterého neexistuje důkaz o jeho prolomení.

3.2 Asymetrické šifrování

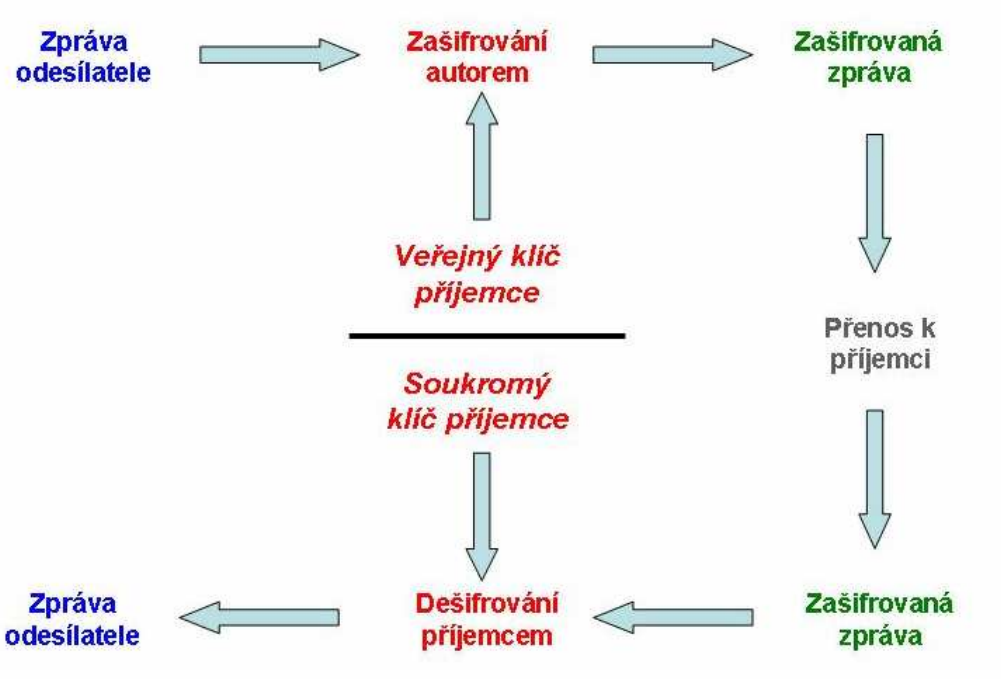
Pojem asymetrické šifrování označuje složitější systém šifrování, než předchozí zmíněné symetrické šifrování. Principem tohoto systému je, že klient má k dispozici dva klíče a to veřejný a privátní, které spolu úzce souvisí.

Veřejný klíč – jedná se o klíč, který je dostupný všem (jak již napovídá název), kteří chtějí jakýmkoli způsobem komunikovat s klientem.

Privátní klíč – jedná se o klíč, který má k dispozici pouze klient, kterému slouží k dešifrování dat, určených pouze pro něj. Tento klíč si musí klient bedlivě chránit, aby mu nebyla prolomena ochrana jeho dat.

Velkou výhodou tohoto systému je, že nepotřebujeme tajný kanál, kterým bychom přenášeli klíče mezi jednotlivými klienty. Oproti symetrickému šifrování je velkou nevýhodou rychlost šifrování, která je několikanásobně pomalejší.

Zjednodušený průběh asymetrického šifrování můžeme názorně sledovat na následujícím obrázku:



Obr. 2: Princip asymetrického šifrování

Z předchozího vyplývá, že vztah mezi veřejným klíčem a a soukromým klíčem b můžeme popsat podle následujícího matematického vzorce, kdy se v principu jednotlivé funkce mohou lišit, ale matematicky si jsou velmi podobné:

Šifrování

$x = f(y, a)$

Dešifrování

$y = g(x, b)$

Asymetrické šifrování běžně požívá různé typy algoritmů, mezi nejznámější a nejpoužívanější patří systém RSA (je pojmenováno po svých autorech, kterými byli R. L. Rivest, A. Shamir a L. Adleman), El-Gamal, D-H (Diffie-Hellman), ECC, DSA (Digital Signature Algorithm), aj. Některé z nich jsou schematizovány v následující tabulce, kde jsou porovnány z hlediska běžného použití. S některými typy algoritmů se seznámíme v následující části.

TYPY ALGORITMŮ	délka klíče (bit)	bezpečnost (v současnosti)	výhody	nevýhody
RSA	min 1024	bezpečný v závislosti na délce klíče	při dostatečné délce (min 1024 bitů) bezpečnost min. 20 let	do r.2000 patent, pomalejší než DES
ECC	proměnná	bezpečnější než RSA	veřejně k dispozici, standardizovány, kratší klíč než RSA	
DSA	min 1024	bezpečný		umožňuje pouze digitální podpis, ne šifrování dat
El-Gamal		bezpečný	lze jej použít jak na šifrování dat, tak i k podepisování dokumentů	šifrovaná data jsou dvakrát větší než nešifrovaná

Tab. 2: Porovnání asymetrických algoritmů

3.2.1 Typy algoritmů asymetrického šifrování

RSA (Rivest, Shamir, Adleman)

Tento šifrovací algoritmus byl popsán na konci 70. let 20. století, jeho autory jsou R. L. Rivest, A. Shamir a L. Adleman. Tento šifrovací algoritmus je v současné době nejrozšířenější na světě, používá také například při digitální podpisu (standardně se používají klíče o minimální délce 1024 bitů). Tento princip je popsán v následujícím příkladu, který pro zjednodušení požívá malých prvočísel:

1. Nejdříve si zvolí dvě různá prvočísla p a q
2. Poté spočítá jejích součin $n = p \cdot q$, který představuje veřejný modul

