Súčasné technologické možnosti kryptografickej ochrany

The Current Technological Possibilities of Cryptographic Protection

Bc. Ľubica Ondrejková

Diplomová práca
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ľubica ONDREJKOVÁ**
Osobní číslo:	**A11326**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Současné technologické možnosti kryptografické ochrany**

Zásady pro vypracování:

1. **Zpracujte prováděcí manuál k orientaci managerů bezpečnostní komunity z pohledu kryptografické ochrany utajovaných informací a know-how.**
2. **Zanalyzujte současný stav z pohledu legislativy.**
3. **Popište možnosti ochrany z technického hlediska.**
4. **Uveďte postup firem PKB při provádění kryptografického zabezpečení dohledových přijímacích a poplachových center.**
5. **Uveďte problémy při realizaci tohoto druhu ochrany v PKB.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 223 s. ISBN 978-80-7318-762-0.**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.**
3. **Česká republika. Zákon č. 412/2005 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: Sbírka zákonů České republiky. 2005.**
4. **JANEČEK, Jiří. Válka šifer: výhry a prohry československé vojenské rozvědky, 1939-1945. Olomouc: Votobia, 2001, 345 p. ISBN 80-719-8505-8.**
5. **VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. 1. vyd. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-000-1888-8.**
6. **PIPER, F a Sean MURPHY. Kryptografie. 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.**
7. **Česká republika. Vyhláška č. 525/2005 ze dne 14. prosince 2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb. In: Sbírka zákonů České republiky. 2005.**
8. **JAŠEK, Roman. Informační a datová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-731-8456-7.**

Vedoucí diplomové práce: **JUDr. Vladimír Lauckÿ**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cieľom práce je poskytnúť čitateľovi informácie o súčasných možnostiach ochrany informácií a dát prostredníctvom prostriedkov kryptografickej ochrany. Práca sa skladá z teoretickej a praktickej časti. Teoretická časť pozostáva z piatich kapitol, v ktorých je najskôr venovaná pozornosť vysvetleniu základných pojmov týkajúcich sa kryptografie a následne je stručne popísaný pohľad do histórie kryptografie. Neskôr je pozornosť v práci upriamená na poznatky o moderných princípoch šifrovania, legislatíve ČR týkajúcej sa kryptografie, možnostiach ochrany utajovaných informácií a napokon o zabezpečení dohľadových a poplachových prijímacích centier. Praktická časť poukazuje na problémy spojené s týmto druhom ochrany a porovnáva legislatívu v ČR a SR.

Kľúčové slová: kryptografia, kryptoanalýza, šifrovanie, dešifrovanie, algoritmus, utajované informácie.

ABSTRACT

A goal of the work is to provide the reader with information about the current possibilities of information and data protection by the facilities of cryptographic protection. The work consists of theoretical and practical part. The theoretical part consist of five chapters, in which at first attention is paid to explanation of the basic concepts related to cryptography and then a view into the history of cryptography is described briefly. Later, in the work attention is drawn to the knowledge of modern principles of encryption, the Czech legislation concerning cryptography, the possibilities for the protection of classified information and at last the security alarm receiving centers. The practical part indicates the problems associated with this type of protection and compares the legislation in the Czech and Slovak Republic.

Keywords: cryptography, cryptanalysis, encryption, decryption, algorithm, classified information.

POĎAKOVANIE

Touto cestou by som sa chcela poďakovať vedúcemu mojej diplomovej práce pánovi JUDr. Vladimírovi Lauckému za jeho ochotu a čas, ktorý mi pri konzultáciách mojej práce vždy venoval a za všetky jeho cenné rady, postrehy a pripomienky, ktorými usmerňoval moje kroky pri písaní mojej diplomovej práce.

MOTTO

„Šifrovanie je často jedinou možnosťou, ako chrániť cenné dáta.” (RNDr. Vlastimil Klíma)

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Každý človek od nepamäti ukrýval v sebe nejaké tajomstvá. Tieto tajomstvá si strážil ako oko v hlave a nechcel, aby boli za žiadnu cenu vyzradené. Mnohokrát však pociťoval potrebu zachovať obsah týchto tajomstiev pre ďalšie pokolenia, a tak začal svoje pocity a príbehy kresliť na steny jaskýň. V podstate už tento úkon možno považovať za predchodcu kryptografie. Postupne kryptografia začala nadobúdať strategický a vojenský charakter, lebo ju využívali hlavne vládcovia krajín a králi k vládnutiu nad svojím územím a k veleniu armády. Nakoľko si uvedomovali následok, aký by nieslo vyzradenie závažných a strategických informácií, rôznymi spôsobmi utajovali svoje správy, aby sa nedostali do rúk nepovolaných osôb a nepriateľov.

Na druhej strane vždy tu bola snaha nepriateľov vylúštiť danú šifru, ktorá sa im dostala do rúk. V tomto prípade sa do popredia dostávajú tzv. kryptoanalytici, teda lúštitelia šifier. Kryptoanalitici svojou snahou lúštiť šifry prispeli k tomu, že sa kryptografia ďalej vyvíjala a to takým spôsobom, že kryptografi museli vymýšľať neustále nové a ťažšie rozlúštiteľné metódy šifrovania. Tento nekončiaci sa boj šifrérov a lúštiteľov šifier pretrváva dodnes.

Napriek bohatej histórii kryptografie je aj dnes jej využitie veľmi významné a dôležité. Súčasnú dobu totiž možno charakterizovať ako dobu informácií a komunikačných technológií, v ktorej sa informácie stávajú určitým druhom tovaru a predmetom obchodovania. V súčasnosti sa informácie prenášajú prostredníctvom rôznych technických komunikačných prostriedkov, ktoré ale nie sú úplne bezpečné. Z toho dôvodu vzniká možnosť získavať a uchovávať častokrát veľmi významné informácie a znalosti. Mnohé z týchto informácií by však mali zostať utajené a byť sprístupnené iba určitému vymedzenému okruhu ľudí. Činnosti spojené s utajovaním informácií sú vykonávané nielen na základe osobných a skupinových záujmov, ale čoraz častejšie aj zo záujmov bezpečnosti ľudstva a štátu, ale nemožno opomenúť ani ochranu firemných informácií.

Šifrovanie má teda širokú škálu využitia. Vhodným príkladom je prenos dát cez internet, ktorý je nutné šifrovať kvôli možnosti odpočúvania. Kryptografia nachádza uplatnenie aj pri šifrovaní hlasovej a dátovej komunikácie prebiehajúcej pomocou mobilných telefónov, pri zabezpečovaní hesiel užívateľov počítačových systémov ukladaných v šifrovanej podobe, pri zaistení elektronickej podoby vlastnoručného podpisu šifrovaním a pri mnohých ďalších významných úkonoch.

I. TEORETICKÁ ČASŤ

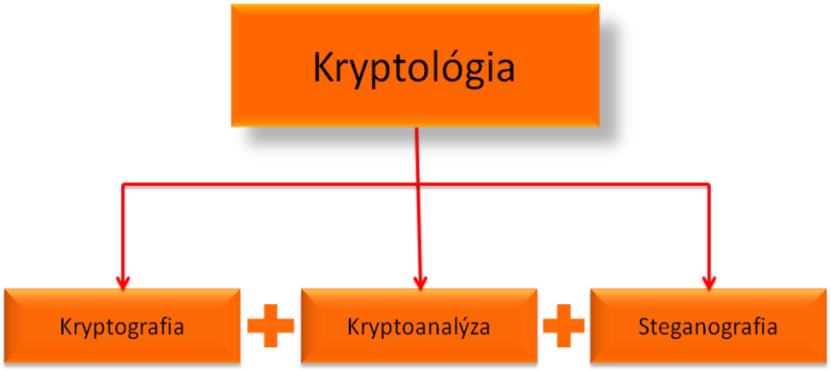
1 ÚVOD DO KRYPTOGRAFIE

Kryptografia je veda, ktorej hlavným cieľom je zašifrovať správu do takej podoby, aby bola nečitateľná a nezrozumiteľná pre všetky osoby, ktorým daná správa nie je adresovaná. Najčastejšie využitie kryptografie nastáva vo chvíli, keď užívateľ potrebuje svoje dáta bezpečne uložiť do počítačového systému alebo ak ich posiela napr. cez internet, ktorý predstavuje nezabezpečený kanál komunikácie. [1]

1.1 Základná terminológia

S pojmom kryptografia sa viaže mnoho ďalších základných termínov a poučiek. Kryptografia spadá pod vedu, ktorá sa taktiež týka šifrovania a nesie názov kryptológia.

Význam pojmu kryptológia pochádza zo spojenia gréckych slov kryptos a logos, kde kryptos v preklade znamená ukrytý a logos znamená slovo. Z uvedeného logicky vyplýva, že sa jedná o vedu zaoberajúcu sa utajením obsahu správ. Kryptológiu tvorí spojenie ďalších vied, medzi ktoré patrí už čiastočne spomínaná kryptografia, ďalej ju tvorí kryptoanalýza a niekedy sa pridáva ešte aj steganografia.



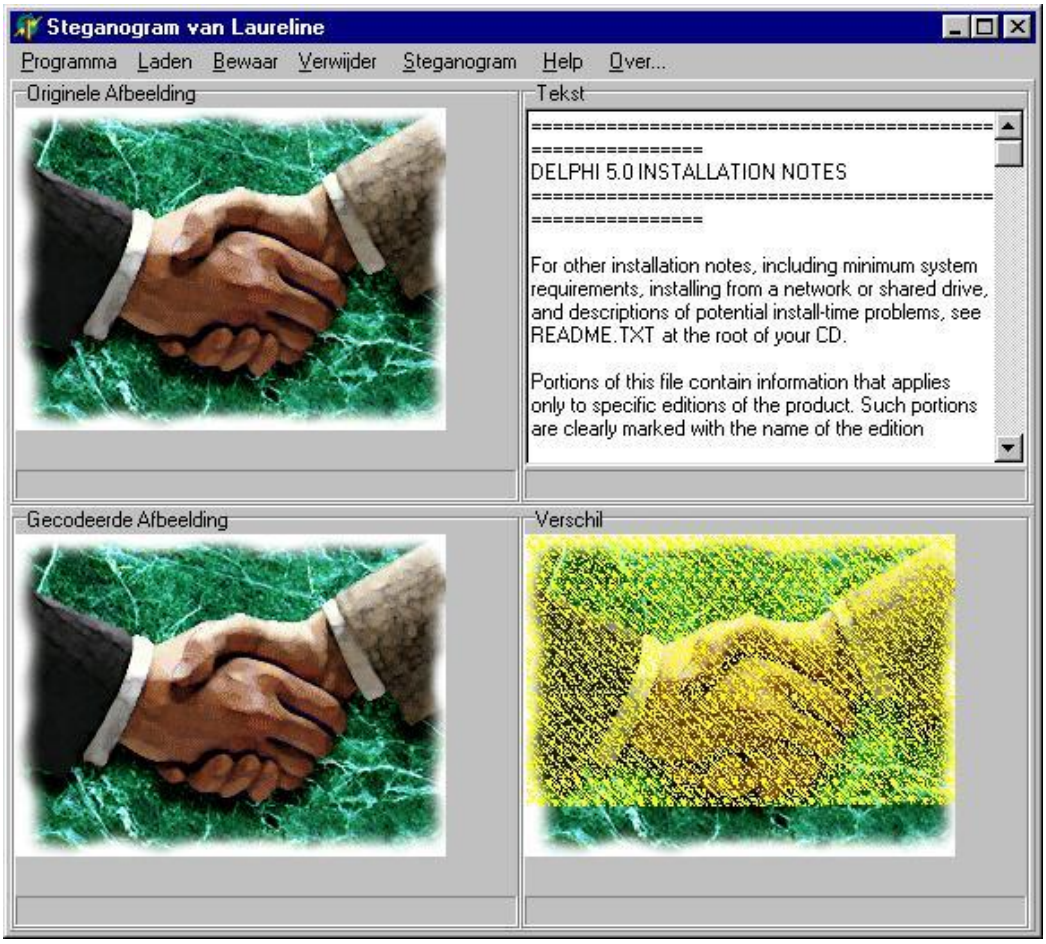
Obr. 1. Rozdelenie kryptografie [autor]

