Moderní kryptologie

Modern cryptology

Gabriela Bílková

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Gabriela BÍLKOVÁ**
Osobní číslo:	**A08646**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Moderní kryptologie**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Vypracujte studii o moderní kryptologii – zahrňte co nejvíce příkladů a ukázek klasických šifrovacích systémů, jejich vzájemné porovnání, včetně ukázek možností prolomení šifer.**
3. **Vytvořte prezentace obsahující popis problematiky, matematický popis a analýzu a grafické ukázky.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **SINGH, Simon. Kniha kódů a šifer.Argo, 2003. ISBN: 80-7203-499-5.**
2. **JANEČEK, J. Odhalená tajemství šifrovacích klíčů minulosti. Naše Vojsko, 1994.**
3. **VONDRUŠKA , P. Kryptologie, šifrování a tajná písma. Albatros, 2006. ISBN 80-00-01888-8**
4. **HANŽL, T. Šifry a hry s nimi. Portál, 2007. ISBN 978-80-7367-196-9.**
5. **KATZ, Jonathan. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall, 1 edition. 2007. 552 s. ISBN 978-1584885511.**
6. **MURPHY, Sean. Kryptografie – Průvodce pro každého . Dokořán, 2006. 157 s. ISBN 80-7363-074-5.**

Vedoucí bakalářské práce: **Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **5. března 2010**

Termín odevzdání bakalářské práce: **1. června 2010**

Ve Zlíně dne 5. března 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Práce v teoretické části představuje základní pojmy šifrování a jeho historii od počátku ve starověkém Egyptě a Mezopotámii přes současné moderní šifry až po výhled do blízké budoucnosti v podobě kvantové kryptografie.

Praktická část podrobně rozebírá jednotlivé šifrovací systémy a jejich principy. Výstupem této části je prezentace, která bude sloužit k výuce moderních šifer na Univerzitě Tomáše Bati ve Zlíně.

Klíčová slova: moderní kryptologie, symetrické šifry, asymetrické šifry, AES, DES, Hash funkce, DSA, digitální steganografie

ABSTRACT

The theoretical part of this work presents the essential concepts in cryptography, together with the history of cryptography since its origins in the ancient Egypt and Mesopotamia, continuing with current modern ciphers, and ending with outlook into near future - the quantum cryptography.

The practical part thoroughly analyzes individual encryption systems and their principles. The output of this part is a presentation, which will aid in modern cryptography lectures on the Tomas Bata University in Zlín.

Keywords: modern cryptography, symmetric cipher, asymmetric cipher, AES, DES, Hash function, DSA, digital steganography

Děkuji svému vedoucímu bakalářské práce, Ing. Romanu Šenkeříkovi Ph.D., za odborné vedení, cenné rady a připomínky, které mi poskytl. A také bych mu chtěla poděkovat za soustavnou pozornost, kterou mi věnoval při vypracovávání mé bakalářské práce.

Dále bych chtěla poděkovat rodičům a přátelům za svatou trpělivost, kterou se mnou měli.

Motto:

Šifrování je často jedinou možností, jak ochránit svá data.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Důvodem vzniku této práce byla potřeba vytvoření kvalitní pomůcky pro výuku problematiky moderních šifer na Univerzitě Tomáše Bati ve Zlíně.

Teoretická rešerše podrobně rozebírá základní pojmy z oblasti šifrování. Vysvětluje princip šifrových systémů. A dále představuje historii šifrování od jeho prvopočátků v období starověkého Egypta a rozvoj ve starověkém Řecku a Římě. Mapuje pomalý posun v období středověku a prudký rozkvět ve 20. století, spojený s vynálezem telegrafu a především s klíčovou úlohou šifrování, během obou světových válek. V závěru poskytuje krátký náhled do budoucnosti oboru šifrování reprezentovaný především předpokládaným rozvojem kvantové kryptografie.

V praktické části detailně představuje moderní šifry, jejich rozdělení na asymetrické a symetrické šifry. Vysvětluje principy a využití těchto šifer, jejich podmínky spolehlivosti a možnosti útoku.

Výstupem je prezentace, která představuje problematiku moderní kryptologie popsanou v této práci a to v podobě vhodné pro studenty. Jejím účelem je využití při výuce na Univerzitě Tomáše Bati ve Zlíně.

I. TEORETICKÁ ČÁST

1 LITERÁRNÍ REŠERŠE

Teoretická část bakalářské práce se zabývá především popisem základních pojmů v kryptologii a stručným přehledem historie. Jednotlivé moderní šifry a jejich ukázky jsou až v části praktické.

1.1 Základní pojmy

Kryptologie

Můžeme ji zjednodušeně označit jako vědu o utajení zpráv [1]. Mezi lidmi měla donedávna nádech tajemna, knihy o kryptologii bychom našli spíše v oddělení o alchymii a hvězdopravectví. Kryptologie se dělí na kryptografii a kryptoanalýzu a někdy se jako samostatná oblast přidává ještě steganografie [1].

Kryptografie

Zabývá se matematickými metodami se vztahem k takovým prvkům informační bezpečnosti, jako je zajištění důvěrnosti zprávy, integrity dat (neporušenosti), autentizace entit (ověření subjektu) a původu dat (vlastnictví) – včetně zkoumání jejich silných stránek a slabin i odolnosti vůči různým metodám útoků [1].

Kryptografové jsou lidé, kteří se zabývají návrhem, používáním a zkoumáním šifrovacích systémů a dalších částí informační bezpečnosti.

Kryptoanalýza

Můžeme ji považovat za "opak" kryptografie. Hlavním cílem tedy je studium metod luštění šifrovacích systémů. Obecně se kryptoanalýza zabývá odolností kryptografických systémů a hledá metody, které vedou k proniknutí do těchto systémů.

Ten, kdo se zabývá kryptoanalýzou, je kryptoanalytik. Kryptoanalytici se snaží získat ze zašifrované zprávy její původní podobu – otevřený text [1].

Steganografie

Jejím hlavním úkolem je skrýt samostatnou existenci zprávy – nejlépe do jiné zprávy. Často je spojována především s používáním neviditelných inkoustů, mikroteček a podobných metod. V současné době je plnohodnotnou disciplínou, která velmi vhodně doplňuje klasické metody kryptografie [1].

Šifrový systém

Je to jakýkoli systém, který můžeme použít ke změně textu, zprávy s cílem učinit ji nesrozumitelnou "třetím" osobám s výjimkou adresované osoby.

Šifrování/Zašifrování

Pokud na nějaký text použijeme jakýkoli šifrový systém, říkáme, že zprávu šifrujeme anebo, že jsme ji zašifrovali. Osoba, která šifrování provádí, se nazývá šifrant nebo šifrér [1].

Otevřený text

Původní text zprávy, ještě před tím, než byl zašifrován, se nazývá otevřený text nebo otevřená zpráva [1].

Šifrová abeceda

Šifrová abeceda respektive šifrové znaky mohou být tvořeny abecedou otevřeného textu, ale mohou být tvořeny i jinými obrazci. Znaky šifrové abecedy vytváří řetězce (skupiny). Od poloviny 19. Století je zvykem zapisovat šifrové znaky do skupin po pěti šifrových znacích [1].

Klamač

Je to znak v šifrové abecedě, který nemá žádný významový ekvivalent, při dešifrování se vynechává. Klamače se vkládají pro zvýšení bezpečnosti šifry.

Dešifrování

Dešifrování je opačný proces k šifrování. Jedná se o rekonstrukci původního otevřeného textu zprávy z šifrového textu pomocí domluvené kryptografické metody a znalosti příslušného klíče [1].

Luštění

Luštění je proces, kdy se kryptoanalytici snaží získat ze zašifrované zprávy její původní podobu. Pokud se tento proces podaří, řekneme, že šifra byla zlomena nebo rozbita, můžeme také použít slangový výraz "brejknuta" (z anglického slova *break*). Prolomení se týká celého šifrovacího systému, tzn. od této chvíle umí luštitel přečíst všechny zprávy. Luštění má 3 základní odlišné fáze: identifikaci, prolomení a zjištění nastavení.

Šifry a kódy

Mezi šiframi a kódy musíme rozlišovat. Pomocí šifry se odesílatel a adresát snaží utajit obsah zprávy před nepovolanou osobou [1]. Smyslem kódu není zprávu utajit, ale upravit ji tak, aby ji bylo možné dále příslušným technickým prostředkem zpracovávat [1]. Kódovaná zpráva tedy může být na základě znalosti příslušného kódování převedena zpět do původního tvaru [1]. K nejznámější kódům patří Morseova abeceda a ASCII kód.

Klíč/Klíčový prostor

Hodnoty (parametry) šifrového systému, které lze měnit a které mají vliv na výsledný šifrový text, se nazývají klíč (key), počet různých klíčů se nazývá klíčový prostor [1].

1.2 Šifrové systémy

1.2.1 Symetrické šifrové systémy

Pokud je klíč pro šifrování a dešifrování stejný, pak se systém nazývá symetrický šifrový systém [1]. V tomto systému má klíč označení symetrický tajný klíč nebo jen tajný klíč. Do této skupiny patří většina klasických šifrových systémů např. Polybiův čtverec, Caesarova šifra, Augustova kniha a další.

1.2.2 Asymetrické šifrové systémy

Asymetrický systém je založen na tom, že jeden klíč, tzv. veřejný klíč, slouží k zašifrování otevřeného textu a druhý klíč, tzv. soukromý klíč, k dešifrování textu [1]. Veřejný klíč je tedy možné zveřejnit, protože jeho znalost není při luštění vůbec důležitá, k tomu potřebujeme znát i soukromý klíč. Vztah mezi veřejným a soukromým klíčem existuje, ale je výpočetně velice náročný a není možné v rozumném čase z veřejného klíče získat klíč soukromý.

1.2.3 Elektronický podpis

Patří mezi asymetrické šifrové algoritmy. Úkolem není utajit obsah zprávy, ale zajistit průkaznost toho, že po podpisu nebyl obsah zprávy změněn a že elektronický podpis mohla vytvořit je konkrétní osoba. Pracuje se opět s dvojicí klíčů – veřejný a soukromý. Veřejný klíč se u nějaké nezávislé autority zaeviduje (osoba předloží autoritě veřejný klíč a ta mu k němu vydá elektronické potvrzení o jeho vlastnictví – certifikát), vlastník soukromého

klíče provede s otevřeným textem transformaci (k tomu určený algoritmus), kterou nazýváme elektronický podpis [1].

1.2.4 Hybridní systémy

Hybridní systémy spojují všechny výhody symetrického i asymetrického šifrování (systému) např. rychlost, není potřeba distribuovat klíč a další. Tímto se potlačují nevýhody, které by vznikaly při použití pouze buď symetrických nebo asymetrických systémů.

1.3 Historie

V této části je stručně popsána historie šifrování. Jedná se o nejzajímavější a nejdůležitější události.

1.3.1 Starověk

Šifrování je téměř stejně staré jako písmo samo [2]. Mezi nejstarší písma patří egyptské, mezopotamské a hebrejské, ale vzhledem k tomu, že v té době uměli číst a psát jen vyvolení, bylo už samo písmo šifrou. Šifry tedy nesloužili ani tak k utajení zprávy, jako udělat ji zajímavější. Jako příklad můžeme uvést šifru ATBASH – je to jednoduché nahrazení pomocí otočené abecedy.

Později se ale šifry začali používat k vojenským a vládním účelům a to hlavně u Řeků a Římanů. Známá je z této doby zejména Caesarova šifra.

Šifrování se také nachází mezi 64 uměními uvedenými v Kámásútře [2]. Podle této knihy má šifrování sloužit milencům k utajení milostné korespondence [2].

1.3.2 Středověk a raný novověk

Mezi 5. a 15. Stoletím se kryptologie rozvíjela pomalu, zhruba ve 14. století se na Předním východě začala rozvíjet kryptoanalýza a z této doby také pochází první dochovaný popis řešení jednoduché substituce založený na frekvenční analýze. Arabové objevili frekvenční analýzu, když se pokoušeli ověřit pravost náboženských textů [2].

V Evropě, kterou zmítaly konflikty, nabývalo šifrování stále více na významu a to jak v mezinárodní politice, tak i na bitevním poli. Pro obléhaná města byly šifry klíčové. V mezinárodní politice připravila slabá šifra např. o hlavu skotskou královnu Marii Stuartovnu. Z vězení, kde byla držena svou sestřenicí, anglickou královnou Alžbětou,

posílala šifrované zprávy svým Košicům [2]. Kvůli rozluštěné šifře byla usvědčena z plánovaného spiknutí proti Alžbětě a popravena [2]. V této době měla většina panovníků své vlastní šifrovací specialisty. Velmocí byla Francie. Šifry byly stále jednoduchá nahrazení, s použitím klamačů či s úmyslným komolením textu. Techniky luštění těchto šifer se brzy staly velice rozšířenými, i přesto byla kryptoanalýza mnohými považována za magii.

Substituční šifrování podle hesla (polyalfabetická substituce) zřejmě vymyslel roku 1553 Giovan Batista Belaso a knižně ji popsal o třicet let později Blaise de Vigenere, pod jehož jménem je tento systém dodnes znám jako Vigenerova šifra (viz. Obrázek 1) [2]. Tato šifra se stala jednou z mnoha, které byly dlouho a mylně považovány za nerozluštitelné.

Ukrývání zpráv ve smysluplném textu je další technika, která se ve středověku rozšířila, zejména v podobě zvané akrostich [2]. Akrostich je báseň či jiný text, jehož počáteční (koncové) slabiky (písmena, slova) ukrývají informaci [2].

Podobně jako hledání údajných skutečných autorů literárních děl bylo velmi oblíbené také hledání skrytých věšteb a kryptogramů v Bibli [2].

Obrázek 1 Vigenerova šifra

1.3.3 Devatenácté století

Důležitým impulsem pro rozšíření šifrování byl vynález telegrafu (1932), ten umožnil předávat zprávy na velkou vzdálenost, ale neposkytoval soukromí, Šifry se staly důležitými nejen pro panovníky a armádu, ale také pro obchodníky. Objem šifrované komunikace začal výrazně narůstat [2].

V této době vznikl nový trend - používání polních šifer. Šlo o šifry určené k použití v terénu, byla důležitá možnost zprávu rychle zašifrovat a rozšifrovat, bezpečnost už tak důležitá nebyla.

Za prvního, kdo se do šifrování snažil dostat matematickou notaci, je považován Charles Babbage, což se v dalších letech ukázalo jako užitečný nápad.

Kryptografové stále přicházeli s novými šiframi a jednou z nejúspěšnějších se stala šifra sira Charlese Wheatstona z roku 1854. Knižně ji popsal Lyon Playfair, pod tímto jménem také vešla ve známost a používala se ještě za druhé světové války.

V tomto století se o kryptografii začala zajímat také veřejnost. Například v Anglii tomu tak bylo čistě z praktických důvodů – milenci si posílali šifrované zprávy v novinách, které v té době byly zdarma, na rozdíl od posílání dopisů. K výměně zprávy používali steganografickou metodu.

1.3.4 Legendy, poklady a stará písma

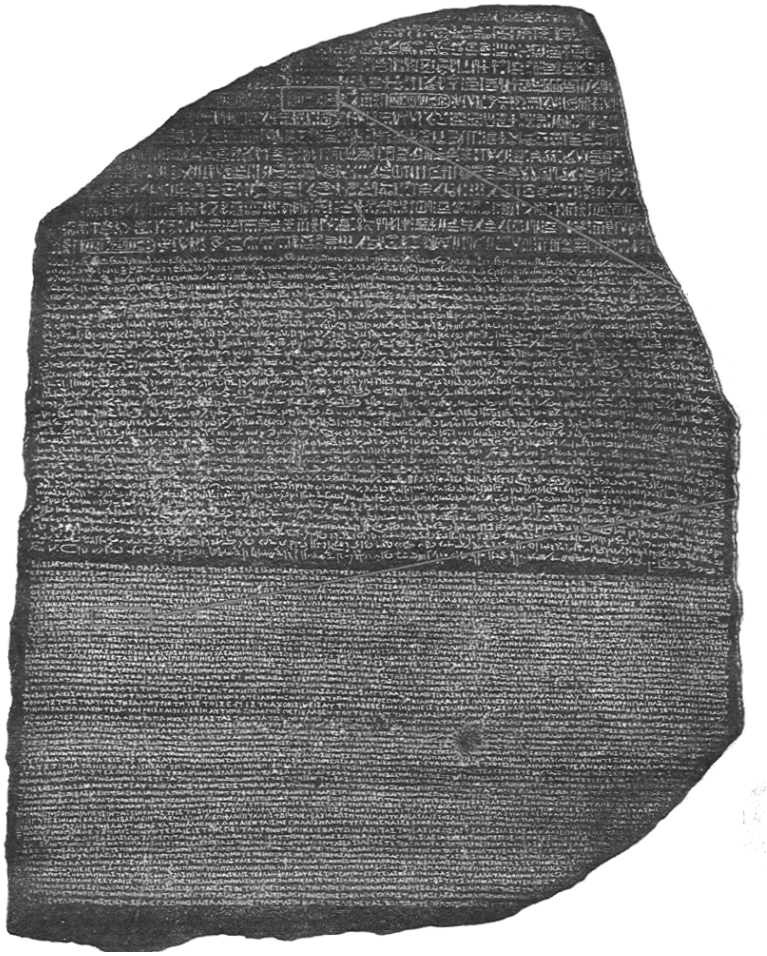
Šifry figurují také v mnoha legendách. Například příběh Ludvíka XIV., který věznil v Bastile muže, který vycházel ven jen v noci a měl na hlavě železnou masku. Spekulovalo se o tom, že je to jeho dvojče. Jiná spekulace ovšem tvrdí, že to byl generál Vivienna de Bulonde, protože v 19. Století, tedy o 200 let později, se podařilo rozluštit dopis, který pochází z této doby.

