Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví

Studijní obor: informační studia a knihovnictví

Bakalářská práce

Jindřich Kinský

Kódování jako ochrana přenášených informací

Cryptology as a method of data protection

Praha 2010

Vedoucí práce: Doc. PhDr. Vladimír Smetáček, CSc.

Oponent bakalářské práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

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

V Praze, dne 20. května 2010

……..

podpis studenta

Identifikační záznam:

KINSKÝ, Jindřich. *Kódování jako ochrana přenášených informací = Cryptology as a method of data protection*. Praha, 2010-05-20. 56 s., 6 s. příl. Bakalářská práce (Bc.). Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí bakalářské práce Vladimír Smetáček.

Abstrakt

Cílem práce je uvedení do problematiky kryptologie jako metody ochrany informací v procesech jejich ukládání a komunikace. Práce se zabývá popisem konkrétních metod a obecných principů kryptografie a kryptoanalýzy a nástinem situace v elektronické komunikaci. Důraz je kladen na popis slabin daných šifrovacích algoritmů, charakteristiky jejich funkce a oblasti použití. V práci jsou obsaženy skupiny algoritmů: substituční a transpoziční šifry, symetrické a asymetrické algoritmy, kryptografické hashovací funkce. Samostatnou kapitolu tvoří kryptoanalýza s charakteristikou základních druhů kryptoanalytických útoků.

[Autorský abstrakt]

Abstract

Aim of this work is to introduce into the field of cryptology as a method of information security during the data storage and communication. Particular techniques are described as well as general principles of cryptography and cryptanalysis and outline of actual situation in electronic communication. Especially weaknesses, field of application and characteristics of each cryptographic algorithm are described. There are included several groups of algorithms: substitutional and transpositional ciphers, symmetric and asymmetric algorithms, cryptographic hash functions. Cryptanalysis is considered as a separate chapter with characteristic of main types of cryptanalitical attacks.

[Author's abstract]

Klíčová slova (česky):

informační komunikace, informační technologie, internet, počítačová věda, telekomunikace, www, zpracování informací, kryptologie

Klíčová slova (anglicky):

information communication, information technology, internet, computer science, telecommunication, www, data processing, cryptology

Obsah

Předmluva

Tématem bakalářské práce je Kódování jako ochrana přenášených informací. Toto téma jsem si vybral vzhledem k tomu, že kryptografie je nedílnou součástí moderní komunikace v počítačových sítích. Lze si těžko představit jakoukoliv komunikaci informací, byť i sebemenší hodnoty, prostředky elektronické komunikace bez toho, aby tyto informace procházely od odesílatele k příjemci v nešifrované podobě. To platí nejen o komunikaci dvou známých za účelem zábavy, komunikaci členů pracovního týmu o oblastech jejich činnosti, ale zejména v oblastech čistě komerčního charakteru jako je internetové bankovnictví, realizace obchodních transakcí a dalších. K výběru tématu mě motivovalo zejména moje dlouhodobé zaměření na oblast elektronické komunikace, World Wide Web a počítačové sítě. Tento zájem není jen na úrovni volnočasových aktivit, ale poznatky využívám i při výdělečné činnosti. Krom toho zastávám názor, že šifrování je klíčové při práci informačních specialistů v prostředí moderních technologií, ačkoliv si to mnohdy ani neuvědomujeme, neboť procedury spjaté s kryptografií probíhají často na pozadí naší činnosti, skrytě. Toto tvrzení lze snadno logicky podložit – pracuje-li informační specialista s hodnotnými informacemi (ne-li přímo s takovými, jejichž cena se dá snadno vyčíslit), musí fungovat takové metody, které zajistí, že nikdo nepovolaný se k daným informacím nedostane a tudíž se neoprávněně neobohatí nebo někoho jinak nepoškodí. Oproti předběžné osnově, která byla obsažena v zadání bakalářské práce, jsem po hlubší rozvaze nahradil první kapitolu kapitolou druhou. Přesněji došlo oproti zadání a předběžné osnově k nahrazení kapitoly „Úvod“ kapitolou „Nastínění aktuální situace v elektronické komunikaci.

Práce si klade za cíl seznámit čtenáře s druhy kryptografických metod, příklady těchto metod a principy jejich funkce, způsoby, jakými se tato bezpečnostní opatření dají překonat a oblastmi, ve kterých se kryptografie využívá.

Práci jsem zpracoval na základě informací v českém a anglickém jazyce. Vycházím převážně z tištěných monografií a elektronických online dokumentů. Nezanedbatelným podkladem se ukázaly i zdroje encyklopedické povahy, protože pomáhají badatelům a studentům nematematických oborů vybudovat základy pro další informační přípravu. Účelné se ukázalo i využívání obrazových zdrojů, které usnadní pochopení složitějších matematických funkcí a kryptografických algoritmů. Částečně jsem využil svou rešerši z roku 2009 vypracovanou na předmět Bibliografické rešeršní služby. Do nejvyšší

možné míry se snažím vyhnout historickým exkurzům vzhledem k tomu, že historie šifrování byla tématem pro jinou bakalářskou práci, zpracovanou jedním z mých kolegů.

Bakalářská práce má tři kapitoly, každá z nich krom závěru je dále členěna do podkapitol. První kapitola poskytuje obecná východiska a základy pro pochopení problematiky kryptologie. Též si klade za cíl zdůvodnit nepostradatelnost kryptografie pro moderní řešení komunikace ve společnosti. Druhá kapitola se zabývá popisem jednotlivých druhů šifrování a vyžaduje hlubší členění v zájmu logické struktury, neboť pro každý z druhů moderních kryptografických metod uvádí i příklady konkrétních šifer a jejich zevrubný popis. Poslední kapitola je závěr práce a slouží jako nastínění dalších možností a oblastí studia daného tématu a objasnění limitace, která plyne z komplexní povahy a odborné náročnosti tématu.

Práce má 57 stran, z toho 5 stran příloh odkazovaných v textu. Informační zdroje cituji dle norem ISO 690 a ISO 690-2. Zvolil jsem způsob citování podle prvního údaje záznamu (Harvardský systém), data vydání a čísla strany, tam, kde je to relevantní. Citace uvádím v hranatých závorkách a velká písmena používám ve shodě se seznamem použité literatury. Seznam bibliografických záznamů je uspořádán abecedně podle prvního údaje záznamu a opatřený odrážkami pro větší přehlednost.

Děkuji vedoucímu práce Doc. PhDr. Vladimíru Smetáčkovi, CSc. nejen za varování před obtížnosti tématu, které jsem v době zadání práce ještě nedokázal plně docenit, ale hlavně za to, že mi ukázal směr, jakým se ubírat a nastínil související problémy a metodiku zpracování práce.

1. Současný stav komunikace informací

1.1 Nastínění situace v elektronické komunikaci

Od vzniku pojmu Internet roku 1987 do současnosti zaznamenala komunikace prostřednictvím počítačových sítí úžasného rozvoje, zatímco ostatní formy telekomunikace se nejvíce rozvíjely spíše v minulosti nebo směřují k podpoře internetové komunikace.
Není ani divu, tak například telegrafie má svoje kořeny na přelomu 17. a 18. století a přestože ještě v osmdesátých letech využívalo jen u nás dálnopis (telex) tisíce firem, 1. července 2008 byl u nás provoz dálnopisné sítě ukončen a posílání telegramů se začalo převádět na jiné technologie [Dálnopis, 1.7.2008]. Tato tendence se stejně tak projevuje i v zahraničí – z evropských států například v Dánsku a Irsku (rušení služby v 80. letech 20. století), Francii a Rakousku (od začátku 21. století) [Telegramy, 30.3.2010]. Je třeba si však uvědomit, že právě telegrafie stála u zrodu kryptografie tak jak ji známe dnes [POP, 2006, s. 7].
Rozvoj a využívání telefonie ve 21. století se naproti tomu zaměřuje spíše na mobilní telefonii a přechod od prostého přenosu hlasu k přenosu dat a je aktuální otázkou a to i co se týče pevné telefonní sítě. Obecně pak telefonie směřuje k propojení výpočetní a komunikační techniky [NAVRÁTIL, 2000].

Lze předpokládat, že kvůli vyššímu počtu uživatelů Internetu a nárůstu souvisejících ukazatelů (viz Příloha č. 1 – Statistiky OECD), došlo během posledních deseti let k nárůstu objemu přenesených dat. Zároveň tento rozvoj způsobil, že je elektronická komunikace postupně využívána k dalším účelům tržního charakteru. Jedná se mimo jiné o elektronické obchodování několika druhů: B2C (Business to Consumer, obchod mezi společnostmi a koncovými zákazníky prostřednictvím elektronických obchodů - e-shopů), C2C (Consumer to Consumer, obchod mezi koncovými zákazníky, ve kterém často figuruje třetí strana – společnost – v roli prostředníka), v poslední době stále více oblíbený Forex (Foreign Exchange – spekulativní směna cizích měn za účelem výdělku), Internetové bankovnictví (metoda přímého bankovnictví, při které klient komunikuje s bankou přes webové rozhraní), ale i o nevýdělečné aktivity jako je například E-Government (transformaci komunikace občana a vlády pomocí informačních a komunikačních technologií) či komunikace prostřednictvím programů třetích stran (nejoblíbenější je v poslední době tzv. Instant Messaging – komunikace mezi uživateli v reálném čase). Nesmíme také opomenout důležitý fakt, že interakce uživatele s počítačem může přinášet cenné marketingové informace.

Závěrem bych jen dodal, že výše uvedené skutečnosti by měly nastínit reálnou hodnotu informací, které se v poslední době přenáší ve stále větších objemech. Nutnost chránit tato data s tím přímo souvisí.

1.2 Technologické aspekty komunikace

Komunikace mezi jednotlivými počítači v síti (nejen v síti Internet) se uskutečňuje pomocí rodiny protokolů TCP/IP (Transmission Control Protocol a Internet Protocol) metodou přepojování paketů.

TCP a IP byly první dva standarty v této rodině protokolů, ovšem nejsou jediné z této sady protokolů. Namátkou jmenujme ještě například ARP (Address Resolution Protocol) a UDP (User Datagram Protocol). Přepojování paketů je technologie, při které se data posílají po částech, ty jsou přijímány samostatně. Přepravu zajišťuje protokol IP a sestavování celé zprávy z paketů protokol TCP (u příjemce).

Síťová komunikace jako taková se dělí na čtyři vrstvy – aplikační, transportní, síťová a vrstva síťového rozhraní. Při komunikaci dvou strojů v síti pak data prochází skrze tyto vrstvy (viz Příloha č. 2 – Architektura TCP/IP).

Nejnižší vrstva je vrstva síťového rozhraní, která zajišťuje přístup k přenosovému médiu, běžně to v dnešní době vzhledem k přijatelným nákladům a odpovídající kapacitě [ETHERNET, 2009] bývá tzv. Fast Ethernet o rychlosti 10 nebo 100 Mbit/s (megabitů za sekundu) propojený do síťové karty počítače kabeláží – koaxiálním kabelem, krouceným párem (neboli kroucenou dvoulinkou) či optickým kabelem pro přenosy na velké vzdálenosti.

Síťová vrstva zajišťuje přenos paketů od původce k cílovému hostiteli a plní tři základní funkce. U odchozích paketů zvolí další bránu (gateway) a přenese pakety do vrstvy síťového rozhraní této brány. V případě příchozích paketů je síťová vrstva zachytí a nechá je projít do transportní vrstvy přes vhodné protokoly. Poslední funkce je zachycování chyb. Nutno však poznamenat, že síťová vrstva jako taková není odpovědná za spolehlivost přenosu, což je důležitý princip, kterým se liší Internet od raného ARPANETU (Advanced Research Projects Agency Network, první světová síť na výměnu paketů).

Podstatným rozšířením protokolu IP z hlediska bezpečnosti je rodina protokolů IPsec. Ta umožňuje jednak autentifikaci (ověření původu dat, odesílatele), ale také samotné šifrování přenášených informací předem domluveným algoritmem. O ověřování původce jednotlivých paketů se stará protokol AH (Authentication Header), samotným šifrováním pak protokol ESP (Encapsulating Security Payload). IPsec však není samo o sobě dostačující

ochranou, ať už kvůli chybějící podpoře ve starších operačních systémech Windows [LUPA, 2007], kompatibilitě s NAT (Network Address Translation) nebo faktu, že ve starším protokolu IPv4 (Internet Protocol version 4) je pouze volitelný. Proto je třeba hledat jiná řešení, která zmíním ve druhé kapitole.

1.3 Nebezpečí nechráněné komunikace

Cílem útoku kriminálních živlů může být jakákoliv část systému informatiky. Systém informatiky tvoří technické prostředky, programové prostředky, paměťová média, data a osoby nějakým způsobem zainteresované na procesech tohoto systému. Zatímco předmětem zájmu běžné kriminality bývá především peněžní hotovost, tak předmětem zájmu počítačové kriminality mohou být například seznamy jmen a adres bankovních klientů [KODL, 1996, s. 8].

Nechráněná komunikace znamená zvýšené riziko vzniku škody. Škoda je většinou způsobena přerušením funkčnosti systému, sledováním přenášených informací či jejich modifikací, případně vytvářením nových („padělaných“) dat neautorizovanou osobou (narušitelem). Zatímco přerušení funkčnosti bývá zpravidla odhaleno poměrně brzy (při prvním pokusu o použití daného prostředku), sledování je podstatně hůř odhalitelné. Taktéž i modifikace a vytváření nových dat má nižší odhalitelnost a při vysoké úrovni provedení nemusí být dokonce odhaleny vůbec.

Je důležité si uvědomit, že tato rizika mají často přímé ekonomické dopady. Například u bankovních ústavů je toto nebezpečí zcela zjevné, avšak i v případě zneužití informací fyzických osob může dojít k nelegálnímu obohacení útočníka, pakliže získané informace mají pro někoho využitelnou hodnotu. Souvisejícím důsledkem bývá i diskreditace poškozeného subjektu – v případě banky, která nedokázala zabezpečit svůj informační systém a za podmínky, že zranitelnost daného systému se stane veřejně známou skutečností, dojde k úbytku potenciálních a stávajících klientů. U známých osobností lze předpokládat zneužití citlivých dat – například informací o nemanželském poměru, aktivitách rodinných příslušníků, morálních či právních prohřešcích a pochybeních – k vydírání nebo ziskovému poskytnutí informací třetí osobě nebo subjektu.

Při projektování ochrany se musíme vždy zamyslet nad praktickými a ekonomickými hledisky. Obecně se předpokládá, že prostředky vynaložené na ochranu informací mají být nižší, než škoda, která vznikne při potenciálním narušení ochrany. Tato hodnota se však při projektování velmi těžko vyčísluje [KODL, 1996, s. 13]. Jakou cenu mají

osobní data klientů, firemní know-how, zákazníci (tedy kontakty na zájemce o dané služby) apod.? Pro ilustraci jen uvedu příklad z 90. let, kdy firma Philip Morris koupila Kraft Foods za 12,9 miliard dolarů. Z toho odhadem 90 procent – 11,6 miliard dolarů – bylo právě za know-how, zkušenosti, zákaznickou základnu atd., tedy v podstatě právě za informace zneužitelné konkurencí. „Pouhých" 1,3 miliard dolarů stála hmotná aktiva [PETERS, 1995, s. 27].

Největší dopady pravděpodobně nese vyzrazení politických a vojenských informací. Pokud se ohlédneme do poměrně nedávné historie týká se to například prolomení šifrování realizovaného přístrojem Enigma v 30. letech, což způsobilo, že spojenecké mocnosti byly schopny číst německé depeše během druhé světové války. A nejen to – ještě v 50. letech 20. století využíval modifikovanou verzi Enigmy Sovětský svaz.

Odborní autoři často uvádějí i jiné příklady, kde se hodnota informací ochráněných kryptografií či odtajněných za pomocí kryptoanalýzy pravděpodobně ani nedá odhadnout. Jedná se mimo jiné o tvrzení, že kryptologie byla rozhodujícím faktorem v obou světových válkách. Ve druhé světové válce přímo ovlivnila přinejmenším čtyři významné události. První z nich byla rozhodující námořní bitva u Midway (3. – 7. června 1942), na kterou se Američané byli schopni připravit díky zpravodajské službě a rozluštění japonských depeší [KAHN, , s. 303-307]. Tato bitva zhatila japonskou námořní nadvládu v Pacifiku. Druhou událostí byla operace Vengeance – sestřelení letounu admirála Jamamota opět díky úspěšné kryptoanalýze a odtajnění jeho časového plánu[KAHN, , s. 328-333]. Kryptologie též podstatně ovlivnila ponorkové bitvy v Atlantském oceánu [WOBST, 2007, s. 5]. A konečně: podle spekulací Sira Francise Harryho Hinsleye (anglický historik a kryptoanalytik, za druhé světové války se účastnil prolomení šifrování Enigmy) byly Spojené státy americké, v případě, že by nedošlo k rozluštění německých depeší, připraveny použít jaderné zbraně i v Evropě [WOBST, 2007, s. 54].

Tolik tedy k ilustraci hodnoty některých informací. Při tvorbě projektu informační bezpečnosti však musíme počítat též s tím, že některá data mají krátkou životnost a jejich hodnota je pomíjivá. To je podstatou tzv. principu časových limitů, který říká, že datové položky je třeba chránit pouze tak dlouho, dokud mají nějakou hodnotu [KODL, 1996, s. 13]. Důsledkem může pochopitelně být snížení nákladů a zátěže technických prostředků.

1.4 Oblasti využití šifrování

Klíčové pro charakterizování oblastí využití šifrování je pochopení základních principů, které si kryptografie, potažmo informační bezpečnost obecně klade za cíl. V úvodu této kapitoly se tedy budu zabývat právě těmito cíli.

Základním cílem informační bezpečnosti je zajištění soukromí a důvěrnosti přenášených informací, tedy omezení přístupu ke komunikaci pouze na oprávněné subjekty. Dále je potřeba zachovat integritu dat, nesmí dojít k jejich změně v procesu komunikace nedovoleným nebo neznámým způsobem. K tomu se využívají například hashovací funkce (viz kapitola 2.5 Kryptografické hashovací funkce). S předchozími cíli souvisí nutnost ověření a identifikace entit zapojených do přenosu. Jedná se nejen o původce, respektive zdroj dat (tedy o osoby), ale také například o jednoznačnou identifikaci počítačových terminálů, kreditní karty a dalších technických prostředků. K propojení entity a přenášené zprávy může například sloužit digitální podpis. K jednotlivým úkonům procesu přenosu a roli v něm jsou dané entity autorizovány. Autorizace bývá následně validována, tedy potvrzena. Neautorizovaným subjektům musí být dané akce a přístupy zamezeny. Důležité informace by měly být certifikovány (schváleny) důvěryhodnou odpovědnou entitou a též opatřeny záznamem o čase vzniku, respektive změny nebo smazání. Tím dojde k potvrzení vzniku, změny či zániku informace entitou odlišnou od původce. V případě komunikace mezi entitami je vhodné zajistit potvrzení příjmu komunikátu, v případě poskytování služeb analogicky potvrzení, že služba byla poskytnuta. Subjektům se dále vydávají oznámení o rozsahu práv a omezení ke konkrétním zdrojům informací. Pokud je třeba, musí též šifrování zajistit anonymitu entity zapojené do procesu komunikace a dále zaručit, že subjekt či entita nebude moci popřít vzniklé závazky a akce, které vykonala. V případě nutnosti pak informační systém zajistí odvolání, respektive zrušení certifikace informace či autorizace entity.

Prostý výčet cílů informační bezpečnosti by byl tedy takový: důvěrnost informace, integrita dat, identifikace a ověření entit, propojení komunikátu a původce, autorizace, validace, kontrola přístupu, certifikace, časové záznamy o procesech, verifikace, potvrzení přijetí zprávy či služby, potvrzení či prohlášení o právech, anonymita, neodvolatelnost a zrušení či odvolání certifikace nebo autorizace. Šifrování je tedy účinné a žádoucí právě tam, kde mají být dosáhnuty výše uvedené cíle.

2. Moderní kryptografické metody

2.1 Vymezení základních pojmů

Jako každý vědní obor používá i kryptologie mnoho termínů, které jsou pro nezasvěcené často nesrozumitelné. V této kapitole se tedy zabývám právě vymezením základních pojmů, jež budu v dalších kapitolách používat.

V první řadě je třeba vysvětlit samotný pojem kryptologie. Jedná se o vědu zabývající se šiframi a zastřešující obory kryptografie a kryptoanalýza. Zatímco kryptografie je nauka o metodách utajování smyslu zprávy, tvořené prostým textem, kryptoanalýza se naopak zaobírá luštěním šifrovaného textu.

Prostý (neboli otevřený) text může každý bez potíží přečíst, za předpokladu, že zná daný přirozený jazyk. Otevřený text se často značí jako M (message, zpráva) nebo P (plain text, otevřený text). Šifrový (neboli šifrovaný) text je naproti tomu takový text, jehož obsah je určitým způsobem ukrytý a v matematických rovnicích bývá označován písmenem C (ciphertext, šifrový text). Jak tedy získat z otevřeného textu šifrovanou zprávu? Pomocí funkce E (encryption function, šifrovací funkce), která působí na M a vytváří C [KODL, 1996, s. 23]: „E(M)=C“.

Funkce E se často označuje jako kryptografický algoritmus. V případě, že bezpečnost algoritmu spočívá v utajení způsobu, jakým pracuje, pak se jedná o tzv. omezený algoritmus [KODL, 1996, s. 23].

Opačnou operací k E je funkce D (decryption function, dešifrovací funkce). Pakliže je možné odvodit šifrovací klíč z dešifrovacího (a naopak), hovoříme o symetrickém algoritmu (symetrické šifře). Jedná se tedy o algoritmus omezený, protože odhalení klíče umožňuje dešifrování zprávy. Asymetrické šifry naopak používají jeden klíč pro šifrování a druhý pro dešifrování zprávy. Klíč šifrovací je veřejný klíč a klíč dešifrovací soukromý. To znamená, že zašifrovat zprávu může pomocí veřejného klíče a se znalostí algoritmu každý, luštit zprávu lze snadno pouze se znalostí daného soukromého klíče. Veřejný klíč tedy není potřeba držet v tajnosti, klíč soukromý však ano. Ztráta klíče jinou metodou než kryptoanalýzou se nazývá kompromitace [KODL, 1996, s. 26].

Klíč specifikuje například uspořádání písmen v šifrovací abecedě, způsob změny pořadí písmen ve zprávě nebo nastavení šifrovacího stroje [KAHN, s. 5]. Šifrovací abeceda je seznam ekvivalentů ke znakům otevřeného textu. Používá se v substitučních šifrách, které spočívají v nahrazení znaků v otevřeném textu podle určitých zásad. Naproti tomu změna

pořadí znaků je principem transpozice. Tyto dvě metody se někdy kombinují, aby bylo dosáhnuto vyšší bezpečnosti.

V současnosti je jediným známým algoritmem s prokázanou absolutní bezpečnosti tzv. jednorázový heslář (one-time pad), neboli Vernamova šifra. O ní si řekneme více v následujících kapitolách, důležité prozatím je, že ostatní algoritmy mohou být pouze výpočetně bezpečné – silné. To znamená, že za dodržení podmínek bezpečnosti (utajení klíče apod.) nemůže být algoritmus prolomen prostředky používanými v současné kryptoanalýze nebo předpokládanými prostředky, které budou používány v blízké budoucnosti. Neznamená to, že algoritmus nemůžeme úspěšně luštit (prolomit), ale z hlediska času a prostředků investovaných do procesu to ztrácí smysl. Právě nalezení takových řešení s ohledem na budoucí vývoj technologií je úkolem kryptografie.

2.2 Druhy šifrovacích metod

Kryptografie má bohatou a dlouhou historii, která dost možná začala už někdy okolo roku 1900 před Kristem v Egyptě, na místě zvaném Menet Khufu. Za tu dobu se vyzkoušelo mnoho druhů šifrovacích metod, které v této kapitole představím.
Výše uvedené první zdokumentované použití šifrování bylo druhem substituční šifry, neboť šlo o použití jakýchsi modifikovaných hieroglyfů. Substitučních šifer se vytvořilo několik druhů, například monoalfabetická, polyalfabetická, polygrafická a homofonní.

2.2.1 Monoalfabetická substituční šifra

Monoalfabetická šifra představuje velmi jednoduchou výměnu jednoho znaku za jiný pomocí klíče. Klíč vlastně představuje tabulka zaznamenávající který znak šifrového textu reprezentuje jaký v textu otevřeném. To ovšem přináší hlavní slabinu těchto šifer a sice že je zachována statistická četnost znaků. Frekvenční analýzou (hlavně spočítáním výskytu písmen) pak lze odhalit, které písmeno se čím nahrazuje. Pakliže například budeme vědět, že zpráva je psána v češtině, kde je písmeno s nejčastějším výskytem písmeno „e“, zatímco v šifrovaném textu to bude písmeno „s“, pokusíme se nahradit všechna „s“ šifrového textu písmenem „e“. Pokračováním v tomto postupu s velkou pravděpodobností odhalíme alespoň podstatné části zprávy, ne-li celý otevřený text. Kromě procentuálního výskytu písmen v daném přirozeném jazyce poskytuje frekvenční analýza i další pomůcky pro kryptoanalýzu, jako například četnost výskytu jednotlivých bigramů a trigramů, nejčastěji se vyskytující písmena na konci a začátku slov daného jazyka apod. Z tohoto důvodu byly substituční šifry často vylepšovány. Jeden ze způsobů jsou tzv. nomenklátory. Jde vlastně o nahrazování celých slov – například místo slova „útok“ použijeme slovo „deštník“ nebo nějaký symbol a u zbytku slov budeme postupovat podle substitučního klíče. Nevýhoda je ovšem v tom, že nomenklátory se musí předem domluvit mezi oběmi stranami komunikace. Předchozí dohodu vyžaduje i využívání nul, neboli klamných znaků. Tyto znaky nemají žádný význam a při překladu do prostého textu se vypouští. Též je možné šifrovat jedno písmeno více způsoby – „e“ zapíšeme jednou jako „c“, podruhé jako „z“. Abecedu pak musíme pochopitelně obohatit dalšími znaky, pouze s písmeny daného přirozeného jazyka to samozřejmě není možné. Tohoto využívá tzv. homofonní šifra, u které je počet zástupných znaků přímo úměrný frekvenci používání daného písmene v přirozeném jazyce (písmeno „e“ by pak tedy v českém otevřeném textu mělo nejvíce zástupných znaků v šifrovém textu). Vylepšením monoalfabetické substituční šifry je též polygramová šifra, ve které šifrování neprobíhá na

úrovni jednotlivých znaků, ale na úrovni jejich skupin – bigramů, trigramů a „vícegramů“. Příklady polygramových šifer jsou například britská šifra Playfair používaná v první světové válce nebo šifra L. S. Hilla. Princip, který předchozí dohodu komunikujících subjektů nevyžaduje (ale snižuje přesnost frekvenční analýzy) je komolení zprávy – záměrné používání gramatických chyb apod. Zajímavým nápadem snižujícím použitelnost frekvenční analýzy je též použití jiného přirozeného jazyka, než se očekává. Ve druhé světové válce například Američané používaly indiánské jazyky (kmenů jako Navajo, Komančů, Čerokézů atd.), s menším úspěchem pak Britové používaly velštinu.

Nejznámějšími v minulosti používanými monoalfabetickými substitučními šiframi jsou Vernamova (již dříve zmíněná šifra s jednorázovým heslářem) a Caesarova šifra (velmi jednoduchý příklad, nahrazovala znak otevřeného textu znakem o tři místa dál – „a“ nahrazeno „d“, „z“ nahrazeno „c“). Zatímco ta první z nich, jak jsme si řekli, je při správné implementaci a dodržení bezpečnostních zásad jediná nerozluštitelná, Caesarova šifra je snadno luštitelná tzv. útokem hrubou silou (z anglického „brute-force attack“; viz kapitola 2.6.7 Bezpečnost algoritmů).

2.2.2 Polyalfabetická substituční šifra

Polyalfabetická substituční šifra v podstatě vylepšuje monoalfabetickou šifru, neboť místo jedné šifrovací abecedy používá dvě či více šifrovacích abeced, které se uplatňují podle určitého klíče. Jako první polyalfabetická šifra bývá uváděna Albertiho šifra, ačkoliv některé zdroje uvádějí, že Arabové tyto šifry používaly již o 500 let dříve [AL-KADI, 1992, s. 97-126]. Tato šifra užívala dvou šifrovacích abeced – první znak otevřeného textu se šifroval první abecedou, druhý znak druhou, dokud nebyl zašifrován celý otevřený text. Složitějším případem Albertiho šifry se stala Vigenenèrova šifra, která umožňuje použití až 26 šifrových abeced, čímž podstatně snižuje pravděpodobnost prolomení. Pomůckou k použití této šifry je tzv. Vigenèrův čtverec, který obsahuje oněch 26 abeced. Jedná se o standardní posloupnost znaků v abecedě přirozeného jazyka – první řádek začíná písmenem „a“ a končí písmenem „z“, druhý řádek začíná písmenem „b“ a na konci má „a“, až k poslednímu řádku – od „z“ po „y“. Následně vybereme libovolné slovo jako klíč, čím delší klíč, tím bezpečnější šifra. V případě klíče o délce jeden znak nebo klíče, který je tvořen jen opakováním jednoho znaku se však vlastně bude jednat o Caesarovu šifru (tedy monoalfabetickou, protože budeme používat jen jeden řádek Vigenèrova čtverce), v případě klíče o dvou znacích pak o šifru Albertiho. Po volbě silného klíče tedy postupujeme tak, že první písmeno otevřeného textu zašifrujeme pomocí toho řádku Vigenèrova čtverce, který začíná stejným písmenem, jako

první písmeno klíče, druhé písmeno otevřeného textu zašifrujeme řádkem, který začíná stejným znakem, jako druhá pozice klíče. Takto postupujeme, dokud nevyčerpáme všechny znaky z klíče. Pak začneme nanovo od první pozice klíče. Kdyby měl klíč 20 znaků, pak by každý dvacátý znak otevřeného textu byl šifrován stejným znakem klíče. Tomu se říká perioda klíče (určuje obtížnost luštění šifry) [KODL, 1996, s. 34].

2.2.3 Transpoziční šifra

Transpoziční šifry jsou v podstatě velmi jednoduché, protože otevřený text zůstává stále stejný, pouze dochází ke změně pořadí znaků v šifrovém textu. Základním typem transpoziční šifry je jednoduchá sloupcová transpozice s úplnou tabulkou. Otevřený text je přepsán horizontálně do tabulky, jejíž počet sloupců odpovídá délce klíče. Každému písmenu klíče se dále přiřadí číslo podle jeho pořadí v abecedě (v případě opakovaného výskytu jednoho písmena v klíči má nižší číslo to, které se vyskytuje v klíči dříve). Prázdné buňky tabulky doplníme náhodně zvolenými písmeny. Varianta s neúplnou tabulkou není doplňována náhodnými znaky, rozměr tabulky se proto určuje hůře. Šifrový text dostaneme, pokud v tabulce čteme vertikálně po sloupcích očíslovaných použitím klíče. Tato metoda má hlavní slabinu, stejně jako jednoduchá monoalfabetická substituční šifra, v zachování přibližné četnosti znaků, čili snadnému luštění za pomocí frekvenční analýzy [SCHNEIER, 1996, s. 37].

I přesto, že mnoho moderních algoritmů transpozici využívá, je problematická, protože vyžaduje velkou paměť (výpočetní prostředky) a někdy omezuje i délku zpráv. Substituce je daleko běžnější [KODL, 1996, s. 35]. Transpoziční a substituční algoritmy se často kombinují, což snižuje účinnost frekvenční analýzy. Transpoziční šifru také lze vylepšit přiřazením číselné hodnoty podle pozice písmen abecedy v tabulce (většinou o rozměrech 5x5 nebo 6x6). Metoda přiřazení koordinátů písmenům vychází z tzv. Polybiova čtverce, má mnoho obměn a používala se například v šifře ADFGVX (německá šifra z období první světové války).

2.3 Symetrické algoritmy

Po druhé světové válce se všechen výzkum v kryptografii víceméně odehrával ve vládních organizacích jako například v americké NSA (National Security Agency), britské GCHQ (Government Communications Headquarters) a jejich ekvivalentech v ostatních státech. Do sedmdesátých let se mnoho výsledků výzkumu nezveřejnilo, od roku 1975 se však událo mnoho změn. První z nich bylo zveřejnění standardu DES (Data Encryption Standard) v roce 1975, respektive 1977 (po zásahu ze strany NSA). DES byl symetrický algoritmus, o kterých si povíme více v této kapitole.

Symetrické algoritmy, někdy označované jako algoritmy jednoho klíče či sdíleného klíče, jsou v kryptografii v podstatě považovány za konvenční metodu. Principem jejich funkce je, že stejný nebo mírně upravený klíč se používá pro šifrovací i dešifrovací algoritmus. To vyžaduje, aby si odesílatel a příjemce předali klíč před započetím samotné komunikace, což přináší značnou slabinu těchto metod zabezpečení. Odhalení klíče zpravidla znamená, že šifrovat a dešifrovat zprávy bude moci kdokoliv [KODL, 1996, s. 25].
Symetrické algoritmy se dále dělí na proudové a blokové šifry. Zatímco proudové algoritmy zpracovávají otevřený text po jednotlivých bitech (nejmenší jednotka informace ve výpočetní technice) nebo Bytech (jeden Byte je 8 bitů), blokové algoritmy pracují se skupinami (bloky) bitů – běžně s 64 bity nebo i 128 bity (viz kapitola 2.3.3 Advanced Encryption Standard (Rijndael)) – jako s jedním celkem.

2.3.1 Data Encryption Standard

Data Encryption Standard, označovaný zkratkou DES, se stal po svém zveřejnění roku 1977 jednou z nejznámějších blokových šifer. I přes značnou kontroverzi tohoto standardu, o které se ještě zmíním, byl DES zvolen organizací NBS (National Bureau of Standards), dnes známou jako NIST (National Institute of Standards and Technology), za prostředek komunikace vládních nevojenských organizací Spojených států. Širokého využití se brzy dočkal i v jiných zemích. Hlavní zásluhu na vývoji DES mělo IBM (International Business Machines), v letech 1975-1977 probíhala spolupráce IBM a NSA na úpravě algoritmu před zveřejněním.

Jak vlastně DES funguje a co to je? Zjednodušeně řečeno se jedná o blokovou šifru, která překládá 64 bitů otevřeného textu za pomocí série komplikovaných operací a klíče o efektivní délce 56 bitů (respektive 64 bitů, z nichž 8 je použito pro kontrolní funkci a před použitím algoritmu zahozeno), který specifikuje tyto operace, do šifrového textu stejné délky.

Sérii operací tvoří počáteční a finální permutace (uspořádání prvků množiny do určitého pořadí) – IP a FP, které jsou vzájemně inverzní (aplikováním jedné a následně druhé na množinu prvků dostaneme původní nezměněnou množinu) a nemají v podstatě žádný význam pro kryptografii, v 70. letech sloužily pro usnadnění nahrávání bloků bitů do a z přístrojů – a 16 kol zpracování. Před zpracováním je blok otevřeného textu rozdělen na dvě části o velikosti 32 bitů. Každá z částí se zpracovává zvlášť tzv. Feistelovou funkcí – funkcí F, což lze znázornit ve Feistelově schématu (viz Příloha č. 3 – Feistelovo schéma šifry DES). Funkce F zakóduje polovinu bloku částí klíče, výstup funkce se poté zkombinuje s druhou půlkou bloku a před další fází se bloky vymění (povšimněte si křížení ve Feistelově schématu). Funkce F tedy operuje s polovinou bloku (32 bity) v jednom okamžiku a má čtyři fáze:

1. Expanze - 32 vstupních bitů se rozšíří expanzní permutací (polovina z 32 bitů je duplikovaná a pořadí bitů změněno), někdy označovanou jako E-expanze. Na výstupu jsou šestibitové části – každá sestává ze 4 bitů uprostřed korespondujících se vstupem. První a poslední bit jsou vlastně kopie prvního, respektive posledního bitu ze dvou sousedních vstupních částí. Výsledkem této operace je tedy 48 bitů v osmi skupinách.

2. Aplikování klíče - výsledek expanze zkombinujeme se subklíčem za použití operace XOR[1]. Pro každou z 16 fází se používá jiný subklíč získaný zvláštní funkcí z původního . Celkem tedy máme 16 částí klíče, každou o velikosti 48 bitů.

3. Substituce - po aplikování subklíče se blok dat rozdělí na 8 šestibitových částí a postoupí ke zpracování do S-boxu[2]. Každý z osmi S-boxů přepíše 6 vstupních bitů čtyřmi bity výstupními.

4. Permutace - na závěr je 32 bitů, které vyjdou z S-boxů uspořádáno neměnnou permutací, někdy označovanou jako P-box, která zajistí rozptyl bitů do různých S-boxů v dalším kole.

Základem celého DES jsou tedy S-boxy, které zajistí bezpečnost šifrování. Právě nelineární substituce v S-boxech, permutace v P-boxu a E-expanze zajišťují tzv. „konfúzi a difúzi“, koncept označovaný za nezbytnou podmínku bezpečné šifry[3].

Proč tedy, když je tato bezpečnostní podmínka zachována, není v současnosti DES považováno za bezpečnou šifru? Jednak kvůli diskutované roli NSA na procesu vývoje:

[1] XOR - Operace exkluzivní disjunkce (XOR má návratovou hodnotu „pravda“, právě když každá vstupní hodnota nabývá unikátní, odlišnou hodnotu, než další vstupní hodnota).
[2] S-boxy – substituční boxy – jsou v blokových šifrách používány pro skrytí vztahu mezi klíčem a šifrovým textem, což odpovídá principu „konfúze“ podle C. Shannona a má ztížit případnou kryptoanalýzu.
[3] Tento koncept stanovil Claude Shannon ve 40. letech 20. století.

mnozí spekulují, zda nebyla do algoritmu implementována tzv. „zadní vrátka“[4]. Otázkou zůstává, nakolik jsou tyto spekulace jen součástí různých konspiračních teorií ve stylu „Velký bratr tě sleduje“[5]. Vzhledem k malé velikosti klíče (pouhých 56 bitů, které se na šifrování podílí), což se stávalo s postupem času (a zdokonalováním výpočetních prostředků) stále větší slabinou, se tak jako tak DES dočkal zdokonalování (například v algoritmu Triple DES) a nahrazování jinými algoritmy. V roce 1997 proběhl projekt DESCHALL (DES Challenge) a poprvé došlo k veřejnému rozluštění zprávy zašifrované algoritmem DES. O rok později vyzkoušela společnost EFF (Electronic Frontier Foundation) přístroj Deep Crack[6] k úspěšnému prolomení šifrování DES za 56 hodin [TEFF, 1998]. Roku 1999 přístroj Deep Crack díky projektu distributed.net[7] prolomil DES za méně než polovinu této doby.

2.3.2 Triple DES

Jak jsem uvedl v kapitole 2.3.1, délka klíče algoritmu DES byla brzy nedostatečná, především kvůli překotnému technologickému vývoji. Roku 1998 tedy došlo ke zveřejnění algoritmu TDEA (Triple Data Encryption Algorithm), známému též jako Triple DES.

Triple DES je též bloková šifra a funguje velmi podobně jako DES. Už název naznačuje, že se vlastně jedná o trojí aplikování DES na každý z bloků dat. Místo 16 kol probíhá šifrování celkem v 48 kolech a použitý klíč se skládá z tří klíčů, každý o velikosti 56 bitů (ačkoliv prakticky existují tři možnosti, v té první se používají tři odlišné klíče, v druhé jsou dva klíče totožné a jeden unikátní a v poslední možnosti, která není o nic lepší než původní DES, jsou všechny tři klíče totožné). Efektivní velikost klíče Triple DES tudíž může být až 168 bitů. Triple DES pracuje tak, že blok dat zpracuje standardním algoritmem DES postupně celkem třikrát, pokaždé s jedním ze tří klíčů. Klíče o celkové velikosti 168 bitů, v případě, že každý z nich je jiný, by měly zajistit relativní bezpečnost algoritmu minimálně do roku 2030 [NIST, 2007, s. 65].

2.3.3 Advanced Encryption Standard (Rijndael)

Advanced Encryption Standard, známý pod zkratkou AES, je výherce soutěže patnácti návrhů na nový šifrovací algoritmus. U DES jsem uváděl jisté pochybnosti o zapojení NSA do procesu tvorby algoritmu, ovšem tato soutěž, vyhlášená organizací NIST (National

[4] Zadní vrátka je metoda, často úmyslně zahrnutá do počítačového programu, která umožňuje zasvěceným osobám obejít funkci programu (v našem případě algoritmu).
[5] Známý výrok z antiutopického románu 1948 anglického spisovatele George Orwella.
[6] Přístroj obsahoval přes 1500 čipů a jeho cena byla pod tehdejších čtvrt milionu dolarů.
[7] Tato nezisková organizace se zabývá distribuováním výpočetních požadavků mezi nevyužité procesory uživatelů připojených do celosvětové sítě počítačů.

Institute of Standards and Technology) probíhala veřejně a odborná kryptologická komunita nemá pochybnosti o jejím korektním průběhu. Vítězná šifra, původně nazvaná Rijndael podle kombinace písmen z příjmení obou tvůrců (Belgičané Daemen a Rijmen), zajišťuje šifrování s klíči o velikosti 128, 192 nebo 256 bitů. Po důkladné analýze a standardizačním procesu, což byla součást soutěže, uznala NSA tuto blokovou šifru za vhodnou pro použití u přísně tajných informací (označení „top secret“). AES (Rijndael), stejně jako několik dalších finalistů soutěže, však zůstává k dispozici i veřejně.

Na rozdíl od DES nevyužívá AES Feistelovo schéma, ale tzv. substitučně-permutační síť, která sestává z několika kol či vrstev aplikování S-boxů a P-boxů na otevřený text (viz Příloha č. 4 – Substitučně-permutační síť). AES rozděluje data na bloky o velikosti 128 bitů a provádí operace v tabulce 4x4 (osmibitové). Z toho plyne, že v každé buňce takové tabulky je jeden byte (8 bitů) dat – otevřeného textu.

Algoritmus AES, podobně jako DES, má čtyři fáze:

1. Tvorba klíčů - z původního klíče se odvozují subklíče pro jednotlivá kola pomocí funkce vytvořené autory speciálně k tomuto účelu.

2. Úvodní kolo - každý byte z tabulky se zkombinuje se subklíčem pomocí funkce XOR.

3. Kola: a) substituční metodou se každý byte z tabulky nahradí jiným bytem získaným Rijndaelovým S-boxem,

b) transpoziční metodou se každý řádek tabulky posune o určitou pozici,

c) byty v každém sloupci se smíchají a vrátí zpět do buněk podle určeného pravidla,

d) postoupí se k dalšímu subklíči.

4. Poslední kolo - obsahuje všechny operace z předchozích kol kromě míchání bytů v rámci sloupce.

Algoritmus probíhá v 10, 12, respektive 14 kolech v závislosti na velikosti klíče. Všechny verze AES lze podle NSA použít k šifrování informací klasifikovaných jako tajné (Secret), AES s délkou klíče 192 nebo 256 bitů pro informace klasifikované jako přísně tajné (Top Secret). Bruce Schneier, jedna z uznávaných kapacit kryptologie a jeden z účastníků soutěže potvrdil bezpečnost šifry Rijndael když prohlásil, že nevěří, že někdo vůbec objeví způsob, jak přečíst komunikaci šifrovanou pomocí této šifry a že veškeré potenciálně úspěšné útoky jsou myslitelné pouze na akademické úrovni (tedy v praxi nerealizovatelné kvůli výpočetní složitosti) [AES, 2000]. Znamená to, že AES můžeme považovat za algoritmus

s dostatečnou bezpečností a veškeré průlomy kryptosystémů, které ho používají jsou zatím možné pouze na teoretické úrovni nebo vinou špatné implementace či zanedbání jiné složky informační bezpečnosti.

2.3.4 Serpent

Symetrická bloková šifra Serpent se umístila jako druhá v soutěži AES. Byla vytvořena Rossem Andersonem, Elim Bihamem a Larsem Knudsenem. Jako ostatní algoritmy, které byly zapsané do soutěže, pracuje i Serpent s bloky o velikosti 128 bitů a podporuje klíče s velikostí 128, 192 a 256 bitů. Na rozdíl od Rijndael probíhá šifrování v 32 kolech. Bloky dat se dále dělí na 4 části o velikosti 32 bitů. V každém z kol se používá 8 S-boxů operujících na čtyřech bitech. Všechny operace probíhají paralelně (zároveň). 16 kol se sice obecně považuje za dostatečný počet schopný odolávat momentálně známým kryptoanalytickým útokům, Serpent však vsází na větší bezpečnost, zajištěnou 32 koly. To by mělo zajistit delší životnost šifry, autoři sami uvádí životnost až okolo jednoho století [SERPENT, ???]. Serpent, zveřejněný pod licencí General Public License, je ke stažení volně k dispozici na webové stránce autorů.

Funkce Serpentu, probíhající v každém kole, spočívá v kombinaci klíče s daty za pomocí funkce XOR (podobně jako u Rijndael), 32 paralelních aplikací S-boxu a lineární transformaci. V posledním kole se místo lineární transformace provádí další aplikace klíče funkcí XOR. Vzhledem k tomu, že Serpent šifruje ve větším počtu kol, než Rijndael, jeho použití trvá delší dobu, což byl také jeden z faktorů, který rozhodl o výsledcích soutěže AES. Na druhou stranu i oproti Rijndael by měl Serpent zajistit vyšší bezpečnost, která se pravděpodobně skutečně vyplatí až během následujících let. Otázkou je, zda v té době bude vhodná chvíle pro použití Serpentu namísto Rijndael, nebo spíš pro vytvoření zcela nové šifry podle aktuálních trendů.

2.3.5 Twofish

V kapitole o Rijndael jsem zmínil jméno Bruce Schneiera, odborníka na kryptologii, který se též účastnil soutěže AES. Jeho symetrický blokový algoritmus nese název Twofish a vznikl z přepracování algoritmu Blowfish, dalšího ze Schneierových výtvorů. Na Twofish spolu se Schneirem pracovali John Kelsey, Doug Whiting, David Wagner, Chris Hall a Niels Ferguson. Na kryptoanalýze Twofish i dalších šifer ze soutěže se podíleli Stefan Lucks, Tadayoshi Kohno a Mike Stay. Šifra jako jedna z mála vyšla v rámci standardu OpenPGP a tudíž je bez jakýchkoliv omezení k dispozici.

Také Twofish operuje s bloky dat o velikosti 128 bitů a klíči až do 256 bitů a dostal se do finále soutěže. Typické pro Twofish je použití předem vypočítaných S-boxů závislých na klíči a relativně složitým vypočítáváním subklíčů. Jedna polovina klíče se používá pro samotné šifrování dat a druhá modifikuje algoritmus skrze S-boxy. Twofish používá některé dříve zveřejněné koncepty, ať už Feistelovu strukturu, známou z DES, nebo principy zajišťující kryptografickou difúzi u šifer rodiny SAFER. Twofish šifruje s klíči o velikosti 128 bitů o něco pomaleji, než Rijndael, ale rychleji s 256-bitovými klíči [COMPARISON, 2000, s. 3-5].).

2.3.6 RC4

RC4, na rozdíl od předchozích šifer, je proudová šifra. To znamená, že pracuje s bity otevřeného textu a ne s bloky bitů. Bity otevřeného textu se kombinují s pseudonáhodnými[8] bity zpravidla za použití funkce XOR.

RC4, jako jedna z nejznámějších proudových šifer, má široké využití, například v protokolu SSL[9] (Secure Sockets Layer) a WEP[10] (Wired Equivalent Privacy). Světlo světa spatřila tato šifra roku 1987 a jejím autorem byl Ron Rivest ze společnosti RSA Security. Původně sice RC4 podléhala utajení, ovšem roku 1994 prosákly na veřejnost zdrojové kódy. Hlavní devizou algoritmu se stala velká rychlost a jednoduchost použití.

RC4 se podobá dříve zmíněné Vernamově šifře, ovšem používá na rozdíl od ní klíč pseudonáhodný. Klíč se generuje za pomocí permutace 256 možných bytů a má variabilní velikost – většinou od 40 do 256 bitů.

Šifra se nepovažuje za bezpečnou a proto došlo k vyhlášení projektu eSTREAM s cílem najít nové proudové šifry vhodné pro široké použití. eSTREAM vznikl poté, co všech 6 proudových šifer zaslaných do projektu NESSIE, srovnatelného se soutěží AES, selhalo.

2.3.7 HC-256

HC-256, jedna z proudových šifer zařazených do projektu eSTREAM, umožňuje šifrování velkých objemů dat s vysokou rychlostí a bezpečností. Tvůrcem HC-256 je Hongjun Wu.

---

[8] Pseudonáhodný proces proto, že navenek a statisticky vypadá jako náhodný, ovšem je vytvářen podle daných pravidel, tedy deterministicky.

[9] Protokol zajišťující bezpečnost komunikace v počítačových sítích, například v Internetu.

[10] Algoritmus, který měl zajistit bezpečnost bezdrátových sítí. V dnešní době je považovaný za překonaný, neboť není zcela bezpečný a lze ho prolomit během několika minut za použití speciálního softwaru. Nástupcem WEP má být WPA (Wi-Fi Protected Access).

Jak již název napovídá, využívá klíče o velikosti 256 bitů a inicializační vektor[11] stejné velikosti. Existuje i verze HC-128. Sestává ze dvou tajných tabulek, které jsou podobné S-boxům u blokových šifer. Každá z tabulek obsahuje 1024 řetězců o velikosti 32 bitů. V každém kroku algoritmu je jeden z řetězců v jedné z tabulek změněn, tudíž po 2048 krocích jsou změněny všechny. Nakonec se aplikuje lineární funkce k vygenerování výstupu.

2.3.8 Rabbit

Rabbit, vysokorychlostní proudová šifra, byla poprvé prezentována roku 2003 a roku 2005 zařazena do projektu eSTREAM. Vytvořili ji Martin Boesgaard, Mette Vesterager, Thomas Pedersen, Jesper Christiansen a Ove Scavenius.

Rabbit používá 128-bitév klíče a 64-bitový inicializační vektor. Algoritmus vykazuje vysoké rychlosti šifrování na moderních procesorech. Šifra zpracuje 128 bitů v jednom cyklu a její funkce jsou založeny zcela na aritmetických operacích dostupných na moderním hardwaru, tudíž nepoužívá žádné S-boxy nebo tabulky.

Rabbit prošel rozsáhlou kryptoanalýzou a ačkoliv jeho komerční použití bylo původně placené, od roku 2008 ho lze využívat bezplatně pro všechny účely. Algoritmus se momentálně považuje za bezpečnostně dostatečný proti útokům hrubou silou.

2.3.9 Salsa20

Proudovou šifru Salsa20 zaslal do projektu eSTREAM Daniel Bernstein. Pracuje na principu pseudonáhodné funkce (založené mmj. na funkci XOR a rotační funkci), která zpracuje 256-bitový klíč, 64-bitové číslo „nonce“[12] a 64 bitů pozici v proudu do výstupu o velikosti 512 bitů. Existuje i verze se 128-bitovým klíčem.

V počáteční fázi je 8 řetězců klíče, 2 řetězce pozice v proudu, 2 řetězce čísel nonce a 4 neměnné řetězce. Těchto 16 řetězců se zpracovává v matematické matici[13] o rozměrech 4x4. Po 20 kolech činnosti algoritmu Salsa20/20 vznikne 16 řetězců šifrovaného výstupu. Existují různé verze Salsy20: například Salsa20/8 a Salsa 20/12, u kterých číslo za lomítkem určuje počet kol.

[11] Inicializační vektor je u proudových šifer velikost dat, nutná pro správnou funkci algoritmu. S touto velikostí dat jsou pak algoritmy schopné vytvořit unikátní výstup nezávislý na jiných výstupech vytvořených za použití stejného klíče. Alternativní postup spočívá v obvykle zdlouhavém procesu vytváření nového klíče.
[12] Nonce = Number Used Once. Číslo, které se použije jen jednou v celém procesu a slouží k autentizaci. Zajišťuje, že předchozí komunikace nemůže být použita pro falešnou autentizaci útočníka. Často se vytváří buď v závislosti na aktuálním čase nebo na základě dostatečně velkého náhodného čísla, aby byla zaručena zanedbatelná pravděpodobnost opakovaného vytvoření stejného čísla.
[13] Tabulka daných rozměrů obsahující matematické prvky – nejčastěji čísla.

Salsa20 se dostala do třetí fáze projektu eSTREAM (v těchto fázích se prověřovaly kvality šifer) a stejně jako předchozí dva algoritmy byla vybrána do konečného portfolia projektu. Ačkoliv na různé verze tohoto algoritmu se uskutečnilo mnoho útoků, tak ohledně verze s největším počtem kol – Salsa20/20 – nebyl dle mých zdrojů dosud žádný publikovaný. Roku 2005 vyhrál Paul Crowley tisíc dolarů za „nejzajímavější kryptoanalýzu Salsy20“ a o tři roky později zveřejnil Bernstein příbuznou rodinu šifer ChaCha s pozměněnými funkcemi, které si kladly za cíl zvýšit hodnotu difúze za kolo.

2.4 Asymetrické algoritmy

Když jsem v kapitole „2.3 Symetrické algoritmy“ zmínil převratné změny, které se udály v kryptologii po roce 1975 a uvedl jako jednu z velkých změn vývoj algoritmu DES, záměrně jsem neuvedl všechny převratné objevy. Již samotná povaha symetrických algoritmů naznačuje, že existuje přinejmenším jeden problém, co se těchto metod zabezpečení týká. Jakkoliv bezpečný může nějaký symetrický algoritmus být, v okamžiku snahy realizaci šifrování vznikne podstatná otázka – jakým způsobem předat klíč (který za každou cenu musí zůstat tajný) druhé straně tak, aby k němu získala přístup právě jen tato oprávněná osoba?

2.4.1 Diffie-Hellmanův protokol

Právě problém distribuce klíčů přivedl americké kryptology Whitfielda Diffieho a Martina Hellmana k otevření oblasti kryptografie známé jako šifrování s veřejným klíčem. Proto se první zveřejněný kryptosystém tohoto druhu z roku 1976, na kterém společně pracovali, jmenuje Diffie-Hellmanova výměna klíčů (správně by měl nést název Diffie-Hellman-Merklova výměna klíčů, neboť Ralph Merkle se na jeho vývoji též přímo podílel).

Princip tohoto konceptu spočívá v tom, že dva subjekty, které mají zájem na vzájemné diskrétní komunikaci, sdílejí neskrytě jeden klíč, který jim umožní další výměnu informací, jejíž charakter je již víceméně bezpečný (byť se realizuje nezabezpečenými kanály). Nejsnazší pro pochopení, jak lze něco takového realizovat bude, když uvedu jednoduchý příklad. Příklad jsem převzal z [Diffie-Hellman], využívá se v něm matematická operace modulo[14].

1. Osoba A a osoba B se dohodnou, že použijí prvočíslo „p=23“ a základ „g=5“.
2. Osoba A si zvolí tajné číslo „a=6“ a osobě B zašle vypočtenou hodnotu „$A=g^a \bmod p$“. Dosadíme tedy hodnoty a vypočteme: „$A=5^6 \bmod 23=8$“.
3. Osoba B si zvolí tajné číslo „b=15“ a osobě B analogicky k bodu 2 zašle vypočtenou hodnotu „$B=g^a \bmod p$“. Výpočet vypadá takto: „$B=5^{15} \bmod 23=19$“.
4. Tato čísla – „19“ a „8“ jsou tedy veřejná a A a B je využijí k následujícím výpočtům.
5. A vypočítá „$s=B^a \bmod p$“. „$19^6 \bmod 23 = 2$“.
6. B vypočítá „$s=A^b \bmod p$“. „$8^{15} \bmod 23 = 2$“.

[14] Modulo je matematická operace, která souvisí s celočíselným dělením, vyjadřuje zbytek po dělení dvou čísel a zkracuje se jako „mod“. Takž např. 5 mod 2 = 1, 21 mod 6 = 3, ale 9 mod 3 = 0 (9 je celočíselně dělitelné číslem 3).

7. V tuto chvíli tedy již obě osoby mají stejný klíč, který uchovají v tajnosti a použijí ho pro vzájemnou komunikaci. Přestože si vyměnily veřejně podklady pro jeho výpočet, díky matematickým principům ho znají pouze A a B!

Samozřejmě, že v praxi je to o něco složitější, těžko by někdo použil jako klíč k šifrování číslo 2, ale uvedený příklad by měl alespoň ilustrovat základní myšlenku této výměny klíčů. To naznačuje jeden z problémů tohoto protokolu, a sice potřebu zvolit čísla a, b, p o mnoho vyšší, než je uvedeno výše. Též je třeba hodnoty a, b při každé další komunikaci obměňovat a zajistit potvrzení totožnosti druhé strany, na což už protokol výměny klíčů sám o sobě nestačí. Pakliže by osoba „A“ uskutečnila výměnu skrze Diffie-Hellmanův protokol s osobou „C“ namísto s osobou „B“ a naopak, mohla by osoba „C“ luštit výměnu šifrovaného textu těchto dvou osob. Při striktním dodržení těchto pravidel se otázka prolomení šifrování rovná vyřešení tzv. Diffie-Hellmanova problému, který spočívá v obtížnosti provedení reverzní operace [Diffie-Hellman2].

Je třeba si též uvědomit, že tento protokol neposkytuje v základu ověření totožnosti komunikujících stran. Z tohoto důvodu vznikaly postupem času další algoritmy, které plnily více funkcí.

2.4.2 RSA

Název tohoto algoritmu vznikl podle jmen jeho tvůrců – Rona Rivesta, Adiho Shamira a Leonarda Adlemana. Jedná se pravděpodobně o první algoritmus, který lze použít k digitálním podpisům i k šifrování zpráv. Zprávy, zašifrované veřejným klíčem, se dají dešifrovat pouze privátním klíčem. Klíče se tvoří pomocí určitých matematických pravidel, postup jsem převzal z [RSA] a [KODL, 1996, s. 157].

Nejprve se zvolí dvě rozdílná prvočísla „p“ a „q“, nejlépe náhodně, podobně jako v Diffie-Hellmanově protokolu. Vypočte se hodnota „n=p.q“ („n“ se použije jako modulus pro veřejný i tajný klíč). Pomocí Eulerovy funkce[15] vypočteme „$\varphi(pq) = (p-1)(q-1)$“. Podobný výpočet provedeme ještě jednou, tentokrát zvolíme „e“, pro které platí: „$1 < e < \varphi(pq)$“, „e“ a „$\varphi(pq)$“ mají jen jednoho společného dělitele – číslo „1“. Číslo „e“ se použije pří výpočtu veřejného klíče jako mocnitel (exponent). Pro výpočet soukromého klíče

[15] Eulerova funkce se značí φ(n). φ(n) znázorňuje počet všech přirozených čísel, pro která platí, že jsou větší nebo rovna číslu 1 a zároveň menší nebo rovna číslu n a zároveň největší společný dělitel čísel k a n je 1. Pro prvočíslo p tedy platí: φ(p) = p-1, pro n=9 platí: φ(9) = 6. Vlastnost této funkce vhodná pro použití v kryptografii je, že není znám efektivní algoritmus, který by vypočetl Eulerovu funkci bez znalosti rozkladu jejího argumentu.

je třeba vypočítat číslo „d“ pomocí modula a „$\varphi(pq)$“ (často se využívá rozšíření Euklidova algoritmu[16], ale do podrobností netřeba zabíhat), číslo „d“ se použije též jako mocnitel.

Důležité je si uvědomit, že podobně jako u ostatních metod, ja RSA velmi bezpečné pouze za určitých podmínek. Mimo jiné – veřejný a soukromý klíč se odvozuje ze dvou velkých, několika set místných prvočísel [KODL, 1996, s. 157], nesmí se použít stejný klíč pro šifrování zprávy a digitální podpis [RSA2], ověřuje se totožnost druhé strany komunikace například pomocí digitálních certifikátů, přidávají se „vycpávky“[17] do otevřeného textu před šifrováním atd. Podepisování zpráv se realizuje za pomoci hashovací funkce (viz kapitola 2.5 Kryptografické hashovací funkce).

2.4.3 ElGamal

ElGamalův kryptosystém je asymetrický algoritmus založený na Diffie-Hellmanově výměně klíčů. Byl publikovaný Taherem ElGamalem roku 1985 [Taher]. ElGamalovo šifrování se používá v softwarech pod licencí GNU, raných verzích PGP a dalších kryptosystémech.

Podobně jako RSA sestává ElGamal ze tří fází: generování klíče, šifrovacího algoritmu a dešifrovacího algoritmu. Lze ho použít jak pro šifrování zpráv, tak pro digitální podpis, ačkoliv pro digitální podpis se častěji využívá DSA (viz kapitola 2.4.4 DSA).

Generování klíče probíhá tak, že vytvoříme skupinu „G“ s „q“ elementy za pomocí generátoru „g“. Osoba A zvolí náhodně číslo „x“ z množiny {0, …, q-1}, které slouží jako její privátní klíč. Z privátního klíče vypočítá hodnotu „$h=g^x$“, kterou zveřejní společně s popisem „G“, „q“ a „g“, tyto 4 elementy slouží jako její veřejný klíč.

Pakliže chce osoba B zaslat osobě A šifrovaný text, šifrování využívá tzv. sdíleného tajemství „$s= h^y$“, které se mění s každou zprávou. Jako šifrový text se zasílá „(c_1, c_2)“, kde „$c_1=g^y$“ a „$c_2=m‘.s$“. „m‘“ je obraz zprávy a element ze skupiny „G“.

Osoba A přijme šifrový text „(c_1, c_2)“, vypočítá sdílené tajemství „$s=c_1^x$“ a obraz zprávy „$m‘=c_2.s^{-1}$“, který poté převede do otevřeného textu „m“.

ElGamalův algoritmus se často využívá v hybridních kryptosystémech, kde zpráva samotná je zašifrována symetrickou šifrou a klíč zprávy se zašifruje pomocí ElGamalova algoritmu.

[16] Metoda pro nalezení největšího společného dělitele.
[17] Znaky, slova nebo slovní spojení, která nemají v komunikaci význam a slouží pouze pro ztížení případné kryptoanalýzy.

Bezpečnost ElGamalova šifrování záleží na vlastnostech skupiny „G“ a využití tzv. kryptografických „vycpávek“. Pokud ve skupině „G“ platí tzv. Diffie-Hellmanův výpočetní předpoklad[18], pak je šifrovací funkce jednocestná (vysoká obtížnost až nerealizovatelnost vypočtení inverzní funkce), pokud však platí Diffie-Hellmanův „rozhodovací“ předpoklad[19], pak se šifrování považuje pouze za sémanticky bezpečné[20]. Hlavní slabina ElGamalova algoritmu je v tom, že pokud známe „(c_1, c_2)“ otevřeného textu „m“, pak lze snadno určit odpovídající šifrování „(c_1, $2c_2$)“ otevřeného textu „2m“, přičemž tato slabina se údajně objevuje i u RSA [DOLEV].

2.4.4 DSA

DSA je zkratka pro algoritmus digitálního podpisu (Digital Signature Algorithm). Jedná se o americký standard uznávaný vládou jako standard pro digitální podpisy. Byl navrhnut institutem NIST roku 1991 a používá se od roku 1993. Standard se dočkal vylepšení v letech 1996 [FIPS-186-1], 2000 a 2009 [FIPS-186-3]. Generování klíčů zahrnuje dvě fáze: volbu parametrů algoritmu a výpočet soukromého a veřejného klíče.

V první fázi se zvolí vhodná hashovací funkce, dříve se jednalo o SHA-1, v současnosti jde většinou o SHA-2. Poté se zvolí délka klíčů s označením „L“ a „N“, která určuje sílu šifrování. Velikost klíčů „L“ je celočíselně dělitelná číslem 64, většinou se používají „L“ rovna 2048 nebo 3072, o kterých se tvrdí, že zajistí bezpečnost po roce 2010, respektive 2030. Zvolíme „N“ korespondující k „L“, takže vznikne pár většinou o hodnotách (2048, 224), (2048, 256) či (3072, 256) [FIPS-186-3]. „N“ určuje délku prvočísla „q“ a zároveň „N“ musí být rovno nebo menší než délka výstupu hashovací funkce (výstup hashovací funkce se značí „H“ nebo přesněji „H(m)“). „L“ určuje délku prvočísla „p“, pro které platí, že „p“ je násobkem „q“. Dále musíme vypočítat „$g= h^{(p-1)/q}$“, kde „h“ je libovolné číslo z množiny {1, …, p-1}. Často se používá „h=2“ [Digital].

Druhá fáze spočívá ve výpočtu klíčů. Privátní klíč „x“ je zvolen náhodnou metodou a platí pro něj, že je větší než 0 a menší než „q“. Veřejný klíč „y“ se vypočítá jako „g^x mod p“. Hodnoty „p“, „q“, „g“ a „y“ jsou veřejné.

[18] Předpoklad, že s náhodně zvoleným generátorem „g“ a náhodnými „a, b“ z množiny „{0, …, q-1}“ je výpočetně neřešitelné zjistit hodnotu „g“ umocněnou na „a.b“.
[19] Předpoklad, že ve skupině „G“ s „q“ počtem elementů generované generátorem „g“ a s daným „g“ umocněným na „a“ a „g“ umocněným na „b“ („a, b“ jsou náhodná celá čísla) působí hodnota „g“ umocněná na „a.b“ jako náhodný prvek ze skupiny „G“. Předpoklad úzce souvisí s obtížností výpočtu diskrétních logaritmů ve skupině „G“.
[20] Tj. nelze získat podstatné informace o otevřeném textu, pokud známe šifrový text a veřejný klíč.

Podepisování zpráv se dle [Digital] realizuje za pomocí nenulových hodnot „r“ a „s“, kde „$r = (g^k \bmod p) \bmod q$“ a „$s = (k^{-1}(H(m) + x.r)) \bmod q$“. Hodnota „k“ je náhodná hodnota větší než 0 a menší než „q“ a liší se u každé zprávy. Ověřování podpisu neuspěje, pokud nejsou splněny tyto podmínky: „$0 < r < q$“, „$0 < s < q$“a „$r=((g^{u1}.y^{u2}) \bmod p) \bmod q$“, kde „$w = (s)^{-1} \bmod q$“, „$u1 = (H(m).w) \bmod q$“ a „$u2 = (r*w) \bmod q$“ [Digital]. Co se týče výpočtů je DSA podobné ElGamalovu schématu pro podpisy.

2.4.5 PGP

PGP je označení pro počítačový program a zkratka pro Pretty Good Privacy (překlad by zněl asi jako „dost dobré soukromí“, takže tentokrát ho nebudu používat, mohlo by to být matoucí). PGP vytvořil Američan Philip Zimmermann roku 1991 a často se využívá k podepisování zpráv, šifrování a dešifrování emailů [RFC-4880]. Funguje na základě procedur jako hashovací funkce, komprese dat[21], symetrická kryptografie a asymetrická kryptografie. Veřejný klíč se propojuje s uživatelským jménem či emailovou adresou. Při používání PGP musíme brát v potaz nepříjemnou vlastnost – absenci zpětné kompatibility. Starší verze PGP totiž nedokážou přeložit šifrované texty vytvořené pomocí novějších verzí PGP, což znamená, že uživatelé se musí dohodnout na používané verzi. Krom digitálního podpisu zajišťuje PGP i kontrolu integrity dat, tedy zda byla zpráva po dokončení změněna. Digitální podpis se realizuje buď algoritmem RSA nebo DSA. Další výhodou, kterou PGP poskytuje je ověření, zda veřejný klíč skutečně patří dané osobě, respektive ověření propojení osoby, reprezentované uživatelským jménem, s veřejným klíčem. Toto ověření se realizuje skrze model nazývaný „síť důvěry“ (z anglického „web of trust“), tedy skrze důvěryhodnou třetí stranu. Rozdíl mezi touto sítí a certifikačními autoritami spočívá především v tom, že „web of trust“ je decentralizovaný (mnoho na sobě nezávislých sítí), zatímco certifikační autorita je model centralizovaný (často entita komerční povahy).

Podle veřejně dostupných informací není známa žádná metoda, která by byla schopná prolomit šifrování realizované pomocí PGP. Bruce Schneier roku 1996 označil tehdejší verzi PGP jako „volně dostupný kryptosystém, který je nejblíže kryptosystémům vojenské úrovně“ [SCHNEIER, 1995, s. 587]. Vzhledem k tomu, že PGP se často aktualizuje a vylepšuje podle požadavků a technického vývoje, je prakticky snazší metodou k odhalení otevřeného textu jiná metoda, než obvyklá kryptoanalýza. V praxi to bývají metody jako

[21] Zakódování informací do tvaru, který má méně bitů, než původní zpráva.

například instalování trojského koně[22] či škodlivého softwaru na zachycení stisků kláves [MCCULLAGH, 2007a] [United, 2002]. Proti těmto metodám jsou však zranitelné všechny kryptografické algoritmy a kryptosystémy. Rozluštění dat zašifrovaných pomocí PGP nebyly schopny instituce jako FBI [WILLAN, 2003], americké celní úřady [United, 2001] a britská policie [LEYDEN, 2007]. Zatímco ve Spojených státech amerických bylo uznáno, že občan má dle zákona a ústavy právo tajit před federálními institucemi své šifrovací klíče [MCCULAGGH, 2007b], ve Spojeném království byl již případ muže odsouzeného za odmítnutí poskytnout údaje vedoucí k rozluštění jeho dat [WILLIAMS, 2009].

[22] Trojský kůň je software, který zdánlivě vykonává prospěšnou funkci a tajně na pozadí zajišťuje neoprávněný přístup k datům či celému počítačovému systému uživatele.

2.5 Kryptografické hashovací funkce

Kryptografické hashovací funkce jsou takové funkce, které z vybraného bloku dat libovolné délky vypočítají řetězec bitů pevné délky. Změněným datům pak odpovídá jiná hodnota hashe. Ideálně by hashovací funkce měla vykazovat několik vlastností. Zaprvé – hodnotu hashe lze snadno spočítat pro jakoukoliv zprávu. Odhalení zprávy se známou hodnotou hashe nelze uskutečnit. Nelze změnit zprávu bez toho, aby nová zpráva měla jinou hodnotu hash než původní zpráva. A konečně – nelze najít dvě rozdílné zprávy takové, aby měly stejnou hodnotu hashe. Kryptografické hashovací funkce se využívají například v digitálních podpisech a dalších formách autentizace, pro kontrolu integrity dat, pro indexování dat v tabulkách, generování pseudonáhodných bitů, generování nových klíčů a hesel ze starých apod.

Kryptografické hashovací funkce jsou často založeny na blokových symetrických šifrách a jednocestných kompresních funkcích[23]. Aby mohla hashovací funkce vytvořit vždy výstup stejné délky, je třeba vstupní data rozdělit na stejně velké bloky, proto jsou kryptografické hashovací funkce podobné blokovým šifrám.

Nutno podotknout, že mnoho hashovacích funkcí není považováno za bezpečné, o tom si více povíme u konkrétních zástupců v následujících podkapitolách.

2.5.1 MD5

MD5 je zkratka pro algoritmus obsahu zprávy verze 5 (Message-Digest algorithm 5). Ačkoliv je prokázáno, že tento algoritmus neoplývá bezpečností, využívá se v současnosti v široké škále bezpečnostních aplikací a pro kontrolu integrity dat (počítačových souborů). Pro digitální podpisy je MD5 naprosto nevhodný [XIAOYUN]. Kontrolní součet MD5 typicky reprezentuje 32-místné hexadecimální[24] číslo.

MD5 vytvořil a vydal Ron Rivest roku 1991 jako náhradu za předchozí verzi MD4. Netrvalo dlouho a i u MD5 byly odhaleny bezpečnostní nedostatky. Poprvé roku 1996, především však roku 2004, od kterého již není doporučováno používat ho pro bezpečnostní účely [viz BLACK] [viz DENGGUO]. Roku 2007 přišla skupina vědců na způsob, jakým

[23] Jednocestná kompresní funkce je taková funkce, která ze dvou vstupů pevné délky vypočítá jeden výstup stejné délky, jako měl jeden ze vstupů. Jednocestná proto, že se považuje za prakticky nemožné získat z výstupu vstupní data. Tím se také jednocestné kompresní funkce liší od komprese dat, neboť komprese dat je v principu funkce proveditelná snadno oběma směry.

[24] Hexadecimální řetězec reprezentuje šestnáctkovou soustavu, kde se používají symboly 0-9 a písmena „A, B, C, D, E, F“, které odpovídají hodnotám 10 až 15. „9AD7“ v šestnáctkové soustavě se do decimální – desítkové – převede jako $(9.16^3) + (10.16^2)+(13.16^1)+(7.16^0)=36864+2560+208+7=39639$.

vytvořit soubory se stejným kontrolním součtem [viz STEVENS]. Tato technika byla roku 2008 použita k padělání certifikátu SSL[25] (MD5 se do verze TLS 1.2, která vznikla roku 2008, používala v pseudonáhodné funkci používané v SSL a TLS). Pro americké vládní instituce je doporučováno realizovat nejpozději během roku 2010 přechod na rodinu kryptografických hashovacích funkcí SHA-2 [viz NIST]. Ve skutečnosti došla situace ohledně nebezpečnosti MD5 ještě mnohem dál, než předchozí věty naznačují. Podle [KLÍMA] bylo již roku 2006 možné prolomit MD5 během jedné minuty.

Přesto, že MD5 není již delší dobu bezpečné, popíši zjednodušeně funkci tohoto algoritmu. MD5 pracuje tak, že vstupní zprávu rozdělí na bloky o velikosti 512 bitů, v případě, že velikost zprávy není dělitelná číslem 512, použije kryptografické „vycpávky" tímto způsobem: jako první použije bit s hodnotou 1 a připojí ho na konec zprávy. Následně připojí tolik nul, aby zbylo 64 bitů. Těchto 64 bitů se doplní řetězcem, který reprezentuje délku původní zprávy. Zpracování bloků zprávy probíhá ve čtyřech kolech, každé sestává z šestnácti operací založených na nelineárních funkcích F, modulární adici[26], a rotaci doleva (viz Příloha č.6 – MD5). Ve funkcích F se používají operace jako XOR, konjunkce, disjunkce a negace.

2.5.2 SHA-2

SHA je zkratka pro „spolehlivý hashovací algoritmus" (Secure Hash Algorithm) publikovaný organizací NIST jako federální standard zpracování informací (Federal Information Processing Standard). V současnosti zahrnuje SHA tři generace algoritmů.
První generace – SHA-1 je původně 160-bitová hashovací funkce podobná MD5. SHA-1 bylo součástí DSA. Brzy po zveřejnění však došlo ke stáhnutí algoritmu z oběhu kvůli podstatným nedostatkům a nahrazení revidovanou verzí.

SHA-2 označuje rodinu dvou podobných hashovacích funkcí s rozdílnou velikostí bloků. Proto se také někdy označují jako SHA-256 a SHA-512 – první z nich používá 32-bitové řetězce a druhá 64-bitové.

SHA-3 jako standard je stále ve vývoji. Označení ponese algoritmus, který vyhraje soutěž nevládních subjektů ve veřejném revizním procesu. K vybrání vítěze má dojít roku 2012.

[25] SSL – Secure Socket Layer – je kryptografický protokol, který má za úkol poskytnout ochranu komunikace v sítích, jako je Internet. Nástupcem SSL je TLS (Transport Layer Security).
[26] Systém aritmetiky, ve kterém se čísla po dosažení určité hodnoty „přetočí" zpět na začátek. Příkladem je otáčení hodinových ručiček.

2.5.3 (H)MAC

V kryptografii je MAC označení pro kód autentizace zpráv (message authentication code). Jako vstup používá algoritmus MAC tajný klíč a zprávu, která má být potvrzena. Označení MAC nese výstup tohoto algoritmu a kromě autentizace zajišťuje i integritu dat. V principu algoritmus funguje podobně, jako symetrická kryptografie – tajný klíč se používá pro šifrování i dešifrování.

HMAC je speciální případ algoritmu MAC založený na využití hashovacích funkcí, ať už MD5 nebo SHA-1. Bezpečnost HMAC potom tedy závisí na bezpečnosti těchto hashovacích funkcí a délce klíče a algoritmus MAC se pak často označuje jako HMAC-MD5 respektive HMAC-SHA1. Přesto podle odborníků [viz SCHNEIER 2005] není aplikace těchto algoritmů v HMAC tolik náchylná k prolomení jako tyto hashovací funkce samotné.

HMAC se podle [RFC-2104] definuje takto: máme funkci „H“, kryptografickou hashovací funkci. Tajný klíč „K“ je zprava doplněn kryptografickými „vycpávkami“ sestávajícími z nul až do velikosti bloku, na kterém operuje funkce „H“. Zprávu k autentizaci označme „m“. „||“ je označení pro zřetězení[27], „XOR“ označení pro exkluzivní disjunkci. Vnější „vycpávky“ značíme „opad“ a vnitřní vycpávky „ipad“ (oboje jsou hexadecimální konstanty o délce jednoho bloku). Pak „HMAC(K,m)“ definujeme jako: „HMAC(K,m) = H((K XOR opad) || H((K XOR ipad) || m))“.

[27] Zřetězení obnáší spojení dvou řetězců v jeden. Například u slov „velko“ a „město“ je zřetězením slovo „velkoměsto“.

2.6 Metody realizace kryptografie

Doposud probírané algoritmy spoléhali ve velké míře na softwarovou implementaci a vcelku konvenční kryptografické metody. To má samozřejmě výhodu v tom, že na relativně malém prostoru a s relativně malými znalostmi jsme schopni vcelku snadno pochopit podstatu problematiky. Už jen z důvodu znalosti, že daná řešení existují, je třeba v této kapitole probrat různé méně tradiční nebo veřejnosti méně dostupné metody používané v kryptografii. Proto bude mít tato kapitola a její podkapitoly velmi stručnou povahu a nebude zabíhat do detailů, konkrétních technických řešení, fyzikálních a jiných přírodních zákonů.

2.6.1 Hardwarová kryptografie

Ačkoliv softwarová kryptografie seznala od nástupu osobních počítačů a jejich zpřístupňování veřejnosti velký rozkvět, stále jsou zde důvody, které právě instituce, kde je účinné šifrování nejvíce potřeba, přiměly využívat k šifrování speciální přístroje. Když jsem dříve mluvil o přístroji Enigma, byl to zrovna jeden z příkladů šifrování strojem. V případě Enigmy se jednalo o rotorový mechanický stroj, který ke své funkci využíval určitý počet koleček, jejichž otáčení a propojování elektrických kontaktů způsobovalo změny průběhu elektrického proudu. Podobných strojů vzniklo v historii několik, více či méně úspěšnějších než Enigma. Z příkladu Enigmy lze odvodit, že právě armáda má tendenci využívat hardwarovou kryptografii – a ne bezdůvodně. Krom armády a dalších vládních institucí se hardwarová kryptografie v dnešní době často používá například u velkých komerčních institucí.

Jaké jsou tedy výhody hardwarové kryptografie oproti té softwarové? Tak například všechny soubory, včetně těch dočasných (o jejichž existenci uživatel běžného osobního počítače ani nemusí mít přehled, přestože tyto soubory mohou obsahovat citlivé informace), lze uchovávat na bezpečném disku. Další výhoda s tím související je ta, že systém většinou obstará veškeré nutné operace sám, bez nutnosti zásahu uživatele (naproti tomu uživatel osobního počítače se mnohdy musí prakticky o vše postarat sám – od volby vhodného softwaru, po opakovanou enkrypci, zajištění bezpečnosti hardwarových prostředků atd.). Podstatnou výhodou hardwarové enkrypce je fakt, že u valné většině používaných algoritmů dosahuje větších rychlostí, než lze docílit na běžném osobním počítači [SCHNEIER, 1996, s. 322]. Pakliže považujeme bezpečnost šifrování za důležitější, než rychlost jeho realizace, dokáže i v tomto ohledu hardwarová kryptografie nabídnout lepší řešení. Důvodem je to, že algoritmus, fungující na běžném počítači, nemá v podstatě žádnou

fyzickou ochranu, zatímco speciální přístroje mohou být bezpečně zapouzdřeny. A co víc – vyskytují se i případy zvláštní ochrany, jako například opatření součástek chemickou látkou, která způsobí, že jakýkoliv pokus o zásah způsobí zastavení funkce nebo zničení. Krom toho celý přístroj nebo důležité součástky mohou být chráněny proti vysílání elektromagnetického záření, jež může odhalit právě probíhající operace a vést k úspěšné kryptoanalýze. Posledním podstatným důvodem je snadná aplikace, která se dá provést i u komunikace probíhající na přístrojích jako telefony, faxy, datové linky. S tím souvisí i to, že finančně se více vyplatí k podobným přístrojům zapojit speciální šifrovací stroj, než instalovat do nich procesor se softwarem. Podle [SCHNEIER, 1996, s. 322-323] se dokonce i u osobních počítačů vyplatí realizovat šifrování za použití speciálního hardwaru, ať už z důvodu, že je snazší zapojit další přístroj do sestavy, než instalovat nový software a zajišťovat jeho správnou funkčnost (s tím, že spoléháme na to, že tvůrce softwaru nemá žádné postraní úmysly) nebo proto, že softwarová řešení jako taková mohou uživatele „obtěžovat“ požadavky na podporu jejich regulérní funkce (software většinou bývá poloautomatický, pokud není přímo součástí operačního systému.. to znamená, že čas od času vyžaduje zásah uživatele).

V současnosti se využívají tři druhy šifrovacího hardwaru: šifrovací moduly na ověřování hesel a distribuci klíčů (např. v bankovní sféře), šifrovací boxy specializované na telekomunikační linky a komponenty, které fungují jako součást osobních počítačů.

2.6.2 Kvantová kryptografie

Trendem ve výpočetní technice je miniaturizace. Přestože si to běžný uživatel ani nemusí uvědomovat, osobní počítače fungují na fyzikálních zákonech. Co se ale stane, pokud miniaturizace dosáhne pomocí nejmodernějších technik takového stupně, kdy se dále nebude hovořit o obvodech, součástkách a komponentách, jako spíš o jednotlivých atomech, jejich částech a procesech, kterými se řídí jejich existence? V takovém případě se jejich činnost bude řídit zákony kvantové mechaniky [KODL, 1996, s. 221]. Ač to může znít jako utopie, již na začátku osmdesátých let to bylo prokázáno a od té doby se vytvořilo několik pokusných modelů. Jedná se například o funkční model kvantové distribuce klíčů pánů Bennetta a Brassarda a komunikaci britského Telecomu na vzdálenost deseti kilometrů skrze optické vlákno [viz TOWNSEND].

Jeden z principů kvantové mechaniky je tzv. vlno-částicová dualita. To znamená, že entity, které normálně vnímáme jako pevné částice např. atomy) se za určitých okolností chovají jako vlnění a entity, které běžně popisujeme jako vlnění jindy jako částice. Prvním důsledkem je skutečnost, že atomy mohou existovat pouze v diskrétních energetických

stavech. Když nějaký atom přechází z jednoho stavu do druhého, vyzařuje nebo pohlcuje energii v přesně stanovených množstvích – „kvantech“ – zvaných fotony, které lze chápat jako částice reprezentující světelné vlnění. Vodíkové atomy mohou například zaznamenávat bity informace podobně jako paměťové prvky klasického počítače. Atom v klidovém stavu může představovat nulu a ve vybuzeném stavu jedničku [KODL 1996, s. 222-223]. Operace jako zápis informace pak lze provádět například ozářením atomu laserovým paprskem, což vede k pohlcení nebo vyzáření fotonu [PHOENIX, 1993, s. 65-75]. Pro přenos informace mohou sloužit optická vlákna přenášející fotony (a tedy i bity informace) [KODL, 1996, s. 226].

O fotonech, které kmitají v jedné rovině, hovoříme jako o polarizovaném světle. Díky speciálním polarizačním filtrům, které propustí jen fotony s určitou polarizací, lze využít těchto vlastností ke generování náhodných hodnot (což lze využít například u tajných klíčů). Zjednodušeně řečeno v komunikaci informací lze využít těchto vlastností s revolučními důsledky, což ilustruji na příkladu z [SCHNEIER, 1996, s. 745-746] a [KODL, 1996, s.230-231].

Jestliže osoba „A“ vyšle osobě „B“ sled fotonových impulsů, jsou tyto impulsy polarizované v jednom ze čtyř směrů – horizontálním, vertikálním (souhrnně označované jako rektilineární); levoúhlopříčném a pravoúhlopříčném (souhrnně označované jako diagonální). Osoba „A“ tedy vyšle určitou posloupnost polarizovaných fotonů, graficky znázorněno to může vypadat nějak takto: „ ||/--\-|-/ „. Osoba „B“ vlastní přístroj zvaný polarizační detektor, který je schopen zjistit, zda se jedná o rektilineární nebo diagonální polarizace, ovšem vzhledem k zákonům kvantové mechaniky nelze zjišťovat u jednoho fotonu oba typy polarizace zároveň. Osoba „B“ tedy bude náhodně nastavovat svůj detektor, dosáhne například tohoto nastavení: „ x++xxx+x++ “. Jestliže bude pro daný foton nastavení detektoru odpovídat, pak lze určit způsob, jakým osoba „B“ polarizovala foton. Špatné nastavení detektoru však vede k náhodnému výsledku, který není osoba „B“ schopna rozpoznat. Dostane pak tedy například tento výsledek: „ /|-\/\-/-| „. Prostřednictvím otevřeného komunikačního kanálu pak subjekt „B“ sdělí subjektu „A“ sled použitých nastavení detektoru. Subjekt „A“ v odpovědi oznámí, která nastavení detektoru byla správná, v uvažovaném příkladu se jedná o nastavení pro impulsy 2, 6, 7 a 9. Subjekty tedy budou používat takové způsoby polarizace, které byly detekovány správně. Pomocí předem dohodnutého pravidla se pak například mohou horizontální a levodiagonální polarizace reprezentovat jako binární hodnota „1“ a vertikální a pravodiagonální jako hodnota „0“. V dané situaci by tedy

z posloupnosti „ |\-- „ vygenerovaly bity „0, 0, 1, 1“. Takto získané hodnoty mohou sloužit jako tajný klíč, pakliže jich je dostatečné množství.

Co je ovšem na kvantové mechanice a předchozím příkladu nejlepší je skutečnost, že jakékoliv odposlouchávání komunikace subjekty „A“ a „B“ rozpoznají. Pokud by totiž subjekt „C“ chtěl monitorovat jejich komunikaci, musel by postupovat podobně jako subjekt „B“ – náhodně určit, v jaké posloupnosti bude zjišťovat který druh polarizace. Ovšem v takovéto kvantové komunikaci neexistuje něco jako pozorovatel, který nemá vliv na systém samotný, protože špatné nastavení polarizačního filtru (které se statisticky blíží pravděpodobnosti 50%) způsobí, že se polarizace fotonu změní, tudíž výsledky měření osob „A“ a „B“ nebudou odpovídat a subjekty to okamžitě zjistí. Jakýkoliv pokus o odposlouchávání tohoto typu komunikace ji tedy zákonitě přeruší [SCHNEIER, 1996, s. 746].

Krom výše popsaných způsobů využití kvantové mechaniky se spekuluje o možnosti rychlejšího počítání nejsložitějších matematických operací v budoucnu, jako například problém faktorizace velkých čísel[28]. To by ovšem znamenalo revoluci pro konvenční kryptografické metody jak je známe v dnešní době.

[28] Na obtížnost rozkladu mnohomístného čísla na prvočinitele spoléhá mnoho kryptografických metod – např. RSA a metody asymetrické kryptografie obecně.

2.7 Kryptoanalýza

Kryptoanalýza je věda zabývající se rozkrýváním zašifrovaných zpráv bez přístupu ke klíči. Úspěšná kryptoanalýza může získat otevřený text nebo klíč nebo odhalit slabé místo kryptosystému, které nakonec umožní získat otevřený text. Snaha o provedení kryptoanalýzy se označuje jako luštění [KODL, 1996, s. 26]. Kryptoanalýza a kryptografie jsou vzájemně velmi těsně propojeny – staré, prolomené metody se nahrazují novějšími, u kterých se opět kryptoanalýza snaží odhalit slabiny. Teorie kryptoanalýzy předpokládá, že kryptoanalytik bude mít přístup jednak ke komunikaci odesílatele a příjemce, jednak k informaci o použitém kryptografickém algoritmu. Kryptoanalýza má několik základních způsobů luštění, které popíši v následujících podkapitolách. Vyjmenovat všechny způsoby luštění a jejich popis by ovšem bylo svým rozsahem na další bakalářskou práci, je však třeba si uvědomit, že úspěšný kryptograf musí znát i způsoby kryptoanalýzy, jinak nebude schopen vyvinout bezpečnou metodu šifrování.

2.7.1 Luštění se znalostí šifrového textu

Luštění se znalostí šifrového textu (anglicky „ciphertext-only attack“ nebo také „known ciphertext attack“) předpokládá, že útočník má přístup pouze k šifrovému textu několika zpráv. Útok se považuje za zcela úspěšný, pokud z těchto šifrových textů kryptoanalytik získá otevřené texty nebo ještě lépe klíč. Tento útok umožňují statistické metody jako již zmíněná frekvenční analýza.

V minulosti došlo k úspěšným útokům tohoto typu například u Enigmy, protokolu WEP a u algoritmu RC4, kdy první verze sítě VPN[29] společnosti Microsoft užívaly stejný klíč pro odesílatele i příjemce).

2.7.2 Luštění se znalostí otevřeného textu

Kryptoanalytik má krom zašifrovaných textů několika zpráv přístup i k jejich otevřenému textu (anglicky je tato metoda označována za „known-plaintext attack“). Za úkol tedy má odvodit použitý klíč (či klíče).

Historie zná takových případů několik, např. za druhé světové války Němci odesílali přes den ve stejný čas informace o počasí a díky pevnému stylu zpráv se zde slovo „počasí“ (německy Wetter) vyskytovalo vždy na stejném místě, stejně jako nebylo těžké se

[29] VPN – Virtual Private Network – je propojení dvou počítačů s více či méně úspěšným utajením jejich komunikace. Vzdálený počítač se připojí k jinému tak, že to působí jako běžné spojení v místní síti.

znalostí aktuálního počasí na daném místě odhadnout další obsah zprávy. Klasické šifry, jako Caesarova a obecně i monoalfabetická substituční jsou též náchylné k úspěšnému luštění se znalostí otevřeného textu. V případě Caesarovy šifry k tomu dokonce stačí znalost jediného písmene a jeho pozice v otevřeném textu.

2.7.3 Luštění se znalostí vybraných otevřených textů

Při použití této metody kryptoanalýzy má útočník přístup nejen k šifrovým textům a odpovídajícím otevřeným textům, ale je také schopen způsobit, že jím zvolené otevřené texty jsou šifrovány danou kryptografickou metodou a následně získá přístup i k těmto šifrovým textům (v angličtině je tato metoda kryptoanalýzy známá jako „chosen-plaintext attack“). Ačkoliv se to na první pohled zdá nerealizovatelné (nikdo by přeci útočníkovi dobrovolně nezašifroval zprávu na požádání vlastním klíčem), v případě šifrování s veřejným klíčem to nepředstavuje žádný problém [WOBST, 2007, s. 64]. Každá šifra, která poskytuje ochranu proti luštění se znalostí vybraných otevřených textů poskytuje ochranu i proti luštění se znalostí šifrového textu a luštění se znalostí otevřeného textu.

Zvláštním případem této metody je tzv. adaptivní metoda luštění se znalostí vybraných otevřených textů, kdy kryptoanalytik upravuje svůj výběr otevřených textů k zašifrování podle předchozích výsledků. U luštění se znalostí vybraných otevřených textů si kryptoanalytik vybíral k zašifrování jeden velký blok otevřeného textu, u adaptivní metodu si vybírá menší blok otevřeného textu a potom vybere jiný blok na základě výsledků získaných prvým výběrem atd. [KODL, 1996, s. 27-28].

2.7.4 Luštění se znalostí vybraných šifrových textů

Tato metoda kryptoanalýzy se podobá předchozí, rozdíl je v tom, že útočník může dešifrovat dle svého výběru různé šifrové texty a získá tak přístup k otevřenému textu [KODL, 1996, s. 28]. Tento útok (anglicky označovaný za „chosen-ciphertext attack“) je opět aplikovatelný především na algoritmy veřejného klíče a na digitální podpisy [WOBST, 2007, s. 64].

V praxi lze tento druh kryptoanalýzy využít např. u algoritmu ElGamal, které je jinak sémanticky bezpečné před luštěním se znalostí vybraných otevřených textů nebo u raných kryptografických „vycpávek“ šifrování RSA (používalo se v protokolu SSL), kde použití adaptivní metody luštění se znalostí vybraných šifrových textů odhalilo klíč pro danou

relaci[30]. V kryptosystémech, které používají stejný mechanismus pro šifrování i dešifrování je proto třeba implementovat autentizaci uživatelů a podepisování zpráv, aby útočník neměl možnost „podstrčit“ kryptosystému své zprávy k dešifrování.

2.7.5 Luštění se znalostí vybraného klíče

V angličtině se metoda luštění se znalostí vybraného klíče označuje jako „chosen-key attack“ nebo „related-key attack“. Neznamená, že kryptoanalytik je schopen „podstčit“ do kryptosystému svůj šifrovací klíč, ale že má určité znalosti o vztazích mezi různými klíči. V praxi tato metoda byla použita například proti již zmíněnému WEP. Každý klient sítě Wi-Fi a každý přístupový bod bezdrátové sítě totiž sdílejí stejný WEP klíč. Jelikož šifrování u WEP používá algoritmus RC4, proudovou šifru, je důležité, aby žádný klíč nebyl použit víckrát. WEP tudíž zahrnuje 24-bitový inicializační vektor v paketech každé zprávy a klíč RC4 pro daný paket je zřetězením tohoto vektoru a samotného klíče WEP. Jelikož klíče WEP se musí měnit manuálně, často ke změně klíče dochází velmi nepravidelně a zřídkakdy. Tudíž tento druh luštění je proti WEP úspěšně realizovatelný často během několika minut [viz The Feds].

2.7.6 Další metody kryptoanalýzy

Doposud jsme se zabývali čistě analytickými konvenčními metodami, ovšem často jsou nejsnazším způsobem k prolomení šifrování např. metody známé jako „pendreková kryptoanalýza“ (nebo anglicky – „rubber-hose cryptoanalysis“) [KODL, 1996, s. 28]. Princip těchto metod je velmi jednoduchý – útočník užívá praktik jako výhružky, mučení, korupce nebo vydírání do doby, než získá tajný klíč. Výhoda tohoto způsobu je jasná – není třeba realizovat časově náročnou, někdy i prakticky nemožnou kryptoanalýzu. Proto by měly i osoby, zainteresované v nějakém významném a důležitém kryptosystému, být považovány za jeho součást a patřičně chráněny a monitorovány.

2.7.7 Bezpečnost algoritmů

Různé algoritmy mají různý stupeň bezpečnosti, který závisí na tom, kolik úsilí je třeba k jejich prolomení. Za pravděpodobně bezpečné je považováno i takové řešení, kdy cena k prolomení algoritmu je vyšší než hodnota zašifrovaných dat, kdy doba k prolomení algoritmu je delší než doba, po kterou zašifrovaná data musí zůstat v tajnosti nebo v případě, že množství dat zašifrované jedním klíčem je menší než množství dat potřebné k prolomení

[30] Relace – z anglického session – označuje síťové spojení mezi klientem a serverem.

algoritmu [KODL, 1996, s. 29]. Formálně je to pouze pravděpodobně bezpečné proto, že nikdo si není jist, jaké možnosti bude mít kryptoanalýza v budoucnosti.

Podle [KNUDSEN] se stupně prolomení klasifikují podle závažnosti takto:

1. Totální prolomení (anglicky „total break“), při kterém kryptoanalytik nachází šifrovací klíč.
2. Globální dedukce, při které útočník nachází algoritmus ekvivalentní k tomu použitému při šifrování nebo dešifrování, nezná však tajný klíč.
3. Lokální dedukce, kdy útočník odhalí otevřené či šifrové texty, které dříve neznal.
4. Informační dedukce, když útočník získá nějakou informaci o otevřeném či šifrovém textu nebo klíči (odhalí jejich formu, několik bitů klíče apod.).

Oproti relativní (pravděpodobné) bezpečnosti je absolutní bezpečnost založena na tom, že útočník není schopen získat otevřený text ani pokud má k dispozici libovolné množství šifrového textu. Toto zaručuje pouze správná aplikace jednorázového hesláře, u ostatních metod lze realizovat postup totálních zkoušek (neboli útok hrubou silou) a postupným zkoušením možných klíčů ověřovat, zda získaný text dává smysl.

Kryptografie se však nejvíce zaměřuje na výpočetně bezpečné algoritmy, tedy takové, které nemohou být prolomitelné za použití soudobých nebo v brzké budoucnosti očekávaných kryptoanalytických metod. Složitost luštění se skládá z faktorů jako datová složitost (množství dat vyžadovaných jako vstup pro luštění), výpočetní složitost (čas potřebný pro luštění) a paměťové nároky (rozsah paměti počítače nutný k luštění). V praxi by měla být snaha o dosažení maximalizace všech tří faktorů a navrhování takových kryptosystémů, o nichž se předpokládá, že ani technika dostupná za mnoho let nebude schopná je prolomit [KODL, 1996, s. 30-31].

3. Závěr

Bakalářská práce podává náhled do problematiky moderní elektronické komunikace, poskytuje výčet kryptografických metod a algoritmů s příklady jejich použití a objasňuje základy některých kryptoanalytických postupů.

Dokument si neklade za cíl poskytnout kompletní výpis a definice všech momentálně používaných šifrovacích algoritmů a standardů nebo úplnou charakteristiku problematiky v celé její šíři, což zejména vzhledem k omezenému prostoru dalece přesahuje možnosti tohoto druhu akademických prací. Místo toho by měla být práce chápána jako úvod do kryptografie a přehled oblastí, na které se zájemce o toto složité, rozmanité a zajímavé téma může ve svém dalším studiu zaměřit. Stejně tak nelze očekávat, že pouze s vědomostmi, obsaženými v této práci lze dosáhnout komplexních řešení pro bezpečnost dat v informatice, vzhledem k tomu, že tato problematika přesahuje téma kryptologie.

Při implementaci daných konceptů informační bezpečnosti je třeba nejprve pochopit všechny procesy, kterými se zpracování a moderní komunikace informací řídí a na tomto základě zabezpečit každý z prvků systému proti úniku informací, poškození, zkreslení či jinému nežádoucímu jevu. Vzhledem k odborné náročnosti by zejména v případě aplikací v komerční sféře měly být využity služby profesionálů počínaje zpracováním bezpečnostní analýzy, projektováním vhodných řešení, jejich realizací a konče správou a údržbou výpočetních a datových prostředků v daném systému.

Seznam použitých zdrojů

- AL-KADI, Ibrahim A. The origins of cryptology: The Arab contributions. *Cryptologia*. 1992, vol. 16, no. 2, s. 97–126.

- BENNETT, C. H.; BRASSARD, G.; EKERT, A. K. Quantum Cryptography. *Scientific American*. 1992, v. 267, n. 4, s. 50-57.

- BLACK, J.; COCHRAN, M.; HIGHLAND, T. A Study of the MD5 Attacks : Insights and Improvements. In *List of Papers, John R. Black, March 2006* [online]. Colorado : John R. Black, 2006 [cit. 2010-05-05]. Dostupný z WWW: <http://www.cs.colorado.edu/~jrblack/papers/md5e-full.pdf>.

- CALLAS, J. et al. RFC 4880 : Open PGP Message Format. In *IETF Documents, Network Working Group* [online]. Sommerville (MA) : IHTFP Consulting, Internet Engineering Task Force, November 2007 [cit. 2010-05-05]. Dostupný z WWW: <http://tools.ietf.org/html/rfc4880>.

- Dálnopis po 71 letech v Česku skončí. In *Novinky.cz* [online]. Praha : Borgis a.s., 2003-, 1. července 2008 [cit. 2010-05-05]. Dostupný z WWW: <http://www.novinky.cz/ekonomika/143861-dalnopis-po-71-letech-v-cesku-skonci.html>.

- Diffie-Hellman key exchange. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001-, last modif. 17 May 2010 [cit. 2010-05-05]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange**>.**

- Diffie-Hellman problem. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001-, last modif. 25 March 2010 [cit. 2010-05-05]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Diffie–Hellman_problem**>.**

- Digital Signature Algorithm. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001-, last modif. 16 April 2010 [cit. 2010-05-05]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Digital_Signature_Algorithm**>.**

- DOLEV, D.; DWORK, C.; NAOR, M. Nonmalleable Cryptography. *SIAM Journal on Computing*. 2000, vol. 30, issue 2, s. 391-437.

- ELGAMAL, Taher. A public-key cryptosystem and a signature scheme based on discrete logarithms. *Crypto84*. 1984, s. 10-18.

- Ethernet válcuje ostatní síťová řešení, ukázal průzkum. In *Control Engineering Česko* [online]. Warszawa : Trade Media International Holdings, 2009-, 20. července 2009 [cit. 2010-05-05]. Dostupný z WWW: <http://www.controlengcesko.com/menu-gorne/artykuly/artykul/article/ethernet-valcuje-ostatni-sitova-reseni-ukazal-pruzkum.html>.

- *FIPS1861 : Federal Information Processing Standards Publication* [online]. Washington (D.C.) : National Institute of Standards and Technology, U.S. Department of Commerce, 1998 [cit. 2010-05-05]. Dostupný z WWW: <http://www.mozilla.org/projects/security/pki/nss/fips1861.pdf>.

- *FIPS1863 : Federal Information Processing Standards Publication* [online]. Washington (D.C.) : National Institute of Standards and Technology, U.S. Department of Commerce, 2009 [cit. 2010-05-05]. Dostupný z WWW: <http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf>.

- GARFINKEL, S. *PGP : pretty good privacy : šifrování pro každého*. Přel. Jaroslav Dudr. 1. vyd. Praha : Computer Press, 1998. xxxi, 373 s. ISBN 80-7226-054-5.

- CHEUNG, Humphrey. The Feds can own your WLAN too. In *SmallNetBuilder, 31 March 2005* [online]. Earlysville (VA) : Pudai LLC, 2005 [cit. 2010-05-05]. Dostupný z WWW: <http://www.smallnetbuilder.com/index.php?option=com_content&task=view&id=24251&Itemid=100>.

- IPv6 v MS Windows Vista. In *Lupa : Server o českém Internetu* [online]. Praha : Internet Info s.r.o., 2007-, 1. února 2007 [cit. 2010-05-05]. Dostupný z WWW: <http://www.lupa.cz/clanky/ipv6-v-ms-windows-vista/>.

- KAHN, David. *The Codebreakers : The Story of Secret Writing (abridged by the author)*. 1. vyd. New York : New American Library, 1973. 476 s.

- KLÍMA, Vlastimil. Tunnels in Hash Functions : MD5 Collisions Within a Minute. In *Cryptology ePrint Archive Report 2006/105, 18 March 2006* [online]. Santa Barbara (CA) : International Association for Cryptologic Research, 2006 [cit. 2010-05-05]. Dostupný z WWW: <http://eprint.iacr.org/2006/105.pdf>.

- KNUDSEN, L. R. *Block Ciphers – Analysis, Design and Applications*. Aarhus, 1994. 269 s., Ph.D. Thesis. Aarhus University, Faculty of Science, Department of Computer Science.

- KODL, J. ; PŘIBYL, J. *Ochrana dat v informatice*. 1. vyd. Praha : Vydavatelství ČVUT, 1996. 299 s. ISBN 80-01-01664-1.

- KRAWCZYK, H. et al. RFC 2104 : HMAC, Keyed-Hashing for Message Authentication. In *IETF Documents, Network Working Group* [online]. New York : IBM TJ. Watson Research Center, February 1997 [cit. 2010-05-05]. Dostupný z WWW: <http://tools.ietf.org/html/rfc2104>.

- LEYDEN, John. Animal rights activist hit with RIPA key decrypt demand : UK terror law change kicks in. In *The Register* [online]. London : Situation Publishing, 14th November 2007 [cit. 2010-05-05]. Dostupný z WWW: <http://www.theregister.co.uk/2007/11/14/ripa_encryption_key_notice/>.

- MCCULLAGH, Declan. Feds use keylogger to thwart PGP, Hushmail. In *News Blog, July 10, 2007* [online]. San Francisco (CA) : CNET News, 2007 [cit. 2010-05-05]. Dostupný z WWW: <http://news.cnet.com/8301-10784_3-9741357-7.html>.

- MCCULLAGH, Declan. Judge : Man can't be forced to divulge encryption passphrase. In *News Blog, December 14, 2007* [online]. San Francisco (CA) : CNET News, 2007 [cit. 2010-05-05]. Dostupný z WWW: <http://news.cnet.com/8301-13578_3-9834495-38.html>.

- NAVRÁTIL, Daniel. Splyne v 21. století výpočetní a komunikační technika. In *Fakulta informatiky Masarykovy univerzity*. Brno : Fakulta informatiky Masarykovy univerzity, 2000 [cit. 2010-05-05]. Dostupný z WWW: <http://www.fi.muni.cz/usr/jkucera/pv109/2000/xnavrat1.htm>.

- *National Institute of Standards and Technology* [online]. Washington (D.C.) : NIST, last updated 10 December 2008 [cit. 2010-05-05]. NIST's Policy on HASH Functions. Dostupný z WWW: <http://csrc.nist.gov/groups/ST/hash/policy.html>.

- PETERS, Thomas. Management in chaotischen Zeiten. *Das Tom Peters Seminar*. Frankfurt : Campus Verlag, 1995. S. 27.

- PHOENIX, S.J.D.; TOWNSEND, P.D. Quantum Cryptography and Secure Optical Communication. *BT Technology Journal*. 1993, v. 11, n. 2, s. 65-75.

- PIPER, F.C. ; MURPHY, S. *Kryptografie*. Přel. Pavel Mondschein. 1. vyd. Praha Dokořán, 2006. 157 s. ISBN 80-7363-074-5.

- POP, Tomáš. *Kryptografie a její použiti při zabezpečeném přenosu datových souborů*. Praha, 2006. 52 s., Bakalářská práce. Univerzita Karlova v Praze, Matematicko-fyzikální fakulta, Ústav formální a aplikované lingvistiky. Vedoucí bakalářské práce RNDr. Drahomíra Doležalová-Spoustová.

- RARITY, J.G.; TAPSTER, P.R.; TOWNSEND, P.D. Enhanced Single Photon Fringe Visibility in a 10 km-Long Prototype Quantum Cryptography Channel. *Electronics Letters*. 1993, vol. 28, n. 14, s. 1291-1293.

- RSA. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001-, last modif. 20 May 2010 [cit. 2010-05-05]. Dostupný z WWW: <http://en.wikipedia.org/wiki/RSA**>.**

- *RSA Algorithm* [online]. Sydney : DI Management Services, c2002-2010 [cit. 2010-05-05]. Dostupný z WWW: <http://www.di-mgt.com.au/rsa_alg.html>.

- *Serpent home page* [online]. Cambridge : Computer Laboratory, University of Cambridge, c2010 [cit. 2010-05-05]. Dostupný z WWW: <http://www.cl.cam.ac.uk/~rja14/serpent.html>.

- SCHNEIER, Bruce. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*. 2. vyd. New York : John Wiley & Sons, 1996. 758 s. ISBN 0-471-12845-7.

- SCHNEIER, Bruce. SHA-1 Broken. In *Schneier on Security, February 15, 2005* [online]. London : British Telecommunications, 2005 [cit. 2010-05-05]. Dostupný z WWW: <http://www.schneier.com/blog/archives/2005/02/sha1_broken.html>.

- SINGH, Simon. *Kniha kódů a šifer : tajná komunikace od starého Egypta po kvantovou kryptografii*. Přeložili Petr Koubský a Dita Eckhardtová. 1. v českém jazyce vyd. Praha : Dokořán, 2003. 382 s. Aliter; sv. 9. ISBN 80-86569-18-7.

- STEVENS, M.; LENSTRA, A.; WEGER, B. Vulnerability of software integrity and code signing applications to chosen-prefix collisions for MD5. In *Technische Universiteit Eindhoven* [online]. Eindhoven : Technische Universiteit, 30 November, 2007 [cit. 2010-05-05]. Dostupný z WWW: <http://www.win.tue.nl/hashclash/SoftIntCodeSign/>.

- Telegramy skončí jen na České poště, O2 je bude nabízet dál. In *FinančníNoviny.cz* [online]. Praha : Neris, s.r.o., 2010-, 30. března 2010 [cit. 2010-05-05]. Dostupný z WWW: <http://www.financninoviny.cz/zpravy/telegramy-skonci-jen-na-ceske-poste-o2-je-bude-nabizet-dal/456203>.

- United States v. Boucher. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001-, last modif. 28 April 2010 [cit. 2010-05-05]. Dostupný z WWW: <http://en.wikipedia.org/wiki/United_States_v._Boucher**>.**

- United States v. Scarfo : Key-Logger Case. In *Electronic Privacy Information Center* [online]. Washington (D.C.) : EPIC, 2002 [cit. 2010-05-05]. Dostupný z WWW: <http://epic.org/crypto/scarfo.html>.

- VĚTROVSKÁ, P. *LUPA: Server o českém Internetu* [online]. 1996- [cit. 28. května 2007]. Dostupný z WWW: <http://www.lupa.cz/>. ISSN 1213-0702.

- VLČEK, K. *Teorie informace, kódování a kryptografie*. 1. vyd. Ostrava : Vysoká škola báňská, 1999. 182 s. ISBN 80-7078-614-0.

- *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikimedia Foundation, 2001- [cit. 2010-05-05]. Dostupný z WWW: <http://en.wikipedia.org/wiki/Main_Page**>.**

- WILLAN, Philip. PGP Encryption Proves Poweful. In *PCWorld* [online]. San Francisco (CA) : PCWorld Communications, May 26 2003 [cit. 2010-05-05]. Dostupný z WWW: <http://www.pcworld.com/article/110841/pgp_encryption_proves_powerful.html>.

- WILLIAMS, Chris. UK jails schizpohrenic for refusal to decrypt files : Terror squad arrest over model rocket. In *The Register* [online]. London : Situation Publishing, 24th November 2009 [cit. 2010-05-05]. Dostupný z WWW: <http://www.theregister.co.uk/2009/11/24/ripa_jfl/page2.html>.

- WOBST, Reinhard. *Cryptology Unlocked.* 1. vyd. Chichester : John Wiley & Sons, 2007. 557 s. ISBN 978-0-470-06064-3.

- XIAOYUN, W. et al. Collisions for Hash Functions MD4, MD5, Haval-128 and RIPEMD. In *Cryptology ePrint Archive Report 2004/199, 16 August 2004* [online]. Santa Barbara (CA) : International Association for Cryptologic Research, 2004 [cit. 2010-05-05]. Dostupný z WWW: <http://eprint.iacr.org/2004/199.pdf>.

- XIAOYUN, W.; YU, Hongbo. How to Break MD5 and Other Hash Functions. In *Proceedings of EUROCRYPT, 2005* [online]. Santa Barbara (CA) : International Association for Cryptologic Research, 2005 [cit. 2010-05-05]. Dostupný z WWW: <http://merlot.usc.edu/csac-f06/papers/Wang05a.pdf>.

Přílohy

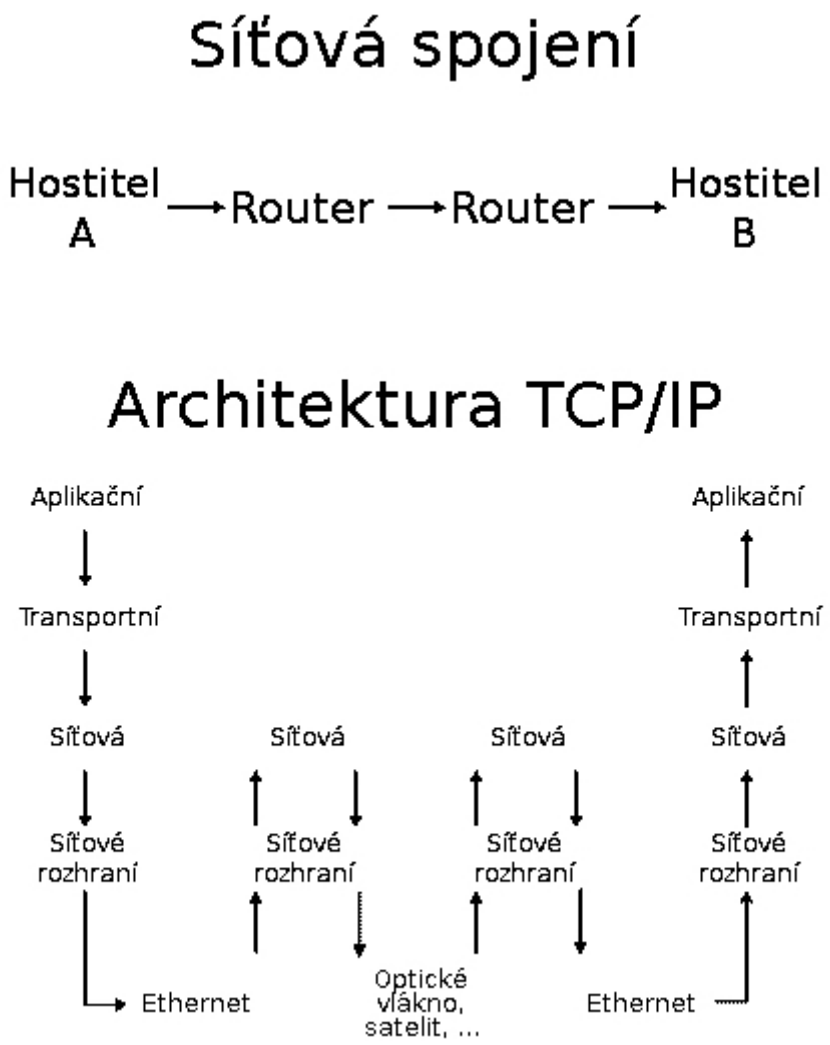
Příloha č. 1

Country	OECD - Total				
Year	2004	2005	2006	2007	2008
Series					
O21: Internet subscribers	246 878 280	337 099 410	353 137 311	382 401 186	..
O211: Number of Dial-up Internet subscribers	129 236 641	104 553 073	40 551 233	29 363 794	..
O212: Total broadband	118 384 670	159 576 860	200 256 408	236 317 566	263 669 680
O212CAB: Cable Modem Internet subscribers	39 770 487	48 431 499	59 604 742	67 755 783	75 610 362
O212DSL: DSL Lines	72 783 466	98 549 854	123 445 042	144 265 488	157 530 195
O212OTH: Other broadband access technologies to Internet	5 830 417	12 595 507	17 206 624	24 296 295	30 529 123
O26: Internet hosts	64 288 630	96 545 352	121 523 617	155 780 525	194 573 016
O722: Cellular mobile traffic	1 290 440 000 000	1 443 640 000 000	1 541 760 000 000	1 777 860 000 000	..

Statistiky OECD.

Převzato z WWW: < http://stats.oecd.org/index.aspx >

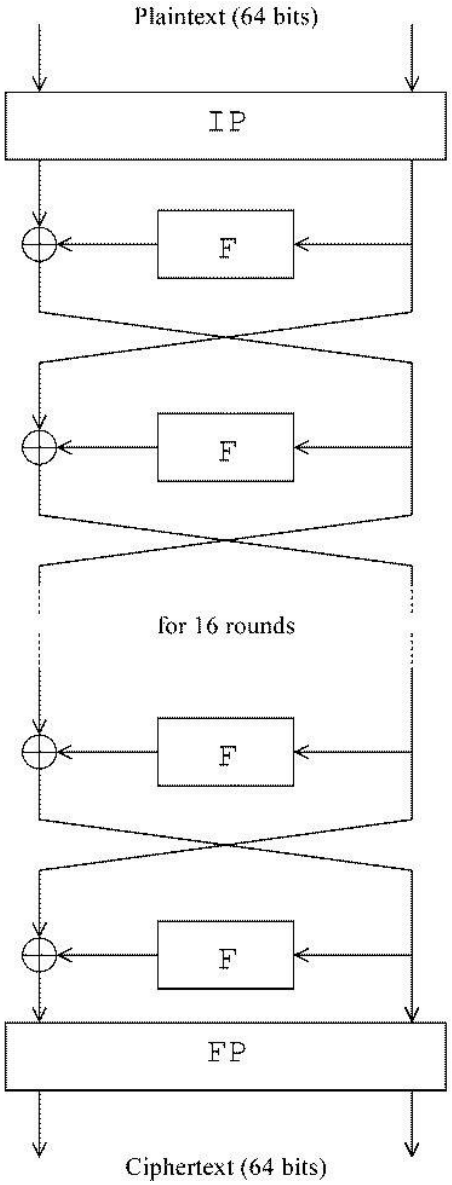
Příloha č. 2



Architektura TCP/IP.

Převzato z WWW: < http://upload.wikimedia.org/wikipedia/commons/thumb/0/0a/Tcpip_vrstvy.svg/490px-Tcpip_vrstvy.svg.png >

Příloha č. 3



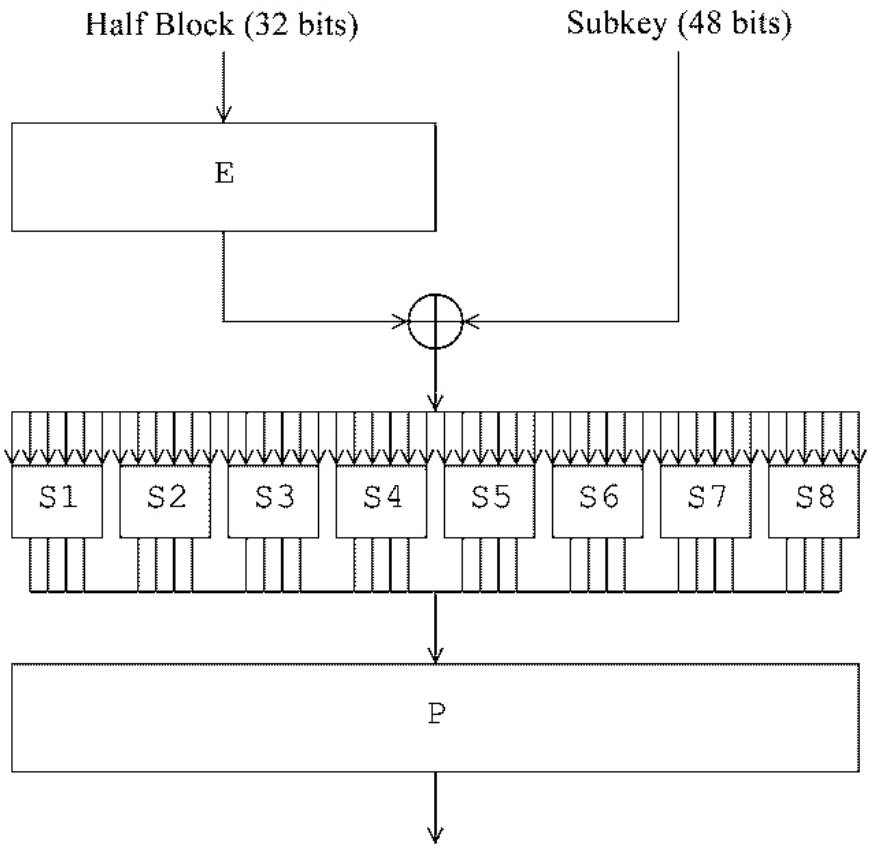
Obecné Feistelovo schéma šifry DES.

Převzato z WWW: < http://upload.wikimedia.org/wikipedia/commons/6/6a/DES-main-network.png >

Vysvětlivky:

IP - úvodní (iniciační) permutace

FP - konečná (finální) permutace



Feistelova funkce F šifry DES.

Převzato z WWW: < http://upload.wikimedia.org/wikipedia/commons/6/6a/DES-main-network.png >

Vysvětlivky:

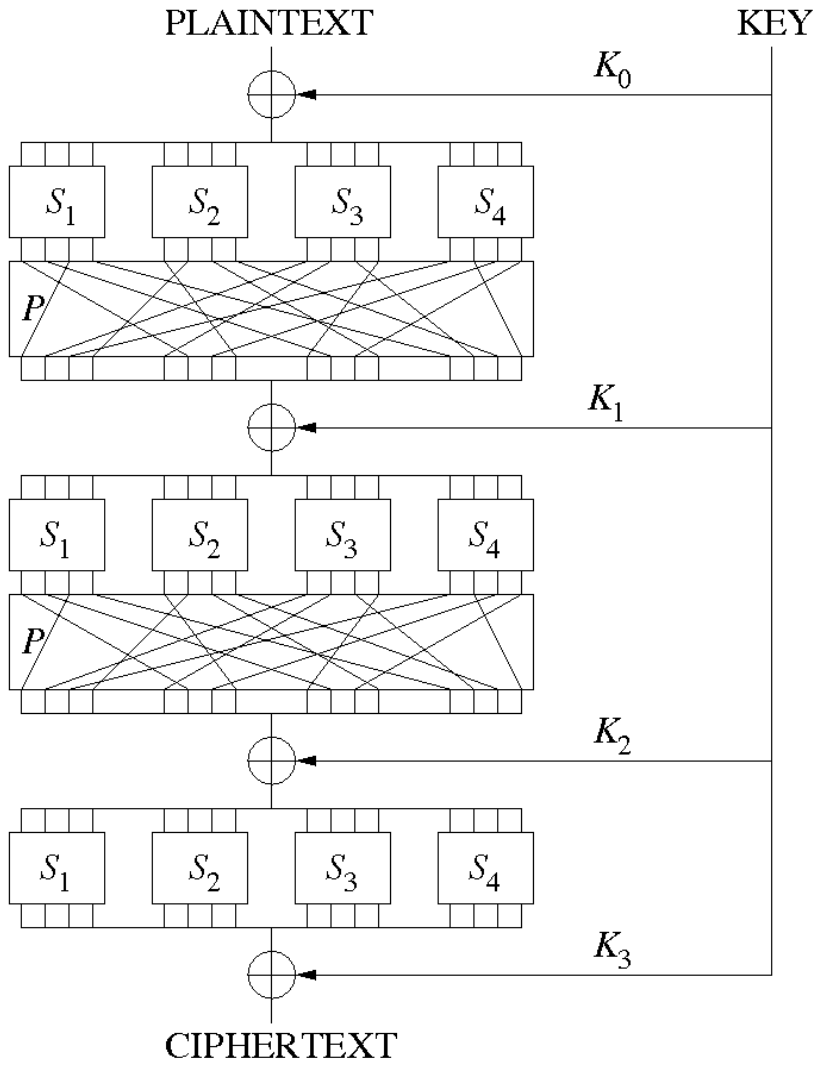
E - expanzní funkce

+ - operace XOR zajišťující smíchání se subklíčem

S_1-S_8 - S-boxy

P - P-box

Příloha č. 4



Substitučně-permutační síť (používá se i v algoritmu AES - Rijndael) o třech kolech šifrující 16 bitů otevřeného textu na 16 bitů šifrového textu.

Převzato z WWW: <
http://upload.wikimedia.org/wikipedia/commons/c/cd/SubstitutionPermutationNetwork2.png
>

Vysvětlivky:

S_1-S_4 - S-boxy

P_1-P_4 - P-boxy

K_0-K_3 - klíče pro jednotlivá kola

Příloha č. 5

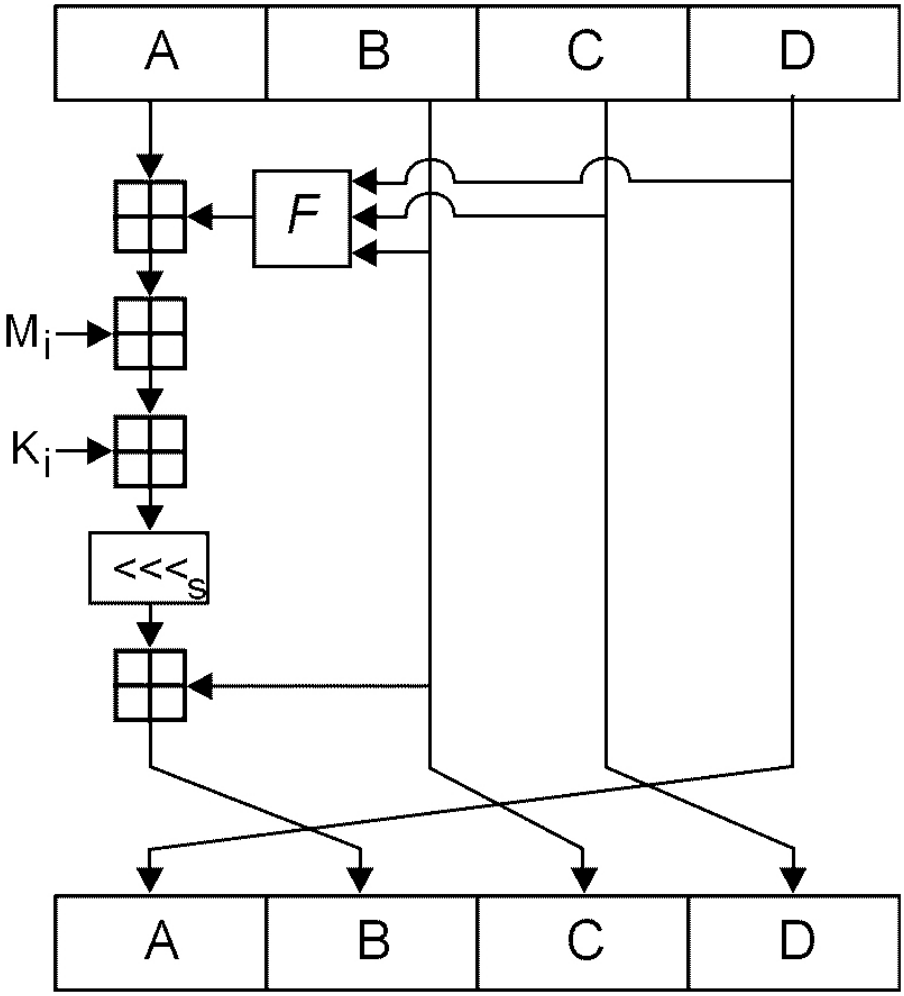


Schéma jedné operace funkce MD5. MD5 sestává celkově z 64 takových operací.

Převzato z WWW: < http://en.wikipedia.org/wiki/File:MD5.svg >

Vysvětlivky:

F - nelineární funkce

M_i - 32-bitový blok vstupu zprávy

K_i - 32-bitová konstanta, která se liší pro každou operaci

$<<<_s$ - rotace bitu doleva o s pozic, s je rozdílné pro každou operaci

+ - přičtení modula 2^{32}