Kryptografia sa z pohľadu informačnej bezpečnosti venuje zaisteniu dôvernosti správy, neporušenosti dát, autentizácii entít (čiže overeniu subjektu) a pôvodu dát, resp. ich vlastníctvu. K zaisteniu spomínaných činností využíva rôzne matematické metódy. Okrem toho musí sledovať silné a slabé stránky týchto činností a musí zisťovať odolnosť pred rôznymi nepriaznivými útokmi. V minulosti bolo prvoradou úlohou kryptografie návrh a používanie šifrovacích systémov tak, aby prenášali informácie do nečitateľnej podoby. Z uvedeného vyplýva, že ak sa nešťastnou náhodou informácie dostali do rúk nepovolanej osoby, tá nedokázala rozlúštiť ich obsah a správu prečítať.

Kryptoanalýza sa zaoberá lúštením zašifrovanej informácie do pôvodnej podoby. V kryptoanalýze ide teda o snahu získať pôvodnú správu zo správy zašifrovanej. Širší význam kryptoanalýzy spočíva v zisťovaní miery odolnosti šifrovacích systémov a v snahe nájsť všetky možné cesty a riešenia k prelomeniu týchto systémov.

Poslednou vedou, ktorá dopĺňa význam pojmu kryptológia, je steganografia. Jedná sa o ukrytie samotnej správy do podoby, v ktorej nie je možné poznať, že je správa prenášaná. V tom je hlavný rozdiel medzi kryptografiou a steganografiou. V kryptografii sa snažíme správu preniesť v zašifrovanej podobe tak, aby nebolo možné rozlúštiť a prečítať obsah správy nepovolanou osobou, zatiaľ čo v steganografii sa správa prenáša v nezašifrovanej podobe, ale takým spôsobom, aby nepovolaná osoba nespoznala, že sa vôbec nejaká správa prenáša. V mnohých literatúrach sa steganografia ako súčasť triedenia kryptológie neuvádza. Pri ukrývaní správ pomocou steganografie sa používali rôzne nástroje ako napr. neviditeľný atrament, či mikrobodky a iné. Dnes sa v steganografii využíva napr. ukrytie správ do podoby obrázkov prostredníctvom rôznych zložitých matematických aparátov. [2]

Obr. 2. Neviditeľný atrament [3]



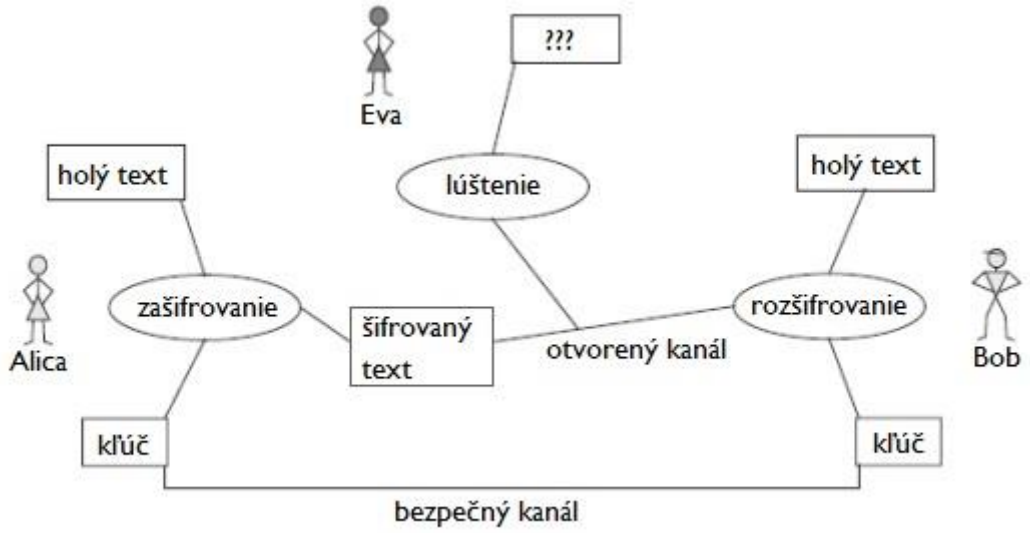
Obr. 3. Ukážka ukrytia správy do obrázka [4]

V kryptografii je ešte potrebné rozoznávať rozdiel medzi kódovaním, šifrovaním a kódom. V kódovaní sa nejedná o utajenie správy ako je tomu v šifrovaní, kde sa odosielateľ a príjemca snažia danú správu utajiť pred nepovolanou treťou stranou, ale ide o úpravu správy prostredníctvom všeobecne známych pravidiel, vďaka ktorým sa zmení tvar správy. Kódovanú správu je možné ďalej spracovávať prostredníctvom vhodného technického prostriedku, napr. ju môžeme preniesť pomocou komunikačného kanála. Vhodným príkladom kódovania je Morseova abeceda, kde je pôvodný text správy nahradený bodkami, čiarkami a medzerami a ktorá v minulosti slúžila k odosielaniu správy s využitím telegramu. Ten, kto pozná všeobecne známe pravidlá Morseovej abecedy, dokáže prijatú správu bez problémov previesť do pôvodnej podoby. Kód sa vyznačuje ako „tajný jazyk", v ktorom sú jednotlivé slová zamieňané za iné slová, prípadne znaky alebo čísla. Kód môže byť všeobecne známy, napr. rádiový Q-kód, alebo môže byť význam kódu utajený prostredníctvom kódovej knihy.

Dešifrovanie a lúštenie sú naoko dva rovnaké pojmy, ale nie je tomu celkom tak. Dešifrovanie je proces, pri ktorom sa šifrovaná správa prevádza na pôvodnú správu prostredníctvom dohodnutej kryptografickej metódy. Dešifrovanie spravidla prevádza príjemca správy, ktorému bola správa adresovaná. Zatiaľ čo pri lúštení správy sa snaží neoprávnená osoba, ktorej správa nebola adresovaná, získať zo zašifrovanej správy správu pôvodnú a to bez znalosti dohodnutej kryptografickej metódy.

Ďalšiu terminológiu týkajúcu sa kryptografie si rozoberieme na ukážkovom princípe šifrovania. [2], [5]

1.2 Princíp šifrovania



Obr. 4. Model princípu šifrovania [5]

Na obrázku (Obr. 4) môžeme vidieť príznačný model klasického šifrovania. V modeli sa nachádzajú traja účastníci komunikácie, z toho dvaja účastníci, v tomto prípade sú nazývaní Alica a Bob, chcú medzi sebou súkromne komunikovať. Alica predstavuje odosielateľa správy a Bob predstavuje príjemcu správy. Nezvaným účastníkom komunikácie je Eva, ktorá má snahu odpočúvať komunikáciu prebiehajúcu medzi Alicou a Bobom.

Pôvodný obsah správy, ktorý chce Alica poslať Bobovi, nazývame holý text, niekedy sa uvádza aj pojem otvorený text. Holý text Alica zašifruje prostredníctvom tajného kľúča (hesla) a tým vznikne šifrovaný text. Šifrovaný text je správa, ktorá putuje otvoreným kanálom a ktorú vidí Eva. Eva sa snaží šifrovaný text rozlúštiť, ale nevlastní tajný kľúč,

ktorý k rozlúšteniu potrebuje. Bob, ktorému je správa adresovaná, však tento tajný kľúč vlastní, a tak sa mu bez problémov podarí rozšifrovať (dešifrovať) šifrovaný text na pôvodnú správu, teda na text holý. Tajný kľúč, ktorý vlastní Alica i Bob, si títo dvaja účastníci vymenili napr. pri nedávnom stretnutí v minulosti, kde stretnutie môžeme považovať za druh bezpečnostného kanála.

Činnosť, ktorú vykonávajú Alica s Bobom, predstavuje kryptografiu, zatiaľ čo Eva zastáva funkciu kryptoanalýzy. [5]

1.3 Základné rozdelenie klasických kryptografických systémov

V kryptografii rozlišujeme tri základné druhy kryptografických systémov. Jedná sa o substitúciu, transpozíciu a kódovú knihu.

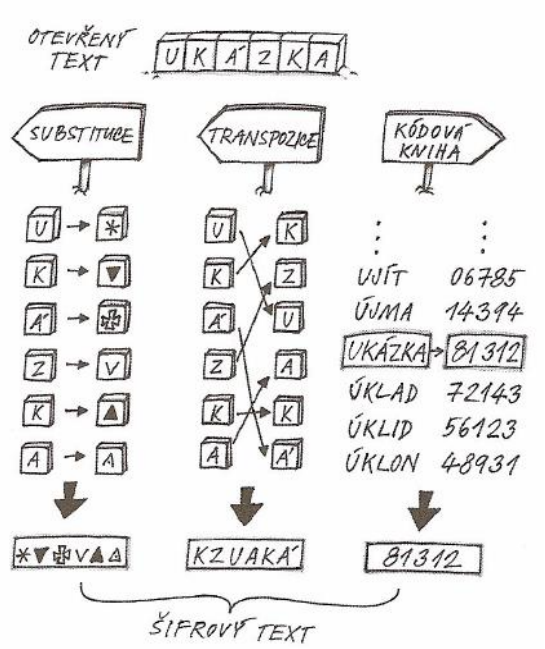
Šifrovanie substitúciou je založené na zámene písmen v abecede otvoreného textu za znaky šifrovej abecedy. Takémuto spôsobu šifrovania sa vraví nielen substitúcia, ale niekedy sa vyskytuje aj pod pojmom zámena. Šifrám utvoreným pomocou zámeny sa hovorí substitučné šifry. Pri šifrovaní otvoreného textu rozlišujeme dva spôsoby použitia substitúcie, prvý spôsob spočíva v použití jednej šifrovacej abecedy pre celý text a druhý spôsob tkvie v použití inej šifrovej abecedy pre každé písmeno zvlášť. Najjednoduchším príkladom použitia substitúcie je Caesarova šifra.