Příchuť hledání pokladů má také luštění starých písem. V tomto případě nejde o kryptologii v tradičním slova smyslu, protože úkolem nebylo zprávu skrýt před čtenářem, to jen čas způsobil, že ji neumíme číst. Metody používané při luštění starých písem jsou však velmi podobné luštitelským metodám [2]. Nejznámějším příkladem je rozluštění hieroglyfů starých Egypťanů, které se podařilo na základě Rosettské desky (viz. Obrázek 2) [2]. Dal ji sepsat roku 196 př. n. l. faraon Ptolemaios, nalezena byla 1799 Napoleonovým vojskem v Egyptě. Deska obsahuje jeden text psaný třikrát – řecky dvěma typy hieroglyfů. Tyto texty pomohli Jean-Francois Champollionovi rozluštit v roce 1824 tajemství hieroglyfů.

Dalším významným objevem bylo rozluštění mykénského písma [2]. Stále však existují stará písma, která na rozluštění teprve čekají.

Zajímavý dokument je takzvaný Voynichův rukopis. Byl objeven roku 1912 americkým sběratelem Wilfridem M. Voynichem ve sbírce Jezuitské univerzity ve Frascati u Říma.

Jde o 400 let starou knihu, která obsahuje nákresy neznámých rostlin, astrologické diagramy, recepty, podivné nákresy lidských postav a podobně. Mnoho lidí se domnívá, že jde o podfuk a že kniha neobsahuje žádný určitý text.



Obrázek 2 Rosettská deska

1.3.5 První světová válka

Kryptologie byla důležitá i v předchozích válkách, ale teprve ve světových válkách 20. století začala hrát opravdu klíčovou roli. Hlavním důvodem byl vynález rádia (1894), které umožnilo výrazně zlepšit komunikaci mezi jednotlivými složkami armád [2]. Šifrování se tak stává naprostou nutností [2]. Jedny z nejpoužívanějších šifer byly šifry založené na složitějších substitucích např. Playfair nebo ADFGX. Časté bylo také použití tzv. kódových knih – slovníků, pomocí kterých se zprávy překládaly do tajných kódů. Téměř jediným způsobem, jak vyluštit zprávu zašifrovanou pomocí kódové knihy, je mít k dispozici onu kódovou knihu [2]. Jeden z prvních úlovků byla kniha z německé lodi Magdeburg, která na začátku války v podstatě náhodou padla do rukou Rusům [2]. Další

knihy pak byly získávány pomocí různých lstí, například oblíbenou fintou Angličanů bylo podstrkování falešných kódových knih a falešných zpráv zašifrovaných pomocí těchto knih.

Klíčovým dokumentem 1. světové války byl Zimmermanův telegram. Jednalo se o zprávu Německa pro Mexiko, ohledně zatažení USA do války. Zprávu zachytili Angličané, podařilo se jim ji rozluštit a pak to narafičili tak, aby to vypadalo, že se anglický agent zmocnil rozšifrované zprávy v Mexiku. William Hall, velitel anglické kryptografické jednotky, se totiž obával, že kdyby zprávu předali přímo, USA by si myslelo, že se jedná o podvod.

1.3.6 Druhá světová válka

Ještě větší význam měla v kryptologii druhá světová válka [2]. Mezi válkami totiž proběhl posun v náhledu na kryptografii, do roku 1931 využívala převážně lingvisty, ale po tomto roce se začali uplatňovat čím dál více matematikové. Stále se ještě používaly šifry typu tužka-papír (např. Playfair), s rozvojem elektromechanických technologií se začalo využívat strojů. Základem těchto strojů byly rotující disky, zapojením více vzájemně propojených rotujících disků se daly vytvářet substituční šifry vysoké složitosti.

Strojů v této době nezávisle na sobě vzniklo několik a byly používány na obou stranách: Sigaba (USA), Typex (GB), Purple (Japonsko), Enigma (Německo)(viz. Obrázek 3). Nejznámějším z nich je německá Enigma, jejíž rozluštění bylo jednou z klíčových událostí druhé světové války [2].

K rozluštění Enigmy vedlo několik faktorů. Počátek se datuje do roku 1931, kdy dal německý nespokojený státní úředník za poplatek okopírovat francouzské tajné službě část k manuálu k Enigmě. Další chybou bylo, aby Němci zabránili chybám v přenosu, vysílali jednorázový klíč dvakrát po sobě.

Také v Pacifiku hrála kryptologie důležitou roli [2]. Američané dokázali luštit japonský přístroj Purple a proslavili se použitím kódu Navajo. Tato pseudošifra spočívala v naverbování příslušníků indiánského kmene Navajo, jejich jazyk byl tak odlišný od všech ostatních, že bylo nemožné tuto šifru rozluštit.

Nezanedbatelnou úlohu sehrála také steganografie, zejména v práci špionů. V roce 1860 francouzský fotograf Dragon vyřešil způsob zmenšování zpráv na velikost inkoustové skvrny. Během války Němečtí špionu tuto metodu zdokonalili tak, že byli schopni zprávu

zmenšit na tečku o velikosti 1,3 mm a zprávy si pak přenášeli v normálních dopisech jako tečky na konci věty. První taková zpráva byla objevena roku 1941.

Jsou zde ale jen ty nejzajímavější příklady, jelikož celá historie válek vydá na samostatné knihy. O tom svědčí i počty lidí, kteří se kryptografií během světových válek zabývali – v první přibližně 400, ve druhé již 16 000.

Obrázek 3 Šifrovací stroj Enigma

1.4 Současnost

Po světových válkách pokračoval vývoj kryptologie velkým tempem, zejména díky rozvoji počítačů [2]. Počítače umožnili provádět veškeré operace daleko snadněji a bez chyb [2]. Vztah kryptologie a počítačů byl obousměrný – zejména v prvních letech byla kryptologie jednou z hlavních aplikací počítačů a hnala jejich vývoj kupředu.

Šifry hráli také důležitou roli ve studené válce (zhruba 1947 – 1991). Klíčovými bojovníky v ní byli tajní agenti a tajné zprávy klíčovými zbraněmi. N straně Západu byla například organizace GCHQ (Government Communication Headquarters), která navazovala na Bletchley Park a na straně druhé Americká NSA (National Security Agency), ta je také přezdívaná *Never Say Anything* nebo *No Such Agency,* protože v prvních letech

nefigurovala ani v oficiálním rozpočtu USA a i dnes je její fungování značně zamlženo, i když má údajně větší rozpočet než známější CIA a FBI.

1.4.1 Nové směry v kryptologii

Až do 70. let 20. století byla kryptologie převážně „magií", které rozuměli jen vojenští a vládní specialisté [2]. Výzkum v oblasti kryptologie byl soustředěn do vládních organizací a přísně utajen, zaměstnanci se nesměli o své práci s nikým bavit a dokonce si mimo pracovní areál ani nesměli dělat jakékoli poznámky o nápadech souvisejících s prací, natož veřejně publikovat své výsledky. Reálný průlom nastal až po roce 1976, kdy se podobné myšlenky objevily ve veřejných akademických článcích [2].

Zásluhu na tom měla kniha Davida Kahna *The Codebreakers,* vydaná roku 1967 a která obsahovala více než 1000 stran s přehledem o vývoji šifrování. Inspirovala celou řadu kryptologů, mezi něž patří i Whitfield Diffie a Martin Hellman, kteří strávili výzkumem v nevládním prostředí mnoho let. V roce 1976 publikovali článek *New Directions in Cryptography,* článek nastínil nové možné aplikace kryptografie, které přesahovali tradiční rámec komunikace mezi dvěma stranami, které sdílejí společné heslo. V tomto článku navrhli myšlenku šifrování s veřejným klíčem, který je založen na dvou částech – soukromém a veřejném klíči. O rok později Ron Rivest, Adi Shamir a Len Adleman vymysleli matematickou realizaci této myšlenky, která je nyní známá jako RSA algoritmus [2].

Od této doby začala kryptologie pronikat do akademických kruhů a dnes je již samostatnou vědeckou disciplínou s mnoha aplikacemi výrazně převyšujícími vojenské a vládní použití [2].

1.4.2 Soukromí versus bezpečnost

Rozvoj šifrování ve 20. století souvisí také s morálními otázkami fungování demokratické a svobodné společnosti, konkrétně rozporem mezi soukromím a bezpečností [2]. Kde končí právo občana na soukromí a kde začíná právo státu na bezpečnost? Šifrování je důležitým krokem k zajištění soukromí, obzvlášť v dnešní době s rozmachem elektronických komunikací je téměř nezbytná. Na jaké straně by tedy mělo stát šifrování, na straně státu nebo občana?[2] Je rozumné dát komukoli šifry tak silné, že jsou prakticky neprolomitelné?[2] Pokud však bude použití šifer omezeno, nestaví se tak stát do role Velkého bratra?[2]

Šifrování se v 70. letech vymanilo z moci vládních agentur a proniklo do akademických a komerčních kruhů, vláda se snažila udržovat kontrolu pomocí vhodně nastavených standardů, nejznámějším je DES (*Data Encryption Standard).* Tato hranice byla nastavena tak, že rozluštění šifry bylo právě na hranici možností tehdejších počítačů [2]. Rozlomení šifry si tak mohl dovolit jen někde s velkou výpočetní kapacitou.

S rozvojem počítačů a internetové sítě se tyto spory staly mnohem aktuálnějšími, protože šifry se pro komunikaci na Internetu staly klíčovými. Odposlouchávání je na internetu stejně jednoduché jako u rádia [2].

Na začátku 90. let Phil Zimmermann dokončoval svůj šifrovací program PGP (*Pretty Good Privacy),* který implementoval algoritmus pro šifrování s veřejným klíčem pro stolní počítač. Kvůli návrhu zákona Senátu USA, zveřejnil svůj program v 1991 jako Freeware, bez nároku na odměnu. V následujících letech Zimmermann čelil několika žalobám, ohledně porušení zákona – porušení zákona o exportu a porušení autorských práv, ale rozšíření algoritmu se již nedalo zabránit a silné šifry se začali široce používat, obžaloby byly nakonec staženy.

1.4.3 Současné aplikace

V dnešní době člověk používá šifrování v podstatě neustále a to kolikrát v oblastech, které překračují tradiční rámec předávání tajné zprávy.

- Internetové informační systémy, elektronické obchodování – komunikace mezi uživatelem a systémem musí probíhat zašifrovaně, protože ji lze jednoduše odposlouchávat.
- Mobilní telefony – signál vysílaný i přijímaný mobilním telefonem lze snadno zachytit, je tedy nutné signál šifrovat.
- Identifikace uživatelů počítačových sítí – veškerá hesla (piny, biometrika) se musí uchovávat zašifrované, aby nedošlo k jejich zneužití.
- Autentizace – proces identifikace neprobíhá jen mezi uživatelem a systémem, ale také mezi dvěma různými systémy např. kreditní karta a bankomat, autentizace probíhá pomocí speciálních kryptografických protokolů.
- Elektronické podpisy – elektronický ekvivalent vlastnoručního podpisu se zajišťuje s využitím šifer.

- Ochrana dat – elektronická data (soubory) má smysl šifrovat nejen během jejich přenosu, ale také preventivně pro případ krádeže PC nebo nabourání do systému prostřednictvím Internetu.
- Celistvost (integrita) dat a vodoznaky – je to kontrola toho, zda byl soubor s daty porušen nebo změněn a také označení dat, aby byl jasný jejich původ, provádí se s využitím kryptografických technik.

V těchto aplikacích si však nevystačíme s pouhým využitím šifer a to ani těch moderních [2]. Musíme se vypořádat například s autentizací či autorizací, ale můžeme si být jisti, že ten s kým komunikuji je opravdu ten, za koho se vydává? A jak zjistím, že veřejné klíče pocházejí z důvěryhodného zdroje? K těmto účelům se využívá různých kryptografických protokolů, které sestávají z několikanásobné výměny různě zašifrovaných zpráv [2].

1.4.4 Kvantová kryptografie

Zatímco kryptoanalytici předvídají příchod kvantových počítačů, kryptografové pracují na vlastním technologickém zázraku – šifrovacím systému, který znovu nastolí soukromí, dokonce i když bude čelit plné síle kvantového počítače [3]. Tento systém bude bezchybný a zaručí nám na věky naprostou bezpečnost, je založen na kvantové teorii, která je také základem kvantového počítače. Takže zatímco kvantová teorie je inspirací pro počítače, které mohou rozlomit všechny současné šifry, je také zároveň jádrem nové, nerozlomitelné šifry zvané kvantová kryptografie [3].

Kvantová kryptografie začala neobvyklou myšlenkou, kterou rozvinul v 60. letech Stephen Wiesner, navrhl podivný koncept kvantových peněz, které měly tu výhodu, že se nedaly padělat. Wiesnerovy kvantové peníze vycházely z fyziky fotonů, když foton cestuje – vibruje. Kvantové peníze jsou vynikající myšlenkou, ale bohužel také naprosto nerealizovatelnou.

První kvantový kryptografický protokol navrhli v roce 1984 Bennett a Brassard. Vymysleli systém založený na principu: Alice chce Bobovi poslat zašifrovanou zprávu, která se skládá z 1 a 0. Nahradí 1 a 0 emisí fotonů s určitou polarizací. Alice má dvě možná schémata pro spojení polarizace fotonů 1 a 0 – rovnoběžné a diagonální. Tento systém má zřetelné výhody [3]. V náhlém okamžiku vytvořili osvícení kvantovou kryptografii nejbezpečnější formu komunikace, která kdy byla navržena.

Kvantová kryptografie není pouze prakticky nerozlomitelná, je nerozlomitelná naprosto [3]. Pokud by se někdy někomu podařilo dešifrovat zprávu chráněnou kvantovou krytografií, znamenalo by to, že je celá kvantová kryptografie mylná a to by mělo pro fyziky naprosto drtivé důsledky – byli by nuceni znovu zvážit svůj pohled na fungování vesmíru na jeho nejzákladnější úrovni [3]. Jestliže se někomu podaří sestrojit systémy kvantové krytografie fungující i na velké vzdálenosti, bude vývoj v oblasti šifer završen a hledání soukromí se přiblíží ke svému konci. Tato technologie by byla schopna zajistit bezpečnou komunikaci pro vlády, armády, obchodníky i veřejnost. Zůstává jediná otázka: Dovolily by nám vlády používat tuto technologii?[3]

1.4.5 Výhled do budoucnosti

I když momentálně vedou kryptografové nad kryptoanalytiky, nemělo by se zapomínat na minulost, kdy si vždycky mysleli, že už našli tu pravou „nerozluštitelnou šifru". Kromě lidí lze však i využít jiných nepřímých metod k útoku tzv. postranních kanálů. Může jím být například elektřina, jejím měřením lze odposlouchávat údery do klávesnice. Je také možné měřit odběr proudu čipové karty v průběhu šifrování a z toho čerpat cenné informace [2]. Podobných informačních kanálů existuje spousta a tvoří nemalou část děr v různých bezpečnostních systémech [2].

Další možnost, jak rozšifrovat zprávu je, si ji uložit a počkat až se objeví technologie k jejímu rozšifrování, vzhledem k rychlému vývoji počítačů i algoritmů, to může být mnohem dříve než by se odesilateli zprávy mohlo líbit.

Nesmíme také zapomínat, že všechny moderní šifry jsou postaveny na faktu, že určité problémy nikdo *neumí* efektivně řešit [2]. Není však dokázáno, že tyto problémy *nejdou* řešit, je klidně možné, že někdo přijde s efektivním řešením a celý souboj kryptografů i kryptoanalitiků se opět převrátí a posune o krok dál.

1.5 Stručný přehled historie šifrování

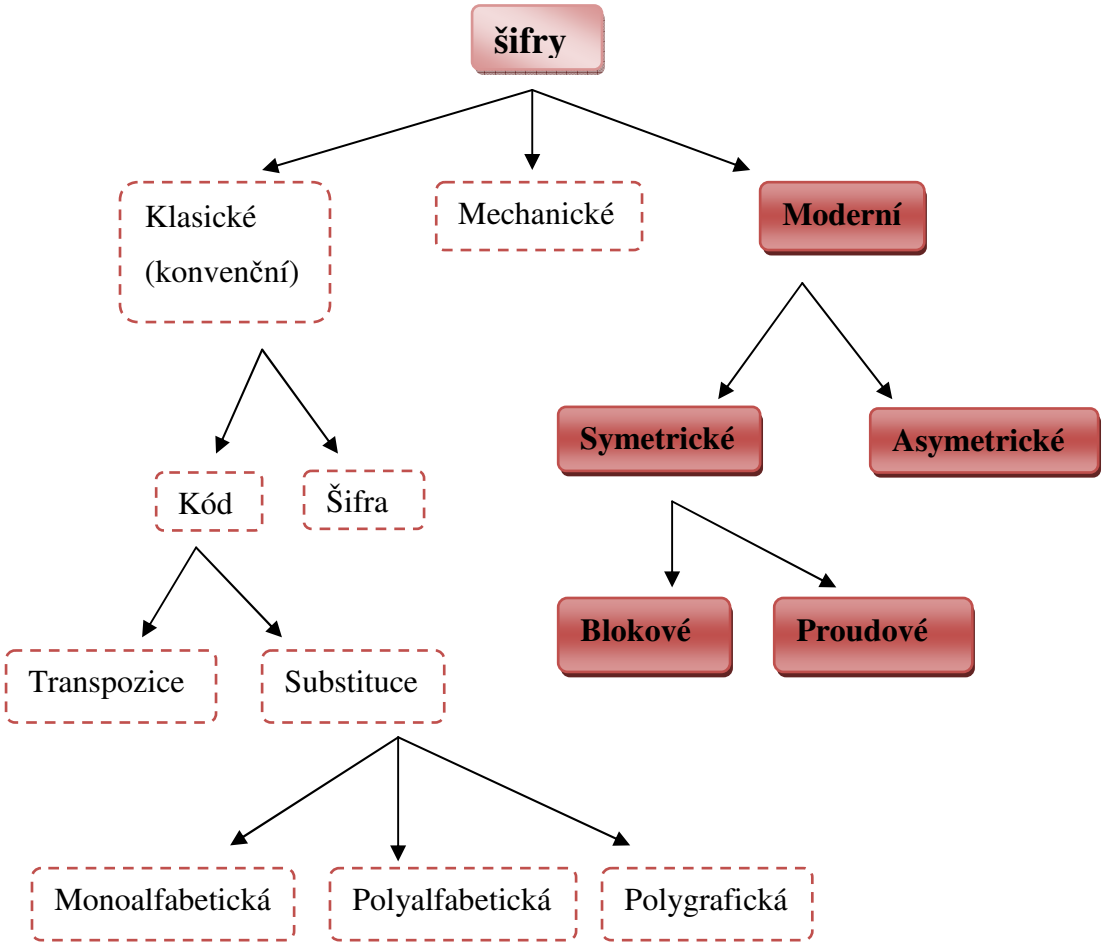
V tabulce 1 můžete vidět souhrn nejdůležitějších dat a vývoj v oblasti kryptografie.

500 př. n. l.	Židé: jednoduchá substituční šifra (ATBASH)
400 př. n. l.	Řecko: jednoduché transpoziční šifry, steganografie
50 př. n. l.	Řím: Caesarova šifra
4. století	Indie: šifrování mezi 64 uměními v Kámasútře
10. století	Arabové: základy kryptoanalýzy včetně frekvenční analýzy
13. a 14. století	Evropa: používá se substituční šifra, případně lehké nástavby
1412	Arabové: encyklopedie obsahující kapitolu o kryptologii
15. a 16. století	první návrhy šifrování podle hesla
16. století	Evropa: kryptologie hraje důležitou roli v politice
1586	Anglie: poprava skotské královny na základě rozluštění šifry
1843	USA: Poe píše o šifrách a zveřejní šifrovací výzvy
1861	Prusko: metoda pro řešení polyalfabetické šifry (Kasiski)
1885	USA: Bealův poklad
19. století	rozvoj telegrafu, rozvoj kryptografie pro komerční účely,polní šifry (Playfair), první mechanické přístroje pro šifrování
1. světová válka	důležitá role ve válce i v politice (Zimmermannův telegram), použití komplikovanějších šifer na klasických principech
1926	Německo: armáda začíná používat šifrovací přístroj Enigma
2. světová válka	klíčová role kryptologie ve válce, použití mechanických šifrovacích strojů
1949	publikovány práce C. Shannona o teorii informace
50. léta 20. století	rozvoj počítačů, první využití počítačů pro šifrování/luštění
1967	USA: kniha D. Khana „The Codebreakers”
1973	Anglie: objeven princip šifrování s veřejným klíčem, kvůli utajení však nebyl zveřejněn
1976	USA: publikován článek „New Directions in Crytography”, začátek rozvoje akademické kryptologie
1978	USA: zveřejněno RSA, algoritmus realizující kryptografii s veřejným klíčem
1991	USA: zveřejněno PGP, implementace kryptografie s veřejným klíčem
90. léta 20.století	rozvoj kvantové kryptografie

Tabulka 1 Přehled historie šifrování *Zdroj: Šifry a hry s nimi*

II. PRAKTICKÁ ČÁST

Jako úvod do praktické části je uveden obrázek základního rozdělení šifer (viz. Obrázek 4). Tato práce se zabývá moderními šiframi, což je vidět ve zvýrazněné části obrázku.



Obrázek 4 Rozdělení šifer

2 SYMETRICKÉ ŠIFRY

2.1 Vernamova šifra

Vernamova šifra nebo také jednorázová tabulková šifra (anglicky *one-time-pad*) je jednoduchý šifrovací postup, který si nechal v roce 13. 9. 1918 patentovat Gilbert Vernam.

Vernamova šifra je v podstatě Vigenerova šifra, u které je klíč stejně dlouhý, jako otevřený text. Vernamova šifra je v principu nerozluštitelná.

2.1.1 Definice

Je-li $p_1,p_2, \ldots p_n$ otevřený text kódovaný čísly (0, 1, … 25) a $k_1, k_2, \ldots k_n$ náhodně generovaný klíč (tvořený čísly 0, 1, … 25) pak šifrový text $c_1, c_2, \ldots c_n$ je definován jako

$$c_i = p_i + k_i mod 26 \quad (1)$$

pro $i=1, 2, \ldots n$. Modulo 26 znamená, že je 26 možností pro $k_1 \ldots k_{j-1}$.

Rovnice (1) je prakticky používána s Tabulkou 2.

2.1.2 Postup šifrování

Spočívá v posunu každého znaku zprávy o náhodně zvolený počet míst v abecedě. Vezeme jednotlivá písmena tajné zprávy a každé z nich posuneme o několik pozic v abecedě. Například první písmeno posuneme o 5 pozic, druhé o 1, třetí o 14 a další o 9, 0, 3, 9, 19. Když při přesouvání překročíme konec abecedy, pokračujeme od jejího začátku. Ze slova ALEDEBARAN tak dostaneme slovo FMRCKAUJG a posloupnost 5, 1, 14, 9, 0, 3, 9, 19 je klíčem k rozluštění zprávy.

Názorná ukázka kódování slova HELLO.

	H	E	L	L	O	zpráva
	7(H)	4(E)	11(L)	11(L)	14(O)	zpráva
+	23(X)	12(M)	2(C)	10(K)	11(L)	klíč
=	30	16	13	21	25	zpráva+klíč
=	4(E)	16(Q)	13(N)	21(V)	25(Z)	⟶
⟶	zpráva+klíč(mod26)					
	E	Q	N	V	Z	šifrový text

Správnost kódu a jeho šifrování je možné ověřit v Tabulce 2.

Klíčové slovo(písmeno)	Nešifrovaný text (písmena)																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabulka 2 Vernamova šifra

2.1.3 Podmínky spolehlivosti

- Klíč je tak dlouhý jak přenášená zpráva.
- Klíč je dokonale náhodný – nepřipadají v úvahu generátory pseudonáhodných čísel.
- Klíč nelze použít opakovaně – je to důsledek předchozí podmínky, protože opakovaný klíč není náhodný.

2.1.4 Možnosti útoku

- Statická kryptoanalýza je znemožněna náhodným charakterem šifrového textu.
- Ani útok hrubou silou, proti kterému není odolná prakticky žádná jiná šifra, neuspěje.

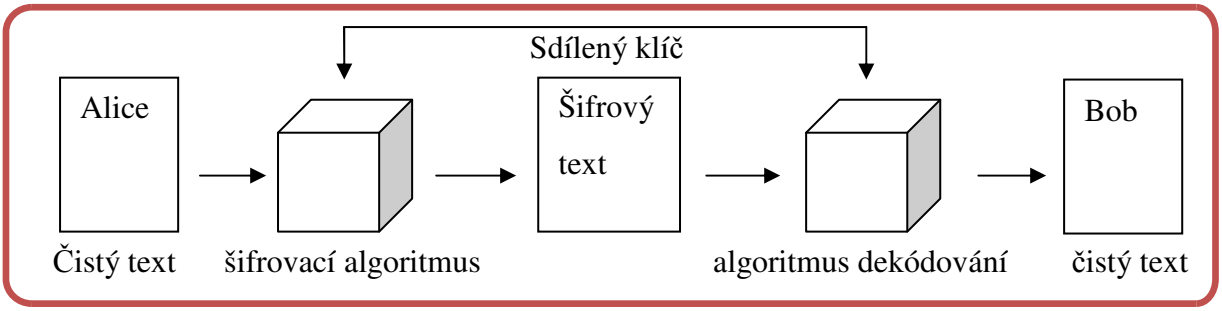
Matematickými důkazy bylo prokázáno, že neexistuje žádná metoda pro útok na tuto šifru.

2.2 DES (Data Encryption Standard)

IBM si ji nechala patentovat v únoru 1975 a přibližně o rok později jej uvolnila k veřejnému hodnocení [4]. V listopadu 1976 byl DES oficiálně přijat za standart s tím, že bude používán po dobu deseti let, každých pět let se podrobí novému testu bezpečnosti a v závislosti na jeho výsledku mu bude případně prodloužena platnost [4].

2.2.1 Definice

Používá se klíč o délce 64 bitů, z toho je 8 kontrolních a 56 efektivních.



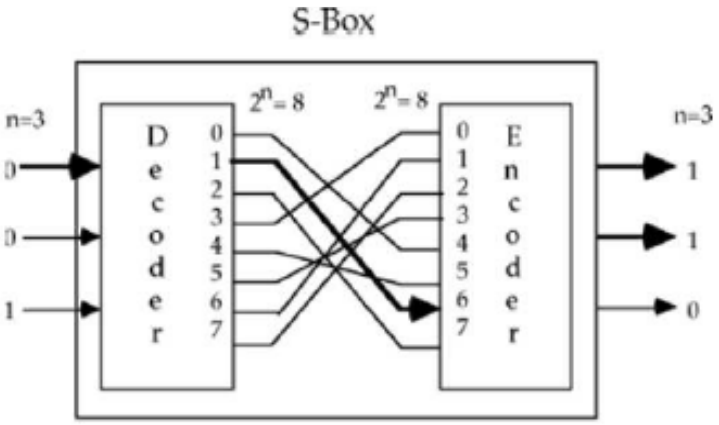
Obrázek 5 Schéma DES

2.2.2 Postup šifrování

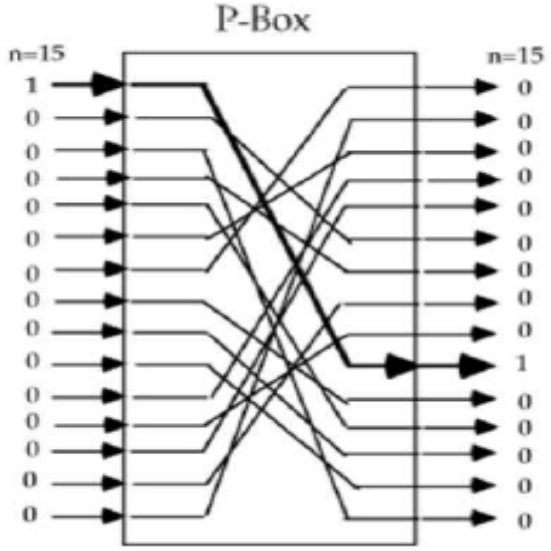
Nejdříve se zpráva rozdělí do bloků pevné délky (v základní verzi velikost 64 bitů) [2]. Každý blok se poté rozdělí na dvě části, které se *mandlují* – kombinují se s klíčem a ještě vzájemně dohromady, a to šestnáctkrát [2].

Každou operací šifrování se zašifruje jeden blok 64 bitů otevřeného textu na blok 64 bitů zašifrovaného textu (viz. Obrázek 5). Pro šifrování se používá klíč o velikosti 56 bitů.

Algoritmus využívá dvou kryptografických technik substituce (tj. nahrazení jisté bitové hodnoty jinou hodnotou na základě tabulky) a permutace (tj. jistá záměna pořadí jednotlivých bitů v bloku). Substituce se provádí pomocí takzvaných S-Boxů (viz. Obrázek 6) a permutace pomocí P-Boxů (viz. Obrázek 7). Základním stavebním blokem algoritmu DES je jednoduchá kombinace těchto technik (substituce následovaná permutací), která je modifikována hodnotou klíče. Tento blok se nazývá cyklus a je na šifrovaný blok bitů aplikovaný šestnáctkrát.



Obrázek 6 Příklad substitučního boxu



Obrázek 7 Příklad permutačního boxu

2.2.3 Podmínky spolehlivosti

Příliš malá délka klíče (56 bitů) je pravděpodobně největší slabinou algoritmu. Klíč je obvykle vyjádřen jako 64 bitová hodnota, avšak každý osmý bit je paritní a je algoritmem ignorován. Navíc algoritmus obsahuje i další slabiny, které dále snižují bezpečnosti šifry.

Bylo statisticky ověřeno, že neexistuje korelace (vztah) mezi otevřeným textem (nezašifrovanou zprávou) a šifrovaným textem a dále neexistuje korelace mezi šifrovaným textem a klíčem. Tímto je prokázána vyšší bezpečnosti algoritmu.

Možným způsobem, jak zvýšit bezpečnost této šifry, je vícenásobná aplikace. Tak vznikl algoritmus TripleDES (více později), který je trojnásobnou aplikací šifry DES.

2.2.4 Možnosti útoku

Na tuto šifru neznáme žádný „inteligentní" útok. Pro klíče délky 64 bitů je však různých klíčů „jen" $7{,}2 \cdot 10^{16}$ [2]. To již můžeme v dnešní době rozlomit hrubou silou, tj. vyzkoušením všech možností [2].

V roce 1998 byl sestrojen DES Cracker, stroj za 250 tisíc dolarů, který dokázal odhalit klíč o délce 56 bitů během 60 hodin [4]. Úspěšné útoky na DES prokázaly, že kterákoli organizace s dostatkem financí je schopna hrubou silou tuto šifru prolomit [4].

2.2.5 Prolomení

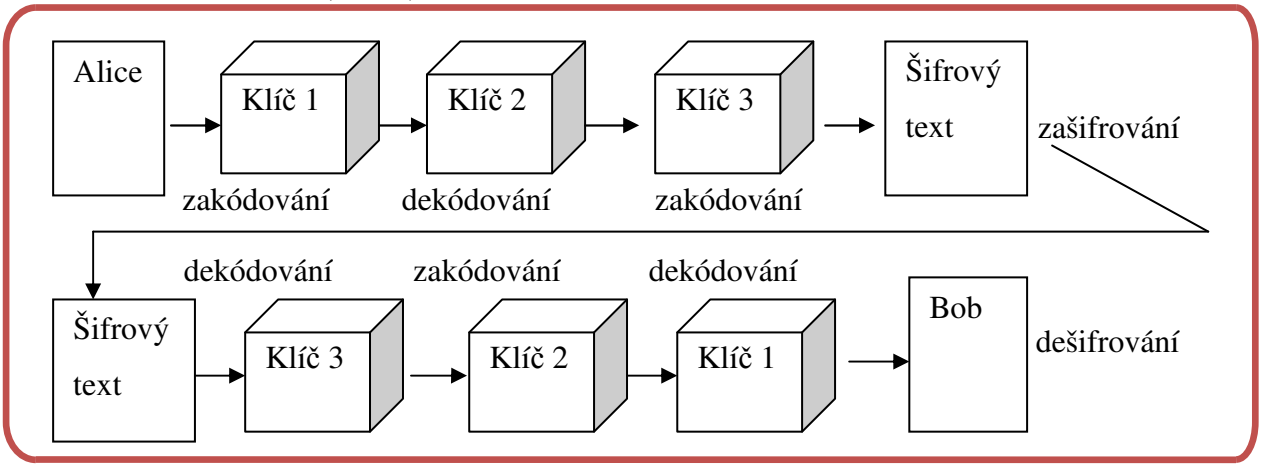
V lednu roku 1997 vypsala agentura RSA kryptoanalytickou soutěž s cílem prokázat reálnou možnost prolomení DES [4]. Úkol byl rozluštit text se známým začátkem a standardní délkou šifrovacího klíče. Nejúspěšnějším luštitelem se o 5 měsíců později stal Rocke Verser. K vyřešení použil internet (přesněji řečeno 14 000 počítačů) a odhalil otevřený text: *strong cryptography makes the Word a safer place* a šifrovací klíč: 8558891AB0C851B6.

2.2.6 3DES (Triple DES)

Vytvořena v roce 1998 jako reakce na prolomení šifry DES. Je to bloková šifra a je založena na šifrování DES, které aplikuje třikrát a tak zvyšuje její odolnost proti prolomení.

Definice

Algoritmus Triple DES je trojnásobnou aplikací šifry DES (viz. Obrázek 8). Pracuje s klíčem o velikosti 168 $(3 \cdot 56)$bitů.