3. Nyní spočítá hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$
4. Poté zvolí celé číslo e, které bude menší než $\varphi(n)$ a zároveň bude s $\varphi(n)$ nesoudělné. Toto číslo představuje veřejný (šifrovací) exponent
5. Nalezne číslo d takové, aby platilo $d \cdot e = 1(\mathrm{mod}\,\varphi(n))$. Toto číslo představuje soukromý (dešifrovací) exponent

Příklad zašifrování datového toku 359:

$p = 61$

$q = 53$

$n = p \cdot q = 3233$

$e = 17$

$d = 2753$

Průběh šifrování:

šifruj $(359) = 359^{17} \bmod 3233 = 1291$

Průběh dešifrování:

dešifruj $(1291) = 1291^{2753} \bmod 3233 = 359$

DSA (Digital Signature Algorithm)

Jedná se o algoritmus, který je standardem digitálního podpisu amerického úřadu NIST (National Institute of Standards and Technology). Obtížnost prolomení bezpečnosti tohoto algoritmu spočívá ve vysoké obtížnosti výpočtu diskrétního logaritmu.

El-Gamal

Jedná se o první asymetrický algoritmus, který v praxi fungoval. Jeho princip spočívá stejně jako u předchozího algoritmu na výpočtu diskrétního logaritmu. V praxi se tohoto algoritmu moc nevyužívá kvůli jeho velké nevýhodě, kterou je dvojnásobné zvětšení velikosti šifrovaných dat.

ECC (Elliptic Curve Cryptography)

Jedná se o veřejný algoritmus, který je již standardizován. Tento algoritmus byl popsán v roce 1985 a navrhli ho nezávisle na sobě V. Miller (IBM) a N. Koblitz

(University of Washington). Jedná se o moderní způsob šifrování pomocí eliptických křivek. V tomto případě je nahrazena matematická aritmetika aritmetikou, která pracuje s body na eliptické křivce. Velkou výhodou oproti RSA je vyšší bezpečnost při použití výrazně kratšího klíče. Tento systém také umožňuje použití delšího klíče i odolnosti beze ztráty rychlosti kódování. Bližší porovnání šifrovacích algoritmů ve vztahu k délce klíče při srovnatelné bezpečnosti je uvedeno v následující tabulce.

Blokové šifry	Eliptické šifry	Asymetrické šifry (RSA)
56	112	512
64	128	768
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Tab. 3: Porovnání délky klíčů šifrovacích systémů při srovnatelné bezpečnosti

3.3 Hash funkce

Jedná se o funkci, která se v dnešní době běžně používá pro potřeby digitálního podpisu. Jedná se o funkci, při kterém se řetězec znaků o libovolné délce transformuje na řetězec znaků s pevnou délkou – na *hash* neboli *otisk*. Kvalitní *Hash* musí splňovat následující kritéria:

- výstup musí mít pevnou délku
- hodnota hash musí být jednoduše vypočitatelná pro jakýkoli vstupní řetězec
- funkce je jednosměrná a bez kolizí

Hash využívá mnoho typů algoritmů, mezi nejznámější dnes patří následující:

- MD4, MD5, SHA-0, RIPEMD, HAVAL-128 – tyto jsou již prolomeny
- SHA-1, SHA-256, SHA-384, SHA-512 – tyto jsou stále bezpečné

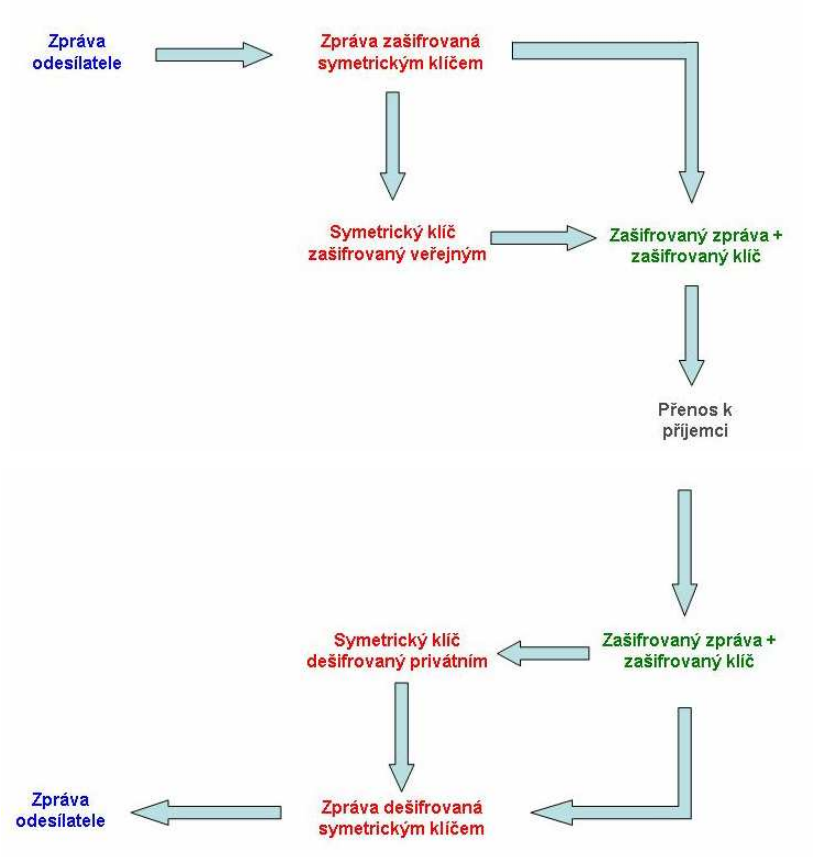
Dle doporučení společnosti NIST je nejlepší variantou používání třídy funkcí SHA-2 a do roku 2010 je předpoklad úplného opuštění SHA-1 a přechod na SHA-2.