Zamenenie postupnosti písmen v texte sa nazýva transpozícia. Jedná sa o prehadzovanie písmen v texte podľa presne stanovených pravidiel a ten, kto tieto pravidlá ovláda, dokáže spätne text dešifrovať. Takýmto šifrám sa vo všeobecnosti hovorí transpozičné šifry. Prostým príkladom jednoduchej transpozície sú tzv. prešmyčky, ktoré sa často nachádzajú v novinách, alebo ďalší jednoduchý príklad je napísanie celého textu odzadu.

Šifrovanie môže prebiehať aj za použitia kódovej knihy. Kódová kniha je vlastne druh slovníka a podľa odvetvia, v ktorom sa kódová kniha používa, sú v nej najpoužívanejšie termíny otvoreného textu nahradené skupiny kódov. Obyčajne sa jedná o skupiny štyroch alebo piatich čísel, písmen, prípadne znakov. Lúštiteľ tak mohol danú šifru rozlúštiť iba za použitia konkrétnej kódovej knihy, pomocou ktorej bol text zašifrovaný.

Použitie týchto troch základných systémov šifrovania je možné rôzne kombinovať a aplikovať viackrát za sebou. Kombinácie a rôzne úpravy týchto troch spôsobov vytvárajú všetky známe typy klasických šifrovacích systémov vysvetlených v ďalších kapitolách.

Navyše tieto metódy tvoria základ aj moderných kryptografických algoritmov, ktoré sa od seba odlišujú použitím rôznych šifrovacích abecied a náročnosťou kryptografických metód. [2]



Obr. 5. Ukážka základných šifrovacích systémov [2]

1.4 Typy šifrovania v informačných systémoch

Šifrovanie je veľmi dobrým pomocníkom pre prácu v informačných systémoch, konkrétne pri spracovávaní a následnej ochrane rôznych dát. Podľa povahy ochrany dát rozoznávame tri druhy šifrovania a to on-line šifrovanie, off-line šifrovanie a on-demand šifrovanie.

Pri on-line šifrovaní sa šifruje a dešifruje priebežne, teda v reálnom čase. K dátam je pripustená iba osoba, ktorá má oprávnenie pre prístup k týmto dátam. Oprávnenie pre prístup k dátam sa overuje pomocou zadania autentizačných údajov konkrétnou osobou. Preverenie zadaných autentizačných údajov sa vykoná prostredníctvom príslušného bezpečnostného softvéru. Dáta sa počas práce s nimi postupne ukladajú na disk v šifrovanej podobe a pri následnom načítaní do pamäte RAM sa priebežne dešifrujú, vďaka tomu môže užívateľ s dátami pracovať v nezašifrovanej, teda pôvodnej podobe. Existuje mnoho softvérov, ktoré umožňujú priebežné šifrovanie a dešifrovanie dát po zadaní autentizačných údajov. On-line šifrovanie sa v niektorých zdrojoch uvádza aj ako „on-access“ alebo „on the fly“.

Princíp off-line šifrovania spočíva v tom, že pri autentizácii užívateľa do systému pomocou príslušného programu a vložením kľúča, užívateľ získa prístup k dátam a v tej chvíli sa dáta kompletne rozšifrujú, k následnému zašifrovaniu dát dochádza až pri uložení dát a odhlásení užívateľa. Z uvedeného vyplýva rozdiel medzi on-line a off-line šifrovaním. Zatiaľ čo pri on-line šifrovaní sú dáta šifrované počas procesu ukladania dát a dešifrované počas procesu načítania dát - čiže priebežne, pri off-line šifrovaní sa dáta dešifrujú pri prihlásení užívateľa a zašifrujú sa až po jeho odhlásení - čiže jednorázovo. Off-line šifrovanie sa vyznačuje vyššou rýchlosťou a je vhodné najmä pre zabezpečenie menšieho rozsahu dát.

Zabezpečenie dát prostredníctvom kryptografie je možné aj v prípade požiadavky na zašifrovanie, takúto možnosť zabezpečenia dát ponúka tzv. on-demand šifrovanie. Požiadavka na zašifrovanie sa môže objaviť napr. pri kliku na pravé tlačidlo myši za predpokladu nainštalovaného šifrovacieho programu. Pri nainštalovaní náležitého softvéru je voľba požiadavky na zašifrovanie dostupná v ponuke miestneho menu operačného systému. Pri zabezpečení dát pomocou on-demand šifrovania existujú aj také kryptografické programy, ktoré umožňujú šifrovanie do tzv. samorozbaľovacích (Self-Extract) EXE súborov. Prvý krok pri šifrovaní do EXE súborov spočíva vo vytvorení kľúča pre zašifrovanie zvolených súborov. Kľúč je vytvorený užívateľom v podobe dlhšieho hesla, resp. frázy. Ďalší krok spočíva v zašifrovaní všetkých zvolených súborov do jedného spustiteľného EXE súboru. Pri prístupe do tohto súboru užívateľ zadá ním vybranú vstupnú frázu, ktorá predstavuje kľúč a súbory sa dešifrujú. Hlavnou výhodou týchto programov je, že užívateľ môže posielať zašifrované súbory aj takým osobám, ktoré nevlastnia potrebný šifrovací program. Stačí, ak im len prostredníctvom nejakého komunikačného kanála predá potrebnú vstupnú frázu. Nevýhoda spočíva v jednoduchom napadnutí EXE súboru vírusom. [6]

1.5 Prehľad histórie kryptografie

Keďže šifrovanie sa datuje už od dávneho staroveku, nemožno v práci opomenúť niektoré dôležité a zaujímavé míľniky týkajúce sa histórie kryptografie a to aj z dôvodu lepšieho pochopenia významnosti a účelu použitia kryptografie v minulosti.

Tab. 1. Prehľad dôležitých termínov v histórii kryptografie [5]

500 p. n. l.	Židia: jednoduchá substitučná šifra (ATBASH/ATBAŠ)
400 p. n. l.	Grécko: jednoduché transpozičné šifry, steganografia
50 p. n. l.	Rím: Caesarova šifra
4. stor.	India: šifrovanie medzi 64 umeniami v Kamasutre
10. stor.	Arabi: základy kryptoanalýzy, vrátane frekvenčnej analýzy
13., 14. stor.	Európa: používa sa substitučná šifra, prípadne ľahké nadstavby
1412	Arabi: encyklopédia obsahujúca kapitolu o kryptografii
15., 16. stor.	prvé návrhy šifrovania pomocou hesla
16. stor.	Európa: kryptológia hrá dôležitú úlohu v politike
1586	Anglicko: poprava škótskej kráľovnej na základe rozlúštenej šifry
1843	USA: Poe píše o šifrách a zverejní šifrovacie výzvy
1861	Prusko: metóda pre riešenie polyalfabetickej šifry (Kasiski)
1885	USA: Bealov poklad
19. stor.	rozvoj telegrafu, rozvoj kryptografie pre komerčné účely
	Poľné šifry (napr. Playfair)
	prvé mechanické prístroje pre šifrovanie
1. svetová vojna	dôležitá úloha vo vojne aj v politike (Zimmermannov telegram)
	použitie komplikovanejších šifier na klasických princípoch
1926	Nemecko: armáda začína používať šifrovací prístroj Enigma
2. svetová vojna	kľúčová úloha kryptológie vo vojne
	použitie mechanických šifrovacích strojov
1949	publikované práce C. Shannona o teórii informácie
50. roky 20. stor.	Rozvoj počítačov, prvé využitie počítačov pre šifrovanie/ lúštenie
1967	USA: kniha D. Kahna „The Codebreakers“
1973	Anglicko: objavený princíp šifrovania s verejným kľúčom, kvôli utajeniu však nebol zverejnený
1976	USA: publikovaný článok „New Directions in Cryptography“

	začiatok rozvoja akademickej kryptológie
1978	USA: zverejnené RSA, algoritmus realizujúci kryptografiu s verejným kľúčom
1991	USA: zverejnené PGP, implementácia kryptografie s verejným kľúčom
90. roky 20. stor.	rozvoj kvantovej kryptografie

1.5.1 Kryptografia v období staroveku

O tom, že šifrovanie spadá už do čias dávnej minulosti, svedčí fakt, že maľby na stenách jaskýň je možné považovať za určitý druh šifier. Svojím spôsobom sa aj v textoch pochádzajúcich spred 3000 rokov nachádzajú šifrované časti. Jedná sa o texty hebrejské, mezopotámske či egyptské. V súvislosti s týmto obdobím treba pripomenúť, že nie každý človek vedel písať, schopnosťou písať sa vyznačovali len vzdelaní ľudia, ktorých bezpochyby nebolo mnoho. [5]

Šifrovanie v starovekom Egypte spočívalo v nezvyčajnej úprave písma a v pridávaní znakov do textu, ktoré boli známe iba vyvolenej skupine ľudí. Obdobne tomu bolo aj v Mezopotámii a v Sumere, ktoré sa vyznačovali používaním klinového písma a neskôr sa tu začali objavovať systémy v podobe upravených pečatných valčekov pre overovanie pravosti správ. [7]

Mnohí odborníci považujú za začiatok dejín kryptografie hieroglyfický text z roku 1900 p. n. l, v ktorom je použitá zámerná transformácia textu. Jedná sa o hieroglyfy vyryté neznámym majstrom do kameňa v hrobke, kde bol uložený jeho pán. Vyrytý text sa vyznačoval zvláštnosťou a síce takou, že v ňom boli nahradené bežné hieroglyfy hieroglyfmi nevšednými a išlo skôr o text opisný. Rytec týmto počinom nesledoval cieľ zašifrovať text do nečitateľnej podoby, ale unikátnosťou písma vyrytého na kameni chcel upútať pozornosť čitateľa a poukázať na život svojho pána.

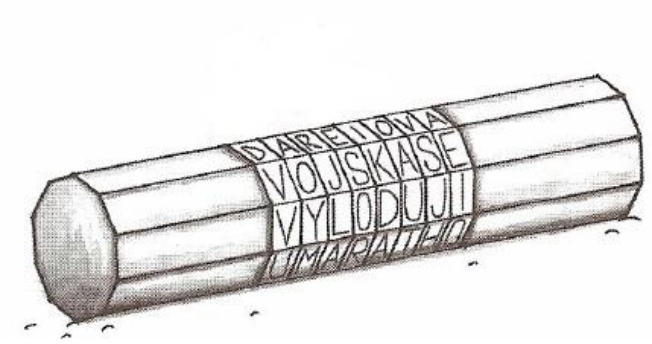
Ďalší pozoruhodný zlom v starovekých dejinách kryptografie nastal približne o 400 rokov neskôr, keď bol v Mezopotámii vyrytý návod na výrobu glazovanej keramiky v podobe zašifrovaného textu do tabuľky. Šifrovaný text spočíval v zámene klinopisných písmen za

iné klinopisné písmená, ktoré však majú totožnú zvukovú podobu. Tento šifrovaný systém nebol príliš bezpečný, a preto sa v priebehu tohto obdobia prestal používať. [2]

Taktiež v Biblii, konkrétne v knihe Starého zákona, sa objavuje šifra zvaná ATBASH (v niektorých zdrojoch literatúry je uvádzaná pod názvom ATBAŠ). V šifre ATBASH sa nahrádzajú písmená zo začiatku abecedy s písmenami idúcimi od konca abecedy, písmeno „A“ sa nahradí za písmeno „Z“, písmeno „B“ za písmeno „Y“ atď. Hlavnou úlohou tejto šifry nebolo učiniť obsah správy nečitateľným, ale skôr v nej šlo o snahu urobiť text zaujímavým.

Obr. 6. ATBASH šifra [8]

Neskôr sa v období staroveku začali ľudia zaujímať o šifry najmä z hľadiska ich strategického charakteru. Jednalo sa hlavne o vojenské a vládne stratégie, ktoré využívali predovšetkým Gréci a Rimania v podobe jednoduchých substitúcií a transpozícií. V 5. stor. p. n. l. Sparťania vynašli prvé známe mechanické zariadenie určené na šifrovanie správ. Zariadenie zvané Skytale pozostáva z dvoch rovnako širokých tyčí, kde jednu tyč vlastnil odosielateľ správy a druhú tyč vlastnil príjemca správy. Odosielateľ namotal na tyč pás papyrusu, látky alebo pergamenu a napísal správu smerom nadol pozdĺž tyče. Po napísaní správy pás s textom odmotal a poslal príjemcovi správy. Príjemca už iba namotal pás so zašifrovaným textom na svoju druhú tyč, totožnú s tyčou odosielateľovou, a správu bez problémov dešifroval. Tento kryptografický systém pracoval na princípe transpozície.



Obr. 7. Skytale [2]

Dôležitým krokom vpred v histórii kryptografie bol kódový systém vynájdený gréckym spisovateľom Polybiom. Polybius zoradil písmená abecedy do štvorca, v ktorom očísloval rady a stĺpce. Každé písmeno tak bolo charakterizované párom čísel. Prvé číslo predstavovalo číslo rady a druhé číslo reprezentovalo číslom stĺpca. Šifra sa z tohto kódového systému stala až vo chvíli, keď sa do štvorca pridalo kódové slovo a následne sa pokračovalo vo vypisovaní ostatných písmen abecedy. Keďže písmen v medzinárodnej abecede je 26 a štvorec je o veľkosti 5x5 riadkov a stĺpcov, bolo potrebné do jednej kolónky vpísať 2 najmenej používané čísla v abecede. V anglickej abecede sa zlučujú písmená I a J a v českej, prípadne slovenskej abecede, je zlučiteľné X s Y.

Tab. 2. Príklad Polybiovho štvorca s heslom SIFRA [2]

	1	2	3	4	5
1	S	I	F	R	A
2	B	C	D	E	G
3	H	J	K	L	M
4	N	O	P	Q	T
5	U	V	W	X/Y	Z

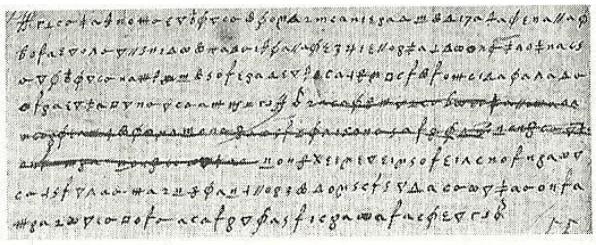
Na prelome datovania rokov pred našim letopočtom na roky nášho letopočtu sa dostáva do popredia Caesarova šifra. Vymyslel ju rímsky cisár Július Caesar pre komunikáciu medzi veliteľmi vojenskej výpravy. Používanie Caesarovej šifry spočívalo v nahradení písmena

správy za písmeno ležiace o tri miesta ďalej v abecede, teda písmeno „A“ sa nahrádza za písmeno „D“ atď. [2]

1.5.2 Stredoveká kryptografia a obdobie raného novoveku

V 5. až 15. storočí nezaznamenala kryptografia žiadny náhly pokrok, ba práve naopak rozvíjala sa pomaly a ešte stále sa používali jednoduché substitúcie a transpozície. Na druhej strane sa v 14. storočí rozvinula kryptoanalýza. Arabi objavili riešenie jednoduchej substitúcie pomocou frekvenčnej analýzy, ktorá vychádza z počtu jednotlivých písmen nachádzajúcich sa v konkrétnom texte.

V Európe sa šifrovanie stáva čoraz významnejšie, našlo uplatnenie v boji, ale aj v medzinárodnej politike. Dôležitosť šifrovania sa dostáva do popredia hlavne pri dobývaní miest. Napr. ak malo dobývané mesto málo munície, potrebovalo túto správu zašifrovať a poslať ďalej. Pokiaľ sa útočiacemu vojsku podarilo zašifrovanú správu zachytiť a text rozlúštiť, stačilo, aby poslali posla s rozlúštenou správou a dobývané mesto sa vzápätí vzdalo. Nedokonalosť kryptografie sa objavila aj v oblasti politiky, kde v zašifrovanej správe stála škótsku kráľovnú Máriu Stuartovú život. Jej sesternica, anglická kráľovná Alžbeta, ju dala zavrieť do väzenia, odkiaľ Mária posielala zašifrované správy svojim spoločníkom. V dôsledku rozlúštenia správy, ktorej obsahom bolo pripravované sprisahanie proti Alžbete, bola Mária pri súde usvedčená a následne popravená.



Obr. 8. Šifra Márie Stuartovej [5]

V tomto období zamestnávala väčšina mocných vládcov svojich vlastných odborníkov na šifrovanie. Stále však išlo o jednoduché a pomerne ľahko rozlúštiteľné šifry. Onedlho sa objavujú bezpečnejšie systémy týkajúce sa šifrovania, avšak tie boli veľmi komplikované, a tak sa často nepoužívali. Až v 16. storočí francúzsky diplomat Blaise de Vigenére knižne popísal tzv. Vigenérovu šifru založenú na princípe polyalfabetického šifrovania. V polyalfabetickom šifrovaní bolo cieľom znížiť počet frekventovaných šifrovaných písmen a

tým sťažiť prelomenie šifrovacieho systému. Zmienené zníženie počtu písmen prebiehalo vďaka tomu, že jeden znak šifrovaného textu reprezentovalo niekoľko rozdielnych písmen otvoreného textu, odlišnosť písmen spočívala napr. v tom, na akom mieste správy sa daný znak nachádza alebo aké písmeno leží pred ním. Teraz späť k Vigenérovej šifre. K zašifrovaniu textu pomocou Vigenérovej šifry sa používa tzv. Vigenérov štvorec, kde otvorený text predstavujú jednotlivé stĺpce a kľúč predstavujú riadky, šifrované písmeno tak vznikne v mieste stretu konkrétneho stĺpca s konkrétnym riadkom. Ak by sme chceli zašifrovať otvorený text, v ktorom sa nachádza písmeno „P“, pomocou kľúčového písmena „f“, tak dostaneme písmeno „U“. [1], [5]

Kľúč	Otevřený text																									
	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. 9. Použitie Vigenérovho štvorca k zašifrovaniu písmena P pomocou kľúča f [1]

1.5.3 Kryptografia v 19. storočí

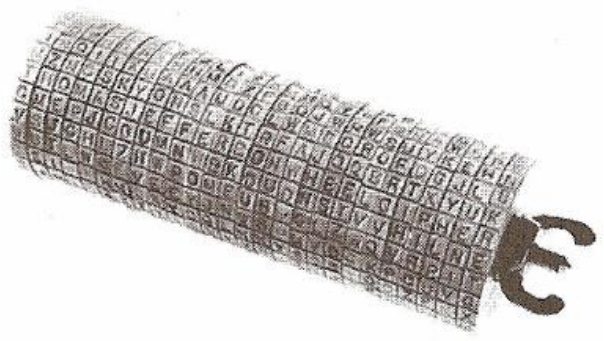
Vynájdenie telegrafu v roku 1832 bolo dôležitým zlomom v oblasti kryptografie. Napriek tomu, že telegraf umožňoval posielať správy na dlhú vzdialenosť a v krátkom čase, neposkytoval žiadne súkromie. Pri odosielaní správy sa dalo jednoducho „napichnúť“ na

telegraf a správu tak bez problémov zachytiť. Šifrovanie už nie je dôležité len pre armádu a šľachtu, ale zohráva kľúčovú úlohu aj v odvetví obchodníctva.

Obr. 10. Telegraf [9]

Pre vojenské účely našli využitie tzv. poľné šifry. Uplatňovali sa priamo na mieste boja. Bezpečnosť šifrovacieho algoritmu nemusela byť vôbec veľká, išlo tu skôr o rýchlosť šifrovania a dešifrovania správy, pričom dôležité bolo, aby šifrovaná správa bola časovo náročná na rozlúštenie pre protivníka. Ak sa napr. šifrovaná správa s textom: „Boj začne o 16:00“ dostala do rúk protivníkovi a ten ju rozlúštil o 16:05, tak jej rozlúštenie stráca zmysel. [5]

V americkej občianskej vojne v rokoch 1861-1865 sa používali okrem poľných šifier i iné kryptografické metódy. Konfederácia severných štátov používala najmä substitučné šifry, medzi ktoré patrila aj vyššie spomínaná Vigenérova šifra, ktorú ale Únia dokázala rozlúštiť. Únia juhoamerických štátov bola na tom lepšie, používala šifrovací mechanizmus zvaný Jeffersonov valček. Pomenovanie dostal podľa tretieho amerického prezidenta Thomasa Jeffersona, ktorý valček vynašiel. Tento šifrovací mechanizmus je tvorený približne 36 diskami, ktoré je možné nasunúť na os valčeka. Po obvode každého disku je napísaná abeceda rôzne prehádzaných písmen a disk je označený číslom pre určenie nastavenia mechanizmu. Pri odosielaní správy sa zoradia disky a nastavia sa tak, aby jedna rada naprieč riadkami tvorila otvorený text. Ako šifrovaný text sa potom zapíše hocijaký riadok z ostatných voľných riadkov. Postupnosť čísel určujúca zoradenie diskov a jedno číslo udávajúce posun v stĺpcoch tvoria kľúč. Tento kryptografický mechanizmus sa považuje za relatívne bezpečný a používala ho americká armáda do začiatku druhej svetovej vojny. [2], [5]



Obr. 11. Jeffersonov valček [2]

V roku 1854 britský vedec Charles Wheatstone vynašiel nový typ šifry. Šifru predstavil svetu až škótsky barón a poslanec anglického parlamentu Lyon Playfair, podľa ktorého je pomenovaná ako šifra Playfair. Jedná sa o vojenskú poľnú šifru, ktorá bola v užšej miere používaná až do konca 2. svetovej vojny. Šifra je ťažšie rozlúštiteľná, lebo je odolná voči frekvenčnej analýze. Playfairova šifra je výhodná z viacerých hľadísk, je jednoduchá na naučenie sa, je rýchla na prípravu šifrovaných textov a je rýchla pri ich dešifrovaní. Písmená otvoreného textu sa šifrujú po dvojiciach, a teda sa jedná o bigramov princíp šifrovania. Kľúč pozostáva zo štvorcovej mriežky, ktorej obsahom je 5x5 políčok. Z uvedeného vyplýva, že do mriežky sa zmestí iba 25 písmen, pričom v medzinárodnej abecede je písmen 26. Vynecháva sa písmeno, ktoré je najmenej používané v danom jazyku, v anglickom jazyku sa jedná o písmeno „J“, ktoré sa nahradí za „I“, a v českom alebo slovenskom jazyku sa väčšinou vynecháva písmeno „Q“ a nahrádza sa písmenom „K“. Ak budeme šifrovať správu pomocou Playfairovej šifry, tak bude potrebné previesť otvorený text podľa nasledujúcich krokov:

- v anglickom texte nahradíme všetky písmena J za písmena I (v českom Q za K),
- písmená v správe rozdelíme do dvojíc,
- ak by sa dve rovnaké písmená vyskytli vedľa seba, treba ich oddeliť vložením písmena Z,
- ak bude mať správa nepárny počet písmen, na koniec správy sa pridá písmeno Z.

Na príklade si názorne predvedieme princíp šifrovania Playfairovou šifrou. Zvolíme si kľúčové slovo, napr.: HESLO. Neodporúča sa, aby kľúčové slovo malo menej ako 5 písmen. Následne sa vytvorí tzv. abecedný štvorec, kde sa na začiatok napíše kľúčové

slovo a ostatné písmená sa doplnia, s vynechaním písmena J. Abecedný štvorec vyzerá nasledovne:

Tab. 3. Abecedný štvorec Playfairovej šifry s kľúčovým slovom HESLO [autor]

H	**E**	**S**	**L**	**O**
A	B	C	D	F
G	I	K	M	N
P	Q	R	T	U
V	W	X	Y	Z

Pri šifrovaní je nutné sa riadiť niekoľkými zásadami:

1. Zásada - ak sa obe písmená nachádzajú v jednom riadku, tak sa každé z týchto dvoch písmen nahradí písmenom, ktoré leží napravo od nich. Posledné písmeno ležiace v danom riadku sa nahradí písmenom prvým tohto riadku.
2. Zásada - ak sa obidve písmená nachádzajú v jednom stĺpci, tak sa každé písmeno z bigramu nahradí písmenom, ktoré leží o jedno miesto smerom nadol. Posledné písmeno v stĺpci sa nahradí prvým písmenom.
3. Zásada - ak sa obidve písmená nenachádzajú v rovnakom stĺpci a ani v rovnakom riadku, tak sa pri prvom písmene najskôr vezme riadok prvého písmena a stĺpec druhého písmena a tam, kde sa pretnú, leží zašifrované písmeno. Pri druhom písmene sa postupuje obdobne, vezme sa riadok druhého písmena a stĺpec prvého.
4. Zásada - zašifrovaný text sa zapíše do skupín po päť písmen. Ak nám v poslednej skupine písmen nevyjde pätica, doplníme ju písmenom X.

Pri zašifrovaní správy: „Táto šifra je celkom jednoduchá.“, odstránime diakritiku, za J nahradíme I a do párneho počtu písmen pridáme Z. Vzniknú nám nasledujúce bigramy: TA TO SI FR AI EC EL KO MI ED NO DU CH AZ. Následne použijem šifrovú abecedu s kľúčovým slovom HESLO, ktorá je zobrazená vyššie. Zašifrujeme text podľa štyroch

spomínaných zásad, vznikne nám: PDULE KCUBG SBSON SKNLB UFFTA SFVXX. Pri dešifrovaní šifry postupujeme opačným spôsobom ako pri jej šifrovaní. [1], [5]

1.5.4 Kryptografia v období 1. a 2. sv. vojny

Kryptografia v 20. storočí nadobúda veľký význam a to hlavne vďaka objavu rádia v roku 1894. Rádio umožňovalo ešte omnoho rýchlejší prenos komunikácie ako telegraf, nevýhodou tohto vynálezu je, že vysielanie prostredníctvom rádia bolo verejné, a tak neexistovalo žiadne súkromie medzi komunikujúcimi. Preto sa otázka šifrovania stáva nevyhnutnou.

Obr. 12. Rádio [10]

V 1. svetovej vojne boli veľmi často používané poľné šifry, napr. šifra Playfair a časté bolo aj používanie kódových kníh, vďaka ktorým sa správy prekladali do číselných kódov. Správy zašifrované kódovou knihou bolo takmer nemožné rozlúštiť, šlo to len v prípade, ak páchateľ danú kódovú knihu nejakým spôsobom získal. Preto sa k získaniu kníh používali rôzne triky. Angličania boli v tomto smere veľmi prefíkaní a podstrkovali nepravé klamlivé kódové knihy a falošné správy zašifrované prostredníctvom týchto kníh.

Anglické námorníctvo malo počas 1. sv. vojny špeciálnu kryptografickú jednotku, ktorá pracovala pod vedením sira Williama Halla. Ich úspech nastal v okamihu, keď sa im podarilo zachytiť a rozlúštiť telegram, ktorý poslal vtedajší nemecký minister zahraničných vecí Arthur Zimmermann nemeckému veľvyslancovi v Spojených štátoch. V telegrame stálo, že Nemci chystajú ponorkovú vojnu v Atlantiku a ak by sa náhodou USA chceli zapojiť do vojny, tak by bolo potrebné presvedčiť Mexiko, aby sa pridalo na stranu Nemecka a zaútočilo na Spojené štáty. Telegram navyše obsahoval informácie, že Nemecko je ochotné poskytnúť Mexiku vojenskú výpomoc a že Mexiko by mohlo

sprostredkovať jednanie s Japonskom. Hall však nechcel, aby Nemci vedeli, že Angličania dokážu lúštiť ich šifry a navyše, ak by Američanom predal telegram priamo, tí by si mohli myslieť, že sa jedná o lesť, pomocou ktorej chcú Angličania vtiahnuť Američanov do vojny. Hall vymyslel perfektný spôsob, ako obísť predanie správy Američanom priamo, a zinscenoval situáciu tak, že sa anglickému agentovi podarilo získať rozšifrovanú správu v Mexiku. K tomu vyvolal kritiku v anglických novinách mierenú na vlastné služby za to, že sa im nepodarilo tak podstatnú správu zachytiť a následne vylúštiť. Vďaka tomu boli Nemci úplne zmätení.

Obr. 13. Zimmermannov telegram

[5]

V období 2. sv. vojny sa v kryptografii začínajú uplatňovať matematici, do tej doby prevažovalo skôr uplatnenie jazykovedcov. Nastáva mechanizácia šifrovania a s ňou spojené mechanické šifrovacie stroje, v USA to bola Sigaba, Typex v Británii, Japonsko používalo Purple, no a najznámejšia je nemecká Enigma. Všetky tieto mechanické stroje, vrátane Enigmy, pracovali na podobnom princípe, kde základ bol tvorený niekoľkými rotujúcimi diskami s 26 znakmi abecedy. V diskoch boli implikované drôty, tie udávali substitúciu. Stlačením písmena na klávesnici a zašifrovaním prvého písmena došlo k otočeniu rotujúcich diskov a druhé písmeno sa zašifrovalo inou substitúciou, čiže Enigma šifrovala polyalfabetickou šifrou. Šifrovanie polyalfabetickou šifrou umožňovali rotujúce disky, ktoré sa dali medzi sebou prepojiť prostredníctvom prepojovacej dosky a tým rôzne kombinovať. Na začiatku bolo treba Enigmu nastaviť pomocou kľúča, ktorý pozostával z

poradia rotorov, ich začiatočnej pozície a z nastavenia prepojovacej dosky. Nemci s istotou verili, že je Enigma neprelomiteľná, opak bol ale pravdou. Jednou z najvýznamnejších udalostí 2. sv. vojny bolo práve jej rozlúštenie, ktoré umožnilo čítať komunikáciu medzi Nemcami. Pričinil sa o to poľský matematik Marian Rejewski. K Rejewskemu sa dostala časť manuálu Enigmy vďaka nespokojnému nemeckému úradníkovi, ktorý ju za poplatok skopíroval francúzskej tajnej službe. Pri spolupráci Francúzska a Poľska sa časť manuálu dostala k poľskej tajnej službe a odtiaľ putovala do rúk mladého matematika Rejewskeho.

Obr. 14. Šifrovací stroj Enigma [11]

Američania žijúci v Pacifiku dokázali rozlúštiť šifry vytvorené japonským mechanickým strojom Purple. Američania sa zapísali do dejín kryptografie aj používaním kódu Navajo. Bol to vlastne jazyk, ktorým sa dorozumieval indiánsky kmeň zvaný Navajo, a pretože bol tento jazyk tak výrazne odlišný od ostatných, poslúžil ako ideálna šifra. Niektoré technické pomenovania však v jazyku Navajo neexistovali (ako napr. ponorka), a tak sa museli vytvoriť kódové slová. Američania potom pridelili každému členovi kmeňu Navajo osobnú ochranku, aby sa ich protivníci nezmocnili, ale ak by sa tak stalo, ochranka dostala príkaz zadržaného Navaja zastreliť. [5]

1.5.5 Šifrovanie na území ČR v období 2. sv. vojny

Ešte počas 1. Československej republiky si vojenská spravodajská služba v 30. rokoch vybudovala ústredne v mnohých európskych krajinách, z ktorých potom viedla boj proti nemeckým stúpencom nacizmu počas celého obdobia 2. sv. vojny (1939-1945). Ich spravodajská činnosť bola riadená z Londýna prostredníctvom 2. oddelenia Hlavného štábu Ministerstva národnej obrany (MNO) pod vedením generála Františka Moravca - Pavla.

Jednou z dôležitých úloh spravodajskej služby bolo bezpečné predávanie správ v jej rádiovej sieti. Bezpečnosť obsahu správ sa zaisťovala šifrovaním a práve činnostiam spojeným s kryptografiou nebola venovaná dostatočná pozornosť. Rozvoj kryptografie, ktorá zaručovala bezpečnosť prenášaných správ, bol opomínaný aj na najvyšších miestach velenia armády. Na jednej strane československá armáda oplývala v roku 1938 vysokou úrovňou techniky, no na strane druhej táto skutočnosť kontrastovala s nízkou úrovňou zabezpečovaného predávania tajných správ. Úroveň šifrovania správ sa dala porovnávať s armádami menej vyspelých krajín. To sa potom odrazilo na práci vojenskej rozviedky počas vojny.

Zo skúmania odtajnených materiálov londýnskeho velenia československej spravodajskej služby a materiálov londýnskej Vojenskej rádiovej ústredne (VRÚ) z rokov 1939 až 1945, ktoré sú uložené vo vojenskom historickom archíve, boli zistené štyri najčastejšie spôsoby šifrovania, ktoré používala vojenská rozviedka. Po podrobnom skúmaní týchto metód šifrovania vyšlo najavo zistenie, že veľká časť používaných systémov šifrovania nebola vôbec bezpečná, a dokonca bola veľakrát použitá nesprávnym spôsobom, ktorý uľahčoval odhalenie správ. Mnohé materiály zverejnené po vojne dokazujú, že nemeckí kryptoanalytici vedeli bez problémov nielen zachytiť správy posielané v londýnskej rádiovej sieti rozviedky, ale tiež ich vedeli bez väčších problémov rozlúštiť. Kryptografovia a ich velitelia v rádiovej sieti VRÚ sa dopúšťali chýb neúmyselne. Chyby boli odozvou na ich predošlé nedostatočné odborné zaškolenie v oblasti kryptológie. Dôsledkom toho však boli straty na životoch mnohých statočných ľudí v protifašistickom odboji.

Na konci vojny sa v zbernom zajateckom tábore, kde boli umiestnení prevažne nemeckí dôstojníci, objavili dvaja civilisti, ktorí pracovali počas vojny ako lúštitelia vo Výskumnom úrade sídliacom v Berlíne. Pracovnou náplňou oboch civilistov bolo lúštenie

československých šifier. Civilisti vyslovili obavu, že budú deportovaní do lágrov umiestnených na Sibíri, a tak pod podmienkou, že zostanú uväznení v ČSR, poskytli plukovníkovi Rohatému okolo 30 listov formátu A4 s podrobným popisom lúštenia kľúčov ST, TTS, STT, SP, STP a zubatky. Pri štúdiu spomínaných listov plk. Rohatý s údesom zistil, že nemeckí civilisti popísali všetky kľúče, ktoré spravodajcovia v Londýne počas vojny používali.

Neskôr nasledovalo priznanie zo strany oboch civilistov, že depeše londýnskej siete československej rozviedky boli jednoducho identifikovateľné. Vraj už v jeseni roku 1939 čiastočne rozlúštili tabuľku dĺžky 10x10 a zaregistrovali, že číselné depeše sú vlastne písmenovým transpozičným kľúčom s dodatočnou substitúciou. Akurát nevedeli, či sa jedná o jednoduchú alebo dvojitú transpozíciu. Najskôr triedili materiál podľa denných posunov číselnej zámeny a na konci roku 1939 z celkom veľkého množstva číselných dvojíc boli schopní rekonštruovať celú českú substitučnú abecedu.

TTS, čiže dvojitú transpozíciu s jednoduchou substitúciou písmen na číselné dvojice, prvýkrát rozlúštili niekedy v lete roku 1940 a to hlavne vďaka tomu, že medzi Londýnom a Prahou a aj medzi Londýnom a Istanbulom prebiehala výmena veľkého množstva šifrovaných depeší rovnakej dĺžky. Podarilo sa im zachytiť aj 100 depeší za jeden jediný deň, medzi ktorými niekedy bolo aj 10 telegramov s rovnakou dĺžkou. Chvíľu na to odhalili, že sa používa systém 11 hesiel s denným rozdeľovníkom.

V roku 1941 nastal zlom, kedy Nemci začali odhaľovať používané heslové knihy a básne. Najčastejšie používanou básňou bola báseň „Nadšení“, vďaka ktorej sa im podarilo rozbiť celý šifrovací systém. Zo smeru Istanbul, Moskva, Teherán a Jeruzalem boli schopní rozlúštiť všetky šifry, ktoré sa im podarilo odpočúvať.

Nemeckej rozviedke sa v roku 1940 na Balkáne podarilo zakúpiť ofotené šifrovacie smernice a zopár heslových kľúčov. Kľúče síce neboli nikdy použité, ale zo smerníc sa im podarilo vyčítať spôsob používania 11 hesiel podľa dní.

Štúdiom materiálov od spomínaných civilistov plk. Rohatý vyvodil záver, že zásadnou chybou pri šifrovaní v sieti vojenskej spravodajskej služby bolo posielanie nadmerného množstva depeší, ktoré boli šifrované rovnakým kľúčom. Ďalšou chybou bolo posielanie popisov nových kľúčov zašifrovaných v depešiach, kde bol najviac používaný obežníkový kľúč. Všetky spravodajské materiály z Londýna boli uložené do archívu s označením

„PRÍSNE TAJNÉ, chrániť ako šifry“. Plk. Rohatému sa podarilo svojim činom zriadiť lúštiteľské kurzy a zároveň dosiahnuť to, aby absolventi lúštiteľských kurzov tvorili stálu skupinu ľudí a boli schopní postaviť kryptológiu v armáde na pevné základy. Prvý krok ku zvýšeniu bezpečnosti šifrovej služby v československej armáde sa tak po dlhej dobe stal skutočnosťou. [12]

2 SÚČASNÉ METÓDY KRYPTOGRAFICKEJ OCHRANY

Po skončení svetových vojen nastáva prudký rozmach počítačov. Vďaka tomu naberá kryptografia úplne iný charakter. Ručné šifrovanie spôsobovalo mnoho problémov a to najmä z toho dôvodu, že kryptografovia sa pri šifrovaní často mýlili alebo nesprávne pochopili princíp šifrovania. Nástupom počítačov sa tento problém definitívne odstránil, pretože nevznikali žiadne chyby pri šifrovaní. Výhodou bola aj jednoduchosť v šifrovaní, pretože počítače umožnili automatizáciu mechanických početných úkonov. [5]

Súčasné kryptografické metódy, ktoré využívajú k šifrovaniu textu počítač, nie sú založené na nahradzovaní a prehadzovaní písmen, ale pracujú s binárnymi reťazcami, teda s bitmi. Bity sa vyjadrujú prostredníctvom jednotiek a núl. Otvorený text sa do binárnych čísel prenesie prostredníctvom kódovacích tabuliek. Najznámejšia kódovacia tabuľka je tzv. ASCII tabuľka (American Standard Code for Information Interchange, čo v preklade znamená Americký štandardný kód pre výmenu informácií). Otvorený text vyjadrený prostredníctvom bitov je následne zašifrovaný, vďaka tomu dostávame kryptogram vo forme bitového reťazca. [1]

Rozlišujeme dve základné rozdelenia moderných metód kryptografie:

- **Prvé rozdelenie:**

1. Jednosmerné šifrovanie - zo zašifrovaného textu nedostaneme pôvodný text
2. Obojsmerné šifrovanie - pri znalosti kľúča sme schopní dostať zo zašifrovaného textu pôvodný text

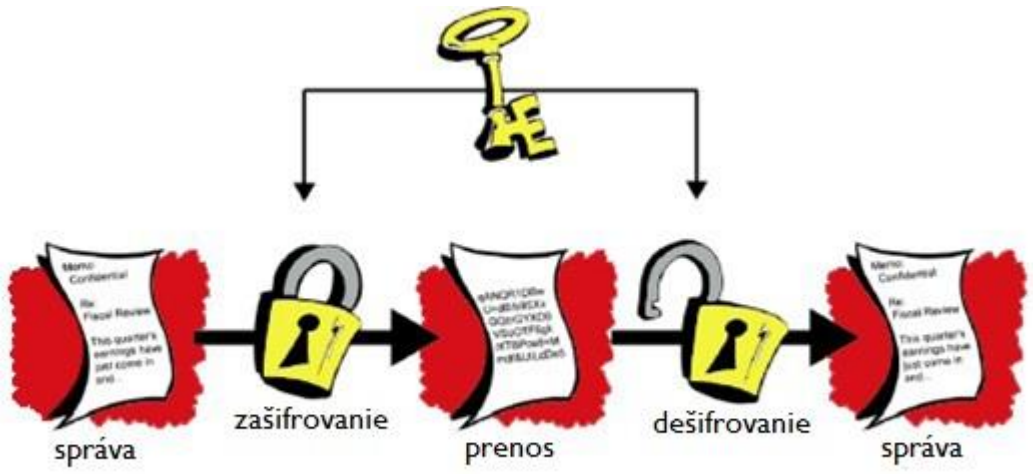
- **Druhé rozdelenie:**

1. Symetrické šifrovanie - použitie súkromného kľúča
    a. blokové šifrovanie
    b. prúdové šifrovanie
2. Asymetrické šifrovanie - použitie verejného kľúča
3. Hybridné šifrovanie - kombinácia symetrického a asymetrického šifrovania [13]

2.1 Symetrické šifrovanie

Moderné symetrické šifry pracujú na podobnom princípe ako klasické šifry spomínané v podkapitolách týkajúcich sa histórie. Súčasná doba nám umožňuje používanie počítačov, z tejto skutočnosti vyplýva hlavný rozdiel medzi symetrickými a klasickými šiframi. Pri symetrickom šifrovaní sme vďaka používaniu počítačov schopní prevádzať omnoho zložitejšie šifrovacie operácie ako pri klasickom ručnom šifrovaní.

Pri šifrovaní otvoreného textu symetrickým šifrovaním sa používa rovnaký kľúč ako pri dešifrovaní zašifrovaného textu. Táto skutočnosť je zároveň nevýhodou systému symetrického šifrovania, pretože je nutné, aby sa odosielateľ s prijímateľom dohodli na jednom konkrétnom kľúči, ktorý si musia medzi sebou predať a to bezpečným spôsobom, aby sa tajný kľúč nedostal k nepovolanej osobe, problém teda nastáva v distribúcii kľúča. Medzi silné stránky symetrického šifrovania patrí rýchlosť algoritmu. Symetrické šifrovanie pracuje na oveľa jednoduchšom princípe ako asymetrické šifrovanie a pri tomto druhu šifrovania nie sú potrebné tak výkonné počítače. [1] [13]



Obr. 15. Princíp symetrického šifrovania [13]

Pri symetrickom šifrovaní je potrebné dbať na dĺžku kľúča, aby nedošlo k jeho prelomeniu. Pri minimálnej dĺžke kľúča, ktorá predstavuje 40 bitov, je počítač schopný vygenerovať 240 rôznych šifrovacích funkcií. Ak by sme chceli takúto šifru prelomiť, museli by sme pomocou počítača vypočítať 240 obsiahlych výpočtov, čo predstavuje niekoľko týždňov počítania. Pre veľké firmy alebo objekty s vysokým utajením však 40-bitová dĺžka kľúča nestačí, tu je potrebná minimálne 56-bitová dĺžka kľúča. Snaha prelomiť šifru s 56-

bitovým kľúčom by prostredníctvom výpočtu na bežnom počítači trvala niekoľko tisíc rokov.

Podľa princípu šifrovania sa symetrické šifry delia na:

- prúdové šifry
- blokové šifry [6]

2.1.1 Prúdové šifry

Prúdové šifrovanie môže prebiehať buď v slovnom tvare, alebo v súčasnosti sa častejšie používa bitový tvar. V slovnom tvare sa otvorený text šifruje písmeno po písmene, ako je tomu napr. pri Vigenérovej šifre alebo pri nemeckom šifrovacom stroji Enigme. Šifrovanie bitovým spôsobom prebieha tak, že sa otvorený text šifruje jeden bit po druhom. Oddelené bity prichádzajú do komunikačného kanálu v pravidelných alebo nepravidelných časových intervaloch, následne sa znaky prevedú na šifrovanú hodnotu. Keďže bity obsahujú len dve hodnoty, je zrejmé, že s nimi môžu nastať len dve situácie, buď sa hodnota bitu zmení na opačnú, alebo zostane nezmenená. [1], [6]

Pri generovaní dlhého hesla sa pri prúdových šifrách najskôr použije krátky kľúč, z ktorého sa následne vygeneruje kľúč dlhý a až tento sa použije pre zašifrovanie správy. Na generovanie hesiel sa používa tzv. generátor binárnych znakov. Bezpečnosť prúdových šifier spočíva najmä v nepravidelnosti kľúča. Ak by sa pri generovaní hesla krátky kľúč pravidelne opakoval, šifra by nebola príliš bezpečná. Nepravidelnosť kľúča je možné celkom ľahko zaistiť. Majme ľubovoľný kľúč dlhý 4 bity. Ostatné bity tohto 4-bitového kľúča získame binárnym súčtom prvých a posledných bitov predchádzajúcej štvorice. Napr. pri kľúči 1111, dostaneme binárny reťazec 111101011001000. Pri generovaní kľúča takýmto spôsobom sa reťazec opakuje až po pätnástich znakoch. Vytváranie dobrých generátorov hesiel je celkom náročné a vyžaduje si znalosti vyššej matematiky.

Zo skutočnosti, že každý bit otvoreného textu určuje iba jeden bit šifrovaného textu, vyplýva jedna veľká výhoda a tou je fakt, že ak pri šifrovaní dôjde k nesprávnemu príjmu bitu, tak pri dešifrovaní vznikne chyba iba v tomto konkrétnom bite. Táto vlastnosť je vhodná najmä pri vysielaní šifrovaného textu komunikačným kanálom s vysokou hladinou šumu. Prúdové šifry sa teda logicky používajú pri šifrovaní reči na mobilných sieťach GSM. Medzi ďalšie výhody patrí relatívna rýchlosť a nenáročná implementácia. Medzi

najčastejšie prúdové šifry patrí klasická matematická operácia XOR a Vermanova šifra. [1], [5]

2.1.1.1 XOR

Pri práci s binárnymi číslami sa v prúdových šifrách často používa operácia binárneho sčítania. Spravidla sa jedná o bežný spôsob kombinácie dvoch bitov, ktorý sa zapisuje ako XOR alebo plus v krúžku, teda $\oplus$.

Pri operácii XOR platia nasledovné pravidlá: $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ a $1 \oplus 1 = 0$. Zjednodušene si to môžeme predstaviť v tabuľke nižšie.

Tab. 4. XOR [autor]

$\oplus$	**0**	**1**
0	0	1
1	1	0

Použitie tejto binárnej operácie umožňuje kombinovať dva bitové reťazce rovnakej dĺžky. Bit v jednom bitovom reťazci sa sčíta s bitom, ktorý leží na tej istej pozícii v druhom bitovom reťazci, pokračovaním takéhoto sčitovania nám vznikne tretí bitový reťazec. Sčítaním bitového reťazca 10011 s bitovým reťazcom 11001 nám vznikne výsledný reťazec 01010. Výsledok nám vznikne tým, že sčítame bit na prvej pozícii zľava v prvom binárnom reťazci s bitom na prvej pozícii zľava v druhom binárnom reťazci, čo znamená $1 \oplus 1$, sčítaním dvoch jednotiek vznikne nula. Takto sa postupuje až ku koncu bitového reťazca. [1]

Tab. 5. Sčítanie bitových reťazcov pomocou XOR [1]

1	0	0	1	1
1	1	0	0	1
$1 \oplus 1$	$0 \oplus 1$	$0 \oplus 0$	$1 \oplus 0$	$1 \oplus 1$
0	**1**	**0**	**1**	**0**

2.1.1.2 Vernamova šifra

Vernamova šifra spočíva vo vylepšení skorších spôsobov šifrovania. Navrhol ju major americkej armády Joseph Mauborgn, ale v roku 1917 si ju dal patentovať Gilbert Sandford Vernam. Vernamov spôsob šifrovania používa rovnako dlhé heslá ako je otvorený text a po použití daného hesla sa príslušné heslo zničí. Z uvedeného vyplýva, že pri šifrovaní sa nikdy nepoužíva to isté heslo dvakrát. [6]

Postup šifrovania Vernamovou šifrou nie je vôbec zložitý. Každé písmeno v otvorenom texte posunieme podľa zvoleného kľúča o niekoľko pozícií naľavo. Máme napr. daný kľúč 7,0,2,5,13 a chceme zašifrovať slovo SIFRA. Zoberieme prvé písmeno, teda S a posunieme ho podľa kľúča o 7 miest doľava, vznikne nám písmeno Z, takto pokračujeme až k poslednému písmenu slova a vznikne nám šifrovaný text ZIHWN. Dešifrovanie potom prebieha pomocou daného kľúča opačným smerom.

Pre dostatočnú bezpečnosť Vernamovej šifry je potrebné dodržať nasledujúce podmienky:

1. Kľúč musí byť rovnako dlhý ako otvorený text - v starších šifrách tomu tak nebolo.
2. Kľúč musí byť úplne náhodný - nesmú byť použité žiadne pseudonáhodné generátory čísel, je totiž možné ich jednoducho predvídať, najlepšie je využitie fyzikálnych metód.
3. Kľúč nemožno použiť opakovane - rovnaký kľúč nesmie byť použitý pre dve rôzne správy.

Ak sa pri zašifrovaní správy dodržia spomínané podmienky, šifra sa stane absolútne neprelomiteľnou. Pri lúštení šifry je dokonca zbytočný útok hrubou silou, pretože výsledkom budú všetky správy o rovnakej dĺžke a útočník nespozná, ktorú správu odosielateľ zašifroval. Jedinečnosť Vernamovej šifry tkvie v jej neprelomiteľnosti, ktorá bola dokázaná v roku 1949 C. E. Shannonom.

Vyvstáva však problém so zapamätaním si tak dlhého náhodného kľúča, a preto musí byť niekde zaznamenaný. Ďalej musí byť zabezpečené, že kľúč pozná iba odosielateľ a príjemca a teda, že sa nešťastným spôsobom nedostane k nepovolanej tretej strane. Účastníci komunikácie sa musia vopred dohodnúť na tajnom kľúči, nejakým zabezpečeným kanálom si ho predať a hneď po odoslaní správy ho zničiť. Teda ak chce

odosielateľ poslať správu dlhú 2MB, musí vyriešiť problém, ako pred tým predať adresátovi kľúč o dĺžke 2MB.

Vernamova šifra používa rovnaký postup ako je uvedený vyššie aj pre binárne znaky. Kľúč tvorí tiež postupnosť binárnych znakov, teda 0 a 1. Posun znakov v binárnej abecede je logicky možný buď o 1 miesto alebo o 0 miest, resp. či sa daný bit podľa kľúča zmení, alebo zostane nezmenený. Jedná sa vlastne o použitie klasickej operácie XOR. [14]

2.1.2 Blokové šifry

Blokové šifry pracujú tak, že najskôr sa bitový reťazec rozdelí do blokov pevnej dĺžky a potom sa aplikuje šifrovací algoritmus na každý blok samostatne. Využitie blokových šifier je celkom rozsiahle, vyznačuje sa vysokou mierou zabezpečenia, integritou dát či overením užívateľa. Je možné ich využiť aj ako generátory hesiel pre prúdové šifry. Blokové šifry sú dobre navrhnuté vtedy, ak je najjednoduchším typom útoku útok hrubou silou, teda skúšaním rôznych kombinácií kódov. Toto tvrdenie platí za predpokladu, že bude dostatočne vysoký počet kľúčov.

Pri navrhovaní šifrovacích algoritmov by každá silná bloková šifra mala obsahovať niekoľko zásadných prvkov. Ak sa útočníkovi dostane do rúk dvojica otvoreného a šifrovaného textu bez znalosti kľúča, nemal by mať možnosť odvodením zistiť, ktorý šifrovaný text zodpovedá konkrétnemu bloku otvoreného textu. V tomto prípade platí tzv. vlastnosť difúzie, kde malá zmena v otvorenom texte má za dôsledok nevyspytateľné zmeny v šifrovanom texte. Môže nastať situácia, že útočník pri hľadaní správneho kľúča vyskúša taký, ktorý sa od pôvodného odlišuje iba na niektorých pozíciách. Ak by sa útočník dozvedel, že vyskúšal kľúč, ktorý sa líši iba jednou pozíciou od správneho kľúča, nepraktizoval by kompletné vyhľadávanie, ale by len skúšal meniť jednu pozíciu po druhej. To by mu zabralo omnoho menej času ako pri kompletnom vyhľadávaní kľúča. Blokové šifry by teda mali mať vlastnosť konfúzie, čo znamená vyvarovanie sa akéhokoľvek naznačovania útočníkovi, že sa pri hľadaní blíži k správnemu kľúču. Šifrovanie blokovými šiframi vyžaduje ešte úplnosť, kde každá časť šifrovaného textu musí vychádzať z každej časti kľúča, aby útočník nemohol zisťovať konkrétne časti kľúča bez ohľadu na jeho zvyšok.

Najmenej náročným šifrovaním dlhej správy prostredníctvom blokovej šifry je rozdelenie bitovej postupnosti na bloky a ich následné šifrovanie každého bloku zvlášť, nezávisle od

ostatných, jedná sa o tzv. mód elektronickej kódovej knihy (electronic code book, ECB). Každý blok textu sa zobrazí na adekvátny šifrovaný výsledok podľa stanoveného kľúča. Ako keby existuje nejaká kódová kniha, ktorá určuje, na akú hodnotu sa má previesť každý blok textu. Dva rovnaké bloky otvoreného textu sa zašifrujú na rovnaké bloky šifrovaného textu, v čom spočíva jednoduchosť kryptoanalýzy ECB šifier. Nevýhodou je tiež fakt, že pokiaľ bolo manipulované s blokmi prenášaného textu, tak to príjemca nemusí vôbec spoznať.

Nevýhodám uvedeným vyššie je možné sa vyhnúť a to prostredníctvom módov spätnej väzby (cipher feedback mode, CFB) alebo sa im tiež hovorí reťazenie šifrových blokov (cipher block chaining, CBC). Pri šifrovaní sa zašifruje každý blok prostredníctvom kľúča a takto šifrovaný blok sa nejakým spôsobom skombinuje a tým pádom previaže s predošlými blokmi. Rovnaký blok sa tak zobrazí na rôzne bloky v šifrovanom texte. Prijímateľ tak ľahko spozná, či bolo s textom manipulované alebo nie, a ak došlo k manipulácii textu, tak mu po dešifrovaní správy začnú vychádzať nezmysly. Medzi blokové šifry sa zaraďujú algoritmy DES, 3DES, Blowfish, IDEA a AES. [1], [5]

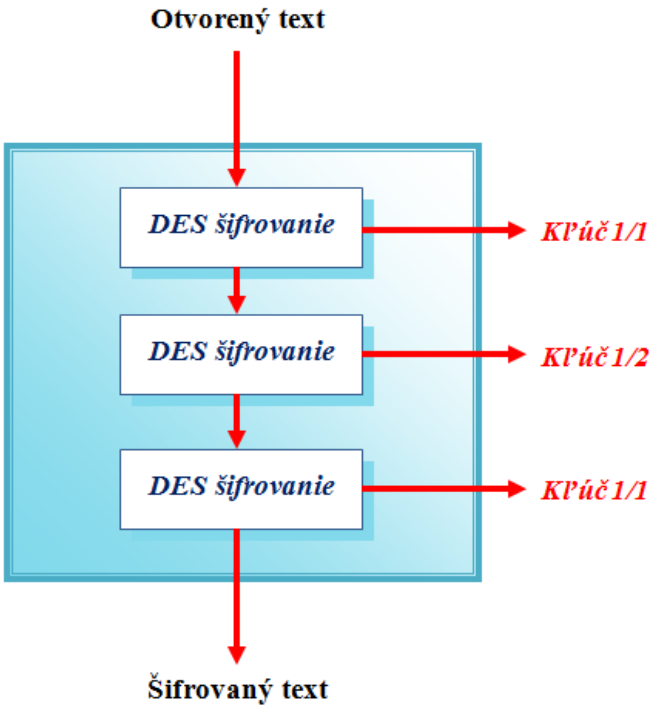
2.1.2.1 DES a 3DES

Šifrovací algoritmus DES (Data Encryption Standard) vyvinula spoločnosť IBM v 70. rokoch. Od roku 1977 sa stal americkým štandardom pre šifrovanie a bol ním 20 rokov. DES už je v podstate zastaraný šifrovací algoritmus, pretože nestačí výkonom modernej výpočtovej techniky, ktorá sa za posledné desaťročia neúprosne rýchlo rozvinula do dnešnej podoby a neustále napreduje. Tento algoritmus sa dokonca podarilo prelomiť hrubou silou, teda skúšaním všetkých možných kombinácií. DES je síce dnes už nemoderný systém, ale keďže sa stal inšpiráciou pre mnoho súčasných kryptografických algoritmov, nemožno ho opomenúť.

DES pracuje so 64-bitovými reťazcami. Veľkosť kľúča je v podstate 56 bitov, niekde sa však udáva veľkosť 64 bitov, ale to z toho dôvodu, že pri 64 bitoch sa posledný bit v bajte, t.j. najnižší bit, dopočítava na nepárnu paritu. Zraniteľnosť algoritmu spočíva práve v dĺžke kľúča, keďže 56-bitový kľúč je veľmi krátky na dnešnú dobu. Už v roku 1998 bol zostrojený dešifrovací stroj, tzv. DES-Cracker, ktorý v súčasnosti dokáže šifru rozlúštiť v priebehu 22 hodín.

Algoritmus DES používa k šifrovaniu 16 cyklov, kde sa v každom cykle prevádzajú dve jednoduché operácie, najskôr substitúcia a následne permutácia. Substitúcia znamená nahradenie bitovej hodnoty inou hodnotou a permutácia značí zámenu poradia jednotlivých bitov v bloku. Tieto operácie sa aplikujú na dva 32-bitové bloky, ktoré vznikli rozdelením 64-bitového bloku a ktoré sa spoja až po ukončení 16. cyklu. Následne sa celý 64-bitový blok transformuje.

Šifru DES kvôli svojej zraniteľnosti spôsobenej krátkosťou kľúča vystriedal silnejší algoritmus 3DES. Už z názvu vyplýva, že 3DES využíva pri šifrovaní správy algoritmus DES, ktorý na danú správu aplikuje trikrát. Dĺžka kľúča môže byť dvakrát väčšia ako pri DES, čiže 112 bitov, alebo sa používa trojnásobne dlhý kľúč, teda 168 bitov. Pri 112-bitovej dĺžke kľúča je kľúč rozdelený na dve časti. Najskôr sú pôvodné dáta zašifrované prvou časťou kľúča, vzápätí na to sú dáta prešifrované druhou polovicou kľúča a do tretice sú dáta znova zašifrované prvou polovicou kľúča, tým nám vzniknú výsledné šifrované dáta. 3DES je pomerne pomalý algoritmus, ale možno o ňom povedať, že je bezpečný. [6]



Obr. 16. Aplikácia 3DES algoritmu [autor]

2.1.2.2 Blowfish

Šifra Blowfish bola publikovaná v roku 1993 B. Schneierom. Výhody tohto algoritmu spočívajú v jeho rýchlosti a jednoduchosti, navyše nie je patentovaný a tým pádom je voľne šíriteľný.

Blowfish používa k šifrovaniu bloky o veľkosti 64 bitov a 32-bitové podbloky. Dĺžka kľúča sa pohybuje od 32 do 448 bitov, najčastejšie sa však používa kľúč dlhý 128 bitov. Pred zahájením samotného procesu šifrovania je vytvorených 1042 polí o dĺžke 32 bitov. Šifruje sa postupne po jednotlivých krokoch, kde sa v každom kroku nahradí 64 bitov poľa, pre nahradenie celého poľa je potrebných 521 krokov, tie sú upravené podľa zadaného kľúča a šifrované algoritmom Blowfish. Šifrovanie textu prebieha po 64 bitoch prostredníctvom spomínaných polí, pričom algoritmus Blowfish je aplikovaný 18-krát. Pri šifrovaní sa používajú matematické operácie XOR a sčítanie 32-bitových slov. [6]

2.1.2.3 IDEA

IDEA (International Data Encryption Algorithm) v súčasnosti patrí medzi modernejšie šifry kryptografie, je založená na kombinovaní rôznych matematických operácií z oblasti algebry. Algoritmus bol navrhnutý tak, aby poskytoval efektívnu implementáciu v hardvéri a aj v softvéri. IDEA pozostáva z 8 zhodných cyklov, po ktorých nasleduje výsledná transformácia. Bloky, s ktorými šifra pracuje, majú veľkosť 64 bitov a podbloky sú veľké 16 bitov. Dĺžka kľúča je 128 bitov. Pre šifrovanie a dešifrovanie sa používa rovnaký algoritmus.

IDEA pracuje s tromi matematickými operáciami:

- Logickou funkciou XOR
- Modulárnym sčítaním 2^{16}
- Modulárnym násobením $2^{16} + 1$

Usporiadanie algoritmu je vymyslené tak, že výstup získaný z jednej matematickej operácie sa nikdy nepoužije ako vstup do matematickej operácie rovnakého typu. [6]

2.1.2.4 AES

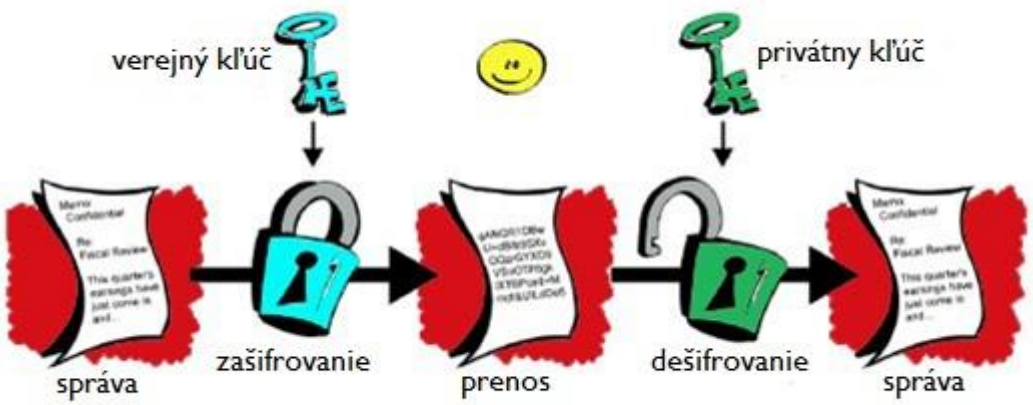
Po prelomení šifry DES hrubou silou v roku 1997, americký štandardizačný úrad vypísal výberové konanie na jej náhradu. Z piatich finálnych účastníkov vybrali algoritmus Rijndael, ktorého autormi sú Joan Daemen a Vincent Rijmen. Pod názvom AES bol schválený americkým národným úradom pre štandardizáciu v oficiálnej publikácii FIPS PUB 197. AES patrí medzi blokové šifry s 128-bitovým blokom, na porovnanie mali predošlé šifry blok s dĺžkou 64 bitov. Rozoznávame tri dĺžky kľúča 128, 192 a 256 bitov.

Šifra pracuje s 32-bitovými slovami, preto ak označíme dĺžku kľúča N_K ako počet 32-bitových slov, dostaneme $N_K = 4$, 6 a 8 pre už spomínanú dĺžku kľúča 128, 192 a 256 bitov. Počet iterácií (opakovaní) N_R sa mení v závislosti na dĺžke kľúča $N_R = N_K + 6$, vyjde nám 10, 12 alebo 14 iterácií. Algoritmus je založený na prvkoch Galoisovho telesa a na polynómoch, ktorých koeficienty sú prvky z Galoisovho telesa.

Vďaka veľkej dĺžke bloku a taktiež kľúča je šifra odolná proti útokom, ktorým neodolala šifra DES. Predpokladá sa, že AES bude platným šifrovacím štandardom niekoľko nasledujúcich desaťročí a bude mať enormný vplyv na počítačovú bezpečnosť. [15]

2.2 Asymetrické šifrovanie

Asymetrické šifrovanie, nazývané tiež šifrovanie verejným kľúčom, je založené na myšlienke, že každá komunikujúca strana má dva kľúče, jeden tzv. verejný kľúč, ktorý je prístupný všetkým, a jeden svoj vlastný, teda súkromný kľúč. Kľúče musia byť zvolené tak, aby odvodenie súkromného kľúča od kľúča verejného nebolo možné. Pri odosielaní správy týmto systémom odosielateľ zašifruje správu použitím príjemcovho verejného kľúča. Prijatú správu bude môcť dešifrovať iba príjemca pomocou svojho súkromného kľúča. Pretože je jediným vlastníkom svojho súkromného kľúča, správu nebude schopný nikto iný prečítať. Ak bude chcieť poslať odpoveď, tak ju zašifruje pomocou adresátovho verejného kľúča.



Obr. 17. Princíp asymetrického šifrovania [13]

Odosielateľ sa ale pred odoslaním musí najskôr uistiť, že verejný kľúč, ktorý použil, je správny a patrí danému príjemcovi. Nepovolaná tretia strana komunikácie môže totiž nahradiť príjemcov kľúč svojím a správu tak ľahko rozlúštiť. Riešenie takéhoto problému spočíva vo využití certifikačných autorít, tie uchovávajú zoznamy osôb a ich príslušných verejných kľúčov a navyše garantujú ich platnosť. Je potrebné si uvedomiť, že verejné kľúče sú prístupné úplne komukoľvek, a preto šifrovaný text nevypovedá nič o identite odosielateľa.

Pri použití asymetrickej kryptografie sú algoritmus a aj verejné kľúče dostupné úplne každému. Z toho vyplýva, že útočník vie, aký algoritmus bol použitý k zašifrovaniu dát. Šifrovací proces preto musí byť vybraný precízne, aby komunikujúce strany nijakým spôsobom neuľahčili rozlúštenie šifry útočníkovi. Dešifrovanie však musí byť zároveň pre príslušného príjemcu jednoduché, preto by mal byť algoritmus šifrovania postavený tak, aby bolo možné správu dešifrovať iba na základe súkromného kľúča. Tejto situácii zodpovedá jednoduchý a praktický príklad. Majme telefónny zoznam nejakého veľkého mesta, ktorého obsahom je niekoľko stotisíc telefónnych čísel. Bude veľmi jednoduché na základe mena a adresy zistiť telefónne číslo konkrétnej osoby, ale na druhej strane bude celkom komplikované zistiť na základe telefónneho čísla meno a adresu danej osoby.

Pri asymetrickom šifrovaní odpadá jeden veľký problém a tým je zdieľanie kľúčov, pretože súkromný kľúč vlastní každý majiteľ a verejný kľúč je sprístupnený každému užