VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

VÝVOJ KRYPTOLOGIE V OBLASTI BEZPEČNOSTI A OCHRANY DAT

Autor práce: Jaroslav Rynda

Studijní obor: Bezpečnostně právní činnost

Forma studia: Prezenční

Vedoucí práce: doc. Ing. Oldřich Pekárek, CSc.

Katedra: Katedra právních oborů a bezpečnostních studií

2015

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

.....

Na tomto místě bych chtěl poděkovat vedoucímu bakalářské práce doc. Ing. Oldřichu Pekárkovi CSc., za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

RYNDA, J. *Vývoj kryptologie v oblasti bezpečnosti a ochrany dat : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2015. 60 s. Vedoucí bakalářské práce : doc. Ing. Oldřich Pekárek, CSc.

Klíčová slova: kryptologie, kryptografie, kryptoanalýza, šifrování, informační systém, informační bezpečnost, počítačová kriminalita

V bakalářské práci s tématem *Vývoj kryptologie v oblasti bezpečnosti a ochrany dat* je věnována pozornost vysvětlení základních pojmů týkajících se kryptologie a následně je stručně popsán pohled do historie kryptologie a její vývoj a další perspektivy. Dále je pozornost v práci upřena na poznatky o moderních principech šifrování, kryptoanalýze, rizikům která s sebou přináší moderní technologie bezpečnosti informačních systémů a legislativa České republiky týkající se kryptografie. Práce není zaměřena příliš technologicky, neboť je vypracována v rámci studia bezpečnostně právního oboru. Bakalářská práce má pomoci čtenářům porozumět odborné terminologii, popisuje základní principy šifrování a v neposlední řadě pomáhá pochopit, jak kryptografie ovlivnila lidské dějiny.

ABSTRACT

RYNDA, J. The progress of cryptology in security and data protection : Bachelor thesis. ČeskéBudějovice : The College of European and Regional Studies, 2015. 60 p. Supervisor : doc. Ing. Oldřich Pekárek, CSc.

Key words: cryptology, cryptography, cryptoanalysis, encryption, informational system, informational security, computer criminality

In the bachelor work with the topic of „The progress of cryptology in security and data protection“ is the attention payed to the explication of the basic concepts concerning cryptology and subsequently is made a brief description of the history sight of cryptology and its progress and next perspectives. Further is the attention in work fastened upon piece of knowledge about modern principles of encryption, cryptoanalysis, diversification that breeds modern technology, safety of information system and legislative of the Czech Republic concerning cryptography. Work is not concentrated too technologically because it is drawn up in terms of security legal branch study. The bachelor work is due to help to readers make sense of words of art, describes basic principles of encryption and last but not least then understand how cryptography has influenced the human history.

Obsah

Úvod

Bez informačních technologií je práce s informacemi dnes nejen neefektivní, ale již i nepředstavitelná. Informační systémy zajišťují chod jak výrobních podniků, tak i chod veřejné správy, zdravotnictví, finančnictví i sektoru služeb. S prudkým rozvojem moderních technologií vzrůstá však i možnost zneužití důvěrných informací, a proto je třeba tyto odpovídajícím způsobem chránit. To je především úkolem moderní kryptografie, která musí hledat stále dokonalejší metody ochrany.

Kryptografie - umění utajení informace - je velmi stará disciplína. Už ve starém Egyptě, 2000 let před naším letopočtem, používali šifru, tedy tajné písmo, kde místo obvyklých hieroglyfických znaků používali jiné. Utajení informací před neoprávněnými osobami bylo důležité pro každý stát, i starověký. Podle významného historika Hérodota právě umění psaní tajných zpráv zajistilo převahu Řeků nad Peršany v 5. století před naším letopočtem. Známá je i Caesarova šifra, kterou popisuje Suetonius[1] ve svém díle Životopisy dvanácti císařů. Ale máme i nedávné příklady, kdy prolomení šifrové ochrany umožnil významné zvraty ve vojenských konfliktech, konkrétně ve 2. světové válce, laické veřejnosti většinou známé pod názvy ENIGMA a PURPUR. Nejvýraznějším faktorem rozvoje kryptografie ve dvacátém století byl vznik elektronických počítačů a s ním spojený rozvoj digitálního komunikačního prostředí.

Kryptografie se dnes již netýká jen špionáže či ochrany státních zájmů. Je součástí běžného života člověka, požívajícího moderní prostředky. Pracuje souběžně na pozadí všech technologických procesů spojených se zpracováním a přenosem informací a to nezávisle na tom, zda jde o ochranu dokumentu, obrazu nebo zvuku. Kryptografie je používána vedle ochrany komunikačních kanálů i k ochraně elektronických archivů citlivých dat. Obecně kryptografii můžeme charakterizovat jako nejúčinnější nástroj k udržení důvěrnosti informací a jejich autenticitě. V řadě aplikací i jako nástroj kontroly integrity informace.

[1] Gaius Suetonius Tranquillus (70 - 130), jeden z nejznámější antických životopisců

1 CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Cílem bakalářské práce je poukázat na význam kryptologie od jejího vzniku, její vývoj až po současnost, posoudit její možné ohrožení v souvislosti s dalším rozvojem výpočetní mohutnosti počítačů, kterou potenciální protivník bude mít k dispozici. Vysvětlit základní terminologii kryptologie a osvětlit základní požadavky na fungování informačního systému. Analyzovat hrozby a rizika pro budované informační systémy a význam informací v současné společnosti.

Bakalářská práce je strukturovaná do pěti základních kapitol. První kapitola popisuje cíle a metodiku této bakalářské práce. Druhá kapitola práce vysvětluje základní pojmy kryptologie, odborné termíny spjaté s kryptologií, základní rozdělení šifrovacích technik a historický vývoj kryptologie od starověku až po současnost.

Třetí kapitola práce popisuje kryptografické postupy a metody rozdělené do symetrické a asymetrické kryptologie, základní rozdělení šifer a jejich možnosti polomení. Dále popisuje Shannonův teorém o perfektní šifře. Čtvrtá kapitola práce se zaměřuje na rizika moderních technologií, která mají původ ve zvyšování výpočetní mohutnosti podle Moorova zákona, principy kvantových počítačů a význam kryptografie v případě použití skutečného kvantového počítače v praxi.

Poslední pátá kapitola bakalářské práce se věnuje bezpečnosti informačního systému a kybernetické kriminalitě. Dále práce popisuje, jaké jsou základní cíle informační bezpečnosti, bezpečnostní funkce a požadavky na informační systém a jeho možnosti napadení různými formami útoku s různou motivací a odkazuje na českou legislativu řešící informační bezpečnost.

Při zpracování bakalářské práce jsem čerpal především z odborných publikací jako jsou například *Aplikovaná informatika* od autorů R. FEREBAUEROVÁ, - O. PEKÁREK, kniha *Kryptologie, šifrování a tajná písma* od P. VONDRUŠKY a nebo kniha od L. DOBDY *Ochrana dat v informačních systémech.*

2 ZÁKLADNÍ POJMY A HISTORIE

Kryptologie (cryptology) vědní obor o metodách utajení a odtajnění informací. Opírá se o rozsáhlý matematický aparát a svým použitím je pevně svázána s informatikou, speciálně pak s bezpečností informačních systémů. Zahrnuje tvorbu kryptografických technik, algoritmů, hashovacích funkcí, kryptografických protokolů, kryptokanalytických útoků a podobně. Kryptologie se rozděluje na kryptografii, kryptoanalýzu a steganografii.[2]

Kryptografie (cryptography) Slovo kryptografie pochází z řečtiny - *kryptos* je skrytý a *gráphein* znamená psát. Kryptografie je věda o šifrování zpráv, jejich převodem do podoby, která je čitelná jen s odbornou znalostí a její obsah je před neautorizovanými osobami skryt. Kryptografie se zabývá matematickými metodami transformace otevřené zprávy do utajené formy se vztahem k prvkům informační bezpečnosti jako je důvěrnost, integrita dat (celistvost, neporušenost), autentizace entit (ověření subjektů v procesu práce s informacemi) a původu dat (vlastnictví).[3]

Kryptoanalýza (cryptoanalysis), je "opakem" kryptografie, cílem je získat ze šifrované zprávy její původní podobu a hledání metod k proniknutí do šifrových systémů, respektive prolomit šifrovací algoritmus. Kryptoanalytici se snaží o objevení a rozlišení takzvané principiální rozluštitelnosti (prolomitelnost algoritmu myslitelnými způsoby), a reálné rozluštitelnosti, postupu, který je současnou technikou jen velmi obtížně realizován, ale je za určitých podmínek možný. V tomto smyslu se kryptoanalýza jeví nejen jako ofenzivní činnost, ale je nedílnou součástí tvorby a testování vyvíjených kryptografických principů a zařízení.[4]

Steganografie (řecké *steganos* - schovaný) je oblast utajování informací, jejímž cílem je zatajit existenci dané zprávy její implementací do běžných neutajovaných informací (do jiné zprávy). Je tedy utajována skutečnost svědčící o existenci utajované informace, není však transformována do jiné množiny znaků, čímž se liší od kryptografické ochrany. Steganografické metody obsahují například používání neviditelných inkoustů, mikroteček, ukrytím zprávy do digitalizovaného obrázku, a pod. Nově jsou principy

[2] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 94.
[3] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s. 195.
[4] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové,2003, s. 12-13.

steganografie kombinovány s kryptografickými metodami. Použití moderní steganografie se objevilo i u teroristických organizací jako je Al Kaida. Proto moderní formy steganografie spadají právem do oblasti zájmu kryptologů.[5]

2.1 Odborné termíny kryptografie

Kód (code) systém pro ukrytí smyslu zprávy, který nahrazuje každé slovo nebo frázi původní zprávy (otevřeného textu) jiným znakem nebo skupinou znaků. Kódy používají kódová slova, (symboly, skupiny čísel). Seznam nahrazení je pak definován v kódové knize.

Šifra (cipher) je obecně jakýkoliv systém pro ukrytí obsahu zprávy tak, že je každý původní znak otevřeného textu (například písmeno, číslo a tak podobně), nahrazeno jiným znakem. Důsledná digitalizace přenosu a zpracování dat způsobily, že proces transformace otevřené informace na zašifrovanou a naopak je prováděn pouze v číselné formě. Šifry s ručním šifrováním dnes patří většinou historii oboru.

Šifrování (encryption) si klade za cíl transformovat vstupní data do podoby, ve které jsou pro potenciálního útočníka nesrozumitelné a není schopen rekonstruovat jejich původní tvar. Způsob šifrování je svázán se sdílením společné tajné informace – kryptografického klíče, odesilatelem a příjemcem šifrované informace.

Dešifrování (decryption) opačný proces šifrování, rekonstrukce původního otevřeného textu plynoucí ze znalostí příslušného šifrového algoritmu a klíče.

Šifrový algoritmus je matematickým postupem, kterým se realizuje proces šifrování a dešifrování.

Luštění snaha získat informace ze zašifrované zprávy bez znalosti klíče nebo algoritmu.

Otevřený text (clear text) zkratka CT, je původní nezašifrovaná informace, která je obecně srozumitelná.

Šifrový text (encrypted text) zkratka ET, je otevřený text po zašifrování

Kryptografický systém je jakýkoliv systém, jehož funkcí je kryptografická transformace otevřeného textu na šifrovaný text a to pomocí příslušného šifrovacího algoritmu a klíče.

Kryptografický klíč (key) slouží k nastavení procesu šifrování a dešifrování. Odolnost zašifrované informace je dána pouze klíčem. Rozesílání kryptografických klíčů probíhá tajným (zašifrovaným) kanálem, například kurýrem.[6]

[5] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové,2003, s. 50.

Distribuce klíčů (key distribution) proces zajišťující, že odesilatel i příjemce mají k dispozici kryptografický klíč nezbytný pro zašifrování a dešifrování zprávy a zároveň brání tomu, aby se klíč dostal k neautorizované osobě.

2.2 "Klasická" kryptografie

Někdy také nazývána jako "ruční" kryptografií. Jsou to nejjednodušší postupy, které se používaly k šifrování od samého počátku. V zásadě se dělí na transpozici a substituci.

Transpozice je systém šifrování, v němž se každé písmeno otevřeného textu přemístí do libovolné části šifrovaného textu, ale zachová si identitu (všechny alfanumerické znaky).[7]

Substituce neboli záměna je systém šifrování, v němž je každý znak otevřeného textu nahrazen jiným znakem, ale ve zprávě zachovává svou pozici. Takto vytvořené šifry se nazývají substituční šifry a dělí se na další podskupiny. Jsou to monoalfabetické systémy, homofonní systémy a polyalfabetické systémy.[8]

Kódová kniha je seznam kódových slov nebo čísel (náhrad) pro slova nebo fráze z otevřeného textu, která jsou pak přenášena jako zašifrovaný text. Šifrování podle kódových knih je dnes méně časté a patří spíše do historie kryptografie.[9]

Prvé dvě metody – substituce a transpozice lze spolu vzájemně kombinovat a používat i vícekrát za sebou. Modifikace a vzájemná kombinace těchto metod vytváří všechny známě druhy šifrových systémů a i v dnešní době speciálních kryptografických zařízení a výkonných počítačů jsou základem všech moderních algoritmů.[10]

---

[6] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice : Vysoká škola evropských a regionálních studií, 2014, s. 95.
[7] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*.Praha, 2006, s. 29.
[8] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*.Praha, 2006, s. 30.
[9] SINGH, S. *Kniha kódů a šifer.* Praha, 2009, s. 368.
[10] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*.Praha, 2006, s. 31.

2.3 Historický vývoj kryptografie

Jelikož šifrování se datuje již od dávného starověku, nelze v práci opomenout některé důležité a zajímavé milníky týkající se historie kryptografie a to také z důvodu lepšího pochopení významnosti a účelu použití kryptografie v minulosti.

2.3.1 **Kryptografie v období starověku**

O tom, že šifrování spadá už do dob dávné minulosti, svědčí fakt, že malby na stěnách jeskyní lze považovat za určitý druh šifer. Svým způsobem se i v textech pocházejících před 3000 lety nacházejí šifrované části. Jedná se o texty hebrejské, mezopotámské či egyptské. V souvislosti s tímto obdobím je třeba připomenout, že ne každý člověk uměl psát, schopností psát se vyznačovaly pouze vzdělaní lidé, jejichž bezpochyby nebylo mnoho. Proto byl sám zápis pomocí písma šifrou.[11]

Šifrování ve starověkém Egyptě spočívalo v nezvyklé úpravě písma a v přidávání znaků do textu, které byly známy pouze vyvolené skupině lidí. Obdobně tomu bylo i v Mezopotámii a v Sumeru, které se vyznačovaly používáním klínového písma a později se zde začaly objevovat systémy v podobě upravených pečetních válečků pro ověřování pravosti zpráv[12].

Mnozí odborníci považují za počátek dějin kryptografie hieroglyfický text ze starého Egypta z roku okolo 1900 před naším letopočtem vyrytý neznáním písařem ve městě Menet Khufu. Jedná se o hieroglyfy vyryté do kamene hrobky, kde byl uložen jeho pán. Vyrytý text se vyznačoval zvláštností, místo obvyklých hieroglyfů byly použity nestandardní hieroglyfické symboly. Rytec tímto počinem nesledoval cíl zašifrovat text do nečitelné podoby, ale unikátností písma rytého na kameni chtěl upoutat pozornost čtenáře a poukázat na život svého pána.[13]

Dalším pokusem o šifrování byla tabulka z Mezopotámie (1500 před naším letopočtem), na které byl vyrytý návod na výrobu glazované keramiky v podobě zašifrovaného textu do tabulky. Šifrovaný text spočíval v záměně klínopisných písmen

[11] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ,O . *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 13.
[12] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ,O . *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 13.
[13] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 196

za jiné klínopisné písmena, které však mají totožnou zvukovou podobu. Tento šifrovaný systém nebyl příliš bezpečný, a proto se v průběhu tohoto období přestal používat.[14]

Kolem roku 600-500 před naším letopočtem Hebrejci vynalezli a začali používat jednoduchou substituční šifru zvanou Atbash (Obr.1). Její použití je možné nalézt ve Starém zákoně, konkrétně v knize Jeremiášově. V šifře Atbash se nahrazují písmena od začátku abecedy písmeny jdoucími od konce abecedy ve stejné vzdálenosti. Hlavním úkolem této šifry nebylo učinit obsah zprávy nečitelným, ale spíše v ní šlo o snahu udělat text zajímavým. Méně známé byly další dva jednoduché, Hebrejci používané substituční systémy albam a atbah.[15]

11	10	9	8	7	6	5	4	3	2	1
כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
12	13	14	15	16	17	18	19	20	21	22

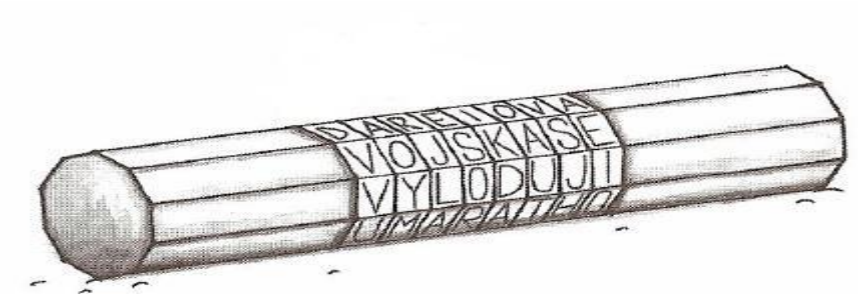
Obr. 1 ATBASH šifra[16]

Později se v období starověku začali lidé zajímat o šifry zejména z hlediska jejich strategického charakteru. Jednalo se hlavně o vojenské a vládní strategie, které využívaly především Řekové a Římané v podobě jednoduchých substitucí. Téměř každá učebnice šifrování zmiňuje poněkud neoperativní způsob který Řekové pro utajení zpráv používali. Svému poslu nejprve vyholili hlavu, napsali nebo vytetovali na jeho lebku vzkaz a teprve až když mu vlasy dorostly, mohl se vydat na cestu. Dokonce i jedna z nejdůležitějších zpráv, která zabránila zničení západní civilizace a pomohla Řekům v boji proti Peršanům, byla také předána utajeně.[17]

Ve starém Řecku (500 před naším letopočtem) Sparťané používali známé a prokazatelné mechanické zařízení určené k šifrování zpráv. Zařízení zvané *Skytalé* (Obr.2) je tvořeno ze dvou tyčí o stejném průměru, kde jednu tyč vlastnil odesílatel zprávy a druhou tyč vlastnil příjemce zprávy. Odesílatel navynul na tyč pás papyru, látky nebo pergamenu a napsal zprávu směrem dolů podél tyče. Po napsání zprávy pás s textem odvynul a poslal příjemci zprávy. Příjemce už jen navinul pás se zašifrovaným

[14] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 196.
[15] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 197-198.
[16] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 31.
[17] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ,O . *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 13.

textem na svou druhou tyč, totožnou s tyčí odesílatelovou, a zprávu bez problémů dešifroval. Tento kryptografický systém pracoval na principu transpozice.[18]



Obr. 2 Skytale[19]

Ve starověké Indii (300-500) se také rozvíjela praktická kryptografie a to nejen mezi obchodníky a vojenskými kruhy, ale i mezi širšími vrstvami obyvatelstva. Dokladem je známá kniha *Kámasútra,* která mimo jiné, popisuje umění vyznat se v tajných písmech a znacích.[20]

Julius Caesar (100-44 před naším letopočtem) používal jednoduchou substituční šifru, která nese po něm i pojmenování . Caesar používal několik šifer, ale kniha, kde se popisovaly, se nezachovala. V Caesarově šifře se každé písmeno nahradí písmenem, které v abecedním pořadí leží tři písmena za ním. Například slovo LIST by v Caesarově šifře nabylo tvaru OLVW. Na tu dobu to byla prakticky nerozluštitelný šifra, jednoduchá a účinná, dokud ji neprozradil Cicero, který přešel do tábora Caesarova protivníků.[21]

2.3.2 Středověk a raný novověk

V 5. až 15. století se kryptografie rozvíjela velmi pomalu, stále se používaly jednoduché substituce a transpozice. Na druhé straně se v 14. století rozvinula kryptoanalýza. Arabové objevili řešení jednoduché substituce pomocí frekvenční analýzy, která vychází z počtu jednotlivých písmen nacházejících se v konkrétním textu. Až na práce arabských matematiků a kryptologů navázala středověká Evropa.[22]

Nejstarší zachované nomenklátory (1379) sestavil tajemník papeže Klementa VII. Gabrieli di Lavinde. Nomenklátory obsahují kromě úplné substituční abecedy

[18] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 198.
[19] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 198.
[20] SINGH, S. *Kniha kódů a šifer*. Praha, 2009. s. 29.
[21] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 199.
[22] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ,O . *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 13.

i dvoupísmenné kódy pro jeden až dva tucty nejfrekventovanějších slov nebo jmen, a navíc také takzvané klamače, nevýznamové skupiny písmen, které měly ztížit kryptoanalýzu zašifrovaných textů. Nomenklátory postupně rozšiřovali svůj slovník na stovky až tisíce kódových slov. Zajímavé je, že se používaly dlouho a masově, a to i přesto, že byly známy mnohem dokonalejší metody šifrování. Měly totiž jednu nepřekonatelnou výhodu, jejich použití bylo snadné. Každý si mohl složitost nastavit podle svého slovníku kódů. Je to první řešení obecného rozporu mezi bezpečností a rychlostí (praktičností) šifer.[23]

Leon Battista Alberti (1404-1472), nazývaný také otcem západní kryptologie. Byl všestranně vzdělaný člověk, je známý jako autor první tištěné knihy o stavitelství. Napsal stručnou dvaceti pěti stránkovou práci, která se stala jednou z nejvýznamnějších prací tohoto druhu napsanou v západní Evropě. Dílo obsahuje výklad luštitelských postupů na základě jazykových znalostí, rozdělení systémů šifrování na substituci a transpozici, objev polyalfabetické substituce a šifrování kódů. K substituci sestrojil Alberti šifrovací disk sestávající se ze dvou otáčivých kotoučů reprezentujících otevřené a zašifrované znaky, přičemž jejich otáčení simulovalo polyalfabetickou substituci.[24]

V 16. století francouzský diplomat Blaise de Vigenér knižně popsal takzvanou Vigenérovu šifru založenou na principu polyalfabetické šifry.[25]V polyalfabetické kryptografii je cílem snížit počet frekventovaných šifrovaných písmen a tím ztížit prolomení šifrovacího systému. Zmíněné snížení počtu písmen probíhalo díky tomu, že jeden znak šifrovaného textu reprezentovalo několik rozdílných písmen otevřeného textu, odlišnost písmen spočívala například v tom, na jakém místě zprávy se daný znak nachází nebo jaké písmeno leží před ním. K zašifrování textu pomocí Vigenérovi šifry se používá takzvaný Vigenérův čtverec (Obr.3), kde otevřený text představují jednotlivé sloupce a klíč představují řádky, šifrované písmeno tak vznikne v místě střetu konkrétního sloupce s konkrétním řádkem. Jedná se o substituci.[26]

[23] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 212.
[24] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 213.
[25] SINGH, S. *Kniha kódů a šifer*. Praha, 2009, s. 58-61.
[26] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 228.

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Obr. 3 Vigenérův čtverec[27]

2.3.3 **Kryptografie v 19. století**

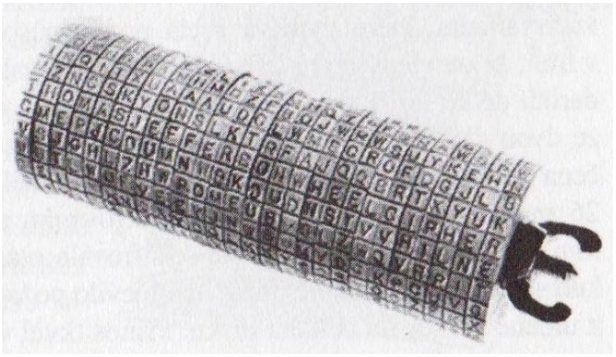
Vynalezení telegrafu v roce 1832 bylo důležitým zlomem v oblasti kryptografie. navzdory tomu, že telegraf umožňoval posílat zprávy na dlouhou vzdálenost a v krátkém čase, neposkytoval žádné soukromí. Při odesílání zprávy se dalo jednoduše odposlouchávat a zprávu tak bez problémů zachytit. Šifrování v tomto období již počalo hrát klíčovou roli i v obchodu a vojenství.[28]

Pro vojenské účely našly využití takzvané polní šifry. Uplatňovaly se přímo na místě boje. Bezpečnost šifrovacího algoritmu nemusela být vůbec velká, šlo zde spíše o rychlost šifrování a dešifrování zprávy, přičemž důležité bylo, aby šifrovaná zpráva byla pro protivníka dostatečně časově náročná. Pokud se například šifrovaná zpráva s textem: „Boj začne o 16:00", dostala do rukou protivníkova a ten ji rozluštil v 16:05, tak její rozluštění ztrácelo smysl. (takzvaná expirace tajemství).[29]

V americké občanské válce v letech 1861-1865 se používaly kromě polních šifer i jiné kryptografické metody. Konfederace jižních států používala zejména substituční šifry, mezi které patřila i zmiňovaná Vigenérova šifra, kterou ale Unie dokázala rozluštit. Unie severních států byla na tom lépe, používala šifrovací mechanismus zvaný Jeffersonův váleček (Obr.4). Pojmenování dostal podle třetího amerického prezidenta Thomase Jeffersona, který váleček vynalezl. Tento šifrovací mechanismus je tvořen

[27] SINGH, S. *Kniha kódů a šifer.* Praha, 2009, s. 120.
[28] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ,O . *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 15.
[29] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ, O. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 15.

přibližně třiceti šesti disky, které lze nasunout na osu válečku. Po obvodu každého disku je napsána abeceda různě zpřeházených písmen a disk je označen číslem pro určení nastavení mechanismu. Při odesílání zprávy se seřadí disky a nastaví se tak, aby jedna řada napříč řádky tvořila otevřený text. Šifrovaný text se pak vypíše z náhodně vybraného řádku. Posloupnost čísel určující seřazení disků a jedno číslo udávající posun ve sloupcích tvoří klíč. Tento kryptografický mechanismus se považuje za relativně bezpečný a používala ho americká armáda do začátku druhé světové války.[30]



Obr. 4 Jeffersonův váleček[31]

V roce 1854 britský vědec Charles Wheatstone vynalezl nový typ šifry. Šifru představil světu až skotský baron a poslanec anglického parlamentu Lyon Playfair, podle něhož je pojmenována jako šifra Playfair. Jedná se o vojenskou polní šifru, která byla v užší míře používána až do konce 2. světové války. Šifra je těžce rozluštitelná, neboť je odolná vůči frekvenční analýze. Playfairova šifra je výhodná z několika hledisek, je jednoduchá na naučení se, je rychlá na přípravu šifrovaných textů a je rychlá při jejich dešifrování.[32]

2.3.4 Kryptografie v období 1. a 2. světové války

Kryptografie v 20. století nabyla velkého význam a to hlavně díky objevu rádia v roce 1894. Rádio umožňovalo ještě mnohem rychlejší přenos informací než telegraf, nevýhodou tohoto vynálezu je, že vysílání prostřednictvím rádia bylo veřejné, a tak neexistovalo žádné soukromí mezi komunikujícími. Proto se otázka šifrování stala nezbytnou. Počátkem 20. století se kryptografie dynamicky rozvíjela a vznikalo mnoho

[30] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma.* Praha, 2006, s. 241.
[31] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma.* Praha, 2006, s. 241.
[32] SINGH, S. *Kniha kódů a šifer.* Praha, 2009, s. 351-352.

různých šifrovacích strojů. Tato etapa trvala do konce padesátých let a byla typická používáním složitých elektromechanických strojů.[33]

Během 1. světové války se objevuje jeden z prvních velikánů kryptografie 20. století William Frederic Friedman (1891-1969). V americké armádě nastoupil dráhu úspěšného kryptologa a pro USA vybudoval vzorně fungující kryptoanalytickou službu. Vydal čtyřsvazkové dílo *Základy kryptoanalýzy*, které se stalo biblí všech kryptologů prvé poloviny 20. století. Obsah tohoto díla zásadně ovlivnil rozvoj kryptografie ve všech státech mezi dvěma světovými válkami. Ale v té době se Američané dopustili neuvěřitelné chyby a nepředvídavosti, která je stála těžce získaný náskok – zrušili celé kryptoanalytické oddělení ministerstva zahraničí a všechny jeho členy propustili. Tehdejší ministr zahraničí Henry Stimson to odůvodnil nechvalně proslulou větou „Gentlemani si navzájem nečtou dopisy". Naštěstí si tuto chybu velice rychle uvědomili a povolali Friedmana zpět ke službě a dali mu k dispozici veliké prostředky.[34] Nakonec to byl Friedman, kdo prolomil japonský šifrový systém PURPUR a zasloužil se tak se svými spolupracovníky o vítězství v Pacifiku.