3.4 Hybridní šifrovací algoritmy

V tomto případě se jedná o spojení dvou šifrovacích systému, popsaných v předcházejících kapitolách. Jedná se o spojení symetrického a asymetrického šifrování z důvodu prozaického. Asymetrické šifrování je velmi pomalé, proto se na zašifrování použije klíče symetrického, který je posléze zašifrován asymetricky pomocí veřejného klíče. Tento balíček obsahující zašifrovanou zprávu a klíč se odešle jako celek příjemci, který pomocí svého privátního klíče dešifruje nejprve symetrický klíč a posléze díky symetrickému klíči i vlastní zprávu. Z toho vyplývá, že hybridní šifrovací algoritmy spojují výhody obou předchozích typů šifrování. Těmito výhodami jsou že:

- roste počet klíčů lineárně s počtem komunikujících dvojic
- tento systém má přijatelnou rychlost
- je vhodné k použití pro digitální podpis

Zjednodušený princip hybridního šifrování je znázorněn na následujícím obrázku.



Obr. 3: Princip hybridního šifrování

Nejpoužívanějším kryptosystémem, ve kterém se využívá princip hybridního šifrování je systém PGP, dalším je například X.509, GnuPG.

PGP

Autorem tohoto systému je Paul Zimmermann. Princip šifrování probíhá podle výše popsaného principu, pouze před zašifrováním zprávy odesílatele je ještě tato zpráva zkomprimována pro následné rychlejší šifrování. tento systém využívá tři typy symetrických a dva typy asymetrických klíčů. Symetrické jsou klíče IDEA, TripleDES a CAST. Algoritmy IDEA a CAST používají 128 bitový klíč a TripleDES používá 168 bitový klíč. Asymetrickými algoritmy pro zašifrování symetrického klíče jsou RSA a DH/DSS. Obě zašifrované zprávy jsou po zašifrování spojeny do jednoho souboru, který je následně odeslán k příjemci, který jej opačným způsobem dešifruje.

4. ZPŮSOBY OVĚŘOVÁNÍ PŘÍSTUPOVÝCH PRÁV A PŘÍSTUPU UŽIVATELE

Jednotlivé zabezpečené aplikace využívají pro zabezpečení svých dat různé principy zabezpečení a přístupu. Souhrnně se tyto principy nazývají *autentizace* a *autorizace*.

4.1 Autentizace

Tento proces je založený na ověření totožnosti entity nebo uživatele. Nejjednodušším příkladem je např. přihlášení uživatele na počítač. Na podobném principu funguje jak komunikace mezi počítači tak i přihlašování do různých aplikací atd. Existují tři možné způsoby autentizace využívající jiný způsob přístupu k aplikacím:

- **Pomocí hesla** – tento typ autentizace používá drtivá většina internetových aplikací. Je to nejednodušší způsob, jeho hlavní nevýhodou je nižší bezpečnost než u následujících typů a možnost zapomenutí hesla a s tím spojené problémy při obnovování přístupu do aplikace. Autentizace probíhá pomocí zadání uživatelského jména a hesla.
- **Pomocí tokenu** – (z angličtiny – znamení, znak pravosti) u tohoto typu autentizace uživatel používá paměťové nebo čipové karty pro potvrzení identity. Tento způsob je výrazně bezpečnější než předchozí typ, jeho nevýhodou je ale možnost ztráty karty a tím i ztráty přístupu do aplikace.
- **Pomocí biometrik** – ještě donedávna to byl spíše futuristický způsob autentizace pomocí např. otisku ruky, obrazu sítnice, hlasu apod. V poslední době hlavně díky vyšší hrozbě napadení teroristy, se tento způsob stává běžnějším. Tento typ autentizace se ovšem dá použít pouze pro např. otevírání dveří místností apod. Sice např. otisk ruky prstu má oproti běžnému heslu velikost až 1000 bajtů, ale jeho neměnnost dává příležitost pro odchycení na síti a následné zneužití.

4.2 Autorizace

Tato kontrola je přímo závislá na autentizaci. Po správné autentizaci se ověřuje, zda má uživatel právo na přístup a využívání dané aplikace – jeho přístup se autorizuje. Toto se provádí na základě příslušnosti v přístupových seznamech, členství v různých uživatelských skupinách apod.

5. DIGITÁLNÍ PODPIS

Pojem digitální podpis se začal objevovat v souvislosti se vznikem asymetrického šifrování. Postupem času se vyvinul do fáze, kdy může být používán pro důvěrný styk mezi uživateli, státními orgány, bankami apod. Digitální podpis v různých podobách používá pro svou funkčnost všechny algoritmy a způsoby šifrování, které byly popsány v předchozích kapitolách. Různé kombinace záleží na dané společnosti, která tento podpis vyžaduje. Oproti obyčejnému šifrování ovšem využívá ještě certifikátu, který slouží k ověření podpisu třetí nezávislou osobou. Tímto je zaručena maximální bezpečnost v komunikaci mezi uživatelem a institucí. V českém právním řádu je digitální podpis definován jako elektronický podpis. V praxi si může svůj certifikát vytvořit každý, proto je v praxi dělíme podle míry důvěrnosti, kterou jim přikládáme:

- elektronický podpis
- zaručený elektronický podpis
- zaručený elektronický podpis založený na certifikátu
- zaručený elektronický podpis založený na kvalifikovaném certifikátu
- zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb

Poslední z uvedených elektronický podpisů je nejdůvěryhodnější a v současné době ho používají orgány státní správy.

Nejpoužívanějším algoritmem pro digitální podpis je šifrovací algoritmus RSA.

Digitální podpis se vytváří ve dvou krocích:

1. zpráva se zašifruje pomocí šifrovacího algoritmu a vytvoří se otisk
2. tento otisk se zašifruje soukromým klíčem uživatele, který se pošle příjemci. Takto zašifrovaný dokument se nazývá digitální podpis zprávy

Ověřování podpisu oproti předchozímu probíhá ve třech krocích:

1. příjemce dešifruje otisk přijaté zprávy
2. příjemce dešifruje digitální podpis veřejným klíčem odesílatele

3. následně porovná oba dešifrované soubory a pokud souhlasí, pak je autorem právě ten odesílatel, který poslal zprávu zašifrovanou soukromým klíčem.

Při příjímání zprávy příjemce ověřuje následující náležitosti:

a. *Autentičnost* – ověřuje, zda je odesílatel skutečně ta osoba, která má k deklarovanému klíči správný privátní klíč
b. *Integritu zprávy* – ověřuje, zda nebyla zpráva neoprávněně změněna
c. *Neodmítnutelnost odpovědnosti* – ten, kdo tuto zprávu poslal, je za ni zodpovědný a nemůže její autorství popřít

Velkou výhodou tohoto postupu je, že příjemce ihned zjistí pravost dokumentu a digitálního podpisu s tím souvisejícího a zároveň je tím zaručeno i to, že zpráva nebyla změněna. Jako třetí osoby, zajišťující pravost podpisu, se zavedly certifikační autority (CA). Mezi tyto CA v české republice patří například autority uvedené v následující tabulce.

Název CA	**odkaz na internetové stránky**
I. CA	www.ica.cz
ACTIVE 24	www.active24.cz/cz/webhosting/sluzby/ssl-certifikaty/
CA Czechia	www.caczechia.cz
CA České pošty	http.qca.postsignum.cz
CA Docent Hosting	www.decent.cz/cert.php
AEC TrustPort CA	www.trustport.cz
CESNET	www.cesnet.cz
Certifikační autorita UK	www.cuni.cz/cucc/ca
eIdentity	www.eidentity.cz/app

Tab. 4: Seznam certifikačních autorit

CA je instituce, která se skládá z následujících základních částí:

1. **registrační autority (RA)** – tyto můžou mít podobu klasické přepážky, kam si uživatel přijde s žádostí o vydání certifikátu.. Díky RA potom i

následný vydaný certifikát od RA obdrží. Tato komunikace může být zprostředkována také elektronicky.

2. **aplikace vydávající certifikáty** – tyto jsou elektronicky podepisovány soukromým klíčem CA. Tento klíč si pak CA bedlivě chrání, protože je největším aktivem CA.
3. **databáze** – spravuje databázi uživatelů a auditní záznamy o činnosti CA.
4. **archiv** – udržuje archiv vydaných certifikátů a CRL (Certificate revocation list – seznam certifikátů, které byly odvolány). Tento archiv může být dostupný přes webové rozhraní nebo přes protokol LDAP (Lightweight Directory Access Protocol).

5.1 Akreditované CA

Tyto CA musí splňovat podmínky dané zákonem o elektronickém podpisu (viz zákon o elektronickém podpisu č. 227/2000 Sb.) Tuto akreditaci vydává ministerstvo informatiky a činí tak na základě splnění podmínek daných zákonem o elektronickém podpisu a prováděcí vyhláškou. To, že CA plní zadané normy, je dokládáno kontrolou bezpečností shody. V současné době působí v České republice tři akreditované CA a to První CA, a.s., Česká pošta, s.p. a eIdentity a.s. Jmenované CA mohou vydávat kvalifikované certifikáty a kvalifikované systémové certifikáty a komerční certifikáty, pouze První CA může navíc vydávat kvalifikovaná časová razítka. Kvůli vysoké ceně za používání této autority je vhodnější pro podnikatelskou sféru, kdy se komunikace s orgány státní správy za těchto podmínek pro jednotlivce nevyplatí. Nejvíce se služeb CA využívá ve sféře bankovnictví, kde je tato služba nezbytná.

Ceny služeb jednotlivých CA jsou uvedeny v následujících tabulkách.

název	doba platnosti	cena s DPH
Kvalifikované certifikáty		
typ Standard	12 měsíců (365 dní)	752,-
typ Comfort (prvotní)	12 měsíců (365 dní)	1 728,-
typ Comfort (následný)	12 měsíců (365 dní)	752,-
Kvalifikované systémové certifikáty		
typ Standard (žadatel má vlastní HW zařízení)	12 měsíců (365 dní)	780,-
typ Comfort (prvotní)	12 měsíců (365 dní)	1 756,-
typ Comfort (následný)	12 měsíců (365 dní)	780,-
Podpisový certifikát ke kvalifikovanému systémovému certifikátu - kvalifikovaný	12 měsíců (365 dní)	390,-
Komerční certifikáty		
typ Standard	6 měsíců (183 dní)	322,-
typ Standard	12 měsíců (365 dní)	580,-
typ Comfort (prvotní)	12 měsíců (365 dní)	1 556,-
typ Comfort (následný)	12 měsíců (365 dní)	580,-
Certifikát pro server	6 měsíců (183 dní)	1 073,-
Certifikát pro server	12 měsíců (365 dní)	1 931,-

Tab. 5: ceník I.CA

U kvalifikovaných a kvalifikovaných systémových certifikátů I.CA využívá 1024 bitový kryptografický klíč a pro typ Comfort ještě navíc dodává čipovou kartu a ovládací software I.CA.

U komerčních certifikátů využívá při době platnosti 6 měsíců 512 bitového kryptografického klíče a při době platnosti 12 měsíců opět 1024 bitového kryptografického klíče. Stejně jako u předchozích certifikátů pro typ Comfort dodává jak čipovou kartu, tak i ovládací software I.CA.

Tato společnost zároveň umožňuje vydání testovacího certifikátu, který slouží pro ověření funkčnosti technologie pro realizaci tvorby elektronického podpisu. Platnost tohoto testovacího certifikátu je omezena na 14 dní, kdy je poté jeho platnost automaticky ukončena. Tyto certifikáty jsou neveřejné a pro tento typ certifikátů není vydána Certifikační politika.

název	doba platnosti	cena s DPH
Certifikáty pro ověření elektronického podpisu zaměstnance	1 rok	190,-
Certifikáty organizace pro ověření elektronické značky	1 rok	2 856,-
Certifikáty pro ověření elektronického podpisu fyzické osoby	1 rok	190,-
Certifikáty pro ověření elektronické značky fyzické osoby	1 rok	2 856,-

Tab. 6: ceník QCA České pošty

Společnost QCA České pošty využívá klíče pro algoritmus RSA s délkou klíče 1024 nebo 2048 bitů. Klíčové páry obsluhy jsou generovány v čipových kartách.

název	doba platnosti	cena s DPH
Ceny akreditovaných služeb		
Kvalifikovaný certifikát	12 měsíců	702,-
Kvalifikovaný systémový certifikát	12 měsíců	3 451,-
Ceny komerčních služeb		
Komerční certifikát (k již vydanému kvalifikovanému certifikátu)	12 měsíců	238,-
Komerční serverový certifikát (k již vydanému kvalifikovanému systémovému certifikátu)	12 měsíců	752,-
Balíčky služeb		
Balíček kvalifikovaného certifikátu a k němu vydaného komerčního certifikátu	12 měsíců	821,-
Balíček kvalifikovaného systémového certifikátu a k němu vydaného komerčního serverového certifikátu	12 měsíců	3 827,-
Ceny dalších služeb		
Zneplatnění certifikátu	trvale	0,-
Podání žádostí o zjištění IKMPSV (identifikátor klienta Ministerstva práce a sociálních věcí)	trvale	0,-

Tab. 7: ceník eIdentity

Společnost eIdentity a.s. využívá klíče s minimální délkou 1024 bitů.

Současně s akreditovanými CA působí na trhu CA, které nespadají pod kontrolu ministerstva informatiky a zároveň nemají stanovenu oznamovací povinnost jako předchozí CA. Tyto CA mohou ovšem vydávat pouze komerční certifikáty. Používají je různé instituce pro bezpečný přístup do vlastních souborů, které si hlídají a spravují samostatně. Patří mezi ně např. banky pro podpis transakcí v elektronickém bankovnictví. Dále pak například vysoké školy pro přístup k dokumentům týkajících se např. studia v daných školách.

Počáteční problémem tohoto projektu byla situace, kdy jednotlivé CA vydávají vlastní certifikáty, a následně je ukládají na svůj kořenový certifikát. Díky tomuto se stává situace velmi nepřehlednou a nastávají problémy s rozhodováním o důvěryhodnosti daných CA. Jednotlivé CA nemají dostatek údajů a popřípadě i času, aby tyto údaje mohly prozkoumat. Proto musely vzniknou systémy umožňující vzájemné uznávání jednotlivých certifikátů mezi doménami.

5.2 Certifikát

Certifikát můžeme ve své podstatě přirovnat k občanskému průkazu, ovšem v elektronické podobě. Certifikát jednoznačně spojuje fyzickou totožnost s elektronickou totožností osob (subjektů) a tím umožňuje jeho využití pro určení vlastní identity. Postup k získání certifikátu je obdobný s postupem získávání občanského průkazu. V mnohých evropských zemích se již dokonce vydávají občanské průkazy, které obsahují v čipu zakódovaný certifikát držitele karty. Základní součástí certifikátu je veřejný klíč držitele certifikátu. Pro příklad si můžeme uvést porovnání důležitých položek občanského průkazu a certifikátu.

Položka certifikátu	Položka občanského průkazu (OP)
Verze	Verze formátu OP (knížka, karta apod...)
Pořadové číslo	Číslo OP
Algoritmus podpisu	Způsob podpisu úředníka, typy ochranných prvků
Vydavatel	Vydal
Platnost	Platnost
Předmět: jméno, adresa,...	Jméno a adresa
Veřejný klíč	-
-	Fotografie
Rozšíření certifikátu	Nepovinné údaje
Elektronický podpis	Rukou psaný podpis, aplikace ochranných prvků

Tab. 8: Porovnání certifikátu a občanského průkazu

Z předchozí tabulky můžeme vidět, jak moc si jsou podobné certifikáty a občanské průkazy. Nyní si v krátkosti vysvětlíme jednotlivé položky certifikátu.

Verze (Version) – toto přímo souvisí s tím, jestli je certifikát odvozen od normy X.509 verze 1,2 nebo 3 (*Version 0* = verze 1; *Version 1* = verze 2; *Version 2* = verze 3).

Pořadové číslo (Serial number) – jedná se o celé kladné číslo, které vydává konkrétní certifikační autorita. Ta musí zaručovat, že žádné dva certifikáty , které vydá, nebudou mít stejné pořadové číslo.

Algoritmus podpisu (Signature algorithm) – tato položka upřesňuje algoritmy, které daná CA použila pro vytvoření elektronického podpisu certifikátu. Vždy určuje dva algoritmy – jeden pro výpočet otisku a druhý určuje asymetrický algoritmus použitý pro zašifrování otisku.

Vydavatel (Issuer) – označuje CA, jež daný certifikát vydala

Platnost (Validity) – ta určuje, jak je z názvu patrné, dobu platnosti daného certifikátu (od do). Nevýznamnějším důvodem tohoto opatření je bezpečnost. Doba platnosti být kratší než doba potřebná k prolomení certifikovaného veřejného klíče.

Předmět: jméno, adresa,... (Subject) – označuje držitele certifikátu a upřesňuje jeho původ. Je to proto, aby se nestalo, že budou dva držitelé jednoho certifikátu.

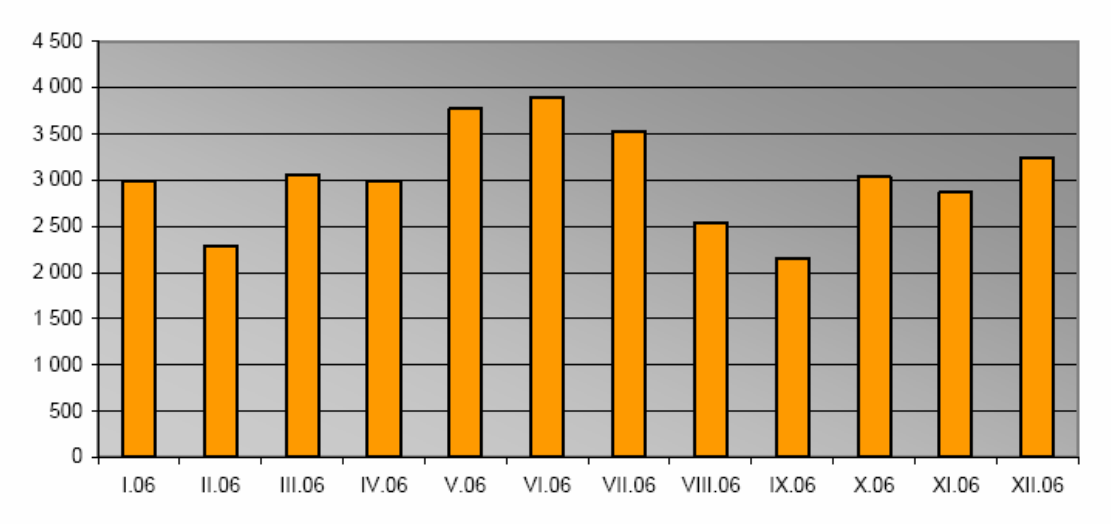
Veřejný klíč (Subject Public Key) – zde jsou obsaženy dvě informace – je to identifikátor algoritmu, pro který je veřejný klíč určen a zároveň samotným veřejným klíčem.

Rozšíření certifikátu (Extension) – tato položka obsahuje bývají upřesňující k předešlým položkám, patří sem např. identifikátor klíče úřadu, použití klíče, platnost soukromého klíče, mapování zásad, alternativní jméno předmětu, základní omezení,omezení politik, přístup k informacím úřadu, název šablony certifikátu, aj.

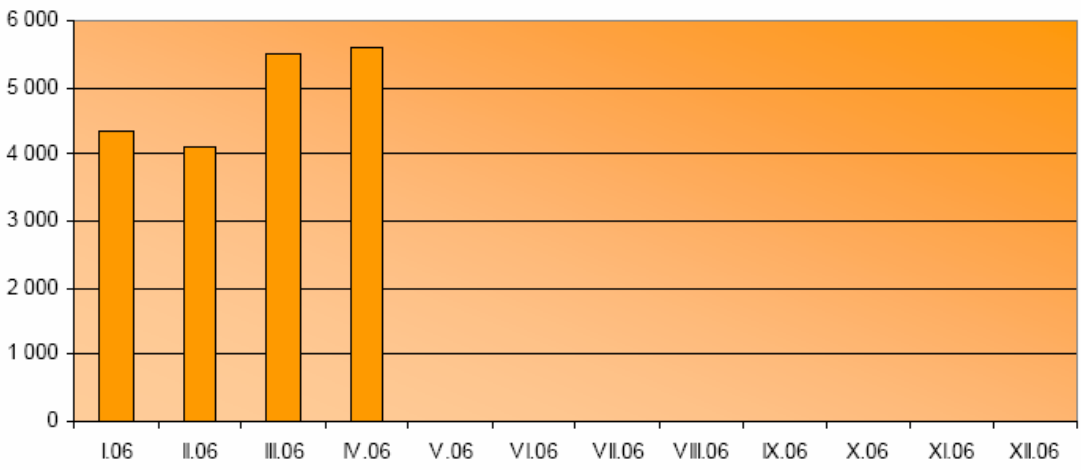
Elektronický podpis (Digital signature) – samotný digitální podpis sloužící k ověřování pravosti a původu dokumentu.

5.3 Grafy vydaných a aktivních kvalifikovaných certifikátů

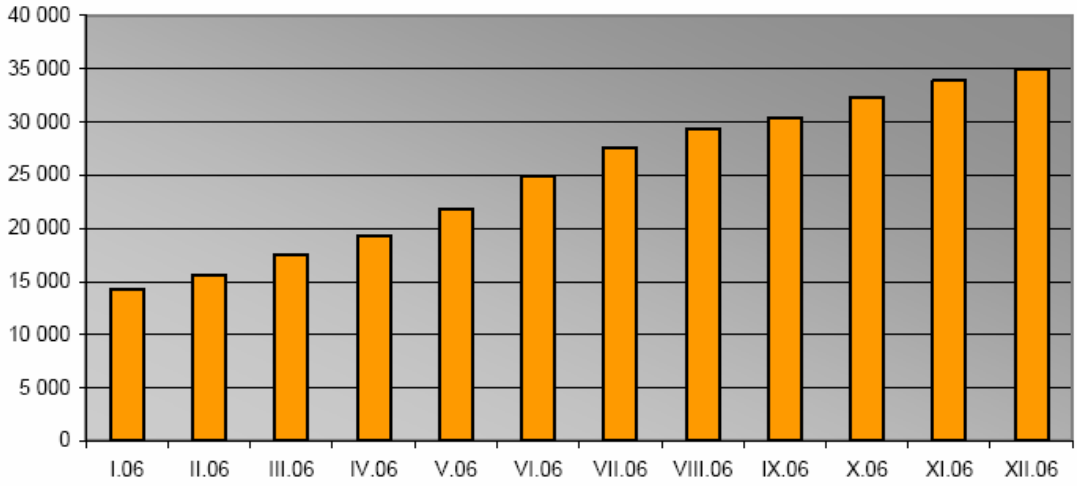
V následujících grafech názorně vidíme trvalý nárůst využívání certifikátů firmami, veřejnými subjekty a fyzickými osobami. Díky úpravám právních předpisů mají tyto subjekty více možností komunikace s orgány státní správy. Jsou zde zahrnuty i certifikáty, jež jsou nutné pro komunikaci mezi jednotlivými úřady. Z grafů je patrná neustálá tendence zvyšování využívání těchto služeb. Toto bezpochyby souvisí s rozvojem internetu a služeb nabízených jednotlivými úřady a subjekty.



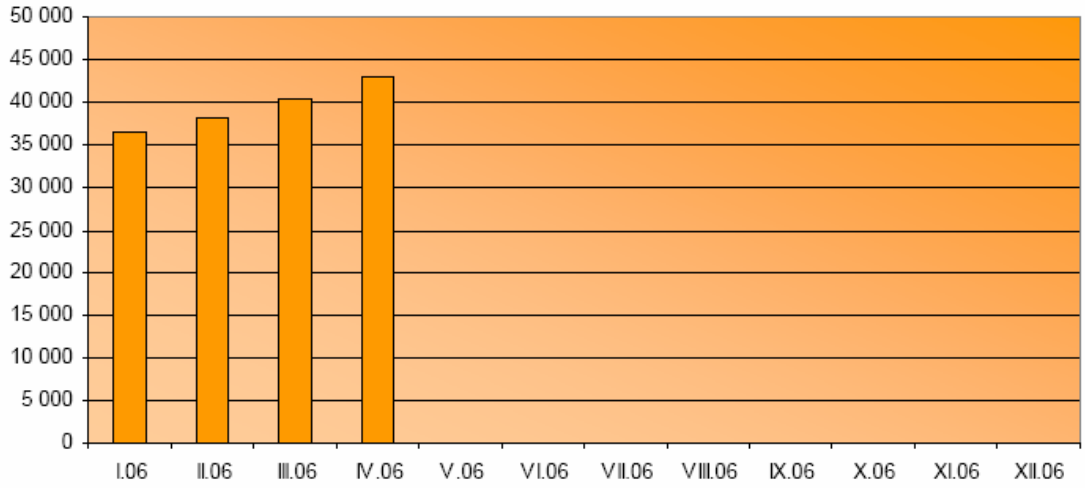
Graf 1: Vydané kvalifikované certifikáty v roce 2006 [17]



Graf 2: Vydané kvalifikované certifikáty v roce 2007 [17]



Graf 3: Počty aktivních kvalifikovaných certifikátů v roce 2006 [17]



Graf 4: Počty aktivních kvalifikovaných certifikátů v roce 2007 [17]

5.4 Využití kvalifikovaných certifikátů v praxi

Po přijetí zákona o elektronickém podpisu (zákon 227/2000 Sb., po přijetí jeho novelizací a dalších právních norem) si zřídily všechny orgány státní moci a jim podléhající instituce e-podatelny. Veškeré záležitosti, které bylo s těmito institucemi nutno dříve vyřizovat klasicky, nyní můžeme pomocí kvalifikovaných certifikátů vyřídit z domu.

Mezi tyto instituce patří např. Ministerstvo práce a sociálních věcí, Ministerstvo financí ČR, Ministerstvo spravedlnosti ČR, Celní správa ČR, Úřady práce, Česká obchodní inspekce, Státní úřad inspekce práce, Státní energetická inspekce, aj.

Nejvíce využívanou aplikací je jistě Elektronické podání pro daňovou správu. Pro ilustraci vývoje nárůstu objemu počtu elektronických podání uvádím tabulku podání podaných od roku 2002.

	Rok					
	2002	2003	2004	2005	2006	2007
celkový počet elektronických podání	311	7018	20205	48978	102866	147269

Tab. 9: Počty elektronických podání daňové správě

Mezi tyto podání patří např. podání daňového přiznání k dani z nemovitosti, podání vyúčtování daně z příjmů fyzických a právnických osob, daň z přidané hodnoty, závislá činnost, daň silniční, daň z nemovitostí, aj.

Dalšími institucemi, kde lze využít kvalifikovaného certifikátu jsou převážně zdravotní pojišťovny. V současné době jsou využívány následujícími pojišťovnami – Všeobecná zdravotní pojišťovna ČR, Hutnická zaměstnanecká pojišťovna, Česká národní pojišťovna, Odborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví, Revírní bratrská pokladna, zdravotní pojišťovna, Zaměstnanecká pojišťovna Škoda, Zdravotní pojišťovna Metal-Aliance.

Zdravotní pojišťovny využívají certifikátů pro jednoduchou, rychlou a efektivní komunikaci se svými klienty (pojištěnci, zaměstnavateli, lékaři a zdravotnickými zařízeními). Slouží např. ke změně údajů o plátci, vyřízení průkazu pojištěnce, záznamu o dlouhodobém pobytu v cizině, přehledu o platbách pojistného, zasílání dávek, výpisu plateb, faktur a jejich příloh, aj.

Dalšími institucemi využívajícími tyto certifikáty jsou např. Středisko cenných papírů Praha, Česká národní banka, RM-SYSTÉM, banky, aj.

Tyto společnosti certifikátů využívají pro umožnění snadnějšího obchodování např.na trhu cenných papírů a při zadávání platebních operací. Středisko cenných papírů Praha jej využívá pro výpis z registru emitenta a své služby hodlá rozšiřovat.

Veškeré instituce ve většině případů doporučují použití kvalifikovaného certifikátu I.CA.

6. APLIKACE VYUŽÍVAJÍCÍ DIGITÁLNÍ PODPIS

6.1 Elektronické bankovnictví

V současné době patří mezi nejdynamičtěji se rozvíjející oblasti bankovnictví. Synonymem tohoto pojmu je přímé bankovnictví – jedná se o neosobní (přímou) komunikaci mezi klienty a bankami. Hlavními důvody pro vznik tohoto typu styku klienta s bankou byli úspora nákladů (méně zaměstnanců) a zatraktivnění služeb pro klienty (není nutná návštěva banky, lze komunikovat v jakoukoliv hodinu). Nevýhodami jsou na straně banky vysoké nároky na bezpečnost vzájemné komunikace a ze strany klienta odpovídající technické vybavení alespoň pro základní komunikaci.

Pod elektronické bankovnictví spadají následující pojmy:

- **Home banking** – komunikace s bankou prostřednictvím Internetu. Nevýhodou tohoto systému je nutnost instalace speciálního programu dodaného bankou. Oproti následující komunikace je výrazně dražší.
- **Internet banking** – jednodušší a v současné době nejrozšířenější způsob komunikace s bankou prostřednictvím Internetu, kdy uživateli pouze stačí mít nainstalovaný webový prohlížeč.

Pro zabezpečení služeb Home a Internet banking se používají šifrovací systémy popsané v předcházejících kapitolách. Typy šifrovacích algoritmů a šifrovacích systémů závisí na každé z bank. Většina bank používá pro bezpečnou komunikaci s klienty vlastní certifikáty a komerční CA.

7. ZÁVĚR

Cílem mé bakalářské práce bylo shrnout základní pojmy týkající se digitálního podpisu a věcí s tím souvisejících. Základní stavebním kamenem digitálního podpisu jsou šifrovací metody, díky jejichž rozvoji můžeme poměrně bezpečně komunikovat s různými institucemi, např. bankami, orgány státní správy, apod. Další praktickou výhodou je, že nám odpadá stání ve frontách na úřadech a můžeme si vše potřebné vyřídit z domu

Na druhou stranu v neprospěch digitálního podpisu přispívá fakt, že podléhá rychlému rozvoji výpočetní a komunikační technologie. Již dnes jsme schopni pomocí speciálních optoelektronických zařízení tento systém rozbít. [11]

V současné době fungují v ČR tři akreditované CA (od r. 2005), díky čemuž se zvýšila dostupnost komunikace se státními orgány veřejnosti. Z uvedených grafů jasně vyplývá tendence vyššího využití tohoto způsobu komunikace s institucemi.

8. SEZNAM OBRÁZKŮ, TABULEK A GRAFŮ

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů

9. SEZNAM POUŽITÉ LITERATURY

[1] Dostálek L., Vohnoutová M., *Velký průvodce infrastrukturou PKI*. Computer Press, Brno 2006, ISBN: 80-251-0828-7

[2] Informační systém veřejné správy: Lorenc M., *E-podpis/podatelny*, 2007, http://www.isvs.cz/e-podpis-podatelny/

[3] CA Czechia: *Elektronický podpis, Certifikáty*, 2003-2004, http://www.caczechia.cz

[4] Archiv.cz: Peterka J., *Elektronický, nebo digitální podpis*, 2000, http://www.earchiv.cz/b00/b0004001.php3

[5] A && L soft: *Otázky k principu bezpečnostních prvků*, 2000-2005, http://www.alsoft.cz/cz/Products/Security/FAQ-Security-Technology/#id909717

[6] Crypto-World: Mgr. Vondruška P., *Informační sešit GCUCMP*, 11/1999, http://crypto-world.info/casop1/crypto11_99.pdf

[7] Ministerstvo vnitra ČR: Bc. Hobza J., *Bezpečnost a vydávání certifikátů*, 2002, http://www.mvcr.cz/casopisy/s/2002/0050/tema.html#12

[8] Wikipedia: *Elektronický podpis*, 2007, http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis

[9] IT Systems: Brechlerová D., Nezdarová L., *Certifikáty jako základ e-podpisu, autentizace i šifrování*, 12/2004, http://www.systemonline.cz/clanky/certifikaty-jako-zaklad-e-podpisu-autentizace-i-sifrovani.htm

[10] Svět sítí: Nádeníček P., *Pravdy o elektronickém podpisu a šifrování*, 2003, http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=244

[11] Sdělovací technika*: Moderní koncepce a nová filozofie autentizačních metod*, 2004, http://www.stech.cz/articles.asp?ida=388&idk=168

[12] Interval.cz: Doležal D., *Jak funguje digitální podpis*, 2002, http://interval.cz/clanky/jak-funguje-digitalni-podpis/

[13] Owebu.cz: Baar O., *Šifrování*, 2007, http://www.owebu.cz/bezpecnost/vypis.php?clanek=1216

[14] Fyzikální ústav AV ČR: Ing. Kodl J., *Elektronický podpis*, http://fzu.cz/texty/ruzne/el_podpis.html

[15] Bitto O., *Historie kryptologie*, http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm

[16] PC tuning.cz: *Moderní metody šifrování*, 2005, http://www.pctuning.cz/index.php?option=com_content&task=view&id=4711&Itemid=95

[17] Ministerstvo vnitra ČR: *Archiv stránek bývalého Ministerstva informatiky*, http://www.mvcr.cz/micr/epodpis/default.htm

[18] Ministerstvo financí ČR: *sekce Komunikace s MF, ePodatelna*, http://www.mfcr.cz/cps/rde/xchg/mfcr/xsl/epodatelna.html