Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Diplomová práce

Bc. Pavel Mika

Aplikace kryptografie v informačních systémech

Application of cryptography in information systems

Kladno 2013

Vedoucí práce: prof. RNDr. Jiří Ivánek, CSc.

Děkuji vedoucímu diplomové práce profesorovi Jiřímu Ivánkovi za cenné rady a konzultace, které mi pomohly při vypracování práce.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

V Kladně, dne 26. července 2013

……..

Pavel Mika

Klíčová slova (česky)

kryptografie, šifrování, informační bezpečnost, porovnání, evaluace, informační systémy

Klíčová slova (anglicky):

cryptography, encryption, information security, comparison, evaluation, information systems

Abstrakt (česky)

Diplomová práce popisuje a porovnává nejrozšířenější algoritmy využívané v informačních systémech. Konkrétně se jedná o algoritmy: Vernamova šifra, DES, 3DES, AES a Blowfish (symetrická kryptografie) a protokol Diffie-Hellman pro výměnu klíčů, RSA, ElGamal, McEliece a systémy založené na eliptických křivkách (asymetrická kryptografie). Dále se práce zabývá oblastí informační bezpečnosti, především jednotlivými bezpečnostními mechanismy (důvěrnost, dostupnost, integrita, autentizace, autorizace a nepopiratelnost), které bývají zajištěny právě pomocí kryptografie. Zmíněno je také téma standardizace, kde jsou především představeny odpovědné instituce tvořící normy a standardy a pak také některé normy. Popisované algoritmy jsou v závěrečné kapitole porovnány pomocí několika kritérií (čas, průchodnost, paměť potřebná pro implementaci, lavinový efekt a délky klíčů). Data, na jejichž základě je porovnáváno, jsou převzata z dalších studií a vědeckých materiálů.

Abstract (in English):

This thesis describes and compares the most popular algorithms used in information systems. Specifically, there are: Vernam cipher, DES, 3DES, AES, and Blowfish (symmetric cryptography) and Diffie-Hellman key exchange, RSA, ElGamal, McEliece and systems based on elliptic curves (asymmetric cryptography). The thesis deals with the areas of information security, in particular the various security mechanisms (confidentiality, availability, integrity, authentication, authorization and non-repudiation), which are secured by using cryptography. There is also mentioned the theme of standardization, where the responsible institutions and some standards are presented. Described algorithms are compared using several criteria (time, throughput, memory needed for implementation, avalanche effect and key lengths) in the final chapter. Data used for comparison are taken from other studies and scientific materials.

Obsah

Předmluva

Diplomová práce představuje základní kryptografické algoritmy, které se využívají k zabezpečení nejen v informačních systémech. Jedná se o přehledovou práci, která sumarizuje poznatky k danému tématu a prezentuje je spolu se závěry plynoucími převážně z daných vlastností jednotlivých algoritmů. Kromě základního popisu algoritmů jsou představeny okruhy informační bezpečnosti, ve kterých jsou kryptografické algoritmy aplikovány. V rámci kapitoly informační bezpečnosti je také nastíněna politika standardizace a normalizace algoritmů a bezpečnostních postupů. Stěžejní kapitolu práce tvoří porovnání algoritmů podle různých hodnotících kritérií. Hodnoty, na jejichž základě jsou algoritmy porovnávány, byly převzaty z dalších materiálů – studií a vědeckých prací zaměřených přímo na jejich hodnocení.

Téma práce jsem si vybral především díky absolvovaným předmětům (Kódování a šifrování a Kódování informací), které ve mně vzbudily zájem o toto téma. Kryptografie je velice široký vědní obor, který se stále rozvíjí. Vzhledem k jeho nezbytnosti pro zabezpečení dat a informací v dnešní informační společnosti je to jistě vhodné téma pro zpracování a to také i z trochu jiného pohledu než je čistě technický respektive matematický.

Práce vznikla na základě důkladné rešerše v různorodých informačních zdrojích zaměřené na klíčové studie, články a publikace k danému tématu v českém a anglickém jazyce. Materiály pro kapitoly popisující algoritmy a informační bezpečnost nebylo obtížné získat, naopak bylo důležité zorientovat se v celkem velkém množství informací. Zásadní ovšem bylo získat podklady pro srovnávací kapitolu, která tvoří asi nejpřínosnější část této práce.

Po určení klíčových zdrojů a jejich získání následovalo studium a hlubší seznámení se s tématem. Pro utřídění informací mi například pomohlo vytvoření si myšlenkové mapy se základními termíny a okruhy, které jsem hodlal zpracovat.

Vzhledem k povaze uváděných informací – tedy hlavně těch, které popisují samotné procesy algoritmu, bylo někdy nutné doslova citovat. Všechny použité zdroje jsou citovány podle normy ISO 690 za použití tzv. Harvardského systému.

Úvod do kryptografie

Kryptografie má dlouhou a zajímavou historii. Jako první ji začali v omezené míře používat Egypťané před 4000 lety. Nejvýznamnější roli sehrála kryptografie v obou světových válkách dvacátého století. Historie klasické kryptografie se uzavírá počátkem šedesátých let, kdy nastupují elektronické počítače. [PŘIBYL, 2004, s. 5] Převážnými uživateli klasické kryptografie byly vojenské okruhy, vládní a diplomatické orgány.

Rozvoj a rozšíření počítačové techniky v šedesátých letech mělo za následek zvýšení požadavků na prostředky pro ochranu informací v digitální podobě v rámci soukromého sektoru. Vývoj potřebného kryptografického mechanismu začal počátkem sedmdesátých let u IBM a kulminoval v roce 1977 přijetím výsledného produktu jako americké normy DES pro šifrování netajných informací. DES se stal nejznámějším kryptografickým systémem v historii a v rozšířené podobě je stále standardním šifrovacím prostředkem.

Zvrat v historii kryptografie nastal v roce 1976, kdy Diffie a Hellman publikovali článek s názvem New Directions in Cryptography. V tomto článku byla popsána revoluční myšlenka kryptografie veřejného klíče a rovněž nová metoda pro diskrétní výměnu šifrovacích klíčů. V roce 1978 Rivest, Shamir a Adleman představili první prakticky použitelný systém pro šifrování veřejným klíčem a elektronický podpis označovaný jako RSA. [PIPER, 2006, s. 9]

Velkým přínosem šifrování s veřejným klíčem byl právě elektronický podpis, nazývaný také digitální. První mezinárodní norma pro elektronický podpis (ISO/IEC 9796) byla přijata v roce 1991. [PŘIBYL, 2004, s. 6] Je založena na systému veřejného klíče RSA. Stejně tak byla v roce 1999 schválena směrnice pro elektronický podpis v EU a ČR přijala 29. května roku 2000 zákon č. 277 o elektronickém podpisu.

Hledání nových systémů veřejného klíče, zlepšování stávajících kryptografických mechanismů a testování bezpečnosti pokračuje úžasnou rychlostí. V praxi nalézá uplatnění řada různých norem a infrastruktur s kryptografickými prvky. Pro zajištění bezpečnosti rychle se rozvíjející informační společnosti se vyvíjejí stále nové bezpečností produkty. Následující text by měl objasnit základní principy, techniky a algoritmy, které nacházejí uplatnění v kryptografické praxi.

1 Základní terminologie

Každý vědní obor se opírá o přesné definice vycházející ze základních pojmů. Tak je tomu i u kryptologie. V této krátké kapitole jsou představeny termíny a základní pojmy z této oblasti, jež jsou pak použity v dalším textu.

1.1 Kryptologie

Kryptologie je obor zabývající se kryptografií a kryptoanalýzou.

Kryptografie je věda o tvorbě šifer, kdy informace mají abecedně číslicový charakter. [PIPER, 2006] Kryptografie studuje šifrovací algoritmy, kryptografické nástroje, hardwarové implementace šifrovacích algoritmů, kryptografické protokoly apod. Zabývá se tedy souhrnně problematikou převádění otevřených informací do podoby nesrozumitelné pro útočníky. [POŽÁR, 2005, s. 191]

Kryptoanalýza je obor, který se zabývá studiem matematických postupů zaměřených na prolamování kryptografických metod.

Kryptosystém je obecný termín, který se týká množiny kryptografických prostředků a který slouží k zajišťování informačních bezpečnostních servisů. [PŘIBYL, 2004, s. 23]

1.2 Šifrovací algoritmus

Šifrovací algoritmus E je jistý přesně vymezený postup, který utajuje data pomocí **šifrovacího klíče** K_1. Jde tedy o proces transformace, při níž se převede **otevřený text** M na **šifrovaný text** C. Tato transformace se nazývá šifrovací transformace nebo také šifrovací funkce.

Opakem šifrovacího algoritmu je **dešifrovací algoritmus** D, který za pomoci dešifrovacího klíče K_2 transformuje zašifrovaný text zpět na text otevřený.

1.3 Účastníci komunikace

Entita, subjekt nebo účastník je něco nebo někdo, kdo odesílá, přijímá nebo upravuje informace. Entitou může být osoba, počítačový terminál, apod.

Odesílatel A je entita v komunikačním procesu dvou účastníků, která je oprávněným odesílatelem informace.

Příjemce B je entita v komunikačním procesu dvou účastníků, která je zamýšleným příjemcem informace.

Narušitel je entita, která se snaží narušit informační bezpečnost komunikace mezi odesílatelem a příjemcem. Ekvivalentem tohoto termínu může být například protivník, nepřítel, útočník, oponent a vetřelec. Narušitel se často pokouší hrát roli buď oprávněného odesílatele, nebo oprávněného příjemce.

1.4 Kanály

Kanál je prostředek dopravy informací od jedné entity k druhé.

Fyzicky bezpečný kanál neboli bezpečný kanál je prostředek, který je fyzicky nepřístupný pro narušitele.

Nezabezpečený kanál je prostředek, v němž narušitel může měnit, odstraňovat a vkládat nebo sledovat informace.

Jeho opakem **je zabezpečený kanál**. Tento kanál může být zabezpečen fyzickými nebo kryptografickými prostředky.

1.5 Prolomitelnost

Kryptosystém je označován za **prolomitelný**, pokud třetí subjekt může v přijatelné době systematicky vyhledat k šifrovému textu odpovídající otevřený text bez předchozí znalosti dešifrovacího klíče. [POŽÁR, 2007 s. 84]

1.6 Šifrování a kódování

Je důležité oddělit tyto dva pojmy, které jsou si sice blízké, ale zároveň je mezi nimi výrazný rozdíl. **Šifrováním** rozumíme provádění šifrovacího algoritmu, tedy transformace informace pomocí utajeného klíče. **Kódování** je také proces transformace informace, ale bez použití jakékoli tajné informace. [JIROUŠEK, 2006]

2 Útoky na kryptosystémy

Přestože se tento text nezabývá kryptoanalýzou, je užitečné uvést základní typy útoků na kryptosystémy, abychom věděli, v čem mohou být slabé stránky kryptosystémů, jakým způsobem mohou být prolomeny a jak se tomuto prolomení vyhnout. U popisu jednotlivých algoritmů budou tyto útoku zmiňovány.

2.1 Útok hrubou silou (bruce force attack)

K tomuto útoku je zapotřebí dostatečně výkonný výpočetní systém, pomocí nějž jsou zkoušeny všechny možné klíče. Z toho vyplývá, že počet klíčů by měl být dostatečně velký, aby byl tento útok prakticky nerealizovatelný. Útok hrubou silou se také nazývá vyčerpávající průzkum prostoru klíčů nebo průzkum prostoru klíčů metodou totálních zkoušek. [PŘIBYL, 2004, s. 21].

Jistou variantou tohoto způsobu luštění je tzv. *slovníkový útok*. Při něm útočník využívá rozsáhlý slovník obsahující slova v různých jazycích, která se nejčastěji používají jako hesla. Tento typ útoku se často zaměřuje na uživatelské a správcovské účty v systémech firem, bank, státních organizací atd.

2.2 Luštění ze znalosti šifrového textu (cipher only attack)

K tomuto útoku může dojít, pokud má útočník k dispozici dostatečně velké množství šifrovaného textu zašifrovaného stejným algoritmem a stejným klíčem. Daný klíč se pak zjišťuje pomocí tzv. metody lineární kryptoanalýzy.

2.3 Luštění se znalostí otevřeného textu (known plaintext attack)

Tento útok je podobný tomu předchozímu, rozdíl je pouze v tom, že útočník má navíc k dispozici i otevřený text k textu šifrovému. Ke zjištění použitého klíče pak vede metoda tzv. diferenciální kryptoanalýzy.

2.4 Kompromitace uživatelů

Tato metoda, označovaná též jako *social hacking*, představuje v podstatě vydírání za účelem získání klíče. Nejedná se tedy o technickou kryptoanalýzu.

2.5 „Člověk uprostřed“

Útok „člověk uprostřed“ (*man in the middle*) je založen na snaze útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem. Tento

útok je používán především proti asymetrickým šifrám, jelikož při nich dochází k výměně klíčů otevřeným kanálem.

Útok vypadá tak, že během výměny veřejných klíčů je útočník zachytí a vymění za své veřejné klíče, které jsou však označeny tak, že vypadají jako od předpokládaného odesílatele. Nyní si obě komunikující strany myslí, že mají veřejný klíč toho druhého, což však není pravda. Cokoliv si mezi sebou pošlou, útočník zachytí, dešifruje, přečte, eventuálně změní, znovu zašifruje a odešle původnímu příjemci jako by to byla pravá zpráva.

Je důležité podotknout, že v prostředí počítačových sítí není nutné, aby útočník byl fyzicky na cestě mezi účastníky komunikace, protože lze síťový provoz snadno přesměrovat.

Nejlepší možnou obranou proti tomuto útoku je ověření získaného veřejného klíče například pomocí certifikační autority (viz dále).

2.6 Útok postranním kanálem

Jedná se o jakýkoliv útok založený na zneužití informací získaných ze samotné fyzické implementace kryptosystému. Tento druh útoku se tedy nesnaží najít slabiny v matematické struktuře algoritmu. Cílem útoku postranními kanály nemusí být pouze kryptografický klíč, ale například jen informace o tom, jaký algoritmus se pro šifrování používá, jak dlouho trvá vykonání algoritmu nebo jeho části.

Mezi hlavní druhy útoků postranním kanálem patří:

2.6.1 Časová analýza (*Timing attack*)

Jedná se o útok založený na měření toho, jak dlouho jednotlivé výpočetní operace trvají. Doba výpočtů prováděných s tajným klíčem je totiž na tomto klíči závislá.

2.6.2 Odběrová analýza (*Power analysis attack*)

Odběrová analýza může poskytnout celkem detailní informace o použitém kryptosystému pomocí sledování spotřeby energie zařízení (procesor, šifrovací okruh, čipová karta). Pokud je útočník schopen sledovat, jak se mění spotřeba zařízení během provádění kryptografických operací, může zjistit nejen to, jaké operace zařízení provádí, ale také mu tato informace může pomoci k získání tajného klíče, se kterým je kryptografický algoritmus prováděn.

Odběrovou analýzu lze dále rozdělit do dvou skupin na jednoduchou a diferenciální. Jednoduchá odběrová analýza může poskytnout informace, jaký algoritmus je používán,

identifikovat jeho části nebo odhalit posloupnost instrukcí. Diferenciální odběrová analýza využívá ke zjištění klíče statistické metody založené na několika tisíci měření.

2.6.3 Útok zaváděním chyb (*Fault induction attack*)

Při tomto typu útoku se útočník snaží zavést do průběhu výpočtu chyby tak, aby mu jejich výskyt prozradil něco o systému.

2.6.4 Elektromagnetická analýza (*Electromagnetic analysis attack*)

Tento typ útoku je založen na měření a následné analýze elektromagnetického pole, které je generováno změnou proudů při činnosti zařízení.

[QUISQUATER, 2002]

3 Symetrické šifry

Symetrické šifry neboli šifry tajného klíče jsou takové šifry, kde ze znalosti šifrovacího klíče K_1 lze „početně jednoduše“ odvodit dešifrovací klíč K_2 a naopak. Protože u mnoha symetrických šifrovacích algoritmů jsou tyto dva klíče shodné, označuje se obecně klíč za symetrický. Pro šifrování se používají algoritmy, u kterých platí, že při znalosti vstupního a zakódovaného textu je velmi obtížné vygenerovat klíč, přestože vlastní šifrování a dešifrování pomocí tohoto klíče je rychlá záležitost. Obtížnost eventuálního zjištění klíče záleží zejména na vlastní délce klíče.

Zásadním aspektem komunikace, která využívá symetrické šifry, je tzv. problém distribuce klíčů. [PŘIBYL, 2004, s. 24] Ke komunikaci je zapotřebí další kanál, sloužící pro výměnu klíčů. Tento kanál musí být zabezpečený a je zásadní pro neprolomitelnost šifry.

3.1 Dělení symetrických šifer

Běžně se rozlišují dvě třídy šifer symetrického klíče: blokové a proudové šifry.

3.1.1 Blokové šifry

Bloková šifra je kryptosystém, který rozděluje zprávu otevřeného textu za účelem přenosu do posloupností (nazývaných bloky) pevné délky, které jsou následně postupně šifrovány. Velikost bloku šifry má zásadní význam pro bezpečnost celého algoritmu. Pokud by velikost tohoto bloku byla malá, bylo by možné sestavit kompletní seznam (při určitém klíči) vstupních hodnot algoritmu a jim odpovídajících hodnot výstupních. To by mělo negativní dopad na bezpečnost algoritmu. V současnosti se používají bloky o délce 64 bitů a více. [POŽÁR, 2007, s. 86]

3.1.2 Proudové šifry

Proudové šifry jsou šifrovací algoritmy, které mohou zpracovávat zprávu libovolné délky tak, že šifrují její jednotlivé prvky, tj. bity či byty. Jsou to vlastně jednoduché blokové šifry s délkou bloku jedna. Výhodné je, že před šifrováním se nemusí shromáždit celý blok dat. Proto se užívají také tam, kde data musí být zpracována po jednotlivých symbolech (nedostatečná paměť, omezené ukládání dat). Dále jsou proudové šifry velmi výhodné tam, kde je velká chybovost přenosu, protože u nich nedochází k šíření chyb.

3.2 Základní algoritmy

V této kapitole budou představeny základní kryptografické algoritmy využívající symetrické šifrování. Většina z nich byla používána po velmi dlouhou dobu, ale dnes jsou již zastaralé a nevyhovují bezpečnostním nárokům. Přesto jsou často součástí tzv. složených šifer, které jsou naopak používány hojně a jejichž bezpečnost je vysoká. Proto zde budou tyto základní algoritmy popsány. Práce si neklade za úkol věnovat se historii kryptografie, historická stránka bude tedy zmíněna pouze okrajově.

3.2.1 Substituční šifry

Jedná se o jednoduchý způsob šifrování, který používali již staří Římané. Dochází při něm k nahrazování jednotlivých znaků otevřeného textu znaky jinými. Pokud je na celý otevřený text používána pouze jedna substituce, mluvíme o monoalfabetickém šifrování, pokud se substituce mění např. podle pozice znaku v textu, jedná se o polyalfabetické šifrování.

Monoalfabetická Césarova substituční šifra

Tímto názvem je obvykle označována šifra, při jejímž použití jsou písmena uspořádané abecedy o m znacích nahrazována písmeny následujícími v abecedě o daný počet míst dále. Uvažujeme samozřejmě cyklický posun. Klíčem algoritmu je tedy délka cyklického posunu k, přičemž $1 \leq k \leq m$. [JIROUŠEK, 2006, s. 242]

Kryptoanalýza takové šifry je velice jednoduchá. Frekvence znaků v šifrové zprávě zůstane zachována. Pomocí frekvenční analýzy, která porovná nejfrekventovanější znaky v daném jazyce s nejfrekventovanějšími znaky v šifrovém textu, by mělo být možné text rozšifrovat.

Homofonní substituční šifra

Tato šifra poskytuje určitou ochranu proti frekvenční kryptoanalýze. Vysoce frekventovaným znakům přiřazuje více možných šifer, kdežto málo frekventovaným pouze jednu. Samozřejmě i tato šifra je však prolomitelná.

Polyalfabetická Vigènerova substituční šifra

Polyalfabetické šifry jsou vesměs založeny na spojení více monoalfabetických šifer. Základním typem je Vigènerova šifra, což je v minulých stoletích rozšířený kryptosystém tvořený postupným periodickým používáním souboru d Césarových šifer (s různými posuny) na jednotlivé znaky otevřeného textu. Vigènerova šifra tedy umožňuje řádově zvětšovat počet

možných klíčů prodlužováním *periody d*. Klíč K je zadáván jako heslo (slovo délky *d*, jehož jednotlivá písmena určují posuny).

Kryptoanalýza této šifry se skládá ze dvou částí: nalezení periody *d* a následné frekvenční analýzy (jako u Césarovy šifry). Hledání periody je založeno buď na analýze koincidencí v šifrovém textu, nebo analýze odstupu stejných posloupností v šifrovém textu. [JIROUŠEK, 2006, s. 245]

3.2.2 Transpoziční šifry

Další třídu šifer symetrického klíče představuje jednoduchá transpoziční šifra, která pouze permutuje znaky ve zprávě či bloku. Dochází tedy pouze ke změně pořadí těchto znaků. I tato šifra je snadno prolomitelná a samostatně se již nepoužívá. [POŽÁR, 2007, s. 86]

3.3 Používané algoritmy

V této kapitole jsou představeny algoritmy, které jsou stále používány a jsou hojně rozšířeny a jejichž prolomení je nemožné nebo velice obtížné. U každého algoritmu je popsán základní princip šifrování (není zacházeno do matematických detailů) a zmíněna jeho bezpečnost. Uvedené algoritmy představují základ v praxi používaných algoritmů. Existují různé úpravy těchto algoritmů a nepřeberné množství dalších šifrovacích technik, které jsou používány, na jejichž výčet však v této práci není prostor.

3.3.1 Vernamova šifra

Vernamova šifra má význačné postavení mezi symetrickými kryptosystémy. Je založena na principu Vigenèrovy šifry s tím, že klíč (heslo) má stejnou délku jako zpráva. Jako klíč se může použít například text knihy, na které se odesílatel a příjemce dohodnou nebo zcela náhodná posloupnost znaků.

V tomto druhém případě je Vernamova šifra označována jako one-time pad a je dosud používána pro předávání výjimečně tajných zpráv. Lze totiž dokázat, že se jedná o tzv. perfektní kryptosystém, tj. že ze znalosti šifrového textu se nic nedozvíme o zprávě. Předem připravený klíč potřebné délky je zapotřebí po použití zničit, aby nedošlo k dešifrování odposlechnutého šifrového textu ani v budoucnu. [MENEZES, 1997, s. 22]

3.3.2 DES

Zkratka tohoto algoritmu znamená Data Encryption Standard. Americký normalizační institut ANSI pro něj používá též označení DEA (Data Encryption Algorithm). Jedná se o symetrickou blokovou šifru tvořenou 64bitovými bloky, která využívá 56bitový klíč (ve

skutečnosti má klíč délku 64 bitů, 8 bitů však slouží pouze jako paritní bity pro odhalení chyb pomocí kontrolního součtu).

Algoritmus DES byl vyvinut v 70. letech, v roce 1977 byl zvolen jako standard pro šifrování dat v civilních státních organizacích USA a byl využíván do konce 90. let 20. století. Jak bude popsáno dále, DES se stal postupem času bezpečnostně nevyhovující. Dnes má algoritmus spíše historický význam. Stal se však inspirací pro řadu v současnosti používaných algoritmů, proto je vhodné se s ním seznámit.

Základem DESu jsou dvě po sobě jdoucí operace – substituce a permutace. Ty jsou společně s klíčem použity k zašifrování otevřeného textu. Jeden takový průběh algoritmu se nazývá iterace (runda). Během šifrování vykoná DES plných 16 iterací.

Na vstupu je otevřený text rozdělen na 64bitové bloky. Algoritmus zahájí zpracování bloku počáteční permutací. Po ní je blok rozděleny na pravou a levou polovinu. S těmi se provede 16 iterací substituce a permutace za použití klíče. Tím dosáhneme promíchání dat s klíčem. Po dokončení poslední iterace se levé a pravé poloviny opět spojí. Na závěr dojde na konečnou permutaci. Tím je šifrování u konce.

Konkrétně se v každé iteraci bity klíče posunou a poté se z 56 bitů klíče vybere 48 bitů. Pravá polovina dat se rozšíří expanzní permutací na 48 bitů, zkombinuje se s 48 bity posunutého a permutovaného 48bitového klíče ve sčítačce modulo 2, zpracuje 8 S-boxy na 32 nových bitů a znovu permutuje. Tyto čtyři operace představují funkci *f*. Výstup funkce *f* se potom v další sčítačce mod-2 zkombinuje s levou polovinou dat. Výsledek těchto operací se stává novou pravou polovinou; stará pravá polovina se stává novou levou polovinou. Tyto operace se opakují 16krát a vytvářejí 16 rund DESu.

Bude-li B_i výsledkem i-té iterace, L_i a *Ri* levou a pravou polovinou B_i, K_i 48-bitovým klíčem pro i-tou rundu a funkcí *f* provádějící veškeré substituce, permutace a operace mod-2 s účastí klíče, pak runda bude vyjádřena takto:

$L_i = R_{i-1}$

$R_i = L_{i-1}$ *mod-2* $f(R_{i-1}, K_i)$

K dešifrování se používá naprosto stejné schéma. Jediným rozdílem je, že šifrovací klíče je nutné aplikovat v opačném pořadí, abychom získali zpět otevřený text.

DES existuje i v bezpečnější rozšířené variantě - tzv. trojnásobném DESu (Triple DES, 3DES). Algoritmus je na šifrovaný text použit celkem třikrát za použití dvakrát tak dlouhého klíče. Při prvním a třetím běhu se text zašifruje první polovinou klíče, prostředním

krokem se dešifruje použitím druhé poloviny [PŘIBYL, 1996, s. 124], [FIPS PUB 46-3, 1999].

Bezpečnost

Algoritmus DES byl uznán za americký národní šifrovací standard roku 1977, přestože vůči němu byly vznášeny námitky. Týkaly se především délky jeho klíče (56 bitů). Národní bezpečnostní agentura argumentovala tím, že stroj, který by byl natolik rychlý, aby otestoval všechny klíče v rozumném čase, by stál nerozumně velkou sumu peněz. O dvacet let později se však námitky ukázaly jako oprávněné.

V roce 1998 byla společností RSA Security vyhlášena soutěž na prolomení šifry DES. Nadace Electronic Frontier Foundation (EFF) při této příležitosti postavila stroj Deep Crack, který stál necelých 250 000 dolarů. Tento stroj byl schopen otestovat více než 90 miliard klíčů za sekundu. Otestovat všechny klíče z rozsahu DESu by tímto tempem zabralo asi 9 dní. Průměrná doba nalezení správného klíče je ovšem poloviční.

S pomocí Deep Cracku se podařilo rozluštit soutěžní šifru za 56 hodin. EFF tím dokázala, že pro bohaté korporace nebo vlády v současnosti není problém si opatřit stroj, který DES v relativně krátké době dokáže prolomit. Další rok (1999) byl DES opět potvrzen jako americký národní standard. Tentokrát ovšem ve vylepšené verzi 3DES. Nebezpečně malá velikost klíče DESu společně s relativně vysokou výpočetní náročností 3DESu vyústily v jeho nahrazení novou šifrou AES. Ta vstoupila v platnost jako americký standard 26. května 2002. [ELECTRONIC FRONTIER FOUNDATION, 2013]

3.3.3 AES

Advanced Encryption Standard (AES) je bloková šifra, která byla přijata po náročném výběrovém řízení na nový americký kryptografický standard. Otevřenost celého procesu výběru napomohla ke zvýšení důvěry v bezpečnost nového algoritmu a získala si příznivé ohlasy napříč odbornou veřejností. Vítězem soutěže se stal algoritmus Rijndael, jehož autoři jsou belgičtí kryptologové Joan Daemen a Vincent Rijmen. Jako AES byl schválen Národním úřadem pro standardizaci (NIST) s účinností od května 2002. V současnosti je jedním z nejpopulárnějších algoritmů symetrické kryptografie. [FIPS PUB 197, 2001]

Z přesného pohledu na věc není AES úplně totéž jako Rijndael. Rijndael totiž podporuje větší rozsah bloku a velikosti klíče (může využít jakoukoli velikost bloku a klíče, která je násobkem čísla 32; minimum 128 a maximum 256 bitů). AES má proti němu fixní blok o velikosti 128 bitů a podporuje tři velikosti klíče: 128, 192 a 256 bitů. AES je rychlý

v softwarovém i hardwarovém provedení, je relativně snadný na implementaci a paměťově nenáročný.

Bloky 128 bitů, neboli 16 bytů, se obvykle u tohoto algoritmu zapisují jako dvojice hexadecimálních symbolů uspořádaných do matice 4 x 4 po sloupcích. Tuto strukturu využívají tři pevně dané následující operace, které jsou aplikovány v různých místech algoritmu. [JIROUŠEK, 2006, s. 263]

Bytová substituce (SubByte)

Jednotlivé byty jsou substituovány podle dané tabulky. Byte XY v hexadecimálním zápisu je nahrazen bytem uvedeným v řádku X a sloupci Y.

Rotace řádků (ShiftRow)

Pole v matici bytů 4 x 4 jsou přeházena tak, že v řádku 1 proběhne posun vlevo (rotace) o 1 pole, v řádku 2 o 2 pole a v řádku 3 o 3 pole. V řádku 0 rotace neprobíhá.

Vynásobení mixovací maticí (MixColumns)

Tato operace je realizována tak, že šifrovaná matice je vynásobena zleva danou mixovací maticí.

Podobně jako v systému DES probíhá i v systému AES šifrování v iteracích (rundách), v nichž jsou používány klíče z daného odvozeného klíče. V základní (128bitové) verzi AES probíhá 10 iterací, kdy dojde ke třem popsaným operacím a zadaný klíč je expandován na dalších 10 odvozených klíčů.

Šifrovací algoritmus:

Proces šifrování je zahájen přičtením klíče K. Poté probíhá s maticí 9 iterací následující posloupnosti operací:

1. Každý byte matice je transformován substitucí SubByte.
2. Výsledná matice je rotována operací ShiftRow.
3. Výsledek je vynásoben mixovací maticí MixColumns.
4. Na závěr je takto transformované matici bytů přičten příslušný odvozený klíč, tvořený pro každou iteraci po sobě jdoucími sloupci získanými při expanzi klíče K.

Závěrečná iterace vynechá krok 3. [JIROUŠEK, 2006, s. 267]

Bezpečnost

Objevily se námitky, že poměrně jednoduchá matematická struktura algoritmu představuje bezpečnostní riziko. V roce 2002 oznámili Courtois a Pieprzyk teoretický útok, který nazvali „XSL Attack“. Ten ukázal možnou slabinu AESu. Jeho tvůrci prohlašovali, že je schopný prolomit AES rychleji než běžný útok hrubou silou. XSL Attack používá speciální algoritmus eXtended Sparse Linearization k získání klíče. Tato metoda vyžaduje pouze relativně malé množství známých otevřených textů oproti jiným metodám, které jich potřebují nerealisticky vysoký počet.

I když XSL dokáže prolomit některé moderní algoritmy, útok v současnosti znamená malé nebezpečí, co se týče praktické bezpečnosti. Stejně jako mnoho moderních kryptoanalytických výsledků by mohl být takzvanou *certifikační slabinou*: zatímco je rychlejší než útok hrubou silou, potřebné zdroje jsou stále příliš vysoké a je velice nepravděpodobné, že by jím mohly být skutečné systémy nějak ohroženy. Ovšem budoucí úpravy mohou zvýšit praktičnost tohoto útoku. Jelikož je takový typ útoku nový a neočekávaný, někteří kryptografové vyjádřili znepokojení nad algebraickou jednoduchostí šifer typu Rijndael.

Nebezpečí tak představují zejména útoky postranním kanálem. V roce 2005 Bernstein oznámil útok pomocí časové analýzy na zákaznický server šifrovaný AESem prostřednictvím OpenSSL. Útok vyžadoval přes 200 milionů vybraných souborů textů získaných z údajů o časování serveru. Někteří odborníci namítají, že takovýto útok není v prostředí internetu praktický na vzdálenost větší než jeden hop (metrika používaná k měření vzdálenosti mezi zdrojem a cílem. Každý hop znamená přenos paketu přes jednu síť).

Ve stejném roce jako Bernstein zveřejnili Osvik, Shamir a Tromer výsledky svých útoků pomocí časových analýz proti AESu. Jeden z útoků umožnil získat celý klíč po vykonání pouhých 800 operací během 65 milisekund. Tento útok však vyžaduje, aby byl útočník schopen spouštět programy na stejném systému, na němž běží AES.

3.3.4 Blowfish

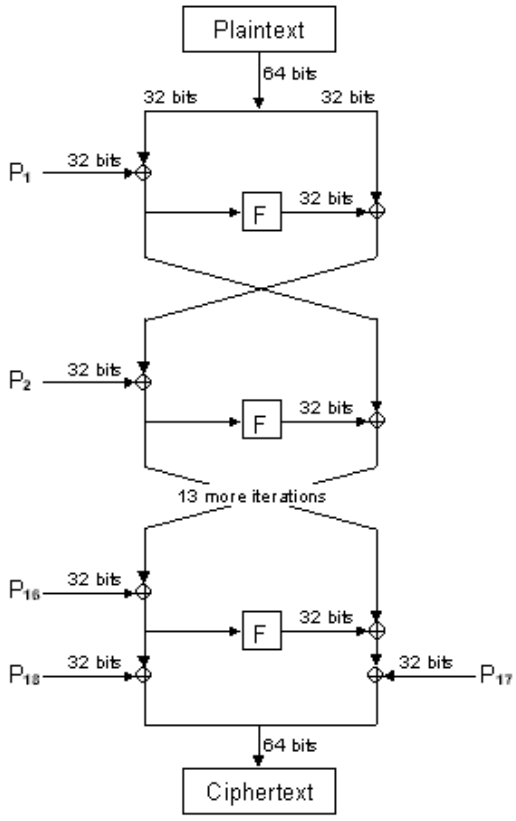
Autorem algoritmu Blowfish je B. Schneier, který jej publikoval v roce 1993. Tento algoritmus není patentován a je volně k dispozici. Jde o velmi rychlý a jednoduchý algoritmus, jak dokazují výsledky měření v kapitole číslo 6.

Šifrování dat je prováděno v šestnácti rundách po blocích 64 bitů, které se dále dělí na subbloky o 32 bytech (obrázek č. 1).

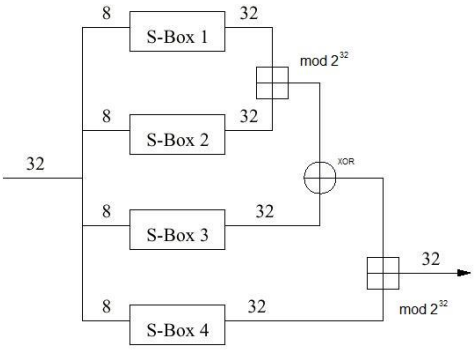
Každá runda provádí permutaci závislou na klíči a substituci závislou jak na kódovaných datech tak i klíči. Algoritmus pracuje s operacemi XOR a sčítání modulo 2^{32}.

Funkce F rozdělí 32bitové vstupní slovo na čtvrtiny *a, b, c, d*. Tyto části po řadě představují jednotlivé byty (8 bitů) vstupního slov zleva doprava (tj. *a* představuje bity 24-31, *b* bity 16-23, atd.) a používají se jako indexy do S-boxů. Výsledná hodnota funkce vznikne tak, jak je vyjádřeno na obrázku č. 2.

Blowfish používá velký počet podklíčů, které musí být vypočteny ze zadaného klíče ještě před samotným šifrováním, respektive dešifrováním dat. Podklíče jsou uloženy celkem v pěti polích. První pole, označované jako P-pole, má celkem 18 32bitových položek, další čtyři pole označované jako S-Boxy mají 256 32bitových položek. Maximální délka klíče je 448 bitů.



Obrázek 1 Schéma algoritmu Blowfish[Šifrování, 2013]



Obrázek 2 Šifrovací funkce algoritmu Blowfish [LULEA UNIVERSTITY OF TECHNOLOGY, 2013]

Bezpečnost

Míru dosažené bezpečnosti lze regulovat délkou použitého klíče. Rovněž lze omezit počet rund šifrovacího procesu. Snížení počtu rund vede k jistému snížení odolnosti vůči kryptoanalýze, výhodou je ovšem vyšší rychlost šifrování. Naopak se nezdá, že by další zvyšování počtu rund mělo zásadní vliv na zvýšení bezpečnosti algoritmu. V současnosti není znám lepší způsob kryptoanalýzy tohoto algoritmu než hrubou silou. [JAŠEK, 2006, str. 104]

4 Asymetrická kryptografie

Asymetrická kryptografie neboli kryptografie veřejného klíče je skupina kryptografických metod, ve které se pro šifrování a dešifrování používají odlišné klíče. Na rozdíl od symetrické kryptografie, která používá k dešifrování i šifrování jediný klíč, mají obě strany komunikace svůj vlastní klíč, přičemž jeden je veřejný a druhý soukromý. Z tohoto nevyrovnaného rozdělení klíčů (veřejný oproti soukromému) vzniklo označení asymetrická kryptografie.

Asymetrická kryptografie byla vyvinuta z důvodů problémů vyskytujících se při symetrické kryptografii, přičemž hlavním problémem je distribuce klíčů mezi dvěma komunikujícími entitami. Tuto skutečnost eliminuje asymetrická kryptografie, jelikož při použití dvou klíčů lze šifrovat jenom veřejným klíčem a soukromým dešifrovat. Eliminuje také distribuci klíčů, protože jedna entita používá pouze jeden klíč. Asymetrická kryptografie byla vyvinutá v polovině 70. let dvacátého století a vyskytla se v protokolu Diffie-Hellman pro ustanovení klíčů mezi dvěma entitami pro šifrovací přenos na nezabezpečeném kanále.

Asymetrická kryptografie se využívá nejen k šifrování dat, ale také pro elektronický podpis, tedy metodu, která jednoznačně prokáže autora dat. Dalším důležitým využitím asymetrické kryptografie je zajištění bezpečné výměny klíčů symetrické kryptografie.

Veřejný klíč nemusí být držen v bezpečí, a jak už z jeho pojmenování vyplývá, může být volně dostupný. Tím pádem odpadá nutnost zabezpečené distribuce klíčů mezi účastníky komunikace. To ale neznamená, že by správa klíčů asymetrické kryptografie byla bezproblémová. Nejdůležitějším prvkem jejího bezpečného využití je autentizace klíčů, kterou zajišťuje digitální certifikace.

4.1 Jednosměrné funkce

Jednosměrné funkce jsou základním mechanismem pro asymetrickou kryptografii.

Jednosměrná funkce je taková funkce $f: X \rightarrow Y$, pro niž je snadné z jakékoli hodnoty $x \in X$ vypočítat $y = f(x)$, ale pro nějaký náhodně vybraný obraz $y \in f(X)$ nelze (neumíme, je to pro nás výpočetně nemožné) najít její vzor $x \in X$ tak, aby $y = f(x)$ [KLÍMA, 2005]. Víme přitom, že takový vzor existuje nebo jich dokonce existuje velké množství. V praxi je pak takovou funkcí například vynásobení ohromných čísel, kdy z výsledného čísla nejsme schopni dostatečně rychlou metodou původní čísla separovat.

Konkrétně jsou jednosměrné funkce využívané v kryptografii založené na některém z následujících matematických problémů.

4.1.1 Problém faktorizace čísla

Problém faktorizace čísla je problém rozložení libovolného velkého celého čísla na součin prvočíselných mocnin

$$n=p_1^{e1}p_2^{e2}p_3^{e3}p_4^{e4} \dots p_k^{ek}$$

Prvočísla mají důležitý význam jak v matematice, tak v kryptografii.

4.1.2 Problém výpočtu diskrétního logaritmu

Problém výpočtu diskrétního logaritmu je další z problémů, se kterými počítají různé systémy asymetrické kryptografie. Spočívá na principu rozložení přirozeného čísla na mocninu jiného čísla $a=g^x$ v modulární aritmetice dané vhodným modulem m. Nalezená mocnina x, kterou lze zapsat jako $x=log_g a$, se pak nazývá diskrétní logaritmus. Na tomto problému pracují systémy ElGamal, Diffie-Helmanův protokol a další. Problém diskrétního logaritmu je považován za neřešitelný problém v reálném čase pro velká celá čísla. Kryptosystémy založené na diskrétním logaritmu jsou považovány za velmi bezpečné při správné délce klíče. [MENEZES, 1997, s. 104]

4.1.3 Problém mřížky

Problém mřížky neboli problém „*lattice*“ je základem jedné z metod moderní asymetrické kryptografie. Tento problém spadá do skupiny post-kvantových algoritmů a je velmi odolný proti útokům hrubou silou a dalším. Teoreticky je také odolný vůči kvantovým počítačům, ale pouze proto, že dnes neexistuje žádný účinný kvantový algoritmus, který by uměl počítat problémy typu mřížky.

4.1.4 Problém batohu

Problém batohu (*knapsack problem*) je další z problémů, na kterých jsou postaveny některé kryptosystémy. Tento problém vychází z kombinační matematiky a můžeme si ho

představit tak, že se snažíme zjistit, jakými závažími je naplněn batoh, pokud známe jejich celkovou hmotnost. [PFLEEGER, 2007]

4.2 Hašovací funkce

Vedle šifrování symetrickým a asymetrickým klíčem existuje ještě jedna oblast šifrování, kde potřebujeme informaci pouze zašifrovat, ale už nikdy dešifrovat. Taková funkce se nazývá hašovací (z anglického *hash*) nebo také hašé funkce, dále se můžeme setkat s označením digitální otisk.

„Hašovací funkce je výpočetně efektivní funkce, která transformuje (mapuje) posloupnosti binárních symbolů libovolné délky na binární posloupnosti určité konstantní délky, nazývané haš (hašé hodnota, otisk).“[PŘIBYL, 2004, s. 46]

Hašovací funkce musí vyhovovat následujícím požadavkům:

- musí být jednosměrná, tedy nesmí být možné z hodnoty haše odvodit původní zprávu
- musí být nekolizní, není tedy možné odvodit dvě různé výchozí zprávy pro tutéž hodnotu haš

Aby hašovací funkce nebyla kolizní, musí být stanovena minimální délka výsledného zašifrovaného řetězce. Pro definici délky haše se využívá princip „narozeninového útoku“ (birthday attack). Principem tohoto útoku je, že s rostoucím počtem osob v jedné místnosti roste i pravděpodobnost, že dvě osoby budou mít narozeniny ve stejný den. V praxi to znamená, že s rostoucím počtem možných vstupních textů se zvyšuje pravděpodobnost, že dva různé texty vytvoří stejný haš. Doporučeným standardem je délka haše 160 bitů, která se používá i pro digitální podpisy. [JAŠEK, 2006, s. 30]

Příkladem využití hašovací funkce je uložení hesla do systému pro možnost následné autentizace pomocí tohoto hesla. Uživatel zadá nové heslo do systému a ten vytvoří jeho haš, který je následně uložen. Při dalším přihlašování systém porovná nově vypočítaný haš s tím uloženým. Algoritmus výpočtu haše zůstává stejný, takže při použití stejného hesla dojde ke shodě. Využití hašovací funkce je jasné – samotné tajné heslo nemusí být nikde ukládáno.

Kryptografické hašovací funkce se nejčastěji uplatňují u digitálních podpisů a datové integrity. U digitálních podpisů se obvykle vytvoří haš dlouhé zprávy a podepíše se jen tento haš. Subjekt, který potom zprávu přijme, vygeneruje haš a ověří, že přijatý podpis patří tomuto haši. To šetří čas a prostor v porovnání s přímým podepisováním zpráv, při kterém by

bylo nutné zprávy dělit na bloky vhodné velikosti a následně jednotlivé bloky individuálně podepisovat.

Hašovací funkce slouží k zajištění datové integrity následujícím způsobem. Nejprve se pro daná data vypočte haš a ten se nějak ochrání. Po nějaké době se provede kontrola datové integrity vstupních dat tak, že se z nich opětovně vypočte haš a výsledek se porovná s původní hodnotou haše.

Pokud hašovací algoritmy slouží k detekci případných modifikací vstupních zpráv, jsou označovány jako kódy pro detekci modifikací (MDC - Modification Detection Code).

Existují také algoritmy, které přidají k vstupnímu textu ještě heslo a pak tento nový zaheslovaný text použijí jako vstup hašovací funkce. Takové algoritmy se nazývají kódy pro autentizaci zpráv (MAC – Message Authenticity Code).

Mezi nejčastěji používané bezpečnostní hašovací funkce patří Message Digest 5, Secure Hash Algorithm 1 a 2 (SHA), Tiger a NIST Secure Hash Standard (SHS).

4.3 Elektronický podpis

Elektronický nebo také digitální podpis (Digital Signature) je autentizační systém pro ověřování pravosti elektronických dat. Využívá při tom algoritmy asymetrické kryptografie, ale v opačném případě jako šifrování pomocí asymetrických systémů – podepisuje se soukromým klíčem a veřejným se ověřuje autentičnost.

Elektronický podpis lze použít pro podepsání elektronického dokumentu libovolné délky a libovolného obsahu. Elektronický podpis je tvořen řetězcem bytů, který je připojen k podepisovanému dokumentu. Délka tohoto řetězce bývá obvykle 50 až 300 bajtů podle použitého algoritmu a požadovaného stupně bezpečnosti a nezávisí na délce podepisovaného dokumentu. Elektronický podpis poskytuje příjemci dokumentu funkce, jako je autenticita, integrita, neodmítnutelnost, utajenost a jednorázovost použití.

Elektronický podpis má následující vlastnosti:

- Je spojen s jedním konkrétním elektronickým dokumentem (tj. potvrzuje pravost a autenticitu tohoto dokumentu) a nemůže být použit pro podepsání jiného dokumentu.
- Může být vytvořen pouze tím, kdo zná jisté tajemství – soukromý klíč.

- Je nemožné vytvořit jiný dokument, sebeméně odlišný od původního dokumentu, pro který by byl původní elektronický podpis stále platný.
- Jakmile je jednou elektronický podpis v dokumentu vytvořen, kdokoli si může ověřit pravost tohoto podpisu a to bez nutnosti znát tajemství – soukromý klíč, kterým byl podpis vytvořen.

Nejčastěji používané algoritmy pro elektronický podpis jsou RSA a DSA (Digital Signature Algorithm). Oba algoritmy používají také hašovací funkce. V případě RSA se pro výpočet haše použije funkce MD5, v případě DSA se použije SHS.

4.4 Digitální certifikace

Šifrování s veřejným klíčem odstraňuje potíže spojené s tradičním symetrickým šifrováním, avšak přináší současně nové problémy. Rozhodující otázkou je nastolení důvěry, že určitý veřejný klíč patří do klíčového páru určité osoby. Můžeme si představit situaci, kdy uživatel elektronicky podepíše důležitý dokument. Vzápětí pozmění dokument nepovolaná osoba a znovu ho elektronicky podepíše jménem původního uživatele. Jak pozná příjemce, že dostal pravý dokument? Bylo nutné vybudovat mechanismy zaručující pravost veřejného klíče ve vztahu k jeho majiteli. Tyto mechanismy shrnuje označení infrastruktura veřejných klíčů (PKI, public key infrastructure). Vztah mezi majitelem a jeho veřejným klíčem potvrzuje digitální certifikát podepsaný důvěryhodnou třetí stranou. Tou je certifikační autorita (CA, certification authority), která má jediná právo certifikáty vydávat, ověřovat a odvolávat jejich platnost. Každý vydaný certifikát je podepsán soukromým klíčem certifikační autority. Příjemce pak může zkontrolovat nejenom integritu dat, ale i jednoznačnou totožnost podepisovatele. Pravost certifikátu si lze ověřit kontrolou jeho podpisu oproti certifikátu certifikační autority.

4.4.1 Certifikační autorita

Také certifikační autorita samotná potřebuje, aby byla důvěryhodná. V tomto směru jsou důležité dvě otázky: kdo certifikační autoritu provozuje a na jakém technologickém základě je postavena. První otázka se vztahuje na určité vyšší ověření certifikační autority. Například pro certifikáty používané v úředním styku může jít o povolení ze strany státu, pro certifikáty používané v rámci podniku se může jednat o schválení ze strany vedení. Druhá

otázka se týká konkrétního technologického řešení certifikační autority. Každé takové řešení musí splňovat určitá základní kritéria, ačkoli v jednotlivostech se může provedení u různých dodavatelů lišit. Jestliže budeme postupovat chronologicky s ohledem na životní cyklus digitálního certifikátu, narazíme nejprve na věc generování klíčového páru, vytvoření žádosti o certifikát a jejího schválení či zamítnutí. Pro tento účel je potřeba on-line server, který žádosti přijímá a eviduje. Další součást řešení se označuje jako registrační autorita. Jejím smyslem je poskytnout aplikační rozhraní pro oprávněné osoby, které budou ověřovat žádosti a vydávat certifikáty. Certifikáty jsou podepisovány v prostředí, které vyžaduje maximální ochranu, neboť narušení bezpečnosti by zpochybnilo veškeré vydané certifikáty. Aplikační rozhraní by mělo být také maximálně mobilní, nejlépe přístupné přes internet. [PFLEEGER, 2007]

4.4.2 Ověřování digitálních certifikátů

Opakovaným úkolem certifikační autority bude příjem dotazů na pravost daného certifikátu. Takový dotaz se objeví pokaždé, když na certifikát narazí nový uživatel, kupříkladu při prohlížení zabezpečené webové stránky či příjmu elektronicky podepsané zprávy. On-line server tudíž musí být postaven s ohledem na objem certifikátů, který bude certifikační autorita pravděpodobně spravovat. Pravost certifikátu se ověřuje buď porovnáním se seznamem odvolaných certifikátů (CRL, certificate revocation list) nebo za pomoci specifického internetového protokolu (OCSP, Online Certificate Staus Protocol). Každý certifikát má nastavenou určitou dobu platnosti, po níž přestává být veřejný klíč důvěryhodný. Nastává ovšem řada případů, například odcizení soukromého klíče, kdy je nutné certifikát zneplatnit ještě před vypršením této doby. Tato potřeba se řeší aktualizací seznamu odvolaných certifikátů. [TRUSCHKA, 2009]

4.5 Používané algoritmy

V této kapitole je představeno několik v praxi často používaných asymetrických algoritmů. U každého z nich je uveden jeho popis a nastíněna bezpečnost použití. Tato kapitola netvoří kompletní soupis všech asymetrických algoritmů. V praxi se často používají i různé úpravy popisovaných algoritmů, proto je třeba brát následující kapitolu jako základ problematiky aplikované asymetrické kryptografie.

4.5.1 Protokol Diffie-Hellman pro výměnu klíčů

Autoři tohoto kryptografického systému Whitfield Diffie a Martin Hellman jako první aplikovali asymetrickou kryptografii, a to v roce 1976. Tento systém je založen na problému diskrétního logaritmu, a jak už název říká, slouží pouze pro generování klíčů, které jsou následně použity pro symetrickou kryptografii.

Komunikující entity A a B se nejdříve shodnou na veřejných parametrech (p, g), kde p je prvočíslo a g je primitivní prvek $g<p$, je to takový prvek, že g^k mod q pro různá k nabývají všech hodnot $1, ..., p-1$. Každý z uživatelů si dále zvolí svůj privátní klíč X_A, respektive X_B jako celé číslo z intervalu $<2, p-2>$ a spočítá k němu svůj veřejný klíč $Y_A=g^{X_A} \bmod p$, respektive $Y_B=g^{X_B} \bmod p$. V okamžiku, kdy si chce A dohodnout s B symetrický klíč, tak si oba sdělí své veřejné klíče. Toto sdělení může probíhat nezabezpečeným kanálem, musí však být zajištěna autenticita jednotlivých klíčů (viz dále).

Na základě znalosti veřejného klíče Y_B, provede A výpočet $K_A= Y^{X_A} \bmod p$. Obdobně B vypočte $K_B= Y^{X_B} \bmod p$. Lze snadno ověřit že $K_A=K_B=K$. Hodnota K je nyní sdíleným tajemstvím mezi A a B, z něhož se dále vhodným definovaným způsobem odvodí symetrický šifrovací klíč. [MENEZES, 1997, s. 114]

Bezpečnost

Nevýhodou tohoto protokolu je bezbrannost proti útoku *Man in the middle* , protože neumožňuje autentizaci účastníků. Pokud tedy není tento protokol kombinován s jinými metodami, je vhodný pouze tam, kde útočník nemůže aktivně zasahovat do komunikace. V praxi se proto nejčastěji používá výměna veřejných klíčů prostřednictvím jejich certifikátů. Je třeba zdůraznit, že autenticita těchto veřejných klíčů je zde zásadním předpokladem bezpečnosti. [KLÍMA, 2004]

4.5.2 RSA

RSA byl objeven roku 1977 a jeho autoři jsou Ron Rivest, Adi Shamir a Joe Adleman. Jedná se o nejrozšířenější asymetrický kryptografický systém. Používá se jak k šifrování, tak k elektronickému podpisu a je založen na problému faktorizace čísla.

Samotný algoritmus můžeme rozdělit na dvě části:

- Vygenerování páru veřejný-soukromý klíč
- Šifrování a dešifrování

Vygenerování páru veřejný-soukromý klíč

Algoritmus pro generování soukromého a veřejného klíče provádí tyto kroky:

Entita zvolí dvě velmi velká prvočísla p a q, která neleží vedle sebe a jsou té samé (nebo podobné) velikosti. V praxi se používají prvočísla 512 až 4096 bitů velká. Nejdřív se vypočítá $n = pq$, a $r = (p - 1)(q - 1)$. Dále se zvolí číslo e takové, že $gcd(e, r) = 1$, což znamená, že tato číslo jsou nesoudělná. Algoritmus nakonec vypočte pomocí Euklidova algoritmu dešifrovací klíč d, $d=e^{-1} \bmod r$.

Nyní jsou prvočísla p, q nepotřebná a je nezbytné je zničit. Čísla n a d tvoří soukromý klíč, n a e je veřejný klíč.

Šifrování a dešifrování

Postup šifrování je jednoduchý a rychlý. Odesílatel si zjistí veřejný klíč příjemce a zprávu Z v digitální podobě rozdělí na bloky o stejné délce. Číselná hodnota každého bloku m_i musí být menší než n, tzn. $m_i < n$. Pak se každý i-tý blok zašifruje

$c_i = m_i^e \bmod n$

a jednotlivá c_i se pak spojí do zašifrované zprávy C. Příjemce ji pak dešifruje s pomocí svého soukromého klíče na původní zprávu takto:

$m_{i=} c_i^d \bmod n$.

Implementace

Největším problémem při implementaci algoritmu RSA zůstává jeho výpočetní náročnost. I přes rostoucí výkon výpočetní techniky je tento algoritmus neúnosně pomalý, což značně omezuje jeho použití v praxi. Důvodem této náročnosti je aritmetika s extrémně vysokými čísly.

Bezpečnost

Bezpečnost RSA závisí na nemožnosti výpočtu faktorizace čísla n, které je součinem čísel p a q. Právě pomocí těchto čísel se počítá proměnná r, která definuje vlastnost soukromého klíče. Při nesprávné volbě p a q není systém bezpečný a útočník může napadnout celý systém. Bezpečnost šifrovacího algoritmu je pak založena na problému výpočtu diskrétního logaritmu. Vhodná délka modulu n je dnes až 1024 bitů s tím, že velikost soukromého klíče by měla být stejné délky. Více o bezpečnosti a doporučených délkách klíčů v kapitole číslo 6.

4.5.3 Systém ElGamal

Systém ElGamal je asymetrický kryptosystém založený na problému výpočtu diskrétního logaritmu. Vychází z principu Diffie-Hellmanova algoritmu pro generování dvojice klíčů. Jeho hlavní nevýhodou je dvojnásobná délka šifrované zprávy oproti nezašifrované zprávě. Jeho nasazení je hlavně v PGP (Pretty Good Privacy) systémech a v GPG (GNU Privacy Guard) systémech. [KLÍMA, 2004]

Generování klíčů

Veřejné parametry klíčů jsou tvořeny dvojící (p, g), kde p je dnes alespoň 1024 bitové prvočíslo a g je „generátor" multiplikativní grupy G. Soukromý klíč je tvořen celým číslem x, které si uživatel volí z intervalu <2, p-2> a k němu příslušný veřejný klíč y vypočítá ze vztahu $y=g^x \bmod p$.

Šifrovací schéma

Šifrování zformátované zprávy m probíhá následovně:

Nejprve je zvoleno náhodné číslo k z intervalu <2, p-2> a vypočtou se hodnoty $\gamma = g^k$ a $K=y^k \bmod p$. Dále dochází k „multiplikativnímu šifrování" m jako $\delta = K * m \bmod p$. Kompletní zašifrovaná zpráva C je pak tvořena dvojicí (γ,δ).

Původní zprávu pak rozšifrujeme pomocí tohoto vzorce:

$m = \delta * \gamma^{p-1-x} \bmod p$.

S ohledem na algebraické vlastnosti použité „multiplikativní šifry" je nezbytné hodnotu k po použití nejen dobře utajit nebo nejlépe zničit, ale také ji generovat opravdu náhodně a nezávisle pro každou zprávu.

4.5.4 McEliece

Systém McEliece byl vyvinut Robertem McEliecem v roce 1978. Tento systém nevyužívá žádný z výše popsaných problémů, ale je založen na samoopravných kódech. Jedná se o tzv. Goppa kódy, pomocí kterých tento systém odolává útokům. Při šifrování používá také náhodné generování čísel. Hlavní výhodou oproti RSA je rychlost výpočtu, bohužel na

úkor náročnosti, protože soukromý a veřejný klíč je reprezentován jako matice s velmi velkým rozměrem. Z tohoto důvodu je systém stále málo využíván v praxi. Tento systém je bezpečný pouze pro určité parametry, pro všechny jiné jej lze považovat za neefektivní a nepoužitelný. Tyto parametry je třeba dodržovat a každá bezpečná kombinace je používaná pro jiné účely.

Generování klíčů se vypočte následovně: k, n a t jsou pevné parametry dané systémem. Entita vypočte $k \times n$ generační matici G, zvolí náhodně $k \times k$ nesingulární binární matici S a $n \times n$ permutační matici P. Vypočte matici $\hat{G} = SGP$. Veřejný klíč je pak $K_{pub}(\hat{G},t)$ a soukromý klíč je $K_{priv}(S,G,P)$.

Odesílatel nejdřív převede zprávu na binární číslo m délky k, zvolí binární chybový vektor z délky n. Vypočte šifrovanou zprávu jako binární vektor $c = m\hat{G} + z$. Příjemce pak zprávu dešifruje jako $\hat{c} = cP^{-1}$ kde P^{-1} je inverzní matice k P. Pak se pomocí $\hat{c}$ vypočte $\hat{w}$, a dále se vypočte m jako $m = \hat{w}S^{-1}$.

4.5.5 Eliptické křivky

Kryptografické systémy na bázi eliptických křivek navrhli nezávisle na sobě Victor Miller a Neal Koblitz v roce 1985. Jedná se o analogii kryptosystému s veřejným klíčem, ve kterých je modulární aritmetika nahrazena operacemi nad eliptickou křivkou. V současné době pronikly eliptické kryptosystémy do řady světových standardů a staly se alternativou ke „klasickému" RSA i DSA. Mají své výhody zejména v rychlosti a menší náročnosti na hardware i software. Jejich rozšíření není však stále tak značné, převážně proto, že „staré" kryptosystémy RSA, DSA, Diffie-Hellman, ElGamal atd. jsou používány, studovány a známy déle a mají vybudovánu potřebnou infrastrukturu. Z těchto důvodů jsou vývojářům a technologům bližší.

Systém na bázi eliptických křivek poskytuje stejnou bezpečnost jako systém RSA, ale s kratší délkou klíče, a proto vede k nižším nárokům na paměť. Pro tutéž bezpečnost potřebuje systém RSA klíč s délkou 1024 bitů, systém eliptických křivek pouze 160 bitů. Rychlost výpočtu je mnohem vyšší než u jiných systémů hlavně při podepisování dokumentů, bohužel nižší při samotném šifrování a ověřování.

Eliptická křivka (označuje se E) je matematický objekt, který je v algebře popsán rovnicí $y^2 = x^3 + ax + b$, kde a,b jsou reálné konstanty. S body vyhovujícími této rovnici lze dělat běžné operace jako sčítání a odečítání.

Pokud se sečtením dvou bodů P a Q na rovinné křivce vytvoří přímka, která se již neprotne s křivkou, tj. protne se v nekonečnu, lze napsat, že má přímka s křivkou společný bod O, neboli „nulový bod“. Pro nulový bod je třeba definovat operace, tzn. že $P + O = P$, $O + O = O$ a také $-O = O$. Soubor všech bodů ležících na křivce E nazýváme grupa E.

Šifrování pomocí eliptických křivek je založeno na modulární aritmetice a na problému diskrétního logaritmu. Mějme bod P ležící na křivce E, dále definujeme přirozené číslo r takové, že $r*P=0$. Nejmenší takové r, pro něž je $r*P=0$ nazýváme řád bodu P, přičemž v praxi se používá číslo o velikosti 256 bitů.

Při šifrování zvolíme tajné číslo k (privátní klíč) tak aby $r-1 \geq k \geq 1$, a vypočteme $Q = k*P$. Součástí veřejného klíče bude čtveřice (E, P, r, Q). Problém diskrétního logaritmu je pak právě úloha, jak z bodů P a Q určit tajné číslo k, tak, že $Q = k*P$.

Existují různé metody šifrování pomocí eliptických křivek. Při šifrování nepostačí jenom znalost veřejného klíče a hodnoty bodu P, je třeba znát i rovnici křivky E, na které systém pracuje. Jedna z nich je například modifikovaná metoda ElGamal pro eliptické křivky. U většiny metod se pouze systém modifikuje pomocí eliptické křivky, která představuje konečné těleso, a tím nahrazuje aktuální množinu, nad kterou metoda pracuje. Většinou se systém eliptických křivek používá pro digitální podpis nebo pro ustanovení symetrického klíče pro šifrování. Eliptické křivky jsou používány v systémech OpenSSL, NSS, GnuPG a jiné. Všechny platformy již tento kryptosystém hojně implementují do svých technologií. [OCHODKOVÁ, 2003], [JAŠEK, 2006]

5 Informační bezpečnost

Informační bezpečnost (*information security*) je obor zabývající se zabezpečením informací v informačních a komunikačních technologiích. „Jedná se o systém ochrany dat a informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace prostřednictvím logických, fyzických, technických, programových a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.“ [POŽÁR, 2007, s. 16]

„Informační bezpečnost můžeme definovat jako vzájemně provázaná opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření bezpečnosti informačních a komunikačních technologií pro zajištění dostupnosti, důvěryhodnosti a integrity informací.“ [SVETLÍK, 2002, s 12]

Obor informační bezpečnosti lze stručně vymezit jako specializaci zabývající se ochranou informací. Informace, které jsou nejčastěji v ohrožení, jsou buďto osobní data občanů nebo komerčně využitelné údaje.

Termínem informační bezpečnost můžeme také zastřešovat celý soubor aktivit směřujících k zajištění třech základních bezpečnostních atributů: důvěrnosti, dostupnosti a integrity.

Okruh informační bezpečnosti je velice rozsáhlé téma, na které nestačí kapacita této práce a ani to není jejím cílem. Následující kapitola představí hlavní aspekty informační bezpečnosti, převážně pak takové, které souvisí s aplikovanou kryptografií.

5.1 Bezpečnostní funkce

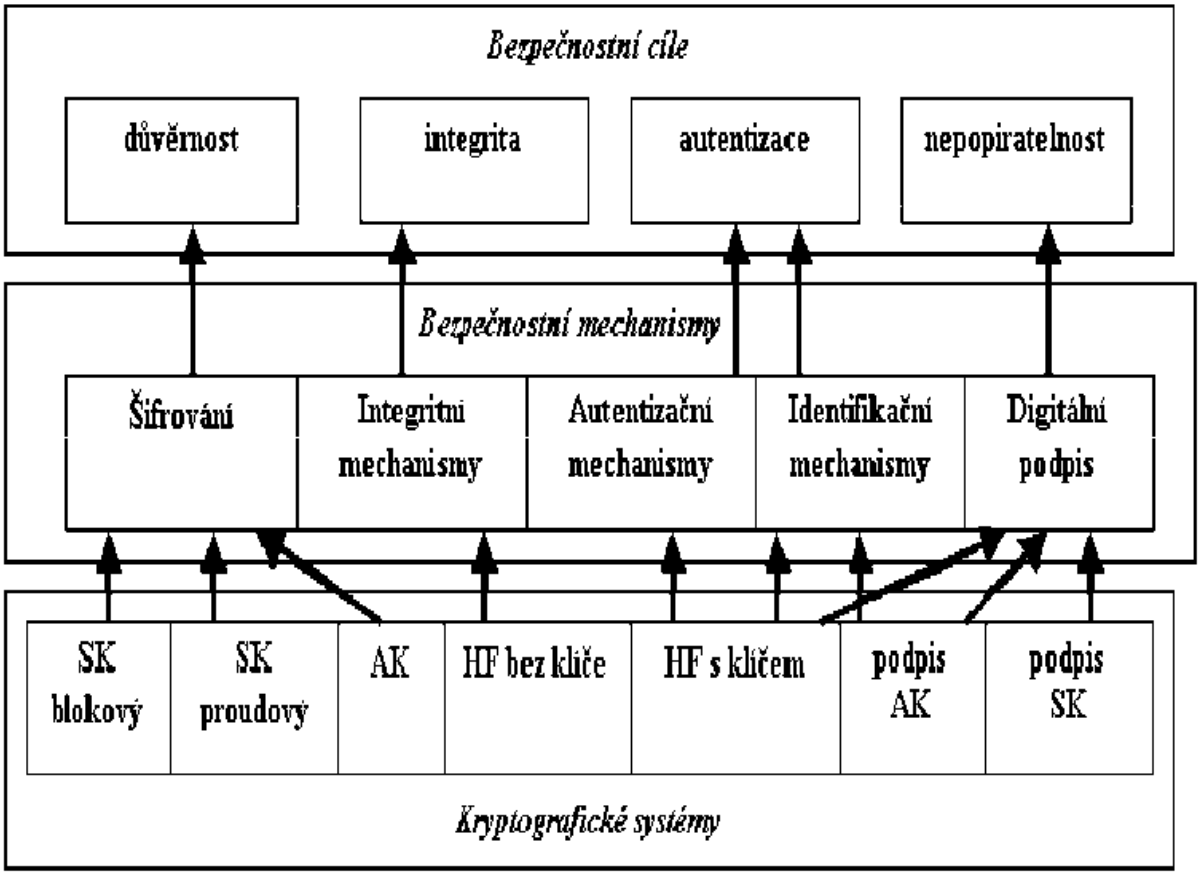
Zabezpečujeme-li informační systém, je třeba nejprve stanovit bezpečnostní cíle a způsob jejich dosažení. Bezpečnostní cíle jsou dílčí přínosy k bezpečnosti, kterou dosahuje informační systém z hlediska udržení důvěrnosti, integrity a dostupnosti. Pro jejich dosažení se aplikuje používání funkcí prosazujících bezpečnost, nazývaných rovněž bezpečnostní funkce nebo bezpečnostní opatření.

Bezpečnostní funkce přispívá buďto ke splnění jednoho bezpečnostního cíle, nebo ke splnění několika bezpečnostních cílů. Aby bylo možné bezpečnostní cíle stanovit, je nejdříve potřeba znát zranitelná místa, jak lze taková zranitelná místa využít, možné formy útoků, kdo může zranitelná místa využít nebo jejich prostřednictvím způsobit neúmyslnou škodu, kdo jsou potencionální útočníci, s jakou pravděpodobností dochází k útoku, jak se lze proti

útokům bránit a jaké škody mohou útoky způsobit. Prostředkem použitým pro dosažení stanovených bezpečnostních cílů informačního systému jsou bezpečnostní funkce informačního systému, které mohou být administrativního, fyzického, logického nebo technického typu, to znamená, že mohou být implementovány takovými mechanismy, jakými jsou administrativní akce, hardwarová zařízení, procedury, programy.

Bezpečnostní funkce musí být implementována dostatečně důvěryhodně, musí být adekvátním způsobem prokázáno, že její implementace vyhovuje její žádané, respektive zadané specifikaci. [LEHTINEN, 2006]

Vztah bezpečnostních cílů (respektive funkcí – ve schématu je tato vrstva sloučena s bezpečnostními cíli) a aplikované kryptografie dokresluje obrázek č. 3 (použité zkratky: SK – symetrická kryptografie, AK – asymetrická kryptografie, HF- hašovací funkce).



Obrázek 3 Vztah bezpečnostních cílů a kryptografie[KLIMEŠ, 2013]

5.2 Bezpečnostní mechanismy

Bezpečnostní mechanismy jsou nástroje používané pro implementaci bezpečnostních funkcí. Stejně jako bezpečnostní funkce je můžeme rozdělit na mechanismy

administrativního, fyzického, logického nebo technického typu. Tyto mechanismy mohou být při implementaci bezpečnostních funkcí spolu různými způsoby kombinovány tak, aby implementace bezpečnostní funkce byla přesná, účinná a ekonomická.

Některé bezpečnostní mechanismy mohou být použity pro implementaci několika i aplikačně odlišných bezpečnostních funkcí. Například kryptografický algoritmus lze použít pro implementaci bezpečnostní funkce zajišťující důvěrnost, integritu i identifikaci a autentizaci.

Některé bezpečnostní funkce mohou být implementovány jediným bezpečnostním mechanismem, jiné pouze více bezpečnostními mechanismy současně. Například bezpečnostní funkce zajišťující důvěrnost bývá typicky implementována vhodným šifrovacím mechanismem a administrativními předpisy pro zacházení s kryptografickými klíči. Bezpečnostní funkce zajišťující nepopiratelnost je obvykle implementována kryptografickým digitálním podpisem a administrativními mechanismy podporujícími důvěryhodnost takového podpisu.

V následujících odstavcích budou popsány základní bezpečnostní funkce.

5.2.1 Důvěrnost

Důvěrnost je definována jako zajištění toho, že informace je dostupná pouze osobám s autorizovaným přístupem, to znamená osobám, které jsou k tomu oprávněny.

Mechanismy důvěrnosti

Důvěrnost dat může záviset na médiu, na kterém jsou data uložena nebo kterým jsou přenášena. Proto důvěrnost uložených dat může být zajištěna použitím mechanismů, které ukryjí sémantiku (jako šifrování) nebo které rozdělí (fragmentují) data. Dále je možno využít mechanismů, které zamezí přístupu pomocí fyzicky chráněných kanálů nebo řízeného přístupu.

Z předchozího textu vyplývá možné rozdělení mechanismů do tří skupin:

- mechanismy, které zabraňují neautorizovanému přístupu k datům
- šifrovací mechanismy, které ukryjí data, ale ponechají je přístupná
- kontextuální mechanismy, které ponechají data přístupná pouze částečně s tím, že data nemohou být z omezeného množství shromážděných dat zcela zrekonstruována.

5.2.2 Dostupnost

Dostupnost nebo také dosažitelnost znamená, že vymezené objekty jsou dostupné pro autorizované subjekty a uživatele. V praxi to znamená, že všechny části systému zpřístupňující daný objekt (samotný informační systém ukládající, zpracovávající a zpřístupňující informace, bezpečnostní mechanismy sloužící k ochraně informací a komunikační kanály používané pro přístup) musí správně fungovat.

5.2.3 Integrita

Integrita neboli neporušitelnost znamená, že modifikovat data mohou pouze autorizovaní uživatelé. Posuzuje se úplnost a neporušenost informace z hlediska možného znehodnocení částečným zničením či pozměněním. [POŽÁR, 2005]

Klasifikace mechanismů integrity

Mechanismy pro zajištění integrity jsou klasifikovány podle prostředků, které používají k poskytování služeb integrity.

Zajištění integrity pomocí kryptografie využívá dvě třídy mechanismů:

- založené na symetrických kryptografických technikách – jedná se o pečetě.
- založené na asymetrických kryptografických technikách – jedná se o digitální podpis

Zajištění integrity pomocí pečetění

Pečetění zajišťuje integritu přidáním kryptografické kontrolní hodnoty k datům, která mají být chráněna. Při pečetění je stejný klíč používán k ochraně i k validaci integrity dat. Je-li použita třída mechanismů, jsou buďto všichni, kdo budou potenciálně provádět validaci, předem známi nebo musí mít prostředky, umožňující jim přístup k tajnému klíči.

Množina entit schopná pečetit data a množina entit schopná provést validaci dat jsou z definice mechanismu shodné.

Zajištění integrity prostřednictvím digitálních podpisů

Digitální podpisy jsou vytvářeny použitím soukromého klíče a asymetrického kryptografického algoritmu. Validace dat s vytvořenou ochranou (data a připojený digitální podpis) může být provedena s využitím odpovídajícího veřejného klíče.

Digitální podpisy dovolují, aby množina entit, které mohou provést validaci dat, byla libovolně velká a libovolného složení.

5.2.4 Autentizace

Autentizace je pojem, který se používá a často i zneužívá ve velmi širokém smyslu. Sám o sobě má tento pojem trochu jiný význam, než jen vyjadřovat myšlenku, že některé prostředky informační bezpečnosti jsou předem určeny k poskytování záruk, že některé entity jsou těmi entitami, za které se vydávají, nebo že s informacemi nemanipulovaly neautorizované subjekty.

Autentizace patří k nejdůležitějším úkolům informační bezpečnosti. Až do poloviny sedmdesátých let se všeobecně věřilo, že utajení a autentizace jsou pojmy, které mají vnitřní vazbu. [MENEZES, 1997] S objevem hašovacích funkcí a digitálního podpisu začalo být jasné, že utajení a autentizace patří skutečně k samostatným a nezávislým cílům informační bezpečnosti. Napoprvé se nemusí zdát důležité oddělovat oba pojmy, ale existují situace, kdy takové dělení není jen užitečné, ale i nutné.

Vzájemná autentizace mezi dvěma subjekty A a B může mít dvě podoby. Buď spolu subjekty mohou komunikovat v reálném čase, tento případ nazýváme autentizace entity nebo jednodušeji identifikace. Druhou možností je takzvaná autentizace původu dat, která nastává v případě, kdy si subjekty vyměňují zprávy s určitým zpožděním.

Identifikace

Identifikace ujišťuje jeden subjekt o identitě druhého subjektu pomocí získání usvědčujícího důkazu a dále o tom, že druhý subjekt byl v době získání důkazu aktivní. Důkazem bývá nějaká informace, kterou zná pouze dotazovaný. Touto informací může být heslo. Přihlašování do systému pomocí jména a hesla je zcela nejpoužívanějším způsobem identifikace. [JAŠEK, 2006, s. 38]

Dalším možným způsobem identifikace je použití biometrických prostředků. Tyto metody jsou založeny na snímání jedinečných fyzických znaků osoby a typicky se jedná o snímání otisků prstů nebo oční duhovky.

Zajímavý způsob, jak vyřešit identifikaci, nabízí použití hardwarových autentizačních prostředků, jako jsou různé čipové karty či tzv. tokeny.

Autentizace původu dat

Metody autentizace původu dat nebo metody autentizace zpráv ujišťují subjekt, který zprávu přijal, o identitě subjektu, který zprávu vytvořil. Identita je zajištěna získáním důkazu.

Často se subjektu B kromě vlastní zprávy zasílá i další informace, z níž B může určit identitu entity, která zprávu vygenerovala. Pro tento způsob autentizace je typické, že neposkytuje žádné časové garance, nicméně je užitečný v situacích, kdy jeden ze subjektů není při komunikaci aktivní.

5.2.5 Autorizace

Autorizace je definována jako určení toho zda, subjekt, tedy uživatel nebo systém, je důvěryhodný z hlediska jisté činnosti, například čtení daného souboru.

Proces autorizace v informačním systému navazuje na autentizaci, respektive identifikaci. Jakmile je uživatel identifikován, systém stanoví na základě jeho identifikačního čísla (ID) a bezpečnostních informací připojeným k němu, co je uživateli v systému umožněno vykonávat. Určí tak vlastně jeho práva v systému. Například pokud se uživatel pokusí zobrazit citlivá data, systém porovná jeho ID se seznamem, kde jsou uvedena ID těch uživatelů, kteří k citlivým datům mají přístup. Pokud se uživatelovo ID na tomto seznamu nachází, systém mu umožní přístup.

Autorizační mechanismus v informačním systému obvykle spravuje soubor obsahující informace o právech a vlastnostech. Tento soubor je nazýván bezpečnostní profil, autentizační profil nebo seznam uživatelů.

5.2.6 Nepopiratelnost

Služba nepopiratelnosti zahrnuje generování, ověřování a zaznamenávání důkazu a následné vyhledávání a opakované ověřování tohoto důkazu s cílem řešit spory. Cílem nepopiratelnosti je poskytnout důkaz o konkrétní události nebo činnosti.

Nepopiratelnost může být poskytována použitím mechanismů, jako jsou digitální podpis, šifrování, notarizace a mechanismy integrity dat s podporou dalších služeb, jako je například označení času. Pro nepopiratelnost mohou být využívány symetrické i asymetrické kryptografické algoritmy. Služba nepopiratelnosti může použít kombinaci těchto mechanismů a služeb přiměřeně k uspokojení bezpečnostních požadavků dotyčné aplikace.

5.3 Kryptografické kontrolní hodnoty

Kryptografická kontrolní hodnota je informace, která je odvozena na základě provedení kryptografické transformace s datovou jednotkou. Kryptografická kontrolní

hodnota se využívá v různých bezpečnostních mechanismech. Pečetě, digitální podpisy a digitální otisky jsou tři příklady kryptografických kontrolních hodnot.

Pečeť je forma kryptografické kontrolní hodnoty vypočítaná pomocí symetrického kryptografického algoritmu a tajného klíče, sdíleného komunikujícími entitami. Pečetě jsou používány ke zjištění modifikace dat v průběhu jejich přenosu.

Digitální podpis je kryptografická kontrolní hodnota, která chrání před padělaním ze strany příjemce, a je vypočítána pomocí soukromého klíče a asymetrického kryptografického algoritmu. Validace digitálního podpisu vyžaduje stejný kryptografický algoritmus a odpovídající veřejný klíč.

Digitální otisk je charakteristika datové položky, která je pro datovou položku dostatečně typická, takže je výpočetně neproveditelné najít jinou datovou položku se stejným digitálním otiskem. Některé formy kryptografické kontrolní hodnoty (například výsledek aplikace jednosměrné funkce na data) mohou být použity k zajištění digitálního otisku. Digitální otisky mohou být zajištěny prostřednictvím jiných než kryptografických algoritmů. Například kopie datové položky je digitální otisk.

Kryptografická kontrolní hodnota nutně nechrání před opakovaným přenosem jednotlivé datové jednotky. Této ochrany může být dosaženo tak, že se do dat vloží nějaká informace, která může být použita ke zjištění opakovaných přenosů, jako je pořadové číslo nebo označení času, nebo použitím kryptografického řetězení. K zajištění této ochrany musí příjemce chráněné datové jednotky tuto informaci zkontrolovat. [ČSN ISO/IEC 10181-1, 1998]

5.4 Požadavky na kryptografické bezpečnostní mechanismy

Jak vyplývá z předchozích odstavců, bezpečnostní mechanismy jsou nejčastěji řešeny pomocí kryptografie. Důvodem využití kryptografických bezpečnostních mechanismů je jejich síla, tedy to, jak silným útokům jsou odolné. Kryptografické bezpečnostní mechanismy je možné využít v různých oblastech počítačových a telekomunikačních systémů (řízení přístupu, uchovávání dat, datová, hlasová a obrazová komunikace) a v různých prostředích (bankovnictví, státní správa, podnikání). Úroveň bezpečnosti kryptografického modulu musí být zvolena tak, aby zajišťovala dostatečnou ochranu dat v závislosti na bezpečnostních požadavcích, provozním prostředí a poskytovaných službách.

Americký standard FIPS PUB 140-2 [2001] představuje požadavky, které musí splňovat kryptografické bezpečnostní moduly ochraňující oklasifikované (tajné, přísně tajné…) i neoklasifikované informace v informačních systémech. Tyto požadavky zahrnují implementace kryptografických modulů ve formě hardwarových komponent nebo modulů, softwarových programů nebo modulů, firmwarových modulů a možné kombinace vyjmenovaných implementací.

5.5 Normy a standardy

Jako většina lidské činnosti, tak i kryptografie a oblast informační bezpečnosti jsou systematicky popsány soubory norem a standardů. V této kapitole je popsáno prostředí a okolnosti, za jakých jsou normy vytvářeny, a je představeno několik konkrétních příkladů.

5.5.1 Instituce

Normy z oblasti bezpečnosti informačních systémů je možné rozdělit do tří kategorií podle institucí, které je vydávají:

Mezinárodní

ISO - International Organization for Standardization, Mezinárodní organizace pro normalizaci zabývající se tvorbou mezinárodních norem ISO a jiných druhů dokumentů ve všech oblastech normalizace kromě elektrotechniky.

IEC - International Electrotechnical Commission, Mezinárodní elektrotechnická komise připravující a vydávající normy pro všechny elektrické, elektronické a příbuzné technologie.

ITU - International Telecommunication Union, Mezinárodní telekomunikační unie je instituce fungující pod OSN zaměřená na informační a komunikační technologie.

IEEE - Institute of Electrical and Electronics Engineers, Institut inženýrů elektrotechniky a elektroniky je největší odborná asociace zaměřená na rozvoj technologických inovací.

Tyto organizace vyvíjejí i společné normy: ISO/IEC, ISO/ITU.

Americké

ANSI - American National Standards Institute, Americký národní standardizační institut je nezisková organizace, která vytváří průmyslové standardy ve Spojených státech a je členem organizace ISO a IEC.

NIST - National Institute of Standards and Technology, Národní institut standardů a technologií je institut pro tvorbu standardů, který funguje pod ministerstvem obchodu USA. Cílem instituce je podpora inovací a průmyslové konkurenceschopnosti USA zlepšováním vědeckých měření, standardů a technologií s ohledem na ekonomickou bezpečnost a zlepšování kvality života. Zkratkou FIPS (Federal Information Processing Standard) jsou označovány normy vyvinuté NIST, určené pro využití americkými federálními ministerstvy. V současné době jsou běžně využívány i velkými společnostmi, bankami a korporacemi na celém světě.

Evropské a národní

Vedle výše uvedených organizací existují dále normy CEN/CENELEC (European Committee for Electrotechnical Standardization, Evropská komise pro elektrotechnickou standardizaci) s evropskou působností, nebo normy vydávané národními normalizačními úřady, například britská BSI (British Standardisation Institut) s národní působností. V České republice zajišťoval tvorbu a vydávání norem ČSNI (Český normalizační institut), od roku 2009 má toto na starost Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

V 90. letech minulého století začaly být tyto právní normy doplňovány „normami“ vyvíjenými různými konsorcii. Takovéto dokumenty obecně představují dohodu mezi hlavními hráči na trhu. Tyto dokumenty tedy nepředstavují široký konsenzus jako normy ISO, avšak splňují potřeby trhu a jsou schopné pružně reagovat na vývoj produktů a marketingové cykly. [JAŠEK, 2006, str. 65], [DOSEDĚL, 2004, str. 143]

5.5.2 Vývoj registrace kryptografických algoritmů

Snaha o registraci algoritmů začala na konci sedmdesátých let se vznikem algoritmu DES. Ten byl přijat jako federální standard státní správy USA FIPS Pub46 a později byl přijat národní normalizační agenturou USA jako národní norma ANSI (X3.92). Rozšíření tohoto algoritmu vedlo ke snahám normalizovat jej jako mezinárodní normu ISO a tato snaha

vedla téměř k úspěchu, než byl tento proces normalizace z politických důvodů zastaven (stejně tak byl zastaven proces normalizace algoritmu RSA). Bylo ujednáno, že kryptografické algoritmy nebudou registrovány jako ISO normy, ale místo toho bude zaveden proces vytváření mezinárodního registru algoritmů. Tento registr a příslušný proces registrace byl definován normou ISO/IEC 9979 z roku 1991 (2. vydání v roce 1999) s názvem Information technology – Security techniques – Procedures for the registration of cryptographic algorithms. Ve vzniklém registru mohly být zaregistrovány tři druhy algoritmů:

- algoritmus, jehož úplný popis je obsažen v registru
- algoritmus, jehož úplný popis je definován v některém ISO dokumentu, v normě spravované některým členem ISO nebo spolupracující organizací
- algoritmus, který není úplně popsaný

V registru bylo zaregistrováno 24 algoritmů a jejich soupis s odkazy na kopie registračních formulářů je možné najít na webové prezentaci registru (http://www.iso-register.com/). Tato norma byla také přeložena do češtiny a převzata jako česká technická norma s názvem Informační technologie – Bezpečnostní techniky – Postupy pro registraci kryptografických algoritmů.

Norma ISO/IEC 9979 byla však v roce 2006 zrušena a odkazované stránky jsou už zachovávány pouze z historického důvodu. Jedním z důvodů pro zánik této normy byl fakt, že se registr stal redundantní vzhledem k mezinárodní normě ISO/IEC 18033 vydané v roce 2005 s názvem Information technology — Security techniques — Encryption algorithms.

Norma ISO/IEC 18033 je čtyřdílná norma s těmito částmi:

1. **Obecné informace** (ISO/IEC 18033-1:2005, Part 1: General)

   Tato část obecné povahy uvádí definice pojmů, které jsou používané v dalších částech. Je zde představena podstata šifrování a některé hlavní aspekty jeho využití.

2. **Asymetrické šifry** (ISO/IEC 18033-2:2006, Part 2: Asymmetric ciphers)

   Druhá část normy se zabývá asymetrickými šiframi – upřesňuje metody jejich správného použití a popisuje podmínky funkčnosti konkrétních algoritmů, kterými jsou:

   - ECIES-HC; ACE-HC: hybridní kryptosystémy založené na metodě ELGamal;
   - RSA-HC: : hybridní kryptosystémy založené na RSA;

- RSAES: výplňové (padding) schéma používáné s RSA;
- HIME(R): schéma založené na faktorizaci čísla.

3. **Blokové šifry** (ISO/IEC 18033-3:2010, Part 3: Block ciphers)

   V této části normy jsou popsány tyto blokové šifry: TDEA, MISTY1, CAST-128, AES, Camellia, SEED.

4. **Proudové šifry** (ISO/IEC 18033-:2011, Part 4: Stream ciphers)

   Nejnovější část normy popisuje pět generátorů náhodných čísel pro tvorbu klíčů (MUGI, SNOW 2.0, Rabbit, Decim^{v2}, Kcipher-2) a dvě výstupní funkce pro kombinování klíče s otevřeným textem – tedy samotné šifrovací algoritmy (binární doplňková šifra, MULTI-S01).

5.5.3 Subkomise IT bezpečnostních technik

Velké množství důležitých bezpečnostních norem je vydáváno ISO/IEC JTC1 SC27, tedy 27. subkomisí IT Security techniques, která je součástí Joint Technical Committee 1. Tato subkomise vydala za dobu svého působení 125 norem. Zde jsou uvedeny některé významné z nich spolu s krátkým popisem obsahu (kromě již rozebrané ISO/IEC 18033):

ISO/IEC 9798 – Entity authentication – šestidílná norma zabývající se autentizací entit, jednotlivé díly představují protokoly pro autentizaci pomocí symetrické (2. díl) a asymetrické (3. díl) kryptografie, protokoly založené na kontrolních součtech (4. díl) a na nulové znalosti (5. díl) a mechanismy využívající manuální přenos dat (6. díl).

Tato norma byla přeložena do češtiny a vydána jako ČSN ISO/IEC 9798.

ISO/IEC 9796 – Digital signature schemes giving message recovery – trojdílná norma popisující metody založené na RSA a Rabin-Williamsově schématu (1. díl), problému faktorizace celého čísla (2. díl) a problému diskrétního logaritmu (3. díl).

Tato norma byla přeložena do češtiny a vydána jako ČSN ISO/IEC 9796.

ISO/IEC 11770 – Key management – trojdílná norma představuje metody a struktury pro správu klíčů založené na symetrické kryptografii (2. díl) a problému diskrétního logaritmu (3. díl).

Rodina norem ISO/IEC 2700 – normy zabývající se systémem řízení informační bezpečnosti (ISMS- Information security management systems), základními normami z této rodiny jsou:

- ISO 27000 *Overview and vocabulary* - přehled a definice pojmů
- ISO 27001 *Information security management systems -- Requirements* – specifikace a požadavky pro ISMS
- ISO 27002 *Code of practice for information security management* – nahrazuje původní ISO 17799
- ISO 27003 *Information security management system implementation guidance* – pokyny pro implementaci guidance
- ISO 27004 *Information security management – Measurement* – měření a metriky v rámci ISMS
- ISO 27005 *Information security risk management* – obsahuje metodologii nezávislé normy pro řízení rizik v rámci informační bezpečnosti
- ISO 27006 *Requirements for bodies providing audit and certification of information security management systems* – pokyny pro získání akreditace na organizaci poskytující ISMS

6 Hodnotící kritéria pro aplikaci algoritmů

V této kapitole jsou představena hlavní kritéria, podle kterých lze hodnotit efektivitu a bezpečnost jednotlivých algoritmů a na jejichž základě může probíhat výběr při konkrétním nasazení. U každého kritéria jsou vždy uvedeny naměřené hodnoty pro konkrétní algoritmy.

Tyto hodnoty nejsou výsledkem přímého měření provedeného pro tuto práci, ale byly převzaty z dalších studií a materiálů zabývajících se touto problematikou. Cílem této kapitoly je tedy sumarizovat tato již provedená měření a z nich odvodit obecné závěry o vlastnostech daných algoritmů a doporučení pro jejich použití. Jednotlivá měření byla prováděna s různě velkými datovými soubory a na různě výkonných počítačích, proto je důležité porovnávat data vždy jen z jednoho zdroje.

6.1 Čas

Jedním z důležitých hodnotících kritérií efektivity je čas potřebný k zašifrování určitého množství dat. Tento změřený čas je také ukazatelem výpočetní náročnosti algoritmů. Je zřejmé, že měřené časy se liší nejen podle velikosti vstupních dat, ale také podle výkonnosti použitých počítačů. S časem souvisí i další hodnotící kritérium – průchodnost, proto jsou výsledky měření času uvedeny společně s výsledky měření návazné průchodnosti. V tabulce č. 1 můžeme porovnat pouze časy algoritmů Blowfish a AES, jelikož DES a 3DES byly měřeny při šifrování jiných velikostí dat. Oproti tomu výsledky uvedené v tabulkách č. 2 a č. 3 nám dávají možnost jasně porovnat časy šifrování dat různých velikostí a na různě výkonných počítačích.

6.2 Průchodnost

Průchodnost (throughput) můžeme vypočítat jako poměr velikosti otevřeného textu v bytech a času potřebného k jeho zašifrování v sekundách. Jedná se tedy o rychlost šifrování.

V tabulce č. 1 jsou představeny výsledky z šifrování pomocí Crypto++ knihovny v jazyce C++ na počítači s procesorem Pentium 4 2.1 GHz a OS Windows XP.

Algoritmus (velikost klíče v bytech)	Velikost šifrovaných dat (megabyty)	Čas (sekundy)	Průchodnost (MB/s)
Blowfish	256	3.976	64.386
AES (velikost klíče 128)	256	4.196	61.010
AES (velikost klíče 192)	256	4.817	53.145
AES (velikost klíče 256)	256	5.308	48.229
DES	128	5.998	21.340
(3DES)DES-XEX3	128	6.159	20.783
(3DES)DES-EDE3	64	6.499	9.848

Tabulka 1 Porovnání času a průchodnosti symetrických algoritmů (Pentium 4 2.1 GHz) [AL TAMIMI, 2006]

Z tohoto měření jasně vyplývá, že nejlepších výsledků (nejnižší čas a nejvyšší průchodnost) dosahují algoritmy Blowfish a AES.

Následujících dvě tabulky (č. 2 a 3) prezentují výsledky měření, kdy byly algoritmy implementovány pomocí programovacího jazyka Java a byly testovány na dvou počítačích s procesory s dosti odlišným výkonem: Pentium II 266 MHz a Pentium 4 2.4 GHz. Pokusné šifrování bylo prováděno na souborech dat různé velikosti.

Velikost šifrovaných dat (byty)	DES	3DES	AES	Blowfish
20,527	24	72	39	19
36,002	48	123	74	35
45,911	57	158	94	46
59,852	74	202	125	58
69,545	83	243	143	67
137,325	160	461	285	136
158,959	190	543	324	158
166,364	198	569	355	162
191,383	227	655	378	176
232,398	276	799	460	219
Průměrný čas (sekundy)	134	383	228	108
Průchodnost (B/s)	835	292	491	1,036

Tabulka 2 Porovnání času a průchodnosti – různé velikosti šifrovaných dat (Pentium II 266 MHz) [NADEEM, 2005]

Velikost šifrovaných dat (byty)	DES	3DES	AES	Blowfish
20,527	2	7	4	2
36,002	4	13	6	3
45,911	5	17	8	4
59,852	7	23	11	6
69,545	9	26	13	7
137,325	17	51	26	14
158,959	20	60	30	16
166,364	21	62	31	17
191,383	24	72	36	19
232,398	30	87	44	24
Průměrný čas (sekundy)	14	42	21	11
Průchodnost (B/s)	7,988	2,663	5,32	10,167

Tabulka 3 Porovnání času a průchodnosti – různé velikosti šifrovaných dat (Pentium 4 2.4 GHz) [NADEEM, 2005]

Z výsledků měření jasně vyplívá, že algoritmus Blowfish převyšuje ostatní algoritmy, co se týče rychlosti i z ní vyplívající prostupnosti. Nejhůře z tohoto měření dopadl algoritmus 3DES, u kterého je možné si povšimnout jeho třikrát menší prostupnosti než u algoritmu DES způsobené trojím opakováním.

Pokud porovnáme obě tabulky (č. 2 a č. 3), je také patrné, jak výrazně se oproti sobě liší naměřené časy v závislosti na výkonnosti počítačů.

6.3 Lavinový efekt

Takzvaný lavinový efekt (avalanche effect) je vlastnost, která je z bezpečnostních důvodů vyžadována hlavně u blokových šifer a hašovacích funkcí. Jedná se o efekt, kdy při i velice malé změně otevřeného – vstupního textu nebo klíče dojde k velké změně u zašifrovaného textu. Pokud bloková šifra nebo hašovací funkce nevykazuje do značné míry vlastnost lavinového efektu, kryptoanalytik může odvodit vlastnosti otevřeného textu pouze ze znalostí šifrovaných textů.

Ve studii [AGRAWAL, 2010], která porovnává tuto vlastnost, byly jednotlivé algoritmy implementovány pomocí programu Matlab 7.0. Při měření se zjišťovala změna velikosti zašifrovaného textu jak po změně jednoho bitu klíče při zachování vstupního textu, tak po změně jednoho bitu vstupního textu při zachování klíče. Výsledky měření jsou

uvedeny v následující tabulce č. 4, přičemž údaje představují změnu oproti původnímu textu v procentech.

Algoritmus	1 bitová změna klíče	1 bitová změna vstupního textu
DES	30	34
3DES	37	33
AES	64	71
BLOWFISH	37	23

Tabulka 4 Porovnání lavinového efektu [AGRAWAL, 2010]

Z výsledků je jasné, že největší lavinový efekt má algoritmus AES, což pro něj může být bezpečnostní výhodou. Ostatní tři algoritmy mají srovnatelné výsledky.

6.4 Paměť potřebná pro implementaci

Různé šifrovací algoritmy mají různé nároky na paměť potřebnou k jejich implementaci. Tyto nároky na paměť závisí na počtu operací, které je potřeba vykonat v průběhu algoritmu. Je žádoucí, aby vyžadovaná paměť byla co nejmenší. Údaje prezentované v následující tabulce (č. 5) jsou převzaty ze stejné studie [AGRAWAL, 2010], ve které byly algoritmy implementovány za pomocí MATLABu.

Algoritmus	Paměť potřebná pro implementaci (KB)
DES	12.8
3DES	14.8
AES	10.6
BLOWFISH	6.88

Tabulka 5 Porovnání paměti potřebné pro implementaci [AGRAWAL, 2010]

Z měření vyplývá, že algoritmus Blowfish je nejméně náročný na potřebnou paměť k implementaci.

6.5 Délka klíčů

U asymetrických šifrovacích algoritmů závisí bezpečnost na délce klíčů, délce zvoleného modula a na velikosti grupy, nad kterou je kryptosystém vytvořen. Čím větší klíč je použit, tím menší je pravděpodobnost vypočítání soukromého klíče z klíče veřejného. Některé systémy jako RSA již neposkytují přijatelné zabezpečení s délkou soukromého klíče 512 bitů, proto se zvýšení bezpečnosti projeví použitím většího klíče. Z toho důvodu je rychlost šifrování celkem nízká na rozdíl od jiných systémů. U systému RSA délky klíčů již sahají do velmi vysokých čísel a samotný systém požaduje velkou paměť a vysoký výpočetní výkon. Proto se hledají jiné alternativy, které poskytují tutéž bezpečnost s menšími klíči.

U symetrických šifer se v současné době doporučuje používat klíče o minimální délce 80 bitů s tím, že v praxi se pracuje s délkou 128 bitů a více. AES podporuje tři délky klíče: 128, 192 a 256 bitů. Tyto délky zaručují, že nebude možné využít útoku hrubou silou, neboť zásadní praktické problémy s konstrukcí a cenou luštícího stroje začínají už u 80 bitů. Klíče o 128 bitech a více pak zaručují utajení minimálně na několik desítek let dopředu (jak popisují následující doporučení).

Délka klíče je důležité bezpečností hledisko, ovšem, jak už bylo zmíněno, není jediné. Velmi záleží na konkrétním algoritmu, který musí zaručit, že metoda zkoušení všech možných klíčů hrubou silou je skutečně jediným možným způsobem útoku. Z praxe je známa řada případů, kde díky slabému algoritmu nebyly ani klíče délky 128 bitů nic platné.

Pro úvodní porovnání velikostí klíčů jsou zde uvedeny závěry studie, která porovnává bezpečnost algoritmu RSA a Eliptických křivek s bezpečností symetrických šifer. Respektive uvádí velikosti klíčů, které jsou potřeba pro dosažení stejné bezpečnostní hodnoty pro jednotlivé algoritmy. Porovnané hodnoty uvedené v tabulce č. 6 jsou velikosti v bitech, přičemž u Eliptických křivek se jedná o velikost tělesa *F* a u RSA o velikost čísla *n*.

Symetrická šifra	**Eliptické křivky**	**RSA**
80	163	1024
128	283	3072
192	409	7680
256	571	15360

Tabulka 6 Porovnání velikosti klíčů [LASOŇ, 2005]

6.6 Doporučené délky klíčů

Použití delšího klíče, než je zapotřebí, může ovlivnit chod celého systému (trvá déle, než se delší klíč vygeneruje, a následující práce s více daty také zabere delší čas). Na druhou stranu při použití kratšího klíče nemusí být zaručena přiměřená bezpečnost. Proto existují různé metodologie, studie a zprávy národních, mezinárodních a nadnárodních organizací, které se zabývají bezpečností kryptografických algoritmů a uvádějí doporučené délky klíčů pro bezpečné použití. Jedněmi z takovýchto institucí jsou Ecrypt II a NIST.

6.6.1 Ecrypt II

Ecrypt II (European Network of Excellence for Cryptology II) je síť propojených vědeckých pracovišť založená v rámci programu Seventh Framework Programme. Jednotlivé výzkumné aktivity jsou prováděny ve třech virtuálních laboratořích. V roce 2012 vydala tato instituce zprávu [*ECRYPT II,* 2012], kde uvádí doporučené délky klíčů pro jednotlivé druhy algoritmů.

V tomto doporučení jsou zavedeny bezpečnostní úrovně, v jejichž popisu jsou zmiňovány druhy útočníků, proti kterým jsou jednotlivé úrovně bezpečné. Jedná se o:

- hacker – nulový rozpočet, pracuje s PC
- malá organizace – rozpočet do 10000$, pracuje s FPGA (Field Programmable Gate Array – Programovatelné hradlové pole umožňující větší výpočetní možnosti)
- střední organizace – rozpočet do 300000$, pracuje s FPGA nebo s ASIC (Application-specific integrated circuit – Zákaznický integrovaný obvod je tvořen pro specifické výpočetní využití)
- zpravodajská služba – 300000000$ rozpočet, pracuje s ASIC

Úroveň	Ochrana	Symetrická kryptografie	Asymetrická kryptografie	Diskrétní logaritmus		Eliptické křivky	Hash
				Klíč	Grupa		
1	Útoky v reálném čase individuálními hackery, velikost přijatelná pouze pro autentifikační kód	32	-	-	-	-	-
2	Krátkodobá ochrana proti malým organizacím, neměla by se využívat pro ověření důvěrnosti	64	816	128	816	128	128
3	Krátkodobá ochrana proti středním organizacím, střednědobá ochrana proti malým organizacím	72	1008	144	1008	144	144
4	Krátkodobá ochrana proti zpravodajským službám, dlouhodobá ochrana proti malým organizacím, nejmenší úroveň vhodná pro všeobecné použití, 4 letá ochrana	80	1248	160	1248	160	160
5	Standardní úroveň ochrany - 10 let	96	1776	192	1776	192	192
6	Střednědobá ochrana - 20 let	112	2432	224	2432	224	224
7	Dlouhodobá ochrana – 30 let	128	3248	256	3248	256	256
8	„Předvídatelná budoucnost“ Dobrá ochrana proti kvantovým počítačům	256	15424	512	15424	512	512

Tabulka 7 Doporučené délky klíčů – ECRYPT II (uvedené hodnoty jsou v bitech) [ECRYPT II, 2012]

6.6.2 NIST

Další doporučení ohledně délky klíčů bylo také v roce 2012 vydáno již zmiňovaným americkým normalizačním institutem. Toto doporučení je určeno pro použití vládními úřady a jeho závěry jsou představeny v tabulce č. 8.

Symetrická kryptografie	Asymetrická kryptografie	Diskrétní logaritmus Klíč	Grupa	Eliptické křivky	Hash
80	1024	160	1024	160	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
112	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512
128	3072	256	3072	256	SHA-256 SHA-384 SHA-512
192	7680	384	7680	384	SHA-384 SHA-512
256	15360	512	15360	512	SHA-512

Tabulka 8 Doporučené délky klíčů – NIST (uvedené hodnoty jsou v bitech)

Míru bezpečnosti porovnávaných délek klíčů prezentuje tabulka č. 9. Doporučení v této tabulce se týkají možnosti využití dané velikosti klíčů do budoucnosti. První sloupec tabulky prezentuje bezpečnostní úroveň algoritmu pomocí délky symetrického klíče a je rozdělen na dvě části: první udává samotnou délku v bitech, druhá upřesňuje použití algoritmu, tedy to, jestli se jedná o jeho aplikaci za účelem zašifrování dat, nebo o proces zpracování zašifrovaných dat – dešifrování. V druhém až čtvrtém sloupci je uvedeno, pro jaké časové období je bezpečnostní úroveň přijatelná. Pro hodnocení přijatelnosti jsou zde použity tyto termíny:

- nepřijatelné - algoritmus o dané bezpečnostní úrovni by neměl být použit
- nedoporučeno - možné použití, při kterém však existuje riziko prolomení algoritmu
- „*legacy*“ využití - použití algoritmu pro přemístění nebo ověření citlivých informací, které byly zašifrovaný stejnou ochranou
- doporučeno - není známo možné nebezpečí

Délka symetrického klíče		2011-2013	2014-2030	2031 a dále
80	Šifrování	Nedoporučeno	Nepřijatelné	
	Dešifrování	„Legacy“ využití		
112	Šifrování	Doporučeno	Doporučeno	Nepřijatelné
	Dešifrování			„Legacy“ využití
128	Šifrování/Dešifrování	Doporučeno	Doporučeno	Doporučeno
192		Doporučeno	Doporučeno	Doporučeno
256		Doporučeno	Doporučeno	Doporučeno

Tabulka 9 Míra bezpečnosti [BARKER, 2012]

Při porovnání doporučení udávaných ECRYPT II a NIST jasně vyplývá, že NIST má přísnější kritéria. Jedná se především o bezpečnostní úroveň určenou symetrickým klíčem o délce 80 bitů, která je již brána jako nedoporučená, zatímco ECRYPT II ji stále udává jako použitelnou ochranu – sice na nejnižší úrovni.

Metodika NIST se ani nezabývá nižšími velikostmi klíčů, než je 80 bitů, a jak je patrné z tabulky č. 7, bezpečností úrovně 1-3 (tedy velikosti menší než 80 bitů) je možné použít v ojedinělých případech: ke krátkodobému použití, kdy například není k dispozici dostatečný výpočetní výkon a z hlediska hladkého chodu systému se vyplatí nasadit tuto nižší úroveň.

Pokud porovnáme jednotlivé bezpečností úrovně definované velikostí klíče pro symetrickou kryptografii, ukáže se, že doporučení vydané institutem ECRYPT II jsou přísnější, respektive že pro dosažení stejné bezpečnosti je zapotřebí větších klíčů než pro asymetrickou kryptografii.

6.7 Datum vytvoření

Zajímavým ukazatelem či hodnotícím kritériem algoritmu je jeho datum vytvoření. V tabulce č. 10 jsou chronologicky seřazeny všechny algoritmy popsané v této práci. Jak je vidět Vernamova šifra je jednoznačně nejstarší a to o několik desítek let, přesto je stále ve formě one-time pad využívána a je prokazatelně neprolomitelná při správném použití. Její nasazení v informačních systémech je však minimální kvůli vysoké výpočetní náročnosti – klíč je stejně dlouhý jako zpráva.

Velký rozmach moderní kryptografie je zřetelný ve druhé polovině 70. let. Obecně jsou starší kryptosystémy stále nasazovány více než mladší, přestože mají horší parametry (čas, náročnost, potřeba delších hesel). Je to především z toho důvodu, že znalosti o starších

algoritmech jsou větší, ví se, že bylo vykonáno více pokusů o jejich prolomení, které systémy přečkaly (neplatí pro DES).

Název algoritmu	symetrický/ asymetrický	Rok vzniku
Vernamova šifra	sym.	1917
Diffie-Hellman	asym.	1976
DES	sym.	1977
RSA	asym.	1977
McEliece	asym.	1978
ElGamal	asym.	1984
Eliptické křivky	asym.	1985
Blowfish	sym.	1993
3DES	sym.	1999
AES	sym.	2002

Tabulka 10 Porovnání dle data vytvoření

6.8 Zhodnocení

Představená hodnotící kritéria algoritmů je možné rozdělit podle jejich vlastností do dvou skupin: implementační a bezpečnostní. Mezi implementační by patřily čas, průchodnost a paměť potřebná pro implementaci a do skupiny bezpečnostních pak lavinový efekt a délky klíčů. Při výběru algoritmu pro konkrétní nasazení je nutné brát ohledy na všechna kritéria, ovšem někdy musí dojít ke kompromisu a to ze strany rychlosti (potřeba silného zabezpečení) nebo bezpečnosti (mobilní zařízení se zabezpečením pro krátký časový úsek).

Implementační kritéria má z porovnávaných algoritmů nejlepší Blowfish, následovaný algoritmem AES. Největší lavinový efekt vykazuje algoritmus AES. Pokud porovnáme délku klíčů potřebnou k zajištění stejné bezpečnostní úrovně, nejhůře jsou na tom algoritmy asymetrické kryptografie (více jak deseti násobně větší klíče než u symetrické kryptografie). Lépe jsou na tom algoritmy založené na eliptických křivkách (přibližně dvojnásobná délka oproti symetrickým), které mají do budoucna předpoklady k širokému využití.

7 Závěr

Diplomová práce popisuje a porovnává nejrozšířenější algoritmy využívané v informačních systémech. Dále se práce zabývá konkrétními okruhy využití kryptografie v informačních systémech. V práci jsou také rozebrána témata informační bezpečnosti informačních systémů z hlediska kryptografie a normalizace a standardizace šifrovacích algoritmů a informační bezpečnosti.

Po úvodním seznámení se s tématem jsou definovány základní termíny používané v oblasti kryptologie. Je představen klíčový pojem šifrovací algoritmus, dále pak často se vyskytující pojmy otevřený a šifrovaný text, odesílatel, příjemce a kanál. Také je vymezen pojem kódování a jeho rozdíl oproti šifrování.

Dalším, spíše stále úvodním tématem, jsou útoky, které mohou být na kryptosystémy provedeny. Základním typem útoku je útok hrubou silou, dále pak útoky ze znalostí textů a také skupina útoků postranním kanálem.

Šifrovací algoritmy se dělí na dvě základní skupiny: symetrické a asymetrické. Jednotlivé skupiny šifer tvoří téma stěžejních popisných kapitol, kdy jsou vždy nejdříve uvedeny základní vlastnosti a poté představeny konkrétní používané algoritmy.

Symetrické šifry se dále dělí na proudové a blokové. Kromě používaných algoritmů jsou v této kapitole krátce představeny základní symetrické šifry (Césarova, Vigènerova šifra), které sloužily většinou po velice dlouhou dobu, avšak dnes je již známa jejich prolomitelnost. Popsanými algoritmy, které jsou široce rozšířeny a stále používány, jsou: Vernamova šifra, DES, 3DES, AES a Blowfish. Algoritmus DES a 3DES je díky menší bezpečnosti nahrazován algoritmem AES, který představuje nejrozšířenější algoritmus symetrické kryptografie a to především díky tomu, že je americkým kryptografickým standardem. Algoritmus Blowfish je nepatentovaný, velmi rychlý a jednoduchý pro implementaci.

Asymetrická kryptografie je založená na jednosměrných funkcích, jakými jsou problém faktorizace čísla, problém výpočtu diskrétního logaritmu, problém mřížky nebo problém batohu. Kromě samotného zašifrování textu se asymetrická kryptografie používá k zajištění hašovací funkce a elektronickému podpisu. Používanými algoritmy, které představuje tato práce, jsou: protokol Diffie-Hellman pro výměnu klíčů, RSA, ElGamal, McEliece a systémy založené na eliptických křivkách.

Všechny popisované algoritmy mohou sloužit pro zajištění základních bezpečnostních mechanismů, tedy důvěrnosti, dostupnosti, integrity, autentizace, autorizace a nepopiratelnosti. Tyto bezpečnostní mechanismy jsou nejčastěji řešeny právě pomocí kryptografie a to především díky možnosti zajištění vysoké odolnosti proti útokům. Kryptografické bezpečnostní mechanismy je možné využít v různých oblastech počítačových a telekomunikačních systémů (řízení přístupu, uchovávání dat, datová, hlasová a obrazová komunikace) a v různých prostředích (bankovnictví, státní správa, podnikání).

Součástí kapitoly o informační bezpečnosti je také část podávající přehled norem a standardů, jež se zabývají touto problematikou. Spíš než o výčet všech existujících norem šlo o to uvést všechny hlavní instituce, které normy vytvářejí a vydávají. Nejvíce mezinárodních norem zabývajících se kryptografií a informační bezpečnostní produkuje Subkomise IT bezpečnostních technik, která spadá pod Mezinárodní elektrotechnickou komisi IEC.

Stěžejní kapitola práce představuje různá kritéria, na jejichž základě lze šifrovací algoritmy hodnotit. Tato kapitola sumarizuje výsledky měření a hodnocení několika studií a vědeckých prací a pomocí nich jsou porovnávány jednotlivé algoritmy. Hodnotící kritéria lze rozdělit na dvě skupiny: implementační (čas, průchodnost a paměť potřebná pro implementaci) a bezpečnostní (lavinový efekt a délky klíčů).

Z provedených měření vyplývá, že nejlepší implementační kritéria z porovnávaných algoritmů vykazuje Blowfish, následovaný algoritmem AES. Naproti tomu má ovšem AES největší lavinový efekt. Pokud porovnáme délku klíčů potřebnou k zajištění stejné bezpečnostní úrovně, nejhůře jsou na tom algoritmy asymetrické kryptografie (více než desetinásobně větší klíče oproti klíčům užívaným u symetrické kryptografie). Lépe jsou na tom algoritmy založené na eliptických křivkách (přibližně dvojnásobná délka oproti symetrickým). Ty mají do budoucna předpoklady k širokému využití.

Seznam použité literatury

AGRAWAL, Himani a Monisha SHARMA. Implementation and analysis of various symmetric cryptosystems. *Indian Journal of Science and Technology*. 2010, roč. 3, č. 12. Dostupné z: http://www.indjst.org/index.php/indjst/article/view/29854

AL TAMIMI, Abdel-Karim. *Performance Analysis of Data Encryption Algorithms*. 2006. Dostupné z: http://www.cse.wustl.edu/~jain/cse567-06/index.html

BARKER, Elaine et al. *Recommendation for Key Management: Part 1: General*. Gaithersburg: National Institute of Standards and Technology, 2012. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

ČSN ISO/IEC 10181-1. *Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů: Přehled*. Praha: Český normalizační institut, 1998.

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004. ix, 190 s. ISBN 80-251-0106-1.

ECRYPT II Yearly Report on Algorithms and Keysizes: 2011-2012. 2012. Dostupné z: http://www.ecrypt.eu.org/documents/D.SPA.20.pdf

FIPS PUB 140-2. *Security requirements for cryptographic modules*. Gaithersburg: National Institute of Standards and Technology, 2001. Dostupné z: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS PUB 197. *ADVANCED ENCRYPTION STANDARD (AES)*. National Institute of Standards and Technology, 2001. Dostupné z: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS PUB 46-3. *DATA ENCRYPTION STANDARD (DES) CATEGORY:*. National Institute of Standards and Technology, 1999. Dostupné z: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

Frequently Asked Questions (FAQ) About the Electronic Frontier Foundation's "DES Cracker" Machine. ELECTRONIC FRONTIER FOUNDATION. [online]. [cit. 2013-07-02]. Dostupné z: http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html

HANÁČEK, Petr; STAUDEK, Jan. *Bezpečnost informačních systémů : Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha : Úřad pro státní informační systém, 2000. 128 s. ISBN 80-235-5400-3.

JAŠEK, Roman. *Informační a datová bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 140 s. ISBN 80-7318-456-7.

JIROUŠEK, Radim et al. *Principy digitální komunikace*. Vyd. 1. Voznice: Leda, 2006. x, 309 s. ISBN 80-7335-084-X.

KLÍMA, Vlastimil. *Základy moderní kryptologie: Symetrická kryptografie I.* 2005. Dostupné z: http://crypto-world.info/klima/mffuk/Symetricka_kryptografie_I_2006.pdf

KLÍMA, Vlastimil; ROSA, Tomáš. Kryptologie pro praxi – Protokol D-H. *Sdělovací technika*, 5/2004, str. 16 Dostupné z: http://crypto-world.info/klima/2004/st_2004_05_16_16.pdf

KLIMEŠ, Cyril. *Kryptografie: Kurz Základy kryptografie pro učitele*. Dostupné z: http://prf-czv.osu.cz/nabidka/seminar/data/Kryptografie.pdf

LASOŇ, Martin. *Porovnání bezpecnosti kryptosystému RSA a Eliptických krivek*. 2005. Dostupné z: http://homel.vsb.cz/~las03/ta/rsa-ecc.pdf

LEHTINEN, Rick, RUSSELL, Deborah a GANGEMI, G. T. Computer security basics. 2nd ed. Sebastopol, CA: O'Reilly, ©2006. xii, 296 s. ISBN 0-596-00669-1.

LULEA UNIVERSTITY OF TECHNOLOGY. *Encryption* [online]. [cit. 2013-07-02]. Dostupné z: http://www.sm.luth.se/csee/courses/smd/102/lek3/lek3.html

MENEZES, Alfred, VAN OORSCHOT, Paul C. a VANSTONE, Scott A. Handbook of applied cryptography. Rev. repr. with updates. Boca Raton, Fla.: CRC Press, ©1997. [26], 780 s. Discrete mathematics and its applications. ISBN 0-8493-8523-7.

NADEEM, A. A Performance Comparison of Data Encryption Algorithms. In: *Information and Communication Technologies: First International Conference on*. 2005. vyd., 84 - 89. ISBN 0-7803-9421-6. DOI: 10.1109/ICICT.2005.1598556.

OCHODKOVÁ, Eliška. Přínos teorie eliptických křivek k řešení moderních kryptografických systému. Ostrava, 2003. Dostupné z: http://www.cs.vsb.cz/arg/workshop/files/ecc_eli.pdf. VŠB - Technická Univerzita

PFLEEGER, Charles P. a PFLEEGER, Shari Lawrence. Security in computing. 4th ed. Upper Saddle River, NJ: Prentice Hall, ©2007. xxix, 845 s. ISBN 0-13-239077-9.

PIPER, F. C.; MURPHY, Sean. *Kryptografie*. 1. vyd. v českém jazyce. Praha: Dokořán, 2006. 157 s. Průvodce pro každého; sv. 3. ISBN 80-7363-074-5.

POŽÁR, Josef a kol. Základy teorie informační bezpečnosti. Vyd. 1. Praha: Vydavatelství PA ČR, 2007. 219 s. ISBN 978-80-7251-250-8.

POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. Vysokoškolské učebnice. ISBN 80-86898-38-5.

PŘIBYL, Jiří. *Informační bezpečnost a utajování zpráv*. 1. vyd. Praha: České vysoké učení technické v Praze, 2004. ISBN 80-01-02863-1.

QUISQUATER, Jean-Jacques. *Side channel attacks: State of the art*. 2002. Dostupné z: http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf

SVETLIK, M. Informační bezpečnost: část 1 – 4, Softwarové noviny, 2002, č. 2-5.

Šifrování. [online]. [cit. 2013-07-02]. Dostupné z: http://foxprv.ic.cz/algoritmy.html

TRUSCHKA, Jakub. Asymetrická kryptografie v praxi. *IT Systems*. 2009. ISSN 1802-615X. Dostupné z: http://www.systemonline.cz/it-security/asymetricka-kryptografie-v-praxi.htm

Seznam obrázků

Seznam tabulek

Seznam zkratek

3DES – Triple Data Encryption Algorithm

ACE-HC – Advanced Cryptographic Engine - Hybrid Cryptosystem

AES – Advanced Encryption Standard

AK – asymetrická kryptografie

ANSI – American National Standard Institute

ANSI – American National Standards Institute

ASIC – Application-specific integrated circuit

BSI – British Standardisation Institut

CA – certification authority

CAST-128 - Carlisle Adams Stafford Tavares Algorithm

CEN/CENELEC – European Committee for Electrotechnical Standardization

CRL – certificate revocation list

ČSN – Česká státní norma

ČSNI – Český normalizační institut

DEA – Data Encryption Algorithm

DES – Data Encryption Standard

DSA – Digital Signature Algorithm

ECIES-HC – Elliptic Curve Integrated Encryption Scheme - Hybrid Cryptosystem

Ecrypt II – European Network of Excellence for Cryptology II

EFF – Electronic Frontier Foundation

FIPS – Federal Information Processing Standard

FPGA – Field Programmable Gate Array

GPG, GnuPG – GNU Privacy Guard

HF – hašovací funkce

ID – identifikátor (identifikační číslo)

IEC – International Electrotechnical Commission

IEEE – Institute of Electrical and Electronics Engineers

ISMS – Information security management systems

ISO – International Organization for Standardization

ITU – International Telecommunication Union

MAC – Message Authenticity Code

MD5 – Message-Digest Algorithm

MDC – Modification Detection Code

MISTY1 – Mitsubishi Improved Security Technology 1

NIST – National Institute of Standards and Technology

NIST – National Institute of Standards and Technology

NSS – Network Security Services

OCSP – Online Certificate Staus Protocol

OpenSSL – Open Secure Sockets Layer

OS – operační systém

PGP – Pretty Good Privacy

PKI – public key infrastructure

RSA – Rivest, Shamir, Adleman Algorithm

RSAES – Rivest, Shamir, Adleman Encryption Scheme

RSA-HC – Rivest, Shamir, Adleman - Hybrid Cryptosystem

SHA – Secure Hash Algorithm

SHS – Secure Hash Standard

SK – symetrická kryptografie

TDEA – Triple Data Encryption Algorithm

XSL – eXtended Sparse Linearization