V 1. světové válce byly velmi často používané polní šifry, například šifra Playfair a časté bylo i používání kódových knih. Zprávy zašifrované kódovou knihou bylo téměř nemožné rozluštit, šlo to jen v případě, jestliže protivník danou kódovou knihu nějakým způsobem získal. Proto se k získání kódových knih používali různé intriky. Angličané byli v tomto směru velmi vynalézaví a aby čelili hrozbě ztráty kódových knih cíleně nechávali na pracovištích nepravé klamavé kódové knihy a falešné zprávy zašifrované prostřednictvím těchto knih.[35]

Anglické námořnictvo mělo během 1. světové války speciální šifrovací jednotku, která pracovala pod vedením sira Williama Halla pod názvem *Room 40*. Jejich úspěch nastal v okamžiku, kdy se jim podařilo zachytit a rozluštit telegram, který poslal tehdejší německý ministr zahraničí Arthur Zimmermann německému velvyslanci ve Spojených státech. V telegramu stálo, že Němci chystají ponorkovou válku v Atlantiku a pokud by se náhodou USA chtěly zapojit do války, tak by bylo třeba přesvědčit Mexiko, aby se přidalo na stranu Německa a zaútočilo na Spojené státy. Telegram navíc obsahoval informace, že Německo je ochotno poskytnout Mexiku

[33] DOBDA, L. *Ochrana dat v informačních systémech.* Praha, 1998, s. 198.
[34] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. 1. vyd. Praha : Albatros, 2006, s. 270.
[35] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ, O. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 18.

vojenskou výpomoc a že Mexiko by mohlo zprostředkovat jednání s Japonskem. Hall však nechtěl, aby Němci věděli, že Angličané dokáží luštit jejich šifry a navíc, pokud by Američanům předal telegram přímo, mohli by si myslet, že se jedná o lest, pomocí které chtějí Angličané vtáhnout Ameriku do války. Hall vymyslel perfektní způsob, jak obejít předání zprávy Američanům přímo, a zinscenoval situaci tak, že se anglickému agentovi podařilo získat rozšifrovanou zprávu v Mexiku. K tomu vyvolal kritiku v anglických novinách mířenou na vlastní služby za to, že se jim nepodařilo tak podstatnou zprávu zachytit a následně vyluštit. Díky tomu byli Němci naprosto zmateni.[36]

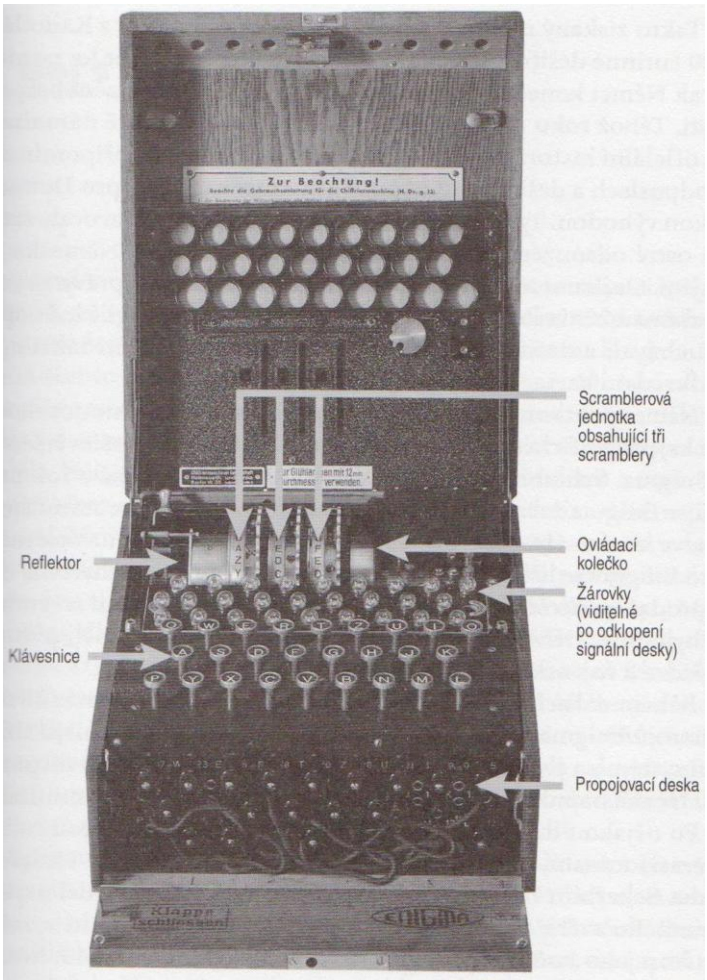
V období 2. světové války (1933-1945) nastává mechanizace šifrování a s ní spojené elektromechanické šifrovací stroje, v USA to byla *Sigaba*, v Británii *Typex*, Japonsko používalo *Purple*, a nejznámější německá *Enigma* (Obr.5). Všechny tyto elektromechanické stroje, kromě *Purple*, pracovali na podobném principu, kde základ byl tvořen několika rotujícími disky (scramblery) s dvaceti šesti znaky abecedy. Šifrování umožňovaly rotující disky, které se daly mezi sebou propojit prostřednictvím propojovací desky a tím různě kombinovat. Na začátku bylo třeba *Enigmu* nastavit pomocí klíče, který se skládal z pořadí rotorů, jejich počáteční pozice a z nastavení propojovací desky. Němci s jistotou věřili, že je *Enigma* neprolomitelná, opak byl ale pravdou. Anglie věnovala její kryptoanalýze obrovské úsilí, které bylo korunováno úspěchem. Jednou z nejvýznamnějších událostí 2. světové války bylo právě její rozluštění, které umožnilo číst komunikaci mezi Němci a získat tak neocenitelné tajné informace, které podle některých historiků významně ovlivnili průběh celé 2. světové války. O rozluštění šifry se zasloužili především kryptoanalytici z Polska Marian Rejewský (*Biuro Szyfrow*) a v Británie Alan Turing a Gordon Welchman (*Bletchley Park*).[37] Kryptoanalýza šifrovacího systému *Enigma* měla veliký vliv na vznik a vývoj počítačů. Při jejím luštění Alan Turing sestrojil jeden z prvních elektronických počítačů na světě (*Colossus*).[38]

Američtí kryptoanalytici pod vedením Williama Frederica Friedmanna dokázali rozluštit šifry vytvořené japonským elektromechanickým strojem *Purple* který byl odlišný od německé *Enigmy*. Nebyl založený na principu rotorů, jako většina

[36] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ, O. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 18.
[37] SINGH, S. *Kniha kódů a šifer*. Praha, 2009, s. 127-136.
[38] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 23.

elektomechanických šifrátorů té doby, ale využíval telefonické součástky (relé). Princip šifrování *Purple* byl ve veřejné literatuře popsán až v roce 1985.[39]

Američané se také zapsali do dějin kryptografie i používáním kódu *Navajo*. Byl to vlastně jazyk, kterým se dorozumívá indiánský kmen zvaný *Navajo*, a protože byl tento jazyk tak výrazně odlišný od ostatních, posloužil jako ideální šifra. Některá technická pojmenování však v jazyce *Navajo* neexistovala (jako například ponorka), a tak se musela vytvořit nová kódová slova. Kódovou řeč se Japoncům nepodařilo rozluštit a proto tento způsob Američané s úspěchem použili ještě v 50. letech ve válce v Severní Koreji a dokonce i v 60. letech ve Vietnamu. Úplná kódová kniha byla uvolněna k publikování teprve v roce 1999.[40]



Obr. 5 Enigma s otevřeným vnitřním víkem[41]

[39] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 272.
[40] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 23-24.
[41] SINGH, S. *Kniha kódů a šifer*. Praha, 2009, s. 139.

2.3.5 Moderní kryptologie

Po světových válkách pokračoval vývoj kryptologie doslova raketovým tempem, zejména zásluhou rozvoje počítačů. Počítače umožnily provádět složité operace daleko rychleji a bezchybně. Předešlé systémy trpěly především složitostí a chybami operátorů. Počítače rovněž umožnily efektivnější metody kryptoanalýzy, proto se zcela změnily požadavky na bezpečnost šifer. Veliký vliv na kryptologii měla studená válka. Obě strany v té době založily rozsáhlé organizace zabývající se odposlechem a šifrováním. Americká NSA (National Security Agency), také přezdívaná Never Say Anithing je největším zaměstnavatelem matematiků na světě a její fungování je i dnes značně mlženo, přesto že má údajně větší rozpočet než CIA a FBI.[42] Stejně tak se rychle rozvíjela kryptografie v tehdejším SSSR.

Během šedesátých let významný vědec Horst Feistel vedl výzkumný projekt v IBM Watson Research Lab, který vyvíjel šifru LUCIFER. Tato šifra později inspirovala vznik amerického standardu DES (Data Encryption Standard) a další šifry označované jako šifry Feistelovského typu. Návrh firmy IBM, založený na šifře Lucifer a upravený americkou bezpečnostní agenturou NSA, byl přijat jako americký národní standard. Algoritmus si získal celosvětové uplatnění až do konce 90. let.[43] Uvedený princip je stále zdokonalován v souvislosti s rostoucí luštitelskou silou potenciálního protivníka a je základem současných symetrických blokových šifer.

V roce 1976 Whitfield Diffie a Martin Hellman publikují "New Directions in Cryptography", zahrnující myšlenku kryptosystému veřejného klíče. Toto dílo znamenalo revoluci v kryptografii. Přínosem byla myšlenka, že klíče mohou existovat v párech - jeden šifrovací a jeden dešifrovací klíč a že není možné jeden klíč odvodit z druhého.[44]

V roce 1978 oznámili Ronald L. Rivest, Adi Shamir a Leonard M. Adleman (z počítačové laboratoře Massachusetts Institute of Technology) objev prvního konkrétního kryptosystému s veřejným klíčem. Byl pojmenován RSA podle

[42] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ, O. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 21-22.
[43] SINGH, S. *Kniha kódů a šifer*. Praha, 2009, s. 235-236.
[44] HANŽL, T. - PELÁNEK, R. - VÝBORNÝ, O. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha, 2007, s. 22.

počátečních písmen autorů. Systém je založen na problému faktorizace velkých čísel a dodnes je neoficiálním světovým průmyslovým standardem.[45]

V roce 1991 Phil Zimmermann zveřejnil jeho první verzi PGP (Pretty Good Privacy). PGP je šifrovací program, kterým se dá zajistit bezpečný přenos elektronické pošty, ale také telefonování přes internet. Využívá algoritmy RSA a IDEA. I v současné době tento program na internetu používá značné množství uživatelů, což je umocněno skutečností, že pro soukromé účely je zdarma.[46]

V roce 1994 byl spuštěn experiment na prolomení RSA. Proces faktorizace probíhal za pomoci Internetu. Do experimentu bylo zapojeno šest set lidí z dvaceti zemí ze všech kontinentů. Podstata experimentu spočívala v tom, že každý počítač zapojen do experimentu vykonával oddělené výpočty, a pak jejich výsledky zasílal na souborový server. Sběr dat pro finální výpočet trval osm měsíců. Fenomén internetu byl poprvé využit na kryptoanalýzu (na útok hrubou silou). V roce 1997 byl rozluštěn 56 - bitový klíč k DES pomocí internetu, podobně jako v roce 1994 u RSA.[47]

Nicméně nutno konstatovat, že asymetrická kryptografie je z hlediska stoupající výpočetní mohutnosti na straně luštitele prolomitelná. Stejně tak i používané moderní symetrické šifry. Proto jsme svědky neustálého zvětšování délky používaných kryptografických klíčů, které mají prodloužit čas nezbytný pro prolomení šifry protivníkem.

V roce 2000 šifrovací standard DES byl, po téměř čtyřleté veřejné soutěži nahrazen belgickou šifrou Rijndael. Blokovou šifru Rijndael přihlásili do soutěže známí dešifrátoři Joan Daemen a Vincent Rijmenam. Přestože jejich šifra podporuje i větší bloky pro AES (Advanced Encryption Standard) je délka kolem vstupního a výstupního bloku definována jako 128 bitů. Délka klíče je volitelná 128, 192 a 256 bitů. Šifra se stane na příštích 20 až 30 let nejpoužívanější šifrou na světě.[48]

[45] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 24.
[46] PIPER, F. C. - MURPHY, S. *Kryptografie*. Praha, 2006, s. 145.
[47] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 285.
[48] PIPER, F. C. - MURPHY, S. *Kryptografie*. Praha, 2006, s. 94.

3 KRYPTOLOGIE A KRYPTOGRAFIE

Kryptografie je nejúčinnějším nástrojem bezpečnosti v informačních systémech . Její vliv na obranyschopnost informačního systému ji řadí na čelní místo použitých technických bezpečnostních protiopatření. Nebezpečí kompromitace informačních systémů je násobeno skutečností, že útok na citlivé informace probíhá zpravidla skrytě a dlouhodobě. Napadený nemusí mít o prolomení svých ochran ani tušení (viz případ ENIGMA). Jediným opravným zpětnovazebním prvkem pak zůstává pro provozovatele informačního systému soustavný bezpečnostní audit obsahující prvky kryptologické analýzy.[49]

Ideálním stavem pro každý stát, jeho orgány, ekonomické subjekty, banky a tak podobně je vytvářet vlastní národní nezávislé kryptografické prostředí. Jak jde čas, kryptologie se dramaticky rychle vyvíjí, kryptoanalytické metody se zdokonalují a výzkum a vývoj v této oblasti se stává výhradní doménou těch nejvyspělejších států s mocenskými ambicemi. Na druhé straně se kryptologie zbavila dřívějšího tabu a stala se přednášeným předmětem „lepších matematických a elektrotechnických fakult“ a tím narostl počet odborníků, kteří posilují řady ochránců informačních systémů ale bohužel i útočnických (nepřátelských) týmů.[50]

Kryptografická technika se dnes vyrábí v namnoze v nadnárodních firmách, které jsou pod kontrolou zpravidla jen mateřské země a to ještě zdaleka ne všechny. Šifrová technika se stala zbožím, které se úspěšně prodává.

Důležité věty, které objektivně v kryptografii platí:

Kerckhoffova téze:

Veškerý mechanismus šifrování s výjimkou tajného klíče je znám kryptologům protivníka a bezpečnost šifrování spočívá výhradně v utajení klíče.

Uvedená téze je stále pravdivá a v podstatě říká, že máme–li dobrý algoritmus šifrování, pak postačí k utajené korespondenci chránit klíče. Algoritmus může být

[49] PEKÁREK O, ČÍŽEK V, FEREBAUEROVÁ R, *Nezávislost kryptografického prostředí jako bezpečnostní problém*, VŠBM Košice/ sborník vedeckých prác, 2010, s. 186-189.
[50] PEKÁREK O, ČÍŽEK V, FEREBAUEROVÁ R, *Nezávislost kryptografického prostředí jako bezpečnostní problém*, VŠBM Košice/ sborník vedeckých prác, 2010, s. 186-189.

veřejný. Znamená to tedy, že pokud nakoupíme certifikovaný kryptografický subsystém a zavedeme dokonalou správu, distribuci a generaci klíčů, měly by být informace šifrované tímto subsystémem dokonale chráněny. Ale i certifikované výrobky nejsou všechny stejné, hodnotitel je zařazuje do tříd podle kvality, která určuje jejich odolnost proti kryptoanalýze. Pochopitelně, že jsou i cenově tyto třídy odlišeny. Tyto odlišnosti mohou být v délce, generaci a správě klíčů, v mediích pro přenos klíčů, v autentizačních protokolech, ve vazbě na operační systém počítače, v samodiagnostice, v stínění a tak podobně.[51]

Je nutno si ale uvědomit, že bezpečnost standardně používaných kryptografických zařízení je pojem relativní.

Při komunikaci dvou jednotlivců si mezi sebou vyměňují informace většinou zapsané v podobě textu. Tento posílaný text, jehož obsahem je daná informace, nazýváme zpráva nebo údaj. Taková zpráva se posílá od jednoho účastníka komunikace - odesílatele, k druhému - příjemce, pomocí přenosového kanálu. Takto přenášenou zprávu může zachytit protivník například odposlechem komunikace. Aby se zabránilo zneužití nebo modifikaci informace uložené ve zprávě, je třeba, aby se zpráva neposílala po přenosovém kanálu v otevřeném tvaru, ale aby byla šifrována.[52]Princip šifrování je dán algoritmem, tj rozsahem a typem matematických operací prováděných nad otevřenou informací. Digitalizace informací a jejich zpracování v binárním kódu předurčuje pro proces šifrování a odšifrování použít samočinný počítač. V praxi to znamená, že buď se šifruje přímo v počítači, ve kterém je informace vytvářena a zpracována (například šifrový algoritmus je přímo implementován do PC, routeru a podobně) nebo šifrovací zařízení tvoří samotný HW/SW přístroj, který se připojuje do IS na vhodném místě.[53]

[51] PEKÁREK O, ČÍŽEK V, FEREBAUEROVÁ R, *Nezávislost kryptografického prostředí jako bezpečnostní problém*, VŠBM Košice/ sborník vedeckých prác, 2010, s. 186-189.
[52] PIPER, F. C. - MURPHY, S. *Kryptografie*. 1. vyd. v českém jazyce. Praha : Dokořán, 2006, s. 14.
[53] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 96.

3.1 Pravidla a zásady kryptologie

Během vývoje kryptologie se postupně vyvíjela i pravidla způsobu provádění šifrování a obdobně se vyvíjely požadavky na kvalitu šifrovacího systému. Nejčastěji jsou uplatňovány následující požadavky na kryptosystém (respektive šifrovací algoritmus).[54]

Spolehlivost kryptosystému - odolnost šifrovaných dat proti rozluštění, kryptosystém má být pokud ne teoreticky, pak alespoň prakticky nerozluštitelný.

Délka klíče co nejmenší (při zachování bezpečnosti šifrování) - tento předpoklad souvisí s rychlostí šifrování, se způsobem uchování klíče a předání klíče. S délkou a množstvím klíčů, které je nutno distribuovat, rostou nároky na utajenou funkci distribučního kanálu. Právě distribuce klíčů je jedním z nejvážnějších rizik šifrového procesu.

Výkonnost operace šifrování a dešifrování - souvisí s konstrukcí algoritmu, s délkou klíče, s použitým SW a HW. Požadavek, aby požadovaná operace proběhla přiměřeně rychle. Cílem je snaha, aby kryptografická ochrana vnášela do přenosu informace co nejmenší zdržení.

Kryptosystém by neměl být prolomitelný v reálném čase s použitím dostupných HW a SW prostředků.

Jednoduchost realizace - implementace šifrovacího algoritmu my měla být co nejjednodušší.

Bezpečnost šifrovacích algoritmů je posuzována ve vztahu k nárokům na prolomitelnost kryptosystému a hodnotě zašifrovaných dat a době aktuálnosti dat. Kryptografické podsystémy se vyvíjejí a nakupují u certifikovaných a spolehlivých firem. Aplikaci těch nejlepších kryptografických podsystémů brání zejména rozpočet, ale i embargo vlád na vývoz zbraňových systémů, mezi které se oprávněně počítají i kryptografická zařízení.[55]

[54] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové. 2003, s. 16.
[55] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 97.

Podmínky spolehlivé funkce šifrového systému jsou: kvalitní algoritmus a jeho implementace do informačního systému, spolehlivý distribuční kanál klíčů a spolehlivá generace a správa náhodných klíčů.

Obrovský vývoj informatiky si vynutil odtabuizování kryptologie a tím současně nastartoval i její rychlejší rozvoj. Vzhledem k složitosti kryptologické analýzy, přiklání se většina uživatelů informačních systémů k vyzkoušeným a v uznávaných laboratořích certifikovaným šifrovým algoritmům, které jsou známy jako kryptografické standardy.[56] Nejznámějším komerčně dostupným standardem byl, dnes již opouštěný, americký DES, od něho byl odvozen 3DES a nový AES, které se jako standardy uvádí v normách ISO/IEC 15408 a americké FIPS[57] a jsou v široké míře používány.

3.1.1 Cíle kryptografie

Základním cílem je vytvořit dokonalý algoritmus zašifrování/odšifrování utajované informace a dodržet následující podmínky: [58]

- **důvěryhodnost** (confidentiality) - také bezpečnost, jedná se o udržení obsahu zprávy v tajnosti. K zajištění důvěrnosti se používají různé způsoby, od fyzikálních ochran až matematickým algoritmům, které přetvářejí informační obsah na nesrozumitelný.
- **celistvost** dat (data integrity) - také integrita, jedná se zamezení neoprávněné modifikaci dat. Tato modifikace může být smazání části dat, vložení nových dat, nebo substituce části původních dat jinými daty. Se zamezením neoprávněné modifikace souvisí i schopnost tuto modifikaci detekovat.
- **autenticita** (authentication) - také identifikace, znamená prokazování totožnosti, tj. ověření, že ten, s kým komunikujeme, je skutečně ten, se kterým si myslíme, že komunikujeme. Autentizace může probíhat na základě znalosti (heslo), vlastnictví (klíče od bytu, kreditní karta) nebo vlastností (biometrické informace - například otisky prstů).
- **autorizace** (authorization) - je potvrzení původu dat. Prokázání, že data vytvořil skutečně ten, o kom si myslíme, že je autorem.
- **nepopíratelnost** (non - repudiation) - souvisí s autorizací, jedná se o jistotu, že autor dat nemůže své autorství popřít.

[56] DES- Data Encryption Standard, AES (Advanced Encryption Standard.
[57] Federal Information Processing Standards (USA).
[58] PŘIBYL, J. *Informační bezpečnost a utajování zpráv*. Praha, 2004, s. 8.

3.1.2 **Dělení šifer**

Postupným vývojem kryptografie docházelo k dělení jednotlivých typů kryptografických algoritmů do několika základních skupin. Každá šifra je popsána algoritmem a klíčem. Nejznámější, nejzákladnější a nejjednodušší dělení je na:[59]

- symetrické šifry
- asymetrické šifry

Pokud bychom toto dělení chtěli rozšířit podrobněji dostali bychom následující skupiny[60]:

1. Transpoziční šifry - šifra, ve které je změněno pořadí písmen otevřeného textu podle tajného klíče (například psaní textu opačně)

2. Substituční šifry - dochází k záměně (substituci) nějaké množiny symbolů za jinou množinu symbolů

3. Kombinované šifry - používají substituci a transpozici

4. Blokové šifry - šifrují skupinu symbolů otevřeného textu jako jeden blok

5. Proudové šifry - převádí každý symbol otevřeného textu ihned na symbol šifrového textu

3.2 Kryptologická analýza

Kryptoanalýza je věda zabývající se rozkrýváním zašifrovaných zpráv bez přístupu ke klíči. Kryptologická analýza moderních algoritmů je velice obtížný a zdlouhavý proces, který vždy vyžaduje kolektiv kvalifikovaných odborníků a velké množství strojového času pro aplikaci opakovaných analytických výpočtů. Obojí mají k dispozici pouze zpravodajská pracoviště světových velmocí a špičková vědecká pracoviště některých univerzit. Srovnatelnou luštitelskou silou disponuje vědeckotechnická veřejnost tisíců nadšenců pro informatiku a kybernetiku spojená internetovou sítí. Zkušenosti ukazují, že algoritmy, které úspěšně prošly prověrkou „kolektivního luštitele“ (byly zveřejněny a odolaly náporu ctižádostivých analytiků),

[59] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 98.
[60] PŘIBYL, J. Ochrana dat v informatice. Praha, 1996, s. 42,76.

možno považovat za více důvěryhodné nežli produkty celkem neznámých firemních tvůrců „utajované“ kryptografické techniky.[61]

3.2.1 Útoky na kryptografické algoritmy

Podle míry znalosti otevřeného s šifrovaného textu se rozlišují následující základní kryptografické úlohy:

1) **Útok hrubou silou** (brute force attack)

K útoku hrubou silou je zapotřebí dostatečně výkonného výpočetního systému, který dovolí rozluštit skrytý text. Jedná se o nejzákladnější luštitelský princip, který postupně zkouší všechny možné klíče. Postup je sice teoreticky vždy úspěšný, ale v praxi jej lze provést pouze tehdy, kdy je prostor klíčů tak malý, že jej lze otestovat v reálném čase.[62]

2) **Luštění se znalostí šifrovaného textu** (ciphertext only attack)

Pokud má kryptoanalytik/útočník k dispozici pouze šifrové texty zpráv, které jsou šifrované stejným algoritmem a klíčem, pak lze takovýto text rozluštit. Cílem je získat otevřený text z co největšího počtu odchycených zpráv nebo odvodit klíč použitý k zašifrování. Dále už je luštění zpráv velice jednoduché a umožňuje čtení dalších a dalších zpráv.[63]

3) **Luštění se znalostí otevřeného textu** (known - plaintext attack)

V tomto případě jsou k dispozici jak šifrované zprávy, ale také jim odpovídající otevřené texty. Cílem už je jen odvodit použitý klíč, který by mohl být následně použit k dešifrování dalších šifrových zpráv (do doby, než bude klíč změněn), nebo najít příslušný algoritmus.[64]

[61] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 102.
[62] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 52.
[63] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 53.
[64] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 24.

4) **Luštění se znalostí vybraných šifrovaných textů** (chosen-ciphertext attack)

V praxi tento případ není příliš obvyklý, je použitelný v případě, kdy má kryptoanalytik přístup ke kryptografickému zařízení, které umí dešifrovat vložený text a úkolem je najít příslušný klíč.[65]

další metody kryptoanalýzy (relativně účinné):

- **luštění pomocí kompromitace uživatele** (purchase key attack) - přímé získání klíče od vlastníka různými metodami (podplacení, krádež, ofocení).
- **pendreková analýza** (rubber-hose attack) - pod hrozbou fyzického násilí,vydírání, vyhrožování, mučení
- **získání otevřeného textu za pomoci analýzy parazitního elektromagnetického pole,** které je vyzařováno z nedostatečně stíněné výpočetní techniky.

Asymetrické šifry používají rozdílné klíče pro šifrování a dešifrování. Používají se především k realizaci elektronického podpisu, při řízení přístupu k datům, k distribuci klíčů pro symetrické šifry a tak podobně Pro systémy s veřejnými klíči platí, že bezpečná délka klíče ve srovnání se symetrickou šifrou je vždy větší.

Luštitelnost algoritmu RSA asymetrické šifry o délce klíče:[66]

- 256 bitů - zvládne rozluštit jednotlivec,
- 384 bitů - skupina kvalifikovaných informatiků,
- 512 bitů - luštitelské profesionální oddělení zpravodajské agentury,
- větší než 768 bitů tvoří hranici luštitelnosti , požaduje vysoké nasazení lidí a strojů,
- za bezpečné lze považovat (k roku 2000) šifry s délkou klíče 1024 bitů a více.

Srovnání symetrických a asymetrických šifer z hlediska odpovídajících délek klíčů (srovnatelné nutné úsilí k prolomení šifry) je (dle Schneier B. Applied Cryptology) v následující tabulce:[67]

[65] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma*. Praha, 2006, s. 24.
[66] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 100.
[67] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 100.

SYM:	ASYM:
50 bit	*384 bit*
64 bit	*512 bit*
80 bit	*768 bit*
112 bit	*1792 bit*
128 bit	*2304 bit*

Tabulka 1, porovnání délek klíčů pro symetrickou a asymetrickou šifru při stejné odolnosti proti prolomení[68]

Pokud jsou všechny možné útoky na algoritmus příliš složité na to, aby je bylo možno provést, pak je možné algoritmus považovat za neprolomitelný. I kdyby tomu tak nebylo, v mnoha případech vědomostní a technické možnosti i finanční zdroje, které jsou potřebné k prolomení algoritmu, mohou přesáhnout cenu, kterou bude mít pro útočníka rozluštění zprávy. Dalším významným faktorem je, po jak dlouhou dobu by měla být data utajena. Každé utajení ztrácí po určité době smysl – tajemství expiruje.[69] Proto například šifrové systémy pro bojové jednotky jsou tvořeny algoritmy s kratšími klíči, u nichž potřebná doba k prolomení není příliš dlouhá, ale vždy delší než předpokládané trvání operace. Na druhé straně šifrové algoritmy uplatňované v diplomatickém spojení pracují s podstatně delšími klíči, protože aktuálnost přenášených informací může být velmi dlouhá (měsíce i roky).[70]

3.2.2 **Perfektní šifrování**

Shannon definoval přesný matematický model bezpečného kryptosystému:

H(Z) >=H(X)

Z je klíč, X vstupní otevřený text a H je neurčitost (entropie). (Shannon, Claude E., 1948)

Ze Shannonova teorému vyplívá, že perfektní šifrou (neluštitelnou) bude jen taková, kde délka kryptografického náhodného klíče bude stejná nebo větší než délka otevřeného textu před zašifrováním. Chtít perfektně šifrovat znamená mít k dispozici stejné množství klíčů jako je množství otevřeného textu. Při tom je nutno splnit, aby klíče byly skutečně náhodné (true random), což se plní technicky velmi obtížně.

[68] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 101.
[69] PIPER, F. C. - MURPHY, S. *Kryptografie*. Praha, 2006, s. 88.
[70] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 102.

Šifrování větších objemů dat vede k nutnosti předzásobit komunikující účastníky obrovským množstvím klíčů.[71]

V praxi se však aplikují převážně „neperfektní šifry“, kde uvedená podmínka není dodržena a odolnost šifry při strojovém luštění je dána potřebným časem k absolutnímu zkoušení všech možných klíčů o určité délce. V podstatě je tak implicitně využívána znalost časového omezení daného aktuálností utajované informace, kdy každé utajení ztrácí po určité době smysl – tajemství expiruje.[72]

Proto se přijala metoda používání šifrových algoritmů, které pracují s krátkými klíči, které jsou dále rozvíjeny(expandovány) do dlouhých pseudonáhodných řad a ty jsou požity pro vlastní zašifrování. Slabinou těchto algoritmů je možnost analytického prolomení a proto jejich bezpečnost dnes charakterizujeme dobou, kterou je nutno vynaložit při využití k strojového (sofistikované) luštění. Lze tedy říci, že všechny dnes prakticky používané šifrové algoritmy odolávají luštění kvalifikovaného protivníka jen po určitou dobu. Proto je nezbytné pro použití šifrové ochrany znát expirační dobu utajované informace ve srovnání s typem použitého algoritmu a podle toho volit typ šifrové ochrany. Znamená to, že budeme volit jiný typ šifrového algoritmu pro ochranu utajovaných informací s dlouhou dobou expirace a jiný typ pro informace na úrovni operativního řízení.[73]

Charakteristiky dobrých šifer

- Stupeň potřebného utajené by měl určovat množství práce potřebné k šifrování a dešifrování
- Prostor klíčů nebo šifrovací algoritmus by měl být zbaven jakýchkoliv omezujících podmínek
- Implementace šifrovacího procesu by měla být co nejjednodušší
- Chyby šifrování by se neměly šířit a narušovat další informaci šifrované zprávy
- Rozsah zašifrovaného textu by neměl být větší než text původní zprávy

[71] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 102.
[72] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 102.
[73] PŘIBYL, J. Ochrana dat v informatice. Praha, 1996, s. 29.

Tyto charakteristiky byly formulovány v době, kdy počítače ještě nebyly připraveny k řešení problémů kryptologie, i když Shannon si byl dobře vědom potenciálních možností počítačů.[74]

3.3 Kryptografické systémy

Kořeny šifrování informací sahají do hluboké minulosti lidských dějin. Až rozvoj matematiky přinesl ovoce v podobě vzniku poměrně silných kryptografických algoritmů. Moderní šifrování je zpravidla založeno na dvou komponentách - šifrovacím algoritmu a klíči, kterým se daný šifrovací algoritmus idividualizuje. Šifrovací algoritmus používá různé matematické funkce, záměny pozic a logické operace, čímž převádí vstupní data na nesrozumitelné informace. Klíč, použitý algoritmus a způsob jeho implementace mají kritický význam pro bezpečnost šifrování. V současné době se podle typů klíčů používají téměř výhradně dvě základní třídy šifrovacích algoritmů. Symetrické s jedním tajným klíčem a kryptosystémy s veřejným klíčem s dvojicí soukromý a veřejný klíč.[75]

3.3.1 Symetrické šifrování

Symetrické, také konvenční šifry, jsou založeny na principu jednoho klíče, kterým lze zprávu jak zašifrovat, tak i dešifrovat. Symetrické šifry mají jako hlavní výhodu rychlost algoritmu. Na druhou stranu je nutné aby se příjemce i odesílatel dohodli na jednom klíči vhodným tajným kanálem, který budou znát jen oni dva. Problémem je tedy distribuce klíče - jak dostat klíč k příjemci, aniž by se ho chopil někdo nepovolaný. Představme si ale, že chceme zajistit komunikaci více než dvou účastníků, přičemž se vyžaduje, aby každá jedna dvojice byla schopna soukromé komunikace. V takovém případě je nutné mít samostatný klíč pro každou z dvojic. Pro komunikaci n účastníků potřeba n různých klíčů. Takové řešení je nepřehledné, složité na realizaci a vede k chybám.[76]

[74] PŘIBYL, J. *Ochrana dat v informatice*. Praha, 1996, s. 79.
[75] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 29.
[76] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 65-66,90.

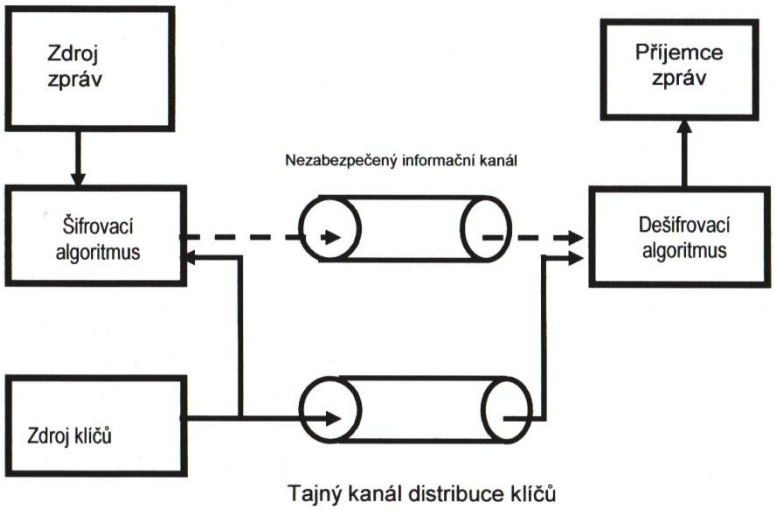
Symetrické šifry používají tentýž klíč pro šifrování i dešifrování

Využívají se především pro šifrování přenosů utajovaných zpráv v komunikačním prostředí, v pamětech počítačů, utajení faxové, hlasové a video komunikace, pro velké objemy dat a velké přenosové rychlosti.

Označme šifrovací algoritmus $\mathbf{E_k}$, dešifrovací algoritmus $\mathbf{D_k}$, otevřený text **M**, zašifrovaný text **C**.[77]

$C = E_k(M,K)$ kde K je kryptografický klíč, pro proces zašifrování {1}

$M = D_k(C,K)$ kde K je kryptografický klíč, pro proces odšifrování {2}



Obr. 6 Obecný model šifrového spoje dle Shannona[78]

Symetrické šifry se dále mohou dělit na dvě kategorie. Proudové a blokové. Proudové šifry zpracovávají otevřený text bit po bitu. Blokové šifry po skupinkách bitů – blocích.[79]

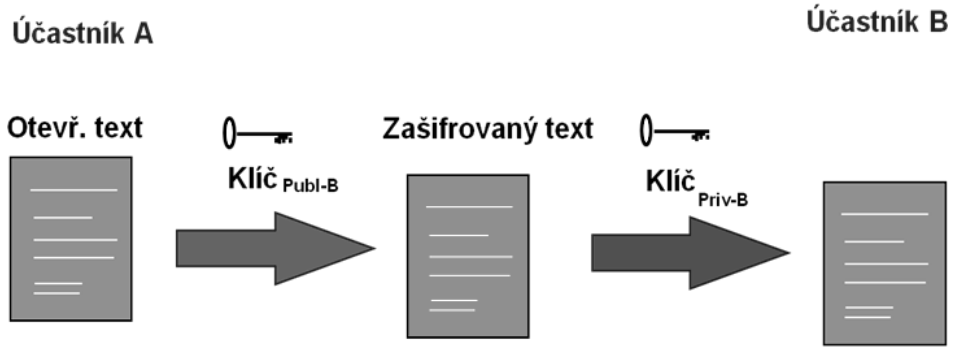
3.3.2 Asymetrické šifrování

Asymetrické šifry používají rozdílné klíče, veřejné a soukromé, pro šifrování a dešifrování. Používají se především k realizaci elektronického podpisu, při řízení

[77] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 99.
[78] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 95.
[79] PŘIBYL, J. Ochrana dat v informatice. Praha, 1996, s. 25.

přístupu k datům a k distribuci klíčů pro symetrické šifry. V odborné literatuře jsou systémy s veřejnými klíči označovány jako " Public Key Infrastructure" (PKI).[80]

Asymetrické šifrování (Obr.7) je postup, kdy jeden klíč - veřejný, slouží k zašifrování otevřeného textu a druhý klíč - soukromý k dešifrování. Veřejný klíč není třeba utajit, protože jeho znalost nevede k rozluštění zašifrovaného textu. Může tak být zveřejněn na internetu. Druhý soukromý klíč potřebný k dešifrování je bezpečně ukrýván majitelem (čipová karta, USB token v trezoru). První část (šifrování - encryption) přemění text M na text T přičemž použije klíč K1 (veřejný klíč - public key). Druhá část (dešifrování - decryption) přemění text T na text M, přičemž se použije klíč K2 (soukromý klíč - private key). V zásadě platí, že z K1 se žádným matematickým postupem nedá získat K2. Soukromý klíč K2 je klíč, který vlastní jen člověk, kterému je zpráva určena a je bezpečně ukrýván majitelem. K1 je veřejný klíč, který může vlastnit kdokoliv (daná osoba jej tedy může poskytovat ke stažení na internetu). Text M zašifrovaný pomocí klíče K1 se tedy dá dešifrovat pouze za pomoci klíče K2, který má jen člověk, kterému je zpráva určena (z toho vyplývá, že text T na text M nemůže dešifrovat ani ten, kdo jej zašifroval, protože nemá soukromý klíč K2, potřebný pro tuto operaci).[81]



Obr. 7 Asymetrické šifrování[82]

Obecně ale platí, že bezpečná délka klíče ve srovnání se symetrickou šifrou je vždy výrazně větší a vlastní algoritmus je výpočetně velmi náročný nejen na složitost, ale i potřebný čas k zašifrování/odšifrování zprávy, proto se asymetrické šifrování nehodí k šifrování dlouhých proudů dat.[83]

[80] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 99.
[81] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 90.
[82] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 101.
[83] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 100.

Rozdíly mezi symetrickou a asymetrickou kryptografií

Symetrická kryptografie: menší výpočetní náročnost - vyšší výpočetní rychlost, problematické šíření klíče, dvě kopie tajemství (obě strany), pro komunikaci mezi partnery je třeba mít N klíčů, pro komunikaci s neznámým partnerem je těžší si ověřit jeho identitu.[84]

Asymetrická kryptografie: značná výpočetní náročnost - až 1000 x nižší výpočetní rychlost než u symetrické kryptografie, pouze jedna kopie tajemství (pod vlastní kontrolou), lehké šíření klíčů (možnost uložit veřejný klíč na veřejně dostupném místě), při komunikaci s neznámým partnerem je poměrně lehké ověřit jeho identitu.[85]

3.3.3 Hashovací funkce

Nedílnou součástí tvorby elektronického podpisu jsou hashovací funkce, které tvoří základ pro zaručení autentifikace a integrity elektronického podpisu. Hashovací funkce je algoritmus, který ze vstupního řetězce znaků vygeneruje jiný řetězec pevné délky znaků, takzvaný digitální otisk. Digitální otisk (fingerprint) je jakýsi abstrakt dané zprávy. Je to výsledná hodnota vygenerována hashovací funkcí, přičemž platí, že: použití algoritmu na tentýž vstupní řetězec, vždy dá stejnou hodnotu, to znamená, že na danou zprávu můžu několikrát aplikovat hashovací funkci, přičemž digitální otisk bude vždy stejný. Je matematicky neuskutečnitelné získat, nebo zrekonstruovat původních řetězec znaků na základě vědomostí výsledné hodnoty, to znamená, že z digitálního otisku se nedá zpět vygenerovat obsah dané zprávy. Je matematicky neuskutečnitelné sestavit dva různé vstupní řetězce znaků se stejnou výslednou hodnotou, to znamená, že pokud se změní obsah dané zprávy (byť jen 1 znak, 1 bit), změní se i digitální otisk této zprávy. Těmto podmínkám vyhovuje nejčastěji používaná hashovací funkce SHA (Standard Hash Algorithm).[86]

3.3.4 Elektronický podpis

Pokud se asymetrickým algoritmem a pomocí soukromého klíče zašifruje digitální otisk, vznikne řetězec znaků, který se nazývá elektronický podpis. Elektronicky podepsat zprávu znamená, svým soukromým klíčem zašifrovat (podepsat) digitální otisk dané zprávy. V případě, aby zpráva byla i důvěrná nestačí ji pouze

[84] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 90.
[85] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 94.
[86] ZELENKA, J. *Ochrana dat : kryptologie*. Hradec Králové, 2003, s. 127.

podepsat (zašifrovat) svým soukromým klíčem, ale navíc celou zprávu i s elektronickým podpisem zašifrovat veřejným klíčem adresáta.[87]Elektronický podpis poskytuje příjemci (i autorovi) **autentizaci**: příjemce dokumentu bezpečně ví, kdo je jeho autorem, **integritu**: příjemce dokumentu má jistotu, že jeho obsah nebyl během přenosu nebo zpracování změněn, **nepopiratelnost autorství**: autor dokumentu nemůže popřít autorství ani jeho obsah, ale neposkytuje **důvěrnost** dokumentu, ta je zajišťovánaěna šifrováním.[88]

Vznik a podepsání elektronického podpisu odesilatelem: (Obr.8)

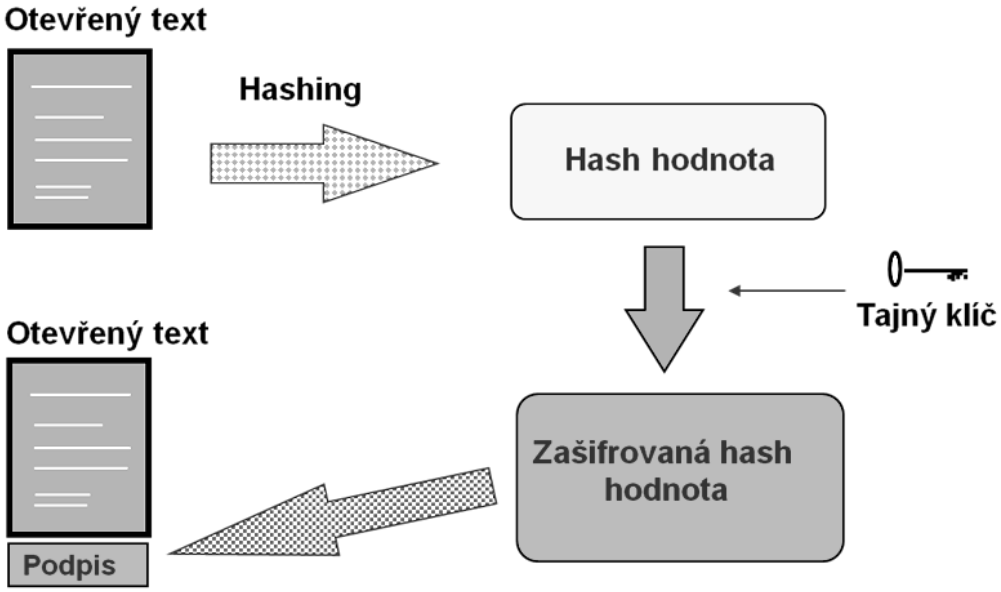
- Program elektronického podpisu aplikuje funkci HASH na otevřeném textu odesílané zprávy.
- Výsledná hodnota funkce HASH se zašifruje tajným klíčem odesilatele.
- Zašifrovaný výsledek HASH(He) se připojí za otevřený text – elektronický podpis
- Odešle se otevřený text s připojeným podpisem k příjemci zprávy (adresátovi)

Příjem podepsané zprávy: (Obr.9)

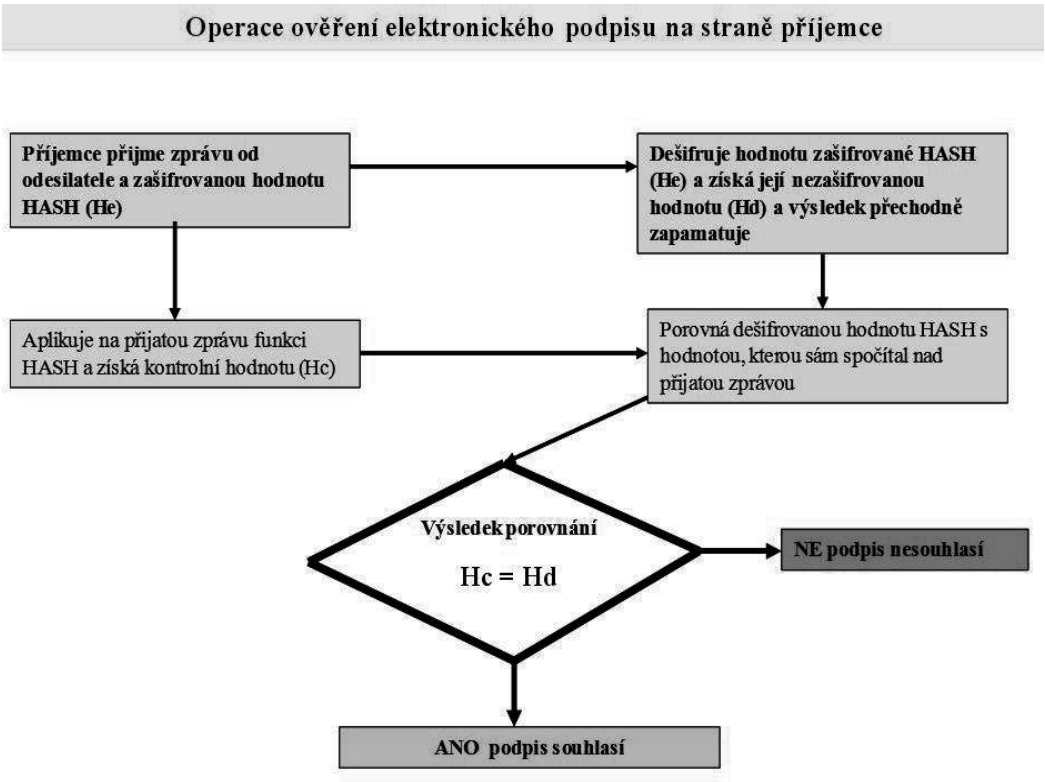
- Ověření pravosti podpisu
- Příjemce přijme zprávu včetně podpisového „přívěsku“HASH(He)
- Příjemce nalezne v databázi veřejných klíčů veřejný klíč odesilatele
- Odšifruje přijatý podpis He pomocí veřejného klíče odesilatele a uloží do paměti jako Hd
- Aplikuje na přijatou zprávu funkci HASH a výsledek uloží do paměti jako Hc
- Porovná vypočítanou hodnotu Hc s dešifrovanou hodnotou Hd
- Jsou-li oba výsledky stejné (Hc = Hd) pak je podpis správný

Elektronický podpis je spojen s jedním konkrétním elektronickým dokumentem (potvrzuje pravost a autenticitu dokumentu) a nemůže být použit pro podepsání jiného dokumentu a může být vytvořen pouze tím, kdo zná soukromý klíč. Ubezpečení, že podpis je správný vychází z předpokladu rovnosti Hc = Hd, to může nastat jedině tehdy, když zašifrování provedl vlastník příslušného soukromého klíče z jedné dvojice veřejného a soukromého klíče.[89]

[87] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s. 219.
[88] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 93-94.
[89] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 108.



Obr. 8 Elektronický podpis[90]



Obr. 9 Ověření podpisu na straně příjemce[91]

[90] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 109.
[91] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 109.

3.3.5 Certifikační autorita

Alfou a omegou elektronické komunikace je bezpečnost. Kritickým bodem je problém pravosti veřejného klíče. Potenciální útočník by mohl ověřovateli poslat místo veřejného klíče podepisující osoby svůj veřejný klíč a tímto klíčem podepsanou upravenou zprávu namísto původní zprávy, aniž tuto skutečnost ověřovatel odhalil. V současnosti se na distribuci a přenos klíčů od signatáře k ověřovateli využívá metoda důvěryhodné třetí strany - Trusted Third Party (TTP) certifikační autoritou. Certifikační autoritu můžeme přirovnat k notáři, který potvrzuje totožnost. Vydaný certifikát tak lze chápat jako elektronický průkaz totožnosti. Před vytvořením elektronického podpisu je nutno nejdříve navštívit certifikační autoritu nebo kontaktní pracoviště (registrační autority) a požádat o vydání certifikátu. Při vydání certifikátu dochází k fyzickému ověření totožnosti. Certifikační autorita svým elektronickým podpisem potvrdí certifikát, který obsahuje veřejný klíč a osobní údaje držitele. Certifikační autorita je důvěryhodná třetí strana, která je odpovědná za vydávání, správu a rušení certifikátů veřejného klíče.[92]V České republice působí tři certifikační autority, První certifikační autorita, a. s., Česká pošta, s. p. a eIdentity a. s.[93]

[92] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s. 223.

[93] *Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb.* [online]. Praha : Ministerstvo vnitra České republiky, [cit. 2015-02-07]. Dostupné z WWW:< http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb-320051.aspx>

4 RIZIKA MODERNÍCH TECHNOLOGIÍ

,,Každý, kdo přemýšlí o kvantové mechanice, aniž by se mu zatočila hlava, jí nerozumí."
Autorem uvedeného citátu je známý americký vědec a nositel Nobelovy ceny za fyziku Niels Bohr.

Při navrhování systému pro komerční využití musejí jejich tvůrci myslet na několik let dopředu a vzít v potaz dopad pokroku a zvyšování počítačové mohutnosti. K tomuto účelu lze použít takzvaný *Moorův zákon*, podle nějž se výpočetní výkon počítačů každých 18 měsíců zdvojnásobí, aniž by se nějak zvýšila jejich cena. Pro lepší představu o velikosti čísel, uvedu názorný příklad. Rok má 31 536 000 vteřin, což je zhruba 2^{25}. Pokud by odzkoušení jednoho klíče trvalo jednu vteřinu, tak by prověření 2^{25} klíčů trvalo déle než rok. Pokud by ovšem útočník měl k dispozici superpočítač schopný zkusit milion klíčů za vteřinu, nezabralo by to ani minutu. *Moorův zákon* umožňuje hrubý odhad postupu vývoje technologií v průběhu nejbližších let. Nepočítá však se zbrusu novými technologiemi, jejichž zavedení by mělo dramatický efekt. Jednou z takových možných technologií jsou kvantové počítače.[94]

4.1.1 Kvantové počítače

Na jakém principu obecně kvantové počítače pracují:

Stávající technologie současných počítačů je založena na principu tranzistoru jako primárního aktivního prvku, kdy tranzistor buď je ve vodivém stavu nebo je uzavřen (logická jednička/nula). Další integrace HW v současných technologiích je již problematická. Kvantové počítače fungují na principu základního prvku – atomu a změna stavu je dána změnou energie při přechodu elektronu z jedné orbity na druhou (logická jednička/nula). Dochází k větší integraci objemu počítačového HW a k obrovskému zvýšení možností paralelismu při řešení úloh.

Kvantové počítače provádějí výpočty prostřednictvím změn kvantových stavů, díky nimž lze výpočty zpracovávat paralelně. Zatím bylo postaveno jen velice málo kvantových počítačů, takže se jedná spíše jen o pracovní prototypy a i přes to panují pochybnosti, zda je to doopravdy výsledek kvantového počítání.[95]Jestliže však bude jejich myšlenka uvedena v život, celá situace se naprosto změní. Na vývoj kvantových

[94] PIPER, F. C. - MURPHY, Sean. *Kryptografie*. Praha, 2006, s. 94.
[95] WOODWARD, A. *Is It Quantum Computing or Not?*. Yahoo news. [online]. 17.5.2013 [cit. 2014-12-02]. Dostupné z: http://news.yahoo.com/quantum-computing-not-140100223.html

počítačů jsou po celém světě vynakládány nemalé částky. Podle hrubého odhadu by takové stroje dokázaly za stejnou dobu vyzkoušet klíč s dvojnásobnou délkou než současné počítače. Prohledávání 2^{128} klíčů by tedy na kvantovém počítači trvalo zhruba stejně dlouho jako hledání mezi 2^{64} klíči dnes. Naštěstí ani největší nadšenci a příznivci kvantových počítačů nepředpokládají, že by se tyto stroje začaly šířeji využívat dříve než na 20 let. Navíc část fyziků se domnívá, že funkční kvantový počítač nebude nikdy sestrojen.[96]

Nejvíce ohroženy protivníkovým (zatím jen hypotetickým) počítačem budou asymetrické šifry, jejichž odolnost proti luštění je dána výpočetní složitostí, ale postup výpočtu je znám. Právě výpočetní náročnost bude použitím kvantového počítače značně snížena.

[96] PIPER, F. C. - MURPHY, Sean. *Kryptografie.* Praha, 2006, s. 95.

5 ZÁKLADY INFORMAČNÍ BEZPEČNOSTI

Informační bezpečnost je disciplína, jejímž hlavním úkolem je zejména ochrana informací a informačních systémů před hrozbami během celého jejich životního cyklu. Pro dosažení svých cílů využívá informační bezpečnost i poznatky jiných technických, ale i humanitních vědních oborů, přičemž nejužší propojení je právě s kryptologií. Kryptologie je vědní oblast, která se zabývá konstrukcí a analýzou kryptosystémů. Zpočátku se kryptologie upřednostňovala k zajištění důvěrnosti údajů, tedy na šifrování. Později se začala zabývat i dalšími požadavky například na integritu dat, autenticitu, nepopiratelnost, či časovou souslednost.[97]

5.1 Informační bezpečnost

Informace mají svoji určitou tržní hodnotu, je možné s nimi zacházet jako s majetkem, kupovat je, prodávat, ale i krást. Hodnotu informace představuje především její výlučnost (vím něco, co jiný ne) ale i přesnost a její integritu. V každé době se důvěrné informace přísně střežily a věnovala se pozornost jejich ochraně a udržení důvěrnosti. Díky nástupu počítačů, vzniku komunikační sítě a celosvětovému Internetu, se informace uložená v elektronické podobě v počítači, rázem stává nejen něčím těžko uchopitelným do ruky, ale také nehmotným statkem. Dokumenty v papírové podobě, rozsáhlé evidence a kartotéky uložené v archivech se pomalu stávají anachronizmem. Avšak stále zde jedna významná skutečnost zůstává a to, že jen tím, že je informace uložena v jiném tvaru, se její hodnota nezměnila. Nutnost chránit data uložená v počítačových systémech je tedy velice aktuální. Zabezpečení takového informačního systému připomíná zabezpečení a ochrany významného objektu. Bezpečností se zde chápe zajištění systému jako celku, přístupu do něj, manipulace s hodnotami,vytváření záloh, antivirová ochrana a další aspekty.[98]

[97] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 16-17.
[98] DOBDA, L. Ochrana dat v informačních systémech. Praha, 1998, s. 10.

5.2 Informační a komunikační systém

Informační a komunikační systém ICT definujeme jako systém technických a programových prostředků, jejichž úkolem je sběr, přenos, zpracování, ukládání a uchování informací. Je zřízen pro dosahování stanovených cílů a plnění definovaných úkolů. Finanční domy vedou ve svých informačních systémech evidence účtů svých klientů, podniky je používají k řízení výroby, armády do nich ukládají i ty neutajovanější informace o obraně státu. IS systém tvoří logický celek, který obsahuje samostatné části, nazývané položky - assets (v analýze aktiva informačního systému). Položkami mohou být i nemateriální entity, údaje, znalosti, dobré jméno organizace, či schopnost poskytovat služby. Hrozba je jakákoliv událost, jejímž následkem je odchylka od pravidel upravujících činnost IS systémů.[99]Pokud taková událost nastane, říkáme, že hrozba byla naplněna, došlo k bezpečnostnímu incidentu. O naplnění hrozby, případně její využití,se mohou pokoušet i konkrétní osoby, v takovém případě jde o útok, osoby označujeme za útočníky. Kromě incidentů způsobených vědomým jednáním lidí, může nastat situace, kdy dojde k naplnění hrozby v důsledku neúmyslného jednání, případně v důsledku technické poruchy. Osoba, zařízení nebo skutečnost, která zapříčinila naplnění hrozby se označuje pojmem nositel hrozby. Výsledky uskutečnění hrozby nazýváme dopady nebo důsledky.[100]

Moderní společnost postupně přechází při zpracovávání údajů k automatizaci. Výhodou automatizovaného zpracování informací je především možnost zpracovat velké množství informací. K tomu je třeba využívat informační systémy založené na informačních a komunikačních technologiích. Jeho provoz je závislý od dalších faktorů, jakými jsou hlavně fyzická organizace systému, rozmístění hardwaru, způsob softwarového řešení systému a v neposlední řadě i technické a legislativní normy, pravidla, zvyklosti a zkušenosti. Souhrn takových faktorů, které nějakým způsobem ovlivňují chod a funkčnost systému, se nazývá bezpečnostní okolí systému. Patří sem všechny entity nacházející se mimo systém. Většinou se zajímáme pouze o takové okolí, se kterým systém vzájemně působí. Pomyslnou dělící čáru mezi systémem a jeho okolím se nazývá hranice systému. Každý informační systém je třeba podrobně popsat, aby bylo možné zajistit jeho spolehlivost a bezpečnost.[101]

[99] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 14-15.
[100] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika.* České Budějovice, 2014, s. 26.
[101] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s. 11.

5.2.1 **Bezpečnostní incident**

Aby mohl nastat bezpečnostní incident, je třeba, aby měl systém takzvaná slabá místa. Jsou to vlastnosti, nedostatky nebo chybné řešení systému, které umožňují hrozbu realizovat a poškodit aktiva systému, s možným narušením dostupnosti, integrity a důvěrnosti zpracovávaných nebo uložených informací. Každý bezpečnostní incident nastává s určitou pravděpodobností což je důsledkem pravděpodobnostního charakteru hrozeb a má pro systém nějaké vážné důsledky. Oba tyto faktory se souhrnně označují jako bezpečnostní riziko. Riziko je potenciální možnost, že daná hrozba využije zranitelnosti určitého aktiva, způsobí jeho ztrátu nebo poškození a tím i škodu organizaci, která informační systém provozuje.[102]

K odhalení možných ohrožení informačního systému je důležitá analýza rizik – odhad (výpočtem) pravděpodobnosti výskytu bezpečnostních incidentů a stanovení míry rizika, kterému je informační systém vystaven.. Stejně důležité je i definovat bezpečnostní opatření, tedy pravidla a prostředky k eliminaci rizik a snížení pravděpodobnosti naplnění hrozeb. Podle rizika lze hrozby rozdělit do tří základních skupin - kritické, středně závažné a nepodstatné. Podle charakteru hrozby se pak navrhují, realizují a kontrolují konkrétní bezpečnostní opatření.[103]Způsob aplikace bezpečnostních opatření tvoří základ bezpečnostní politiky informačního systému.

5.3 Základní cíle informační bezpečnosti

Úkolem informační bezpečnosti je však nejen ochrana systému, ale i ochrana informací, které systém zpracovává a uchovává. Základní cíle informační bezpečnosti je naplnění požadavků na integritu dat, důvěrnost dat, dostupnost dat.. Tyto základní požadavky na bezpečnost jsou společné pro všechny informační systémy a technologie. Ale jejich vzájemná vyváženost je závislá na definovaných požadavcích, kladených na konkrétní systém. Důvěrnost bude určitě převažovat nad integritou a dostupností u vojenských a agenturních systémů, a integrita dat bude zase základním požadavkem u rozsáhlých informačních knihoven a tak podobně.[104]

---

[102] PEKÁREK O., ČÍŽEK VL., *Práce s agenturními a elektronickými informacemi, studijní text*, VŠERS, s. 64-64.
[103] PEKÁREK O., ČÍŽEK VL., *Práce s agenturními a elektronickými informacemi, studijní text*, VŠERS, s. 78.
[104] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s. 23.

Integrita dat (integrity)

Integrita dat, česky řečeno celistvost, zaručuje, že údaje se během jejich přenosu nezmění, ať už úmyslným jednáním třetí osoby, nebo v důsledku snížené kvality přenosového kanálu, či jiných faktorů. Rovněž u uložených či zálohovaných datech třeba zamezit neautorizovaným změnám obsahu. Aby bylo možné zaručit integritu dat, je třeba, v co největší míře zabránit změnám přenášených dat. Obecně není možné na 100% zamezit poškození, či změně údajů důsledkem technických chyb nebo nepříznivých vlivů prostředí. Do jisté míry lze chyby vzniklé vlivem prostředí eliminovat použitím samo opravných kódů, které jsou schopny detekovat a opravit chyby malého rozsahu. Pro zajištění integrity dat je stejně nezbytná schopnost všech komunikujících stran identifikovat případné změny v přenášených datech. Takovou schopnost dosahujeme pomocí hashovacích funkcí, hashovacích funkcí s tajným klíčem a elektronických podpisů.[105]

Důvěrnost

IS systémy mnohdy pracují s údaji, které jsou určeny pouze pro jistou skupinu lidí. Je důležité, aby přístup k těmto informacím měli pouze oprávněné osoby. Říkáme, že tyto informace jsou důvěrné. Zamezit přístupu neoprávněných osob k údajům a tím jejich kompromitaci, tedy zajistit důvěrnost údajů, lze metodou řízení přístupu. Přístup k údajům je povolen pouze oprávněným osobám. Spolehlivější metoda je šifrování. Zamezuje útočníkům přístup k datům i v případě neoprávněného odposlechu komunikačního kanálu, což první metoda zajistit nedokáže.[106]

Dostupnost informací

Dostupnost informací znamená, že informace jsou oprávněným osobám k dispozici tehdy, když je potřebují, v požadovaném rozsahu a na určeném místě. Dostupnost údajů není možné zajistit za všech okolností. Důsledkem úmyslných útoků, vlivů prostředí, či technických poruch mohou nastat situace, kdy se údaje stanou dočasně nedostupnými. V některých případech, jako jsou například trvalé poškození pevných disků, se informace mohou stát nedostupnými natrvalo. Když se mluví o dostupnosti, vždy je třeba určit maximální čas, během kterého se vzniklé příčiny nedostupnosti dat odstraní a obnoví se oprávněným osobám přístup k informacím.

[105] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s 25.
[106] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s 23.

Dostupnost je většinou zajišťována použitím záložních zdrojů, zálohováním, archivováním nebo zrcadlením dat na diskových polích, antivirová ochrana.[107]

Autenticita

Pod autentičností rozumíme schopnost spolehlivě určit původ informací, ověřit identitu osoby, která dokument vytvořila, a přitom zaručit, že dokument nebyl pozměněn, a to dokonce ani samotným autorem dokumentu. Prostředkem k zajištění autentičnosti dat je elektronický podpis. Závisí totiž od obsahu dokumentu, čímž je zajištěno, že informace se nezmění, a na jeho vytvoření je potřebná znalost soukromého klíče autora, čímž je zaručena identifikace autora dokumentu.[108]

Nepopiratelnost

Nepopiratelnost řízení zaručuje, že osoba zúčastněná na komunikaci, případně modifikaci dat, není schopna popřít provedení daných akcí. Jinými slovy, v případě potřeby je možné prokázat, že konkrétní akci provedla konkrétní osoba. Například takto nelze odmítnout provedenou objednávku zboží nebo chybu při editaci a změně údajů, ať už úmyslná nebo neúmyslná.[109]

Časová souslednost

Časová souslednost umožňuje odhalit existenci údajů v čase a zjistit posloupnost provádění akcí, určit jejich vzájemnou souslednost. Nejjednodušším řešením je přidat k informaci údaj o aktuálním čase. Je však ošetřit případnou entropii jednotlivých subjektů pracujících s informacemi.[110]

Těchto vlastností IS dosahuje jednak správně uvolenou bezpečnostní politikou IS, tj souborem organizačních opatření která určují pravidla zacházení s informacemi a určují chování uživatelů IS, jednak využitím relevantních technických, kybernetických a informatických nástrojů k ochraně systému a samotných informací.

5.3.1 Bezpečnostní funkce a požadavky

Zmíněné cíle dosahujeme pomocí bezpečnostních funkcí. Ovšem ne vždy vyžadujeme všechny cíle najednou. Funkční bezpečnostní požadavky určují, které

[107] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 27.
[108] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 28.
[109] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s 27.
[110] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 16.

bezpečnostní funkce má IS systém poskytovat. Realizace funkcí poskytovaných systémem nemusí byt dostatečná, případně může být defektní. Důvěryhodné systémy musí splňovat vedle funkcionálních bezpečnostních požadavků i požadavky na bezpečnostní záruky. Jejich úkolem je poskytnout důvěru, že bezpečnostní funkce jsou dostatečné a správné implementovány. Kromě úmyslných hrozeb a scénářů útoků na informační systém je potřebné odpovídajícím způsobem reagovat na rizika odposlechu a tím i kompromitaci zpracovávaných citlivých informací cestou parazitního elektromagnetického vyzařování z HW prostředků. Tento způsob informatického útoku je sice velmi technicky náročný, ale se zdokonalováním radiotechnického přístrojového vybavení se stává stále aktuálnějším a tím i pro potenciálního útočníka dosažitelnějším.[111]

Cílem nepřátelských informačních operací jsou zpravidla:

- citlivé informace protivníka
- státní, vojenské, bezpečnostní, finanční, zdravotnické a další důležité informační a komunikační IS
- informační technika
- informační části zbraňových systémů
- procesy rozhodování a velení a tak podobně

5.3.2 Možné scénáře útoku

Informační systémy, jejich aktiva, mohou být za splnění určitých podmínek cílem působení různých hrozeb a hrozí jim určité nebezpečí. Hrozby mohou mít mnoho forem. Mohou to být jednak lidé - i přímo vlastní zaměstnanci (nízký stupeň zaměstnanecké loajality), jednak události způsobené přírodními jevy (oheň, povodeň) a vlivy techniky (porucha, výpadek el. energie). Lidské hrozby představují agenti rozvědky, teroristé, organizovaní zločinci, zlomyslní a pomstychtiví lidé, nebo také počítačový nadšenci a studenti.[112]Od útočníka se musí očekávat, že může použít libovolný způsob průniku. Nemusí to být nejzřejmější metoda a útok nemusí být veden proti nejsilnějšímu místu ochrany systému. Útočník může být limitován svými ekonomickými a technickými možnostmi, při čemž náklady na kvalifikovaně vedený informatický útok jsou vysoké a rostou s jeho složitostí. Proto nelze ze strany

[111] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 28.
[112] DOBDA, L. *Ochrana dat v informačních systémech*. Praha, 1998, s 15.

teroristických organizací vyloučit příklon k využívání relativně lacinějšího a snazšího útoku, vedeného hrubou silou proti fyzické integritě informačních systémů. Navíc tento způsob může být velmi účinný a odpovídá lépe mentalitě některých teroristických skupin a hnutí, které takto vedeným útokem sledují současně i své „politické zviditelnění" (půjde především o porušování celistvosti komunikačního prostředí například napadáním retranslačních bodů, ničením anténních systémů, krádeže terminálových počítačů a tak podobně).[113]

Tak zůstane efektivní kvalifikovaný informatický útok i nadále především doménou státních, vojenských a polovojenských zpravodajských organizací a odborně fundovaných skupin a jednotlivců, pro které hrubý útok ve formě sabotáží není vůbec aktuální a nebo pro které bude aktuálním pouze jako součást strategického záměru až ve vyšších fázích informační války.[114]

5.3.3 Zdroje informatických útoků

Existuje celá řada hrozeb pro informační systémy, s nejrůznějšími motivacemi, kde váha jednotlivých hrozeb se v závislosti na okolnostech může výrazně měnit.[115]

a) **zpravodajské služby států**, které se prioritně zaměřují na průmyslovou, politickou a vojenskou špionáž, s cíli zabezpečit jak politické tak i ekonomické zájmy svých vlád
b) **soukromé zpravodajské služby**, které pracují pro velké firmy (soukromé společnosti), pracují zpravidla na zakázku, s orientací na získání a udržení odbytišť, zakázek a technologického "know how " ve prospěch svých klientů. Úloha těchto organizací po ukončení studené války nabyla na účinnosti, protože do jejich služeb vstoupilo značné množství vysoce kvalifikovaných a nyní nepotřebných bývalých pracovníků zpravodajských služeb států.
c) **teroristické organizace a extremistické skupiny** (národní i mezinárodní) a na ně navazující hnutí, často podporované některými totalitními státy, které poskytují odbornou, ideovou i materiální podporu prostřednictvím svých zpravodajských služeb.

[113] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 38-40.
[114] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 28-29.
[115] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 29.

d) **kvalifikovaná kriminalita** namířená především proti finančním, správním a bezpečnostním institucím a jejich informačním systémům, často disponující kvalifikovanými útočníky- hackery (kriminalita takzvaných bílých límečků)
e) **rutinní „hackeři", studenti a zvídaví lidé s odborným vzděláním v oblasti informatiky**, kteří často bez zřejmé motivace pronikají do informačních systémů a rozrušují jejich integritu (platí zvláště pro informační systémy propojené se sítí INTERNET), v poslední době často pracují na zakázku platících klientů
f) **tvůrci a zavaděči počítačových virů**, kteří narušují informační systémy, někdy i bez zřejmého motivu, často však ve službách reálného nepřítele, často jako v bodě e)

Společným jmenovatelem všech uvedených hrozeb je aktivní spolupráce odborníků na straně útočníka a tím i zvýšená pravděpodobnost kvalifikovaně vedených útoků.[116]

Typickými způsoby provádění úmyslných útoků jsou:

- Krádeže, ničení nebo pozměňování dat
- Neoprávněné použití nebo pozměnění aplikačních programů
- Zneužívání přístupových hesel a autentizačních nástrojů, kryptografických klíčů
- Odposlech, kryptologická analýza
- Vytěžování parazitního elektromagnetického pole
- Implementace virů, trojských koní a podobně s cílem narušit činnost počítačů, destruovat databáze, získávat uložená data, monitorovat činnost organizace a tak podobně
- Sabotáže s cílem fyzického poškození komponent informačního systému.

5.3.4 Počítačová (kybernetická) kriminalita

Rozvoj informačních a komunikačních technologií sebou přináší i jisté negativní jevy. Výpočetní technika přinesla na jedné spraně zjednodušení práce lidí, ale na druhé straně se stala zdrojem problémů v oblasti utajení informací a ochrany dat. Počítač obsahuje množství dat a informací, které mohou být lákavým zdrojem pro zloděje. Mnohem častěji jsou odcizována data, která jsou uložena v počítačích či médiích než odcizení počítače jako hmotného zařízení. Pachatel velmi rychle data zkopíruje a nebo

[116] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 29.

je posílá po síti. Odcizená data a programy se pak mohou dobře prodat konkurenci či je využít ve svůj prospěch. Pachatelé těchto krádeží jsou především sami zaměstnanci ve firmách a organizacích.[117]

Z hlediska kriminality jsou nejnebezpečnější skupinou hackeři, kteří vnikají do počítačových sítí profesionálně. Pronikají do systémů jak z recese tak s cílem obohacení, často jen aby dokázali svou nadřazenost nad systémem, kopírují data a prodávají za nejvyšší cenu, případně zahltí systém tak, že přestane fungovat a celý zkolabuje. Zapojení počítačů do světových sítí umožňuje odcizit data odkudkoliv. Stačí se napojit na přenosové kanály (telefonní linky, optické kabely, bezdrátové sítě WIFI). Termínem počítačová kriminalita se obvykle označují trestné činy proti počítačům nebo trestné činy páchané prostřednictvím počítače. Obecně ji lze definovat jako trestné činy namířené proti integritě, dostupnosti nebo utajení informací v počítačových systémech nebo trestné činy, při nichž je použito informačních nebo telekomunikačních technologií.[118]

5.4 Česká legislativa řešící informační bezpečnost

Systém zákonů a předpisů, který upravuje ochranu informací, ochranu informačních systémů a definuje jejich způsobilost pro provoz, jakož i podmínky způsobilosti osob ke styku s citlivými informacemi včetně nezbytných sankcí, respektuje jak nezadatelné právo občana na informace a ochranu soukromí, tak na druhé straně oprávněná omezení tohoto práva. Tak jak se rychle vyvíjí samotný obor informatiky, mění se i škála možných informatických útoků, tak i rychle zastarávají zákonné normy a předpisy. Proto jsme svědky kontinuálního procesu novelizace těchto právních norem a je nutno si uvědomit že se v tomto ohledu jedná o pozitivní jev. Z hlediska úplnosti a metodické propracovanosti se zatím jeví jako nejlépe použitelný zákon č. 412/2005 Sb. s doprovodnými vyhláškami. Přesto, že se uvedený zákon týká informačních systémů pracujících s utajovanými informacemi, lze jeho metodiky uvedené ve vyhláškách úspěšně využít při budování jakéhokoliv jiného důvěryhodného systému. Pro informační systémy veřejné správy pak platí zákon. č. 365/2000 Sb., o informačních systémech veřejné správy[119]

[117] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 127.
[118] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 129.
[119] FEREBAUEROVÁ, R - PEKÁREK, O. *Aplikovaná informatika*. České Budějovice, 2014, s. 33.

Zákon 412/2005 Sb. ze dne 21. září 2005 o ochraně utajovaných informacích a o bezpečnostní způsobilosti

Zákon č. 412/2005 Sb. ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti stanovuje zásady zda se jedná o utajované informace uvedené v seznamu utajovaných informací (§ 139), definuje podmínky pro přístup k utajovaným informacím a nároky na jejich ochranu. Dále zákon upravuje zásady pro stanovení citlivých činností a vymezuje činnost Národního bezpečnostního úřadu (NBÚ).[120]

Utajovaná informace se klasifikuje stupněm utajení

a) Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,
b) Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,
c) Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,
d) Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.[121]

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy

Nejdůležitější právní normou upravující oblast informačních systémů veřejné správy je zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. Tento zákon prošel za dobu od schválení mnoha úpravami:[122]

Změna: 517/2002 Sb. – zrušení Úřadu pro veřejné informační systémy a zřízení Ministerstva informatiky České republiky

Změna: 413/2005 Sb., 444/2005 Sb. – zákon se přestává vztahovat na informační systémy veřejné správy nakládající s utajovanými informacemi

Změna: 81/2006 Sb. – upravuje atestační a akreditační postupy

[120] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 174.
[121] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 175.
[122] Zákon č. 365/2000 Sb. o informačních systémech veřejné správy.

Tento zákon stanovuje práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. Definuje základní pojmy jako například:

- Informační činnost
- Informační systém
- Správce informačního systému – subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá
- Provozovatel informačního systému
- Vytváření a služba IS
- Datový prvek
- Atest a atestační středisko

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Je základním právním předpisem upravujícím ochranu osobních údajů a činnost Úřadu pro ochranu osobních údajů. Listinou základních práv a svobod je zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života, neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů. V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více narušováno. Provádění zákona realizuje především Úřad pro ochranu osobních údajů.[123]

Vyhláška národního bezpečnostního úřadu č. 524/2005, o zajištění kryptografické ochrany utajovaných informací

Vyhláška národního bezpečnostního úřadu 524/2005 stanovuje podrobnosti o zkoušce zvláštní odborné způsobilosti pracovníka kryptografické ochrany, způsoby a prostředky manipulace s kryptografickým materiálem, podrobnosti způsobu vyznačování náležitostí na utajované informaci z oblasti kryptografické ochrany a administrativní pomůcky kryptografické ochrany a další podrobnosti k zajištění kryptografické ochrany utajovaných informací.[124]

[123] Zákon č. 101/2000 Sb. o ochraně osobních údajů.
[124] POŽÁR, J. *Základy teorie informační bezpečnosti*. Praha, 2007, s. 183.

Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti s účinností od 1.1.2015[125]vznikl jako odezva na směrnici Evropské unie, podle které by měly členské státy EU zvyšovat svou schopnost odolávat potenciálním kybernetickým útokům. Díky novému zákonu by tak Česká republika měla být více rezistentní vůči potenciálním útokům na klíčové počítačové systémy, které jsou nezbytné pro bezpečný a bezchybný chod státu (doprava, energetika, ekonomika). Dále by mělo dojít ke sjednocení elektronické komunikace nejen ve státní ale částečně i soukromé sféře a zvýšení bezpečnosti osobních dat uchovaných v sektoru veřejné správy.[126]

Strategie České republiky pro boj proti terorismu od r. 2013

Strategie České republiky pro boj proti terorismu od r. 2013 formuluje základní oblasti, principy a postupy boje proti terorismu v rámci předpokladů České republiky. Je strukturována do pěti základních oblastí, kterým se věnuje podrobněji:

1. Spolupráce subjektů zapojených do boje proti terorismu

2. Ochrana obyvatelstva, kritické infrastruktury a jiných potenciálně zranitelných cílů

3. Bezpečnostní výzkum, vzdělávání a informování veřejnosti

4. Prevence radikalizace ve společnosti a boj proti rekrutování do teroristických struktur

5. Legislativní a mezinárodně-smluvní otázky

Dokument se věnuje zejména preventivními postupy a opatřeními v souvislosti se situací v České republice. Jelikož Česká republika nepatří mezi země s vysokým rizikem teroristických útoků je v tomto ohledu role České republiky v boji proti terorismu zakotvena spíše v jejím spolupůsobení v mezinárodních uskupení, případně ochrany samotného území republiky před případnými teroristickými útoky a dostatečné připravenosti na potenciální rizika. Vzhledem k celkové koncepci dokumentu se otázkou využití internetu k teroristickým účelům příliš nezabývá ovšem ji zcela neopomíjí. Zmíněna je vzrůstající úloha efektivních opatření v oblasti

[125] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti.

[126] Krátký, P.: *Zákon o kybernetické bezpečnosti v praxi*. Časopis IT Systems 9/2014 [online]. 2015 [cit. 2015-03-10]. Dostupné z: http://www.systemonline.cz/it-security/zakon-o-kyberneticke-bezpecnosti-v praxi.

kybernetické bezpečnosti a poukazuje se zde i na vzrůstající reálnost rizika teroristických kybernetických útoků. Další rovinou, při které může být internet využit pro potřeby teroristů, je radikalizace (například džihádistická diskuzní fóra a sociální sítě).[127]

[127] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Strategie České republiky pro boj proti terorismu: od r. 2013*. Praha, 2013.

Naplnění cílů bakalářské práce

Bakalářská práce naplnila cíle zadání tak jak byly na počátku specifikovány. Byly podrobně popsány a analyzovány otázky spojené s úlohou a aplikací kryptografických prostředků v informačních systémech a to v rozsahu jejich historického vývoje až po současnost. Byly vysvětleny základní problémy informační bezpečnosti z pohledu jejich zřizovatelů i uživatelů. Rovněž byly přístupnou formou vysvětleny základní otázky aplikace kryptografických prostředků a specifikována úskalí jejich využívání.

Závěr

Vždy existuje eminentní zájem udržet informatické toky v bezpečí. Informace jsou cílem útoků stále ve větší míře v souběhu s rostoucí závislosti společnosti na jejich přenosu a úschově. To se odráží v strategických úvahách všech moderních států, boj o nově vzniklý informatický prostor (kyberprostor) se stává dominantním. Útoky na informační systémy jsou vnímány jako obzvláště nebezpečné a státy jsou nuceny vytvářet nové instituce pro boj s informačním terorizmem. Kryptografie nachází velice široké uplatnění v celém systému ochrany dat a informací. Šifrování, jakožto součást systému bezpečné komunikace, je velmi účinné, avšak síla bezpečnosti celého systému závisí na síle bezpečnosti jeho nejslabšího prvku. Tím může být zejména špatná správa kryptografických klíčů. Moderní kryptografie se již nezabývá pouze "skrýváním obsahu zpráv", ale slouží i k zajištění autentizace, integrity dat a nepopiratelnosti autorství. Proto je základním kamenem současných elektronických podpisů. Bezpečnost uložených dat lze zvyšovat různými způsoby, nikdy však není možné zcela zamezit riziku jejich úniku a zneužití. Pro velmi citlivá data lze tedy použít šifrovacích technik, které významným způsobem sníží nebo odstraní riziko prozrazení důvěrných informací i při získání těchto důvěrných dat během jejich přenosu či při uložení. V praxi bylo mezinárodně doporučeno několik standardních "modelů" algoritmů pro šifrovou ochranu informací. Pochopitelně, že s růstem výpočetní mohutnosti na straně útočníka v tabulce uváděná odolnost proti luštění přestává platit a je nezbytné přecházet k užití stále delších kryptografických klíčů. Uvedený trend jen potvrzuje geniální platnost Shannonova teorému o perfektním šifrování. Řešení problému informační bezpečnosti je bez použití kryptografie prakticky nemyslitelné.

Seznam použitých zdrojů

Literární zdroje

1. DOBDA, L. Ochrana dat v informačních systémech. Vyd. 1. Praha : Grada Publishing, 1998. 286 s. ISBN 80-7169-479-7.
2. FEREBAUEROVÁ, R. - PEKÁREK, O. Aplikovaná informatika. České Budějovice : Vysoká škola evropských a regionálních studií, 2014. 151 s. Studijní text. ISBN 978-80-87472-74-3.
3. PIPER, F. C. - MURPHY, Sean. Kryptografie. 1. vyd. v českém jazyce. Praha : Dokořán, 2006. 157 s. Průvodce pro každého ; světové3. ISBN 80-7363-074-5.
4. PEKÁREK O., ČÍŽEK VL., Práce s agenturními a elektronickými informacemi, studijní text, VŠERS, ISBN 978-80-86708-40-9.
5. POŽÁR, J. Základy teorie informační bezpečnosti. Vyd. 1. Praha : Vydavatelství PA ČR, 2007. 219 s. ISBN 978-80-7251-250-8.
6. PŘIBYL, J. Ochrana dat v informatice. Vyd. 1. Praha : Vydavatelství ČVUT, 1996. 299 s. ISBN 80-01-01664-1.
7. PŘIBYL, J. Informační bezpečnost a utajování zpráv. Vyd. 1. Praha : Vydavatelství ČVUT, 2004. 239 s. ISBN 80-01-02863-1.
8. SINGH, S. Kniha kódů a šifer : tajná komunikace od starého Egypta po kvantovou kryptografii. 1. vyd. v českém jazyce. Praha : Dokořán : Argo, 2003. 382 s. Aliter ; sv. 9. ISBN 80-86569-18-7.
9. VONDRUŠKA, P. Kryptologie, šifrování a tajná písma. 1. vyd. Praha : Albatros, 2006. 340 s. Oko. ISBN 80-00-01888-8.
10. ZELENKA, J. Ochrana dat : kryptologie. 1. vyd. Hradec Králové : Gaudeamus, 2003. 198 s. ISBN 80-7041-737-4.

Elektronické zdroje

1. WOODWARD, A. *Is It Quantum Computing or Not?*. Yahoo news. [online]. 17.5.2013 [cit. 2014-12-02]. Dostupné z: http://news.yahoo.com/quantum-computing-not-140100223.html
2. KRÁTKÝ, P. *Zákon o kybernetické bezpečnosti v praxi*. Časopis IT Systems 9/2014 [online]. 2014 [cit. 2015-03-10]. Dostupné z: http://www.systemonline.cz/it-security/zakon-o-kyberneticke-bezpecnosti-v praxi.htm

3. *Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb.* [online]. Praha : Ministerstvo vnitra České republiky, [cit. 2015-02-07]. Dostupné z WWW:< http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb-320051.aspx>

Legislativní dokumenty

1. ČESKO. Zákon č. 101/2000 Sb. o ochraně osobních údajů. Dostupný z WWW: < http://www.cz-museums.cz/UserFiles/File/Legislativa/zakon-101-2000.pdf>

2. ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Dostupný z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231>

3. ČESKO. Zákon č. 365/2000 Sb. o informačních systémech veřejné správy. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00365&cd=76&typ=r>

4. ČESKO. Zákon č. 412/2005 Sb. ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti. Dostupný z WWW: < http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/>

5. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Strategie České republiky pro boj proti terorismu: od r. 2013. Praha, 2013, 30 s. Dostupný z WWW: < http://www.mvcr.cz/soubor/3-nap-2013-material-pdf.aspx>

6. Vyhláška NBÚ č. 524/2005, o zajištění kryptografické ochrany utajovaných informací. Dostupný z WWW: <http://www.nbu.cz/download/nodeid-4095/.>

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- PINKAVA, J. *Úvod do kryptologie*. Dokument společnosti AEC, s.r.o., 1998. Dostupný z WWW: <http://crypto-world.info/pinkava/konference/security00.pdf>

Seznam zkratek

AES (Advanced Encryption Standard) - symetrická šifra, standardizovaný algoritmus blokové šifry, v současnosti používaný k šifrování dat v informačních systémech

CT (clear text) - otevřený text

DES (Data Encryption Standard) - symetrická šifra, předchůdce AES, na stejném principu

ET (encrypted text) - otevřený text po zašifrování

HASH - matematická funkce

HW (Hardware) - přístrojové vybavení

IDEA (International Data Encryption Algorithm) - Mezinárodní algoritmus pro šifrování dat

IS - informační systém

NSA (National Security Agency) - národní bezpečnostní agentura USA

PC (Personal Computer) - osobní počítač

PGP (Pretty Good Privacy) - šifrovací program

SW (Software) - programové vybavení

RSA ((iniciály autorů Rivest, Shamir, Adleman) - šifra s veřejným klíčem

FIPS (Federal Information Processing Standards)

PKI (Public Key Infrastructure) - šifrování s veřejnými klíči

ROUTER - směrovač v paketové síti

WIFI - bezdrátové připojení k počítačové síti

Seznam obrázků

Seznam tabulek

Přílohy

CD ROM