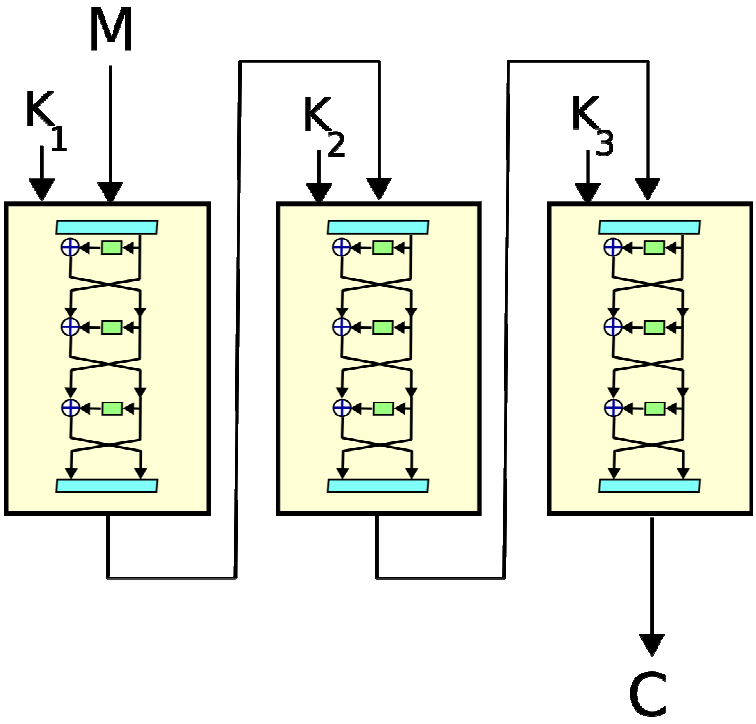
Obrázek 8 Schéma Triple DES

Postup šifrování

Nejjednodušší varianta TDES operuje tímto způsobem:

DES(kk3;DES(kk2;DES(kk1;MM)))

, kde M je blok dat, který má být zašifrován a kk1, kk2 a kk3 jsou klíče šifry DES. Tato varianta je známá jako EEE, protože všechny tři DES operace jsou šifrování. C je výstupní zašifrovaný blok dat. Algoritmus na obrázku 9.



Obrázek 9 Schéma algoritmu 3DES

Podmínky spolehlivosti

Použitím tří implementací šifry DES je vhodné pro předcházení středně velkým útokům, pro které DES již nebyla vhodná. DES není skupina, kdyby byla, byl by výstup TDES rovnocenný k jednotlivé DES operaci a tím pádem by nebyl bezpečný.

Možnosti útoku

V současné době není znám úspěšný útok na prolomení šifry 3DES. Šifra je považována za bezpečnou a je používána.

2.2.7 Další varianty kódu

- DES-X – ke klíči je před každou rundou přičten mod2 (XOR) další 64 bit klíč.

- GDES – zobecněný DES (pro urychlení – zranitelnější).
- DES s alternativními S-Boxy – řešení umožňující měnit jejich uspořádání či strukturu.
- RDES – výměna levých a pravých polovin řízena dle klíče.
- crypt(3) – varianta DES pro Unixové systémy pro tvorbu hesel.
- Silný lavinový efekt – změna pouhého jednoho bitu ve vstupních datech nebo klíči vede ke změně celé jedné poloviny výstupních dat.

2.3 AES (Advanced Encryption Standard)

Je schválený standard amerického úřadu pro standardizaci (NIST), který byl udělen symetrické blokové šifře Rijndael.

Počátkem roku 1997 byla vyhlášena veřejná soutěž o nalezení nového šifrovacího standardu, který by nahradil již poněkud stařičký DES a mohl tak nosit označení AES. Zůstalo 5 finalistů: MARS, RC6, Serpent, Twofish a Rijndael [4].

Zvítězil Rijndael, ale není ojedinělé, že ostatní šifry jsou jako doplňky k AES implementovány do šifrovacích programů, např. open source FreeOTFE a TrueCrypt.

2.3.1 MARS

Přihlašovatelem do soutěže byla firma IBM. Jedná se o šifrovací algoritmus, který podporuje klíče o délce 128 až 448 bitů. Kandidáti museli projít několika testy mezi nimiž nechybělo hodnocení možnosti hardwarové komunikace a právě v tomto bodě firma IBM mírně pokulhávala, protože šifra měla velké nároky na prostor. Mezi výhody naopak patří velice podobný postup při šifrování a dešifrování.

2.3.2 RC6

Tato šifra pochází z RSA Laboratories a návrh pochází z již dříve vyvinutého RC5. Pomyslná vada na kráse je nižší bezpečnost než v případě ostatních finalistů. Mezi jeho klady patří relativní jednoduchost a tedy jednodušší hardwarová implementace.

2.3.3 Serpent

Tato šifra vznikla jako výsledek úsilí mezinárodního týmu, jehož členy byli Ross Anderson (Velká Británie), Lars Knudsen (Norsko) a Eli Biham (Izrael) [4].

Systém podporuje libovolnou délku klíče, která nepřesahuje 256 bitů. Primární cíl návrhářů byla bezpečnost, ale šifra je vhodná především pro jednoduchou hardwarovou implementaci, v softwarové se totiž řadí mezi ty pomalejší.

2.3.4 Twofish

Tento kryptosystém pochází z rukou amerického týmu vývojářů, jimiž jsou B. Scheiner, N. Ferguson, D. Whiting, J. Keisey, D. Wagner a C. Hall [4].

Stejně jako šifra Serpent podporuje klíč o maximální délce 256 bitů. Kvůli velice komplikovanému návrhu nebylo možné hodnotit jeho kvality ve všech kategoriích a objektivně tak posoudit úroveň poskytované bezpečnosti [4].

2.3.5 Rijndael

Tento algoritmus se stal vítězem a je to výsledek úsilí Belgičanů Joana Deamena a Vincenta Rijmena. Vyhází z dříve vyvinutého kryptosystému Square a mezi jeho hlavní výhody patří rychlost a jednoduchá jak softwarová tak hardwarová implementace [4].

Byl přijat 26. Listopadu 2001 americkým úřadem NIST a jeho minimální životnost se odhaduje na přibližně tři desítky let.

2.3.6 Hodnocení AES finalistů

V tabulce 3 je porovnání jednotlivých algoritmů. Je zde jasně vidět, že vyhrál Rijndael.

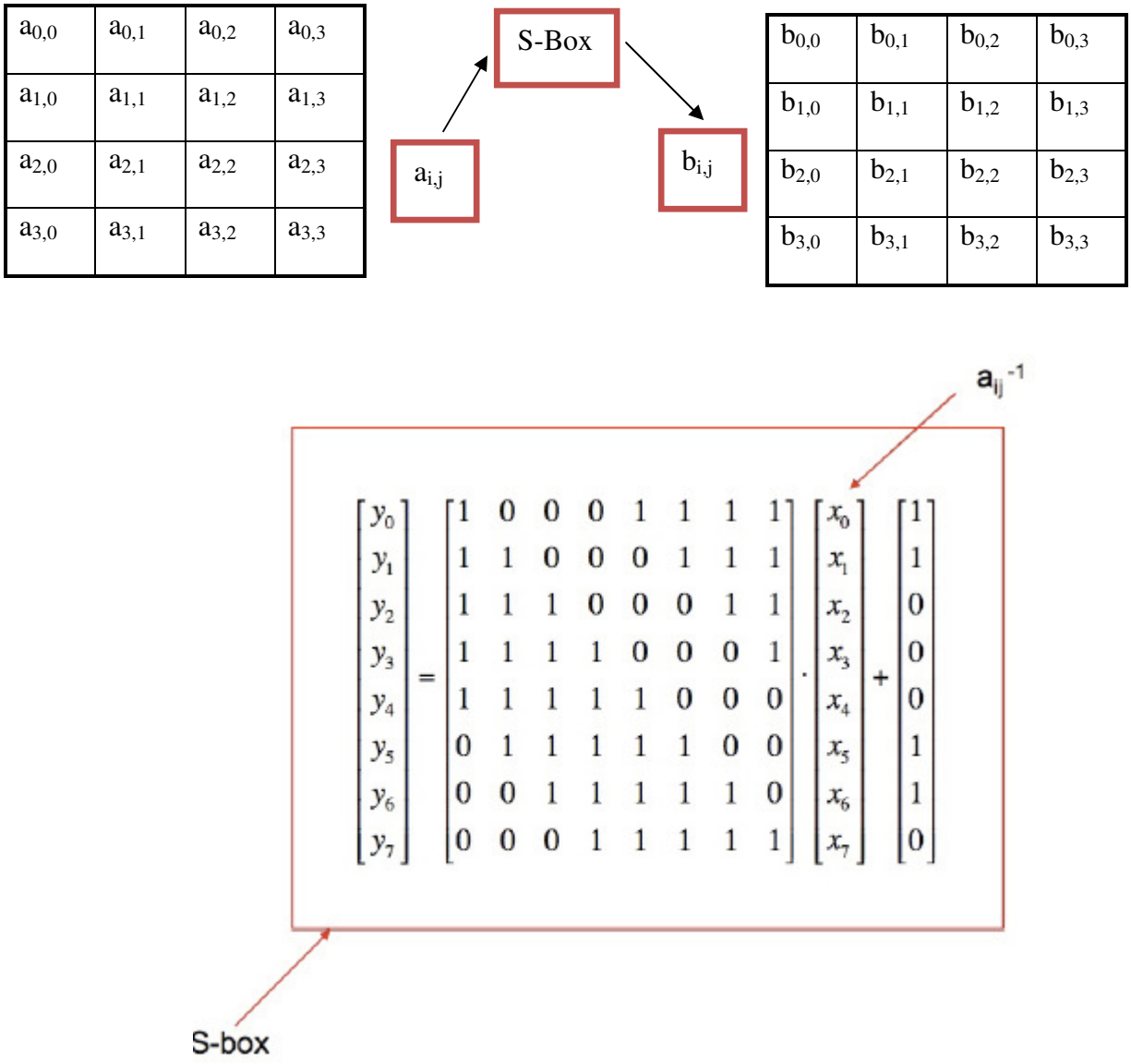
	MARS	RC6	Serpent	Twofish	Rijndael
Obecná bezpečnost	***	**	***	***	**
Softwarová implementace	**	**	*	*	***
Hardwarová implementace	*	**	***	**	***
Vlastnosti návrhu	**	*	*	***	**

Tabulka 3 Hodnocení AES finalistů *Zdroj: Šifrování a biometrika aneb tajemné bity a dotyky*

2.3.7 Základní funkce

- ByteSub Transformation

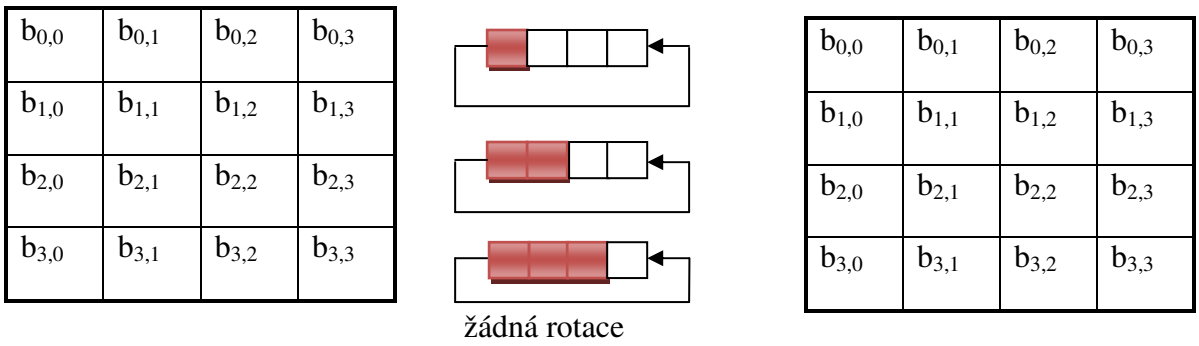
  Nelineární vrstva pro zvýšení odolnosti vůči diferenciálním a lineárním kryptoanalytickým metodám. Princip je vidět na obrázku 10.



Obrázek 10 Princip ByteTub Transformation

- ShiftRow Transformation

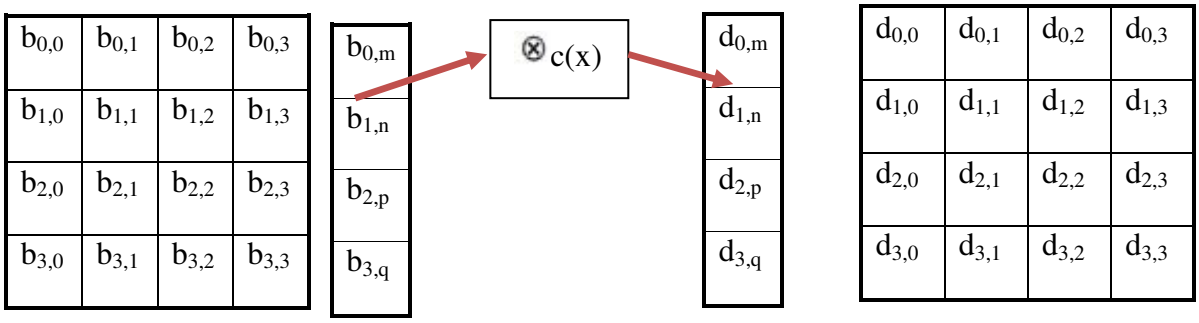
  Lineární vrstva pro mixování bitů slova v cyklickém pořadí. Princip mixování je na obrázku 11.



Obrázek 11 Princip ShiftRow Transformation

- MixColumn Transformation

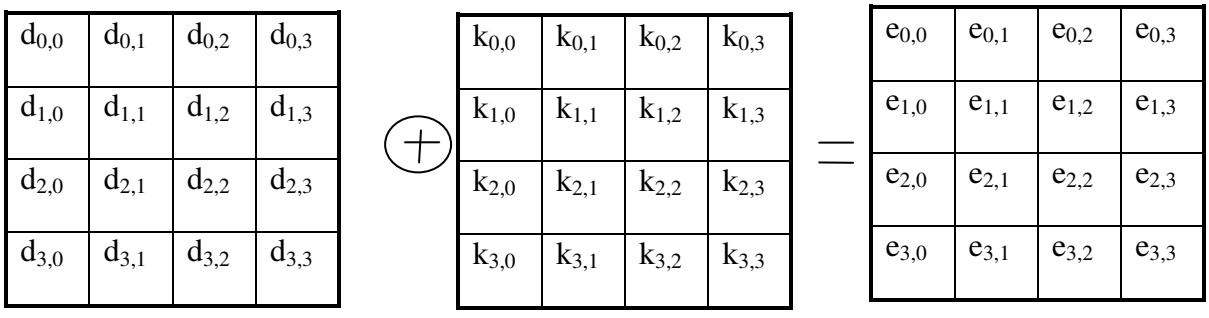
  Jedná se o mixování buněk tabulky. Princip je na obrázku 12.



Obrázek 12 Princip MixColumn Transformation

- AddRoundKey

  Jde o přidání cyklického klíče k datům. Princip je znázorněný na obrázku 13.



Obrázek 13 Princip AddRoundKey

2.3.8 Postup šifrování

Šifra využívá symetrického klíče tj. stejný klíč je použit pro šifrování i dešifrování. Délka klíče může být 128, 192 nebo 256 bitů. Metoda šifruje data postupně v blocích, jednotlivé metody jsou i s principy popsány výše.

Existují tři varianty AES-128, AES-192 a AES-256.

Volitelná délka klíče : 1) 128 bitů – 3,4 x 10^{18} klíčů

2) 192 bitů – 6,2 x 10^{57} klíčů

3) 256 bitů – 1,1 x 10^{77} klíčů

Tabulka 4 je pro volbu délky klíče.

$K_{0,0}$	$K_{0,1}$	$K_{0,2}$	$K_{0,3}$	$K_{0,4}$	$K_{0,5}$	$K_{0,6}$	$K_{0,7}$
$K_{1,0}$	$K_{1,1}$	$K_{1,2}$	$K_{1,3}$	$K_{1,4}$	$K_{1,5}$	$K_{1,6}$	$K_{1,7}$
$K_{2,0}$	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$	$K_{2,4}$	$K_{2,5}$	$K_{2,6}$	$K_{2,7}$
$K_{3,0}$	$K_{3,1}$	$K_{3,2}$	$K_{3,3}$	$K_{3,4}$	$K_{3,5}$	$K_{3,6}$	$K_{3,7}$

Tabulka 4 Volitelná délka klíče

Volitelná délka bloku : 1) 128 bitů

2) 192 bitů

3) 256 bitů

Tabulka 5 je pro volbu délky bloku.

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$

Tabulka 5 Volitelná délka bloku

2.3.9 Podmínky spolehlivosti

V současné době není znám žádný případ prolomení této metody ochrany dat.

2.3.10 Možnosti útoku

V současné době není znám úspěšný útok na prolomení šifry AES. Šifra je považována za bezpečnou a je používána (varianta s délkou klíče 256 bitů).

2.4 IDEA (International Data Encryption Algorithm)

Je to symetrická bloková šifra, kterou navrhli Xuejia Lai a James L. Massey v Zürichu. Poprvé byla popsána v roce 1991. Je patentována v mnoha zemích, ale je volně dostupná pro nekomerční použití. Název „IDEA" je také ochranná známka a její platnost vyprší v letech 2010 až 2011. Je licencována celosvětově MediaCryptem a byla používána v PGP (Pretty Good Privacy), je volitelným algoritmem v OpenPGP.

2.4.1 Definice

IDEA pracuje po 64bitových blocích za použití 128bitového klíče. Skládá se z osmi identických transformací a vstupní transformace (poloviční průchod). Iterativní šifra obsahuje 8,5 rund (vstupní informace se označuje jako půlrunda).

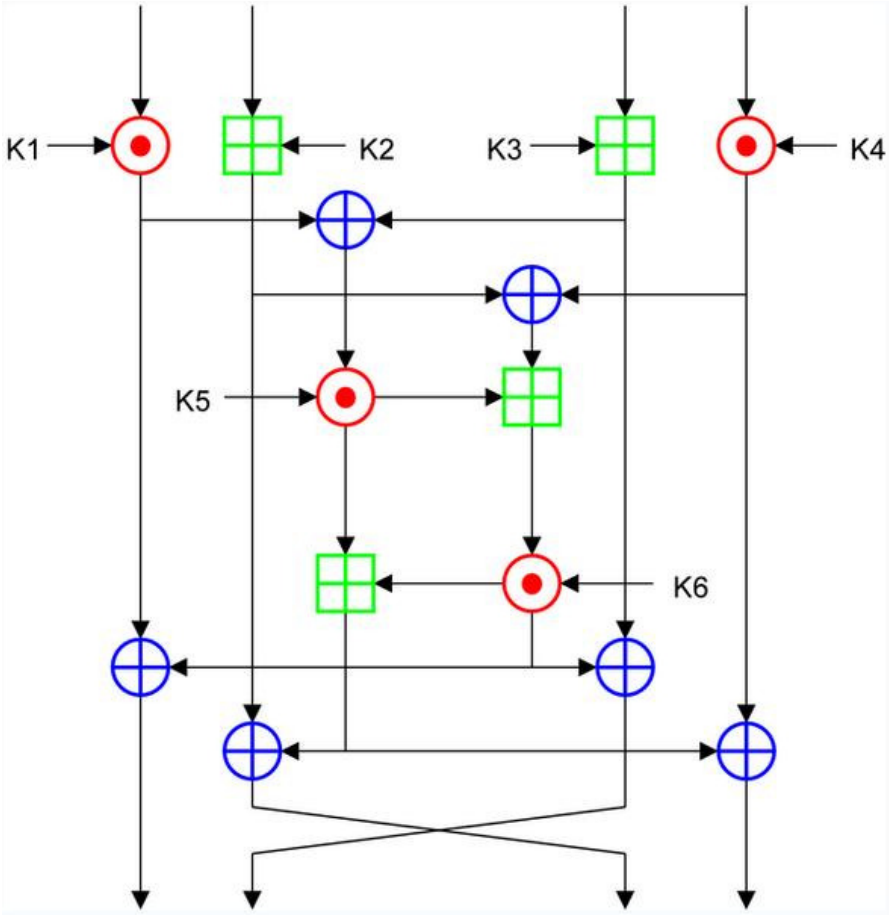
2.4.2 Postup šifrování

Procesy šifrování a dešifrování jsou podobné. IDEA odvozuje velkou část své bezpečnosti ze střídání operací z různých grup – modulární sčítání a násobení a bitové nonekvivalence (XOR) – které jsou v jistém smyslu algebraicky neslučitelné.

Operace, které pracující s 16bitovými řetězci jsou:

- Bitová nonekvivalence (na obrázku znázorněn)
- Sčítání modulo 2^{16} (znázorněno)
- Násobení modulo $2^{16} + 1$, kde nulová slova (0x0000) jsou interpretována jako 2^{16} (znázorněno)

Princip šifry IDEA pomocí 16 bitovýcj řetězců je vidět na obrázku 14.



Obrázek 14 Jeden průchod šifrovacího algoritmu IDEA

Generování klíčů:

- V každé rundě je potřeba 6 unikátních 16bitových klíčů.
- Prvních 8 rundových klíčů vznikne z původního šifrovacího klíče K rozdělením na osm 16bitových částí.
- Dalších osm rundových klíčů vznikne z původního šifrovacího klíče K, který je zrotován doleva o 25 a následně rozdělen na osm (opět po 16 bitech).
- Druhý krok se opakuje tak dlouho, dokud není vygenerováno 52 rundových klíčů.
- Po osmi rundách se zbývající 4 rundové klíče pomocí operace XOR spojí se čtyřmi 16bitovými vstupy a výsledkem je 64bitový blok.

2.4.3 Podmínky spolehlivosti

Je odolná vůči diferenční kryptoanalýze. Žádná úspěšná lineární nebo algebraická slabost nebyla odhalena.

2.4.4 Možnosti útoku

Od roku 2004 nejlepší útok, který se vztahuje ke všem klíčům, může prolomit šifrování IDEA za snížení na 6 průchodů (úplná šifra používá 8,5 průchodu).

Od roku 1999 se IDEA nedoporučuje kvůli dostupnosti rychlejších algoritmů, pokrokům v kryptografii a problému s patentem.

2.5 Přechod k asymetrické kryptografii

2.5.1 Jednosměrná funkce

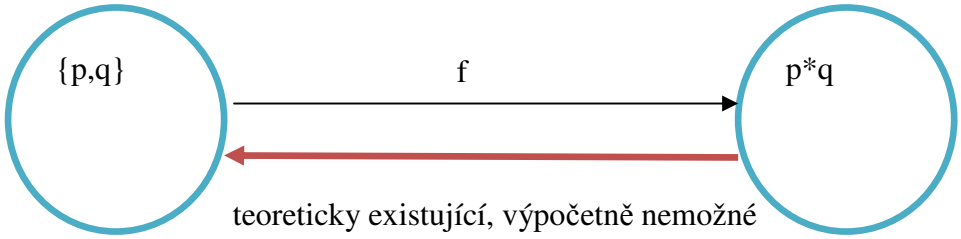
Definice

Funkce $f : X \longrightarrow Y$ se nazývá jednosměrná, jestliže pro libovolný prvek $x \in X$ je snadné (umíme rychle) vypočítat hodnotu *f(x),* ale pro náhodně vybraný prvek $y \in f(X)$ nelze (neumíme, je výpočetně nezvládnutelné) najít nějaké $x \in X$ takové, že $y = f(x)$.

Na existenci jednosměrných funkcí spoléhá velká část asymetrické kryptografie.

Postup šifrování

Víme, ale že takový vzor (viz. Definice) existuje nebo jich existuje dokonce velmi mnoho. Je to třeba, jako když smícháme dvě složky lepidla. Za několik vteřin vytvoří novou sloučeninu se zcela novými vazbami atomů a molekul, které nelze jednoduše rozpojit a vrátit do původní podoby. Podobně to probíhá s ohromnými čísly. Dokážeme je snadno spojit vynásobením. Číslo, které obdržíme má však zcela jinou "molekulární" strukturu, původní dvě složky pevně váže v nové číselné sloučenině a v současné době neznáme dostatečně rychlou metodu, jak tato čísla separovat (viz. Obrázek 15).



Obrázek 15 Jednosměrná funkce

Možné jednosměrné funkce

Mezi funkce, které jsou v současné době používány jako jednosměrné patří například :

- Násobení – součin dvou (i velmi velkých) čísel lze snadno spočítat.
- Rabinova funkce – lze dokázat, že zjišťování druhé mocniny modulo N je výpočetně ekvivalentní faktorizaci čísla N. druhá mocnina na konečném tělese je tedy kandidátem na jednosměrnou funkci.
- Umocňování nad konečným tělesem – výpočet diskrétního algoritmu se obecně pokládá za náročnou úlohu.
- Za další kandidáty se obecně považují některé NP-úplné problémy.

Podmínky spolehlivosti

Existuje velmi vysoký počet řešení, přičemž je nutné všechny ověřit, aby skutečné řešení bylo nalezeno a toto ověření by trvalo neúměrně dlouho (v praxi se požadují tisíce, miliardy i více let).

Možnosti útoku

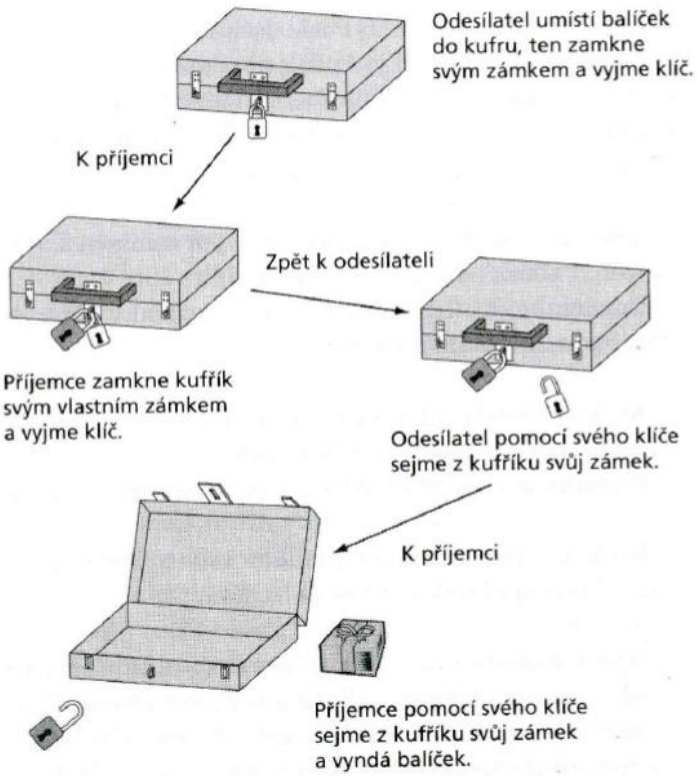
V současné době není matematicky dokázáno, zda jednosměrné funkce vůbec existují.

2.5.2 Shamirův algoritmus

Definice

Algoritmus dovoluje bezpečně poslat jakoukoli zprávu, aniž by se před tím účastníci dohodli na šifrovacím klíči. Myšlenka celého postupu je až překvapivě jednoduchá a ve světě za hranicemi nul a jedniček snadno realizovatelná [4].

Postup šifrování



Obrázek 16 Shamirův algoritmus

1. Alice vloží tajnou zprávu do kufříku a zamkne ho svým zámkem. Uzamčený kufřík pošle Bobovi.
2. Bob od Alicina zámku nevlastní klíč, takže ho nemůže odemknout. Namísto toho kufřík ještě jednou zamkne svým vlastním zámkem a takto nadvakrát zamčený ho pošle nazpět Alici.
3. Alice odemkne svůj zámek, takže kufřík je nyní uzavřen pouze Bobovým zámkem. Jednou zamčený kufřík pošle Alice Bobovi.
4. Bob konečně odemkne svůj zámek a dostane se tak k Alicině zprávě.

Tento postup je vidět na obrázku 16.

Bude-li tajná zpráva **m**, Alicin zámek šifrovací funkce $\mathbf{E_A}$, Bobův zámek šifrovací funkce $\mathbf{E_B}$, Alicina dešifrovací funkce $\mathbf{D_A}$ a Bobova dešifrovací funkce $\mathbf{D_B}$, pak [4] :

- Krok 1 : Alice $\Rightarrow$ Bob E_A (m)
- Krok 2 : Bob $\Rightarrow$ Alice E_B (E_A(m))
- Krok 3 : Alice $\Rightarrow$ Bob E_B (m) = $D_A(E_B(E_A(m)))$
- Krok 4 : Bob : m = $D_B(E_B(m))$

Podmínky spolehlivosti

Nutnou podmínku je použití komutativní funkce a to zejména v kroku 3, tedy nesmělo by záležet na tom, zda nadvakrát zašifrovanou zprávu nejprve dešifruje Alice nebo Bob.

Možnosti útoku

Právě nalezení bezpečné a v praxi použitelné komutativní šifry není vůbec jednoduché [4].

2.5.3 Diffie-Hellman protokol

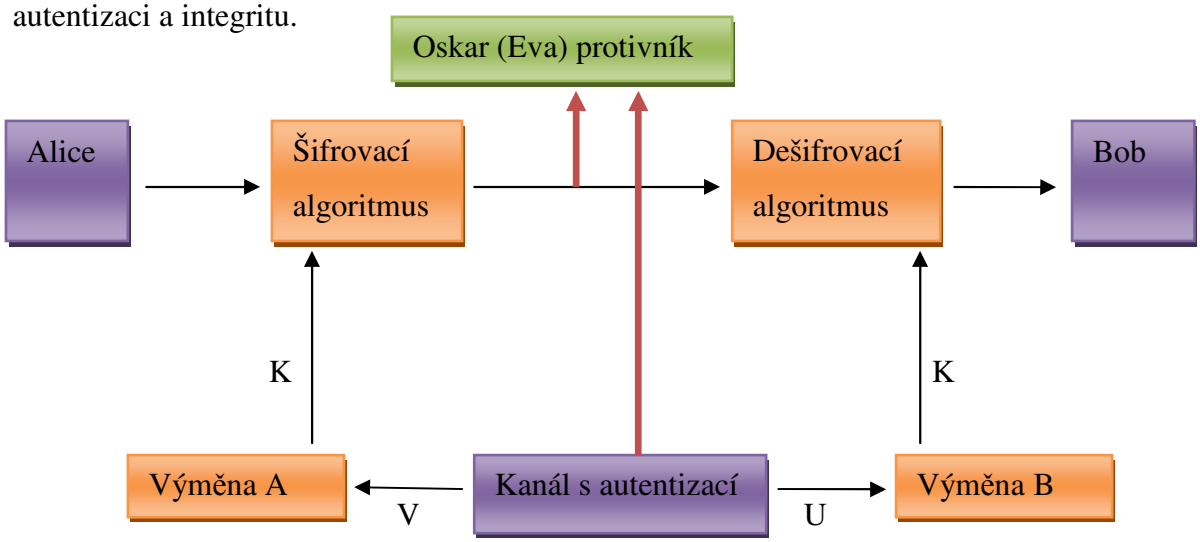
Definice

Je to kryptografický protokol, který umožňuje přes nezabezpečený kanál vytvořit mezi komunikujícími stranami šifrované spojení, bez předchozího dohodnutí šifrovacího klíče.

Výsledkem tohoto protokolu je vytvoření symetrického šifrovacího klíče, který může být následně použit pro šifrování zbytku komunikace.

Postup šifrování

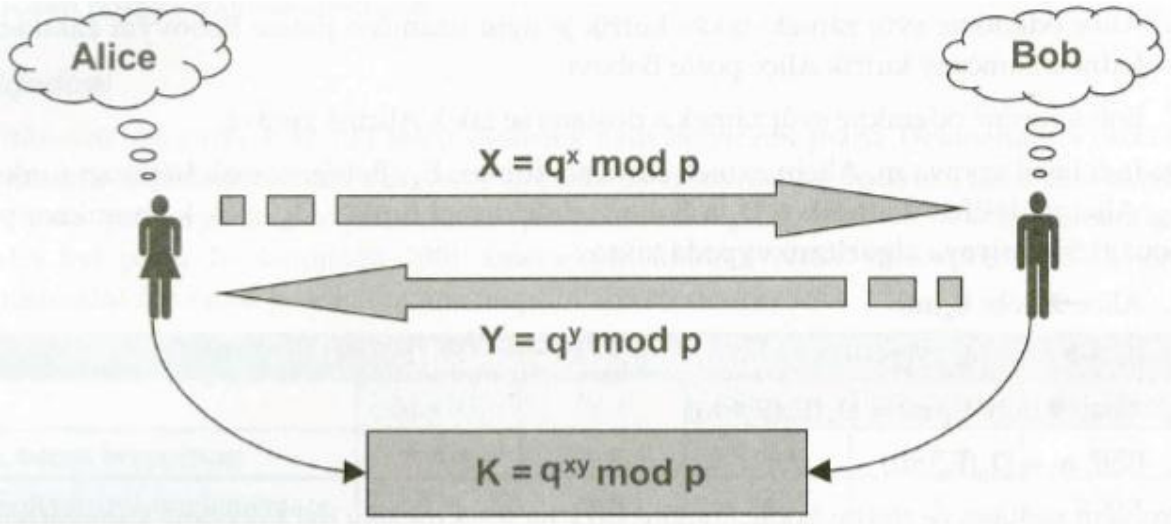
Protokol Diffieho-Hellmana (viz obrázek 17) zajišťuje ustanovení tajného klíče pro symetrickou kryptografii pomocí nezabezpečeného kanálu, který ale musí zajišťovat autentizaci a integritu.



Obrázek 17 Protokol Diffie-Hellman

K … klíč

U, V … zprávy, kroky protokolu



Obrázek 18 Schéma protokolu Diffie-Hellman

Obrázek 18 funguje na tomto principu[4]:

1. Alice a Bob se dohodnou na velkém prvočíslu **p** a **q**.
2. Alice si zvolí libovolné číslo **x** takové, že $\mathbf{1 \leq x < p-1}$, a vypočítá $\mathbf{X = q^x \bmod p}$, které pošle Bobovi.
3. Bob si zvolí libovolné číslo **y** takové, že $\mathbf{1 \leq y < p-1}$, a vypočítá $\mathbf{Y = q^y \bmod p}$, které pošle Alici.
4. Alice vypočítá $\mathbf{Y^x \bmod p}$ a Bob vypočítá $\mathbf{X^y \bmod p}$.
5. Jak Alice tak i Bob nyní vlastní tajný šifrovací klíč **K** pro symetrickou kryptografii, protože $\mathbf{K = Y^x \bmod p = (q^y)^x \bmod p = q^{xy} \bmod p = (q^x)^y \bmod p = X^y \bmod p = K}$.

Podmínky spolehlivosti

Výhodou je, že případný útočník, který odposlouchává komunikaci, nezachytí klíč. Klíč je zkonstruován všemi účastníky komunikace a nikdy není posílán v otevřené formě.

Možnosti útoku

Bez autentizace by mohli zlá Eva s Oskarem postupovat takto:

- Posadí se doprostřed kanálu mezi Alici a Boba.
- Uskuteční protokoly s Alicí a Bobem, s každým zvlášť.
- Získají tak symetrický klíč K pro komunikaci s Alicí a klíč L pro komunikaci s Bobem.
- Pošle-li Alice šifrovanou zprávu Bobovi, Eva s Oskarem ji dešifrují za pomoci příslušného klíče K, poté ji zašifrují pomocí klíče L a pošlou ji dále Bobovi.

Tomuto typu aktivního útoku se anglicky říká *Man in the middle*. Uvedený anglický název se běžně používá, protože vystihuje podstatu celého útoku.

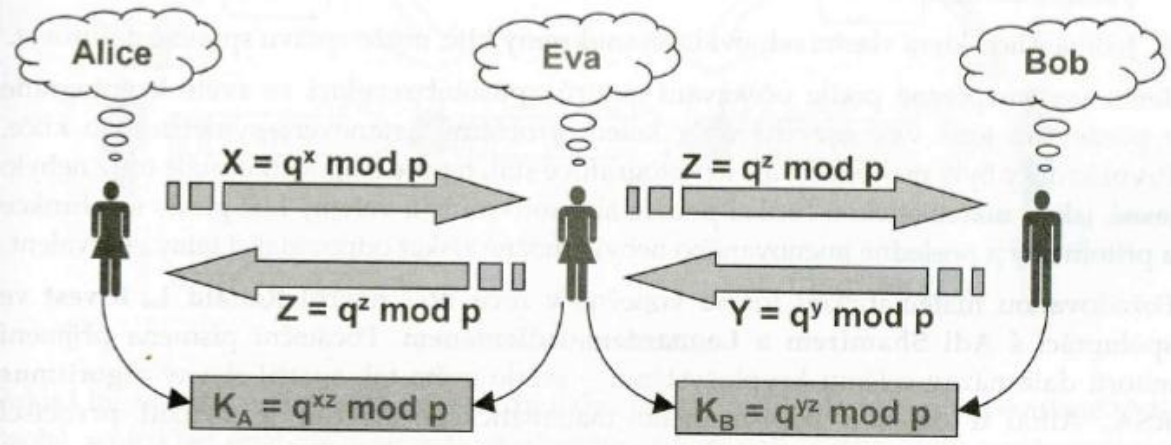
2.5.4 Man in the middle

Patří mezi největší problémy v informatice a kryptografii.

Definice

Jeho podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem. Důležitým faktem je, že v prostředí současných běžných počítačových sítí není nutné, aby komunikace přes útočníka přímo fyzicky procházela, protože lze síťový provoz snadno přesměrovat.

Postup šifrování



Obrázek 19 Schéma útoku Man in the middle

Obrázek 19 funguje na tomto principu [4]:

- Zákeřná Eva si zvolí vlastní číslo **z** a zachytí čísla $\mathbf{q^x \bmod p}$ a $\mathbf{q^y \bmod p}$.
- Eva pošle Alici i Bobovi číslo $\mathbf{q^z \bmod p}$. Alice se v tuto chvíli mylně domnívá, že obdržela číslo $\mathbf{q^y \bmod p}$ původního protokolu. Podobně si také Bob myslí, že obdržel číslo $\mathbf{q^x \bmod p}$.
- Eva vypočítá $\mathbf{K_A = q^{xz} \bmod p}$ a $\mathbf{K_B = q^{yz} = \bmod p}$.
- Alice s Bobem si přesně podle posledního kroku původního protokolu vypočítají svá čísla $\mathbf{K_A = q^{xz} \bmod p}$ a $\mathbf{K_B = q^{yz} = \bmod p}$, která se však díky Evinu zásahu nerovnají!

Když teď Alice pošle zprávu šifrovanou pomocí svého klíče $\mathbf{K_A}$, Eva ji zachytí, dešifruje a pošle Bobovi šifrovanou klíčem $\mathbf{K_B}$. Podobně pak Eva pokračuje, když zprávu pošle Bob. Je šifrovaná pomocí klíče $\mathbf{K_B}$, Eva ji zachytí, dešifruje a pošle Alici šifrovanou klíčem $\mathbf{K_A}$.

Takto má Eva veškerou kontrolu nad komunikací Alice a Boba.

Podmínky spolehlivosti

Obvyklé řešení je použití veřejných klíčů, ale i tady je možné narazit na problém.

Možnosti útoku

Při MITM útoku nemusí být v případě spoléhání na digitální certifikát nutné, aby útočník filtroval celou komunikaci. Stačí otrávit DNS (Domain Name System) nebo ARP (Address Resolution Protocol) cache uživatele a tímto ho nevědomky přesměrovat na jiné webové servery.

Útok lze řešit několika způsoby:

- Vzájemnou výměnou veřejných klíčů jiným, bezpečným kanálem.
- Ověřením získaných veřejných klíčů jiným bezpečným kanálem, nejlépe pomocí jejich otisku.
- Ověřením klíčů pomocí elektronického podpisu Alice i Boba pomocí certifikační autority nebo sítě důvěry.

Kvantová kryptografie umožňuje připravit takový kanál, který je z principu neodposlouchávatelný, protože každou snahu o odposlouchávání dokáže pravý příjemce detekovat.

3 ASYMETRICKÉ ŠIFRY

3.1 RSA (iniciály autorů Rivest, Shamir, Adleman)

Je to šifra s veřejným klíčem, která vznikla v 1977. Jedná se o první algoritmus, který je vhodný jak pro podepisování, tak i šifrování.

3.1.1 Definice

Alfou a omegou popisovaného matematického návrhu je využití prvočísel a faktorizace (rozložení složeného čísla na součin prvočísel), která se považuje za prakticky neřešitelný problém.

Z čísla n = p * q je v rozumném čase prakticky nemožné zjistit činitele p a q. není dosud znám žádný algoritmus faktorizace, který by pracoval v polynomiálním čase.Naproti tomu násobení dvou velkých čísel je elementární úloha.

3.1.2 Postup šifrování

Nejdůležitější je dvojice klíčů (soukromý a veřejný). Generují se následovně:

- Zvolí se dvě různě velká prvočísla **p** a **q.**
- Vypočítá se jejich součin **n = p * q.**
- Vypočte se hodnota Eulerovy funkce **Φ(n) = (p - 1)(q – 1).**
- Zvolí se celé číslo e menší než Φ(n), které je s Φ(n) nesoudělné.
- Nalezne se číslo d tak, aby platilo **d * e = 1 (modΦ(n)).**
- Jestli je e prvočíslo tak **d = (1 + r * Φ(n)) / e**, kde **r = [(e – 1)Φ(n)^(e – 2)].**

Veřejným klíčem je dvojice (n, e), přičemž **n** se označuje jako modul, **e** se označuje jako šifrovací či veřejný exponent.

Soukromým klíčem je dvojice (n, d), kde **d** se označuje jako dešifrovací či soukromý exponent.

Veřejný klíče se uveřejní a soukromí se uchová v tajnosti.

RSA klíče jsou většinou 1024 – 2048 bitů dlouhé.

Pokud bude chtít Bob poslat Alici šifrovanou zprávu **m**, udělá to následovně:

- Sežene si Alicin volně dostupný veřejný klíč (e, n).
- Vypočítá $\mathbf{c = m^e \bmod n}$ a pošle tuto hodnotu Alici.

- Alice zprávu jednoduše dešifruje pomocí $\mathbf{m = c^d \bmod n.}$

Příklad na šifrování a dešifrování

V tomto příkladu jsou pro jednoduchost použita extrémně malá čísla, v praxi se používají o mnoho řádů větší.

p = 61 (první prvočíslo)

q = 53 (druhé prvočíslo)

n = p*q = 3233 (modul, veřejný)

e = 17 (veřejný, šifrovací exponent)

d = 2753 (soukromý, dešifrovací exponent)

Pro zašifrování zprávy 123 probíhá výpočet:

- šifruj $123 = 123^{17} \bmod 3233 = 855$

Pro dešifrování pak:

- dešifruj $855 = 855^{2753} \bmod 3233 = 123$

3.1.3 Podmínky spolehlivosti

S délkou klíče stoupá obtížnost prolomení šifry. Plné dešifrování RSA šifrovaného textu je obtížné a v podstatě neproveditelné, jelikož neznáme algoritmus, pomocí nějž by se to dalo provést.

V roce 1993 byl představen Shorův algoritmus, který ukazoval, že by kvantový počítač mohl v principu vykonávat faktorizaci v polynomiálním čase, což by učinilo RSA a příbuzné algoritmy zastaralými. Realizace principů kvantového počítání se však v současnosti potýká s takovými praktickými problémy, že o bezpečnost zašifrovaných dat se není třeba bát.

3.1.4 Možnosti útoku

Jsou známi útoky, kdy útočník Eva zná dostatečně hardware Alice a je schopna změřit dešifrovací časy na několika známých šifrovaných textech, může odvodit klíč dešifrování d rychle.

Další útok, praktický, schopný obnovovat RSA faktorizaci přes síťové připojení.

Způsob, jak zmařit tyto útoky je, že musíme zajistit, aby operace dešifrování vzala konstantní množství času na každý šifrovaný text.

V současné době je šifra považována za bezpečnou a je používána.

3.2 El-Gamal

Autorem je Taher ElGamal, popsal jej ve své PhD disertaci *Cryptography and logarithms over finite fields*, Stanford University 1984.

Tento systém má ovšem nevýhodu, že šifrovaná data jsou dvakrát delší než data nešifrovaná. To je možná důvod důvodem, proč jeho nasazení není tak masivní. ElGamal spoléhá na problém výpočtu diskrétního logaritmu.

3.2.1 Definice

Nechť jsou zvolena veřejně známá čísla **q**, tzv. modul a **g** co nejvyššího řádu. I-tý účastník si volí svůj tajný klíč $\mathbf{y_i}$ a vypočte veřejný klíč $\mathbf{k_i^{pub}}$ jako $\mathbf{g^{y_i} mod\ q}$. Pokud potom Alice posílá zprávu P Bobovi (zpráva musí být menší ne q), probíhá komunikace podle následujícího schématu:

- Je zvolené náhodné číslo **k**
- Spočte se $\mathbf{g^k\ mod\ q}$ a $\mathbf{Q = P*(}g^{y_B}\mathbf{)^k\ modulo\ q}$ a obě tato čísla pošle Alice Bobovi
- Bob spočte $(\mathbf{q^k})^{y_B}\ \mathbf{mod\ q}$ a k tomuto číslu určí inverzní prvek (vzhledem k operaci násobení)
- Bob spočte zprávu P jako $\mathbf{P = Q * ((q^k)^{y_B})^{-1}}$

3.2.2 Postup šifrování

- Dva veřejné parametry jsou velké prvočíslo **p** a kladné číslo **g** menší než **p** takové, že $\mathbf{g^x\ mod\ p}$ je různé od 1 pro každé kladné $\mathbf{x < p-1}$.
- Generátor klíče nyní vygeneruje náhodné kladné **x** a spočítá číslo $\mathbf{y = g^x\ mod\ p}$.
- Veřejný klíč je $\mathbf{K_P = y}$.
- Tajný klíč je $\mathbf{K_S = x}$.
- Zpráva je zakódována jako nenulové číslo **m** menší než **p**.

Šifrování probíhá tak, že odesilatel zvolí náhodné nenulové číslo **r** menší než **p**, spočítá $\mathbf{u = g^r\ mod\ p}$ a $\mathbf{v = m * y^r\ mod\ p}$. Šifrová zpráva je **(u, v)**.

Dešifrování probíhá tak, že se spočte číslo **v * u^{-x} mod p**. proběhnou-li výpočty správně, pak **m = v * u^{-x} mod p**.

3.2.3 Podmínky spolehlivosti

Na prolomení tohoto systému by musel útočník vyřešit problém diskrétního logaritmu, což je považováno za výpočetně složitý systém.

3.3 DSA (Digital Signature Algorithm)

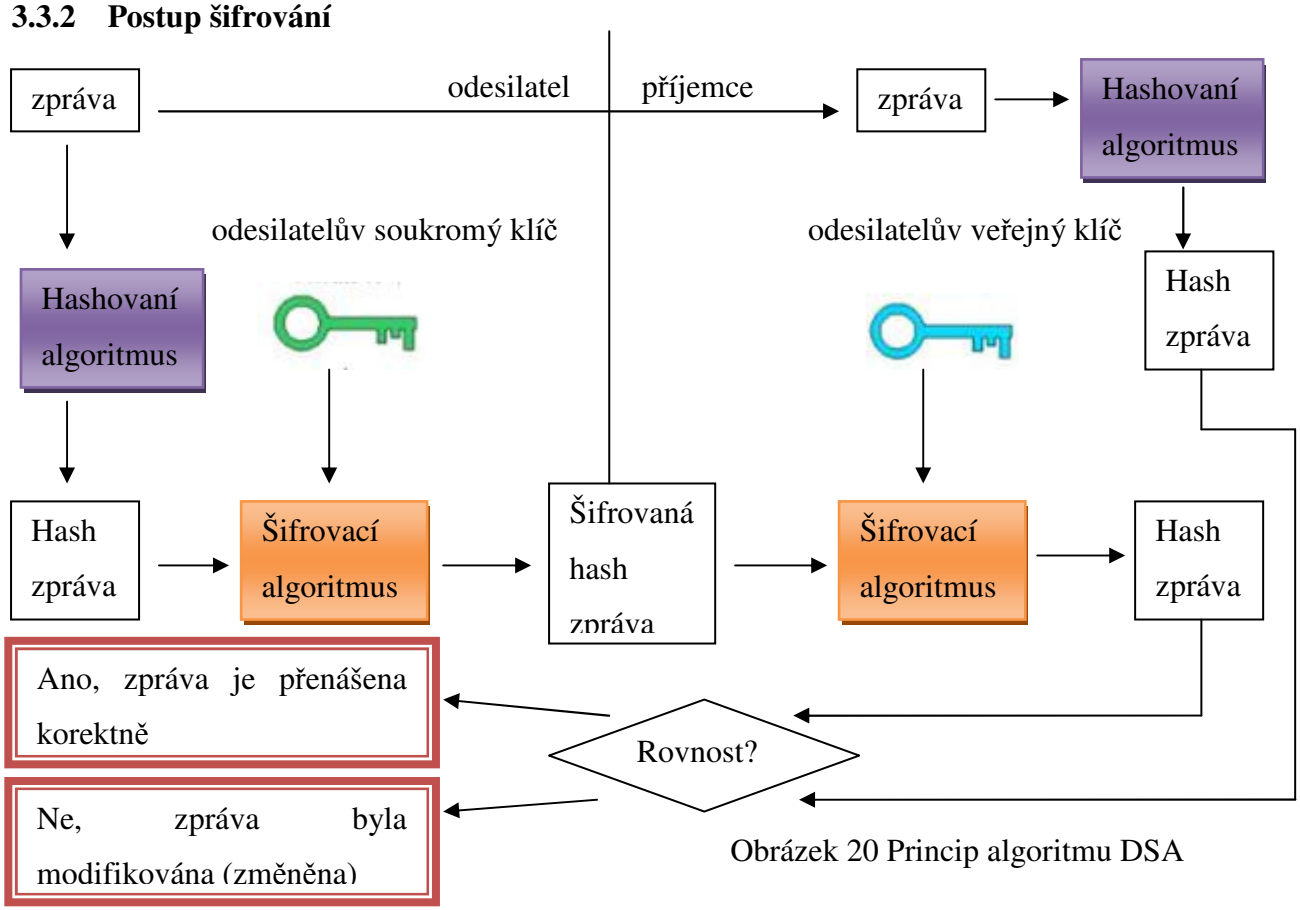
Je to standart americké vlády pro digitální podpis. Byl navržen americkým institutem NIST v roce 1991 pro použití v protokolu DSS (Digital Signature Standard) používaný od roku 1993.

Poslední úpravou prošel v roce 2000 a nyní je veden jako FIPS186-2.

3.3.1 Definice

Elektronický podpis je vlastně informace, která se připojuje k elektronickým datům, aby identifikovala odesilatele příjemci.

3.3.2 Postup šifrování



Obrázek 20 Princip algoritmu DSA

Princip obrázku 20 je následující:

- Vysílač před odesláním zprávy spočítá otisk této zprávy.
- Tento vypočítaný otisk zašifruje svým privátním klíčem a spolu s vlastní zprávou pošle příjemci.
- Příjemce vypočítá veřejným klíčem vysílače také otisk přijaté zprávy a porovná vypočítaný otisk s otiskem, který získal od příjemce.
- Pokud jsou oba otisky totožné, je tedy přijatá zpráva v takovém tvaru, v jakém ji vysílač skutečně poslal.

Vytváření klíčů má dvě fáze. Ve fázi první se vyberou parametry algoritmu, které mohou být sdíleny více různými uživateli systému.

- Především se musím provést výběr kryptografické hashovaní funkce.
- Pak se rozhodne o parametrech **L** a **N**, které určují délku klíče.
- Dále se vybere N-bitové prvočíslo **q**. Délka N musí být alespoň taková, jako délka výstupu použité hashovaní funkce.
- Dále se vybere L-bitové prvočíslo **p** takové, že p – 1 je násobek q.
- Nakonec se vybere takové číslo **g**, jehož multiplikativní řád modulo p je právě q. Toho lze dosáhnout dosazením do vzorce $\mathbf{g = h^{(p-1)/q} mod\ p}$ pro náhodná **h** (kde $1 < h < p-1$).

Tyto metody nejsou tajné, následuje metoda vytvoření samotných klíčů.

- Nejdříve se náhodně vybere **x** v rozsahu $0 < x < q$.
- Pak se spočítá $\mathbf{y = g^x\ mod\ p}$.
- Veřejný klíč je pak dán jako čtveřice **(p, q, g,y)** a soukromý klíč je **x**.

3.3.3 Podepisování

Při označení hashovaní funkce **H** a zprávy písmenem **z** probíhá podepisování takto:

- Pro danou zprávu se vybere náhodná hodnota **k** v rozsahu $0 < k < q$.
- Spočítá se $\mathbf{r = (g^k\ mod\ p)\ mod\ p}$.
- Spočítá se $\mathbf{s = (k^{-1}(H(z) + x * r)\ mod\ p}$.
- V nepříliš pravděpodobném případě, že je r=0 nebo s=0 se výpočet opakuje od začátku.
- Jinak je podpisem dvojice **(r, s)**.

3.3.4 Ověřování podpisu

Pokud neplatí $0 < r < q$ a $0 < s < q$ je podpis automaticky zamítnut. Jinak se počítá následovně:

- Spočítá se $\mathbf{w = (s)^{-1} \bmod q}$.
- Dále se spočítá $\mathbf{u_1 = (H(z) * w) \bmod q}$.
- Pak se spočítá $\mathbf{u_2 = (r * w) \bmod q}$.
- A nakonec se spočítá $\mathbf{v = ((g^{u1} * y^{u2}) \bmod p) \bmod q}$.

Podpis je platný pokud $\mathbf{v = r}$.

3.3.5 Podmínky spolehlivosti

Největším problémem byla ověřitelnost elektronického podpisu, proto byl vytvořen tzv. digitální podpis, který umožňuje jednoznačnou identifikaci osoby.

3.3.6 Možnosti útoku

Systém je považován za bezpečný a je široce využíván, např. OpenSSL, OpenSSH nebo GnuPG.

3.4 PGP (Pretty Good Privacy)

Ječ to výsledek úsilí Phila Zimmermanna, který kombinuje symetrickou a asymetrickou šifru.

První verze byla uvolněna v roce 1991. Je založen na algoritmu RSA.

PGP mělo takový vliv, že byl standardizován, aby byla umožněna spolupráce s různými typy PGP a podobného softwaru. PGP bylo přijato jako internetový standard pod názvem OpenPGP.

3.4.1 Definice

PGP je kombinovaný šifrovací systém. Navenek se jeví jako program s veřejným šifrovacím klíčem, plně využívající asymetrického šifrování.

To se však používá pouze pro zakódování klíče symetrické šifry, kterou je pak zašifrována samotná zpráva. Digitálním podpisem je kontrolní součet zprávy (anglicky hash), který je zašifrován asymetrickou šifrou.

3.4.2 Postup šifrování

- Alice zvolí symetrický šifrovací klíč $\mathbf{K_{AB}}$ a zašifruje jím otevřený text **m**.
- Alice ⟶ Bob : $\mathbf{c = K_{AB}(m)}$ a $\mathbf{V_B(K_{AB})}$, kde $\mathbf{V_B}$ je Bobův veřejný klíč.
- Bob spočítá $\mathbf{K_{AB} = S_B(V_B(K_{AB}))}$ a $\mathbf{m = K_{AB}(c)}$, kde S_B je Bobův soukromý klíč.

PGP tedy kóduje text symetrickým algoritmem. Jeho implementace je mnohem rychlejší. PGP nejprve vygeneruje náhodný klíč pro symetrickou šifru, tento klíč zakóduje do zprávy s pomocí veřejného RSA nebo DH klíče příjemce, a celou zprávu pak zakóduje symetrickou šifrou. Příjemce nejprve s pomocí svého soukromého nebo DH klíče zjistí klíč pro symetrickou šifru, s jehož pomocí pak dešifruje celou samotnou zprávu.

Postup kódování v PC:

Úplně nejdříve je původní text (plaintext) zkomprimován. Pro komprimaci je využita Freeware rutina PKZIP verze 2.x.

Při každém zakódování jakéhokoli dokumentu je prvně náhodně vygenerován konvenční (symetrický) klíč (je generován dle rychlosti stisku kláves a podle pohybu myši – generován soubor Randseed). Tímto klíčem je zakódován zkomprimovaný vlastní dokument. Jelikož jde o symetrickou šifru je proces velmi rychlý.

PGP využívá 3 druhy symetrických klíčů. Všechny tři pracují s 64 - bitovými bloky. Jedná se CAST, TripleDES a IDEA. Tyto byly vytvořeny mimo PGP a do něj pouze přidány. CAST a IDEA používají 128bitové klíče a TripleDES používá 168bitový.

Dalším krokem je zakódování symetrického klíče klíčem veřejným. Zde se již jedná o pomalejší proces, ale jelikož je délka symetrického klíče relativně malá, jde to velmi rychle.

Obě tyto část jsou spojeny do jednoho souboru a teprve potom se jedná o PGP zašifrovaná data.

3.4.3 PGP a digitální podpis

OPenPGP je název standardu, který Phil Zimmermann v roce 1997 navrhl IETF (Komise techniky Internetu). OpenPGP je tak aktivně vyvíjeným internetovým standardem. Tento standard podporuje mnoho e-mailových klientů a umožňuje tak pracovat s digitálními podpisy a šifrovanými zprávami.

Postup je následující:

- Alice podepíše původní zprávu **m** svým klíčem digitálního podpisu $\mathbf{sign_A}$ a dostane tím zprávu $\mathbf{s = sign_A(m)}$.
- Zprávu **s** nyní Alice zašifruje Bobovým veřejným klíčem asymetrické kryptografie $\mathbf{V_B}$ a získá tak šifrovanou zprávu $\mathbf{c = V_B(s) = V_B(sign_A(m))}$.
- Alice $\longrightarrow$ Bob: $\mathbf{c = V_B(s) = V_B(sign_A(m))}$.
- Bob dešifruje zprávu **c** svým soukromým klíčem asymetrické kryptografie a získá tak podepsanou zprávu $\mathbf{s = sign_A(m)}$. Pomocí volně dostupného klíče $\mathbf{versign_A}$, který jediný odpovídá Alicinu podepisovacímu klíči $\mathbf{sign_A}$, si následně ověří, že odesilatelem je skutečně Alice.

3.4.4 Podmínky spolehlivosti

Po vzniku platil zákaz vyvážení programu mimo hranice USA. Z důvodu jeho kvalit byl zařazen do podobné kategorie jako například zbraně. Šifrování s tímto programem je na úrovni šifrování armády Spojených Států.

3.4.5 Možnosti útoku

Systém je považován za bezpečný a je používaný.

3.4.6 Možnosti použití

Komerční i nekomerční – volné použití s omezenou funkčností.

- Elektronický podpis
- Ochrana souborů
- Ochrana disků
- Ochrana na úrovni serverů

3.5 Digitální podpis

Digitální podpis představuje nejúčinnější prostředek pro zajištění integrity odesílaných dat a bezpečné ověření jejich odesilatele.

Použití digitálního podpisu je proto omezeno na případy, kdy je jako komunikační prostředek používán počítač.

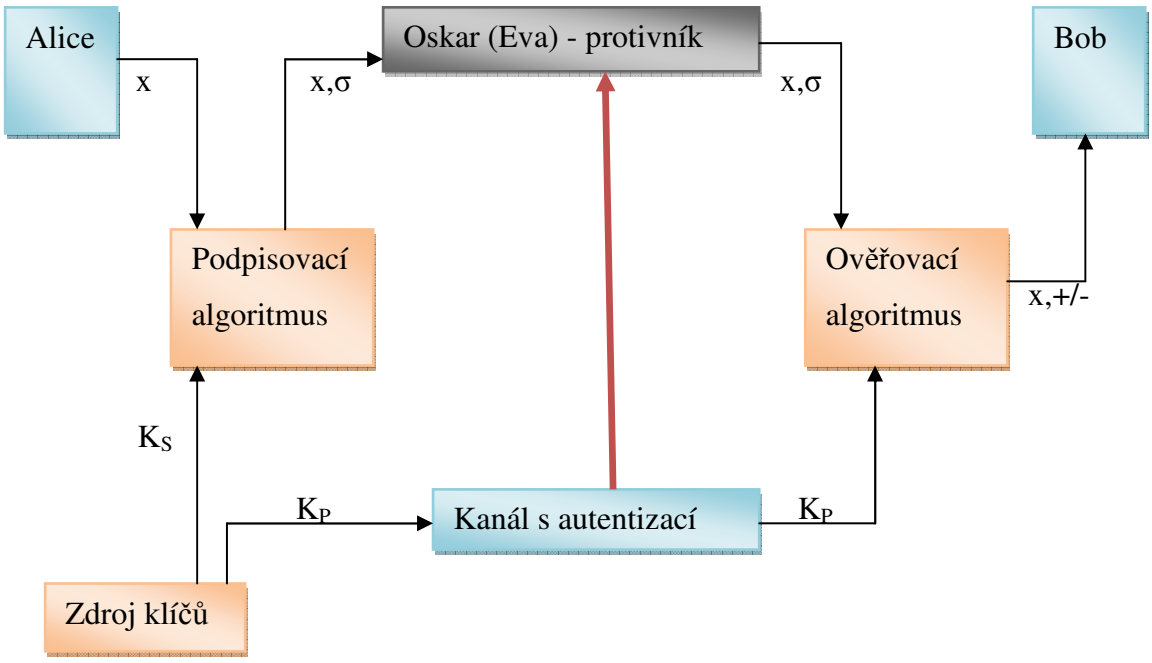
3.5.1 Definice

Digitální odpis je v podstatě spojení klasického elektronického podpisu s certifikátem zajišťujícím identitu člověka.

Tak je zajištěno svázání podpisu s určitou osobou. K tomu, aby byl digitální podpis skutečně důvěryhodný, je dobré, aby byl certifikát ověřen třetí nezávislou osobou, která tak ručí za jeho pravost. Takovou instancí je právě certifikační autentizace.

3.5.2 Princip funkce

Principem běžného elektronického podpisu je zašifrování dokumentu tajným klíčem a jeho následovné dešifrování veřejným klíčem. Oba klíče si můžeme představit jako velmi vysoká čísla. Aby bylo šifrování účinné, nesmí být znám postup, pomocí kterého by bylo možné ani s nasazením nejdokonalejších počítačů vypočítat z veřejného klíče tajný klíč. Kdo nezná tajný klíč, není schopen zašifrovat dokument tak, aby jej bylo možné dešifrovat veřejným klíčem. Tajná klíč tedy musí znát jen autor dokumentu. Postup je vidět na obrázku 21.



Obrázek 21 Princip digitálního podpisu

3.5.3 Postup šifrování

Digitální podpis je vytvořen takto:

- Nejprve je z podepisovaných dat vypočten kryptografický kontrolní součet.
- Z tohoto součtu je na základě tajného klíče vypočten digitální podpis.

Ověřování digitálního podpisu probíhá obdobně:

- Příjemce ověří, že digitální podpis vyhovuje veřejnému klíči odesilatele.
- Vypočte kryptografický kontrolní součet přijatých dat a porovná jej s kryptografickým kontrolním součtem, který obdržel od odesilatele.
- Pokud součty odpovídají, je ověřeno, že data po odeslání nebyla změněna.

Algoritmy pro šifrování digitálního podpisu:

- Asymetrické algoritmy s veřejným klíčem. Nejčastěji to jsou RSA a DSA.
- Bezpečné jednocestné kryptografické algoritmy (hashovaní funkce), nejčastěji MD5 spolu s RSA a SHA (Secure Hash Algorithm) spolu s DSA.

3.5.4 Podmínky bezpečnosti

Digitální podpis musí zajistit několik bezpečnostních cílů:

- Nezfalšovatelnou podpisu – pro útočníka musí být nemožné bez znalosti tajného klíče K_S vytvořit ke zprávě x platný podpis σ.
- Musí to platit i v situaci, kdy útočník má k dispozici několik platných podpisů (x_i, σ_i), dokonce i když si může volit zprávy x_i.
- Nepopiratelnost podpisu – ten kdo zprávu podepsal, nesmí mít později možnost svůj podpis popřít. To znamená, že autor podpisu nemůže dokázat, že podpis lze zfalšovat.

3.5.5 Možnosti útoku

Podvržení podpisu může mít několik podob:

- Úplné prolomení systému - Spočívá v tom, že útočník dokáže ze znalosti veřejného klíče K_P získat tajný klíč K_S.
- Univerzální podvržení – Na základě veřejného klíče K_P útočník dokáže vytvořit algoritmus, který vytváří platné podpisy k libovolné zprávě x.

- Selektivní podvržení – Na základě veřejného klíče K_P útočník dokáže vytvořit zprávu, ke které pak umí připojit platný podpis.
- Existenční podvržení – Na základě veřejného klíče K_P je útočník schopen vytvářet dvojice (x, σ), kde σ je platný podpis zprávy x. Nemá ale žádnou kontrolu nad tím, jak zpráva x vypadá.

3.5.6 Princip bezpečné komunikace

V současné době není na internetu žádný problém zfalšovat podpis a e-mailovou adresu odesilatele, a pak se vydávat ze někoho jiného.

Certifikát však zfalšovat nelze. Jestliže připojíte k e-mailu digitální podpis s certifikátem, adresát si může ověřit, že osoba, se kterou komunikuje, jste skutečně vy.

Typy certifikátů:

- Osobní – určeny k ověření totožnosti jednotlivých osob
- Serverové – určeny pouze pro servery a ty zastupuje vlastník serveru. Tyto certifikáty jsou určeny pro bezpečnou komunikaci uživatelů se serverem.

Dále máme typy certifikátů podle úrovně:

- Kvalifikovaný certifikát – splňuje všechny aktuální požadavky dané legislativou, zejména Zákonem o elektronickém podpisu (Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů ve znění zákona 226/2002 Sb.). Je vhodný především pro komunikaci občanů se státní správou a samosprávou.
- Komerční certifikát – pro použitá v uzavřených systémech, kde je mezi účastníky bezpečné komunikace současně uzavřena smlouva, řešící mimo jiné i podmínky komunikace.

3.6 Hash funkce (hašovací funkce)

Je to matematická funkce pro převod vstupních dat do relativně malého čísla. Výstup této funkce se označuje jako výtah, miniatura, otisk, fingerprint nebo hash (česky někdy jako haš).

3.6.1 Definice

Hašovací funkce pro vstup libovolné délky vytvoří otisk pevné délky, takže z desetimegabytového souboru získáme například 128bitový haš. Malá velikost výsledného otisku patří mezi charakteristické vlastnosti hašovacích funkcí.

Mezi hlavní vlastnosti patří:

- Jakékoli množství vstupních dat poskytuje stejně dlouhý výstup (otisk).
- Malou změnou vstupních dat dosáhneme velkou změnu na výstupu (tj. výsledný otisk se od původního se zásadně liší už na první pohled).
- S hashe je prakticky nemožné rekonstruovat původní text zprávy.
- V praxi je vysoce nepravděpodobné, že dvěma různým zprávám odpovídá stejný hash.

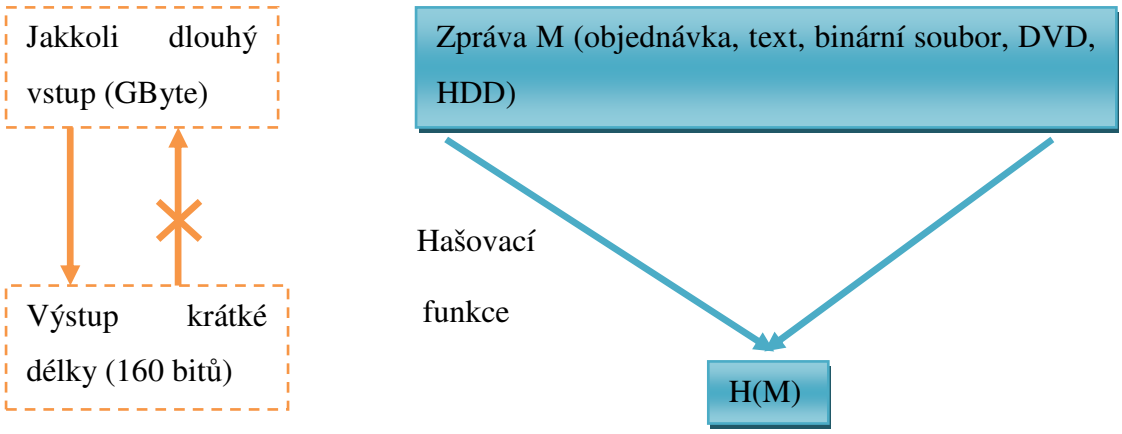
3.6.2 Postup šifrování

Požadovaným rysem je jednosměrnost. Ta zajišťuje, že pro libovolný vstup x je snadné vypočítat výsledný haš **h(x)**, ale v rozumném čase nesmí být možné pro dané **y** nalézt takové **x**, že **h(x) = y** [4].

Také by měla zajišťovat bezkoliznost. To znamená, že pro dané **x** nelze v rozumném čase nalézt **x´** takové, že **x ≠ x´** a **h(x) = h(x´)** (viz. Obrázek 22).

Perfektní hašování je specifická varianta hašování. Předpokládejme, že máme množinu klíčů S. Pak můžeme najít takovou hašovací funkci, která pro danou množinu nebude mít ani jednu kolizi.

Perfektní hašování se dělí na statické a dynamické. A to podle toho, zda se množina S v době existence perfektní hašovací funkce mění.



Obrázek 22 Princip hašovací funkce

3.6.3 MD2

Funkce vyvinuta Ronaldem Rivestem v roce 1989. Algoritmus byl původně optimalizován pro 8 bitové procesory [4]. I v dnešní době se s touto starší funkcí můžeme stále setkat. Výsledný haš má velikost 128 bitů, ale v současné době již není MD2 považován za bezpečný [4].

3.6.4 MD4

Byl také vyvinut profesorem Rivestem a stejně jako jeho předchůdce MD2 vytváří 128 - bitové otisky. Z návrhu MD4 čerpaly některé další hašovací funkce.

Ani MD4 se dnes již nepoužívá, protože byly objeveny slabiny, které působí kolize.

3.6.5 MD5

Nejznámější algoritmus od Ronalda Rivesta navržený v roce 1991. Algoritmus MD5 byl a stále ještě je hojně používán, ačkoliv i v něm se vyskytují slabiny a délka výsledného otisku 128 bitů již není považována za dostatečně bezpečnou [4].

3.6.6 HAVAL

Vznik se datuje rokem 1992, vytvořil jej trojčlenný tým Yuliang Zheng, Josef Pieprzyk a Jennifer Seberryová. MD algoritmy poskytují pouze pevnou délku otisku, naproti tomu HAVAL má možnost volby z více variant – 128, 160, 192, 224 a 256 bitů. Při použití délky 128 bitů však byly nalezeny některé slabiny [4].

3.6.7 SHA

Soubor algoritmů SHA (Secure Hash Algorithm) vznikl v dílnách NSA (National Security Agency) [4]. První verze byla navržena v 1993. Tato první verze dostala později označení SHA-0, aby nedošlo k záměně s jejími následníky.

O dva roky později vzniklo SHA-1 a několik mírně modifikovaných variant SHA-224, SHA-256, SHA-384 a SHA-512, které se někdy společně označují jako SHA-2.

3.6.8 RIPEMD-160

Algoritmus RIPEMD (RACE Integrity Primitives Evaluation Message Digest) navrhli Hans Dobertin, Anton Bossealers a Bart Preneel [4].

Oproti SHA se jedná o výsledek akademického úsilí a jak již sám název napovídá, jedná se o otisk o délce 160 bitů. Jak bezpečností, tak i výkonem jsou si oba zmiňované algoritmy velice podobné [4].

3.7 Steganografie

Úkolem steganografie je skrýt samotnou existenci zprávy, zpráva přitom může být napsána nebo předána ve srozumitelné podobě [1].

Je zřejmé, že sem patří velké množství nejrůznějších technik pro utajený přenos zpráv [1].

Jako malá zajímavost může být uvedena událost, která je považována za jeden z nejstarších příkladů využití steganografie. Jedná se o kuriózní metodu, kdy Histiaeus napsal zprávu na oholenou hlavu svému otroku, který až poté co mu opět narostly vlasy, ji dopravil do Milétu a pomohl tak koordinaci povstání proti Peršanům.

Během staletí byly použity stovky méně či více zdařilých způsobů utajení zpráv [1]. Vyjmenujme zde jen nejpoužívanější:

- Použití neviditelného inkoustu
- Vyznačení písmen v jinak nezávadném textu
- Ukrytí znaků otevřeného textu na předem domluvených pozicích
- První (druhá, poslední) písmena některých domluvených slov v dopise tvoří krátký utajený text
- Zápis šachové partie
- Notový zápis
- Návod na vaření, háčkování, …
- Zmenšení textu
- Použití mikroteček

Všechny uvedené metody byly skutečně používány a za jistých okolností byly používány velmi úspěšně a efektivně.

Tři nejdůležitější jsou Cardanova mřížka, agenturní systém a použití neviditelných inkoustů.

3.7.1 Cardanova mřížka

Tento systém byl navržen v 16. století milánským fyzikem, astronomem a matematikem Girolamo Cardano.

Jedná se typický steganografický systém, založený na jednoduchém skrytí textu v otevřené zprávě, je to jednoduchá a relativně účinná metoda.

Základem systému je obdélníková nebo čtvercová mřížka, ve které se vystřihnou určitá místa, vzniklá šablona se položí na papír a do děr se zapíše utajované sdělení [1]. Šablona se zvedne a doplní se zbytek písmen tak, aby text vypadal jako obyčejná nezávadná zpráva [1]. Dešifrování je opět velmi prosté, příjemce přiloží mřížku na obdrženou zprávu a text v dírkách si jednoduše přečte.

3.7.2 Agenturní systém

Tento systém se v minulosti v různých variantách skutečně používal. Oblíbený byl na obou stranách železné opony a v době studené války.

V textu dopisu bylo na domluveném místě (např. konec druhého slova v každé větě) písmeno otevřeného textu. Charakteristická vlastnost pro takto vytvořené texty byla jejich kostrbatost a nepřirozená slovní zásoba, ale hlavní výhodou bylo, že při běžném zhlédnutí textu se utajilo odesílání senzitivní informace.

Při dodržení různých pravidel může být tento systém bezpečný.

3.7.3 Neviditelné inkousty

Použití této metody zajišťuje, že zapsaný text není při běžném pohledu viditelný. Příjemce zobrazí neviditelný text jemu známým způsobem, což může například být zahřátí, působení nějakých chemikálií případně osvícení ultrafialovým nebo infračerveným světlem.

Obliba tohoto jednoduchého a relativně bezpečného způsobu přetrvala dodnes [1].

Typy inkoustů jsou rozděleny do tří skupin. První skupinu tvoří organické kapaliny, jako jsou třeba moč, mléko, ocet, citronové a ovocné šťávy. Takto napsaný text jednoduše zviditelníme pouhým lehkým zahřáním.

Druhou skupinou jsou chemické látky, které nejsou organického původu, ale zviditelníme je také pouhým lehkým zahřáním. Patří sem například roztok dusičnanu draselného.

Třetí skupinu tvoří využití chemických látek k zviditelnění písma. Toto využití je založeno na tvorbě barevných produktů po reakci s jinou chemickou látkou [1]. Takových inkoustů lze vytvořit celou řadu.

Jako papír pro většinu neviditelných písem je nejvýhodnější používat papír neklížený nebo ještě lépe filtrační [1], protože běžný kancelářský papír obsahuje pojiva, která někdy nevhodně reagují na příslušné chemické reakce.

3.8 Digitální steganografie

Využití digitálních technologií se nevyhnulo ani steganografii, která kromě automatizace jednotlivých metod získala díky různým formátům digitálních dat velké množství prostoru, kam ukrýt utajenou zprávu [2].

Pro digitální steganografii se používají podobné principy, jako v minulosti, jen dnes je zpráva ukrývána do digitálních dat, tedy souborů v počítači, a ne na papír.

Nejčastěji se můžeme setkat s ukrýváním dat do obrázků, zvukových či textových souborů, ale k ukrytí lze využívat také komunikační protokoly, databáze, souborové systémy a podobně.

Příklady:

- Obrázky vložené do video materiálů
- Obecné ukrývání do obrázků
- Ukrývání dat do "nejnižších" bitů zašuměných obrázků či zvuků
- Ukrývání dat do redundantních bitů (LSB) – pro JPEG formáty, software OutGuess, Steghide, atd.
- Ukrývání dat do náhodného či šifrového textu
- Skrývání dat do exe souborů, prodlevách v paketech posílaných po síti např. z klávesnice (vzdálené aplikace atd.)
- Další metody – žluté mikrotečky vytvářené moderními laserovými tiskárnami

Steganografické postupy mají mnoho společného s metodami tvorby vodoznaků, které mají za úkol vložit do dokumentu určité informace [2].

4 BIOMETRIKA

V posledních letech a desetiletích zaznamenaly zvýšenou pozornost biometriky a moderní biometrické systémy. I když kořeny biometriky sahají až do dob pár tisíc let před naším letopočtem.

Co to je vlastně biometrika? Slovo biometrie vzniklo spojením dvou řeckých slov bio a metric, kde prvně jmenované znamená život a druhé měření [4]. Biometrie tedy měří určité charakteristiky člověka a biometrické systémy potom slouží k ověřování identifikace nebo ověření identity člověka na základě jeho unikátních měřitelných fyziologických a behaviorálních vlastností.

4.1 Fyziologické a behaviorální vlastnosti

Mezi fyziologické vlastnosti patří otisk prstu nebo geometrie ruky a mezi behaviorální vlastnosti zase patří dynamika podpisu či dynamika stisku kláves na klávesnici. Porovnání je možné vidět v tabulce 6, tabulka 7 je legenda pro tabulku 6.

Přehled základních biometrik			
Typ	Biometrika	Přesnost	Cena
Fyziologické	otisk prstu	***	*
	geometrie ruky	**	**
	rozpoznání obličeje	**	**
	oční duhovka	***	***
	oční sítnice	***	***
	lůžko nehtu	***	**
	DNA	***	***
Behaviorální	ověřování hlasu	*	*
	dynamika podpisu	*	*
	dynamika stisku kláves	**	*

Tabulka 6 Přehled základních biometrik *Zdroj: Šifrování a biometrika aneb tajemné bity a dotyky*

Legenda	
nízká	*
střední	**
vysoká	***

Tabulka 7 Legenda k tabulce 6

4.2 Identifikace a verifikace

Biometrické systémy mohou pracovat ve dvou režimech: verifikačním a identifikačním [4]. Mnoho lidí si I v dnešní době myslí, že oba významy znamenají totéž.

Verifikace

Při tomto ověřování identity uživatel předkládá svoji totožnost a tu následně potvrzuje znalostí nějakého sdíleného tajemství. S verifikací, i když ne přímo biometrickou, se tedy setkáváme například vždy při přihlašování do PC pomocí hesla.

Skutečná verifikace probíhá tak, že uživatel předloží svoji identitu (login, identifikační kartu, ..) a poté mu čtecí zařízení nasnímá danou biometriku.

Identifikace

Toto ověřování indenty probíhá tak, že je uživatel rozpoznán automaticky, tj. bez předchozího předkládání totožnosti. V tomto případě se tedy jedná o časově tak i výpočetně náročnější proces než v případě verifikace.

4.3 Obecné výhody a nevýhody

Největší výhodou biometrik je, že nemůžou být zapomenuty, ztraceny a jsou nepřenosné [4]. Princip biometrické autentizace je relativně vysoký a stupeň zabezpečení a proto je vhodné nasazovat tyto systémy jako jednu z funkcí pro řízení přístupu.

Při vhodné volbě biometrického systému hraje důležitou roli uživatelská přívětivost. Snímání uživatelova vzorku při identifikaci musí být rychlé a nesmí působit nepříjemně [4]. Rychlost snímání bývá preferována především při frekventovaném využití systému mnoha uživateli [4].

Velkým problémem se stává při výběru jednotné biometrické technologie v masovém rozšíření to, že ne každý uživatel vybranou biometrií disponuje. Ne každý člověk totiž může poskytnout otisk prstu nebo vzorek hlasu.

4.4 Vlastnosti

V tabulce 8 jsou vidět některé vlastnosti základních biometrik. Aby byl biometrický systém snadno aplikovatelný v praxi, musí být uživateli co nejméně nepříjemný [4].

V tabulce 9 je legenda k tabulce 8.

Biometrika	Přesnost	Cena	Proměnlivost v čase	Uživatelská nepřijatelnost	Celkem
Otisk prstu	***	*	*	**	***
Geometrie ruky	**	**	**	**	**
Rozpoznání obličeje	**	**	**	*	**
Oční duhovka	***	***	*	*	***
Oční sítnice	***	***	**	***	**
Lůžko nehtu	***	**	**	**	**
DNA	***	***	*	***	**
Ověřování hlasu	*	*	***	*	**
Dynamika podpisu	*	*	**	*	**
Dynamika stisku kláves	**	*	*	*	**

Tabulka 8 Některé vlastnosti základních biometrik *Zdroj: Šifrování a biometrika aneb tajemné bity a dotyky*

Legenda	
nízká	*
střední	**
vysoká	***

Tabulka 9 Legenda k tabulce 8

ZÁVĚR

Tato práce se zabývá představením problematiky z oblasti moderní kryptologie.

V první části teoretické rešerše byly definovány základní pojmy z oboru šifrování. V dalších bodech se pak teoretická část zabývá historií šifrování v jednotlivých obdobích dějin a postupným vývojem až do současného stavu. Zmiňuje i výhled do budoucnosti v tomto oboru.

Praktická část pak ve svém úvodu nejdříve představuje klasické dělení šifer a poté se věnuje podrobnějšímu popisu šifer moderních. Ze symetrických jmenuje Vernamovu šifru, algoritmy DES, 3DES, AES a IDEA. Z asymetrických pak RSA, El-Gamal, DSA, PGP, Digitální podpis a Hash funkce. Jsou popsány jejich principy a použití. Je poukázáno na podmínky spolehlivosti, ale i možnosti útoku a prolomení těchto šifer a algoritmů.

Pro lepší pochopení je v praktické části vysvětlen i přechod od starší symetrické k asymetrické kryptografii, mezi jinými i princip a využití tzv. jednosměrné funkce.

Výstupem celé práce je pak prezentace, která bude sloužit k výuce problematiky šifrování na Univerzitě Tomáše Bati ve Zlíně.

ZÁVĚR V ANGLIČTINĚ

This work presents the principles of modern cryptography.

Basic concepts of encryption are defined in the first chapter of the theoretical part. Further on, the theoretical part describes the history of encryption in different periods of history and its development to the present state. The vision of the future in this area is also mentioned in this part.

The practical part starts with introducing the standard classification of codes and follows with a detailed description of modern codes. The Vernam cipher, DES, 3DES, AES, and IDEA algorithms are used to represent symmetrical codes. Then RSA, EL-GAMAL, DSA, PGP algorithms, digital signature and hash function are named as examples of asymmetric codes. Their principles and applications are described. The conditions of reliability, but also the possibilities of attack and breaking of these codes and algorithms are pointed out. For a better understanding of the transition from older symmetric to asymmetric cryptography, the process is explained in the practical part. Among others, the principle and the use of so-called one-way functions is described.

The output of the whole work is a presentation that will be used in cryptography lessons at Tomas Bata University in Zlín.

SEZNAM POUŽITÉ LITERATURY

[1] VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. 1. vydání Praha: Albatros, 2006. 340 s. ISBN 80-00-01888-8

[2] HANŽL, Tomáš, PELÁNEK, Radek, VÝBORNÝ, Ondřej. *Šifry a hry s nimi.* 1. vydání Praha: Portál, 2007. 198 s. ISBN 978-80-7367-196-9

[3] SINGH, Simon. *Kniha kódů a šifer.* 1. vydání Praha: Dokořán a Argo, 2003. 382 s. ISBN 80-86569-18-7 (Dokořán) a ISBN 80-7203-499-5 (Argo)

[4] BITTO, Ondřej *Šifrování a biometrika aneb tajemné bity a dotyky.* 1. vydání Kralice na Hané: Computer Media s.r.o., 2005. 168 s. ISBN 80-86686-48-5

[5] JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti*. 1. Vydání Praha: Naše vojsko, 1994. 183 s. ISBN 80-206-0462-6

[6] VANĚK, Tomáš *Skripta Katedry telekomunikační techniky ČVUT v Praze, Fakulta elektrotechnická.*

[7] JANEČEK, Jiří *Rozluštěná tajemství, luštitelé, dešifranti, kódy a odhalení.* 2. vydání Praha: XYZ, 2008 268 s. ISBN 978-80-86864-96-9

[8] PIPER, Fred, MURPHY, Sean. *Kryptografie, průvodce pro každého.* 1. Vydání v českém jazyce Praha: Dokořán, 2006. 157 s. ISBN 80-7363-074-5

[9] STIX, Gary *Nejlépe střežená tajemství: kvantová kryptografie vykročila od teorie přes laboratoře až ke skutečným produktům*. Scinetific American české vydání, ročník 2005, s. 77 – 81

[10] VONDRUŠKA, Pavel. *Cesta kryptologie do nového tisíciletí.* 4 články v časopise Computer World, dostupný z www: <http://www.cw.cz/>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES Schválený standard udělený šifře Rijndael.

ARP Address resolution protokol, používá se k získání ethernetové MAC adresy.

CD Compakt disk, přeloženo jako kompaktní disk.

DES Data encryption standard, symetrická šifra.

DNS Domain name system, hierarchický systém doménových jmen.

DSA Algoritmus digitálního podpisu.

DVD Formát digitálního optického datového nosiče.

IBM Přední světová společnost v oboru informačních technologií.

IDEA International data encryption algorithm, mezinárodní algoritmus pro šifrování dat.

IETF Komise techniky Internetu.

JPEG Standardní metoda ztrátové komprese pro ukládání počítačových obrázků.

LSB Least significant bit, nejméně významný bit.

PC Personal computer, osobní počítač.

PGP Počítačový program, který umožňuje šifrování a podepisování.

RSA Šifra s veřejným klíčem.

SHA Rozšířená hašovací funkce.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Přílohou práce je prezentace do výuky v PowerPointu, přiložena na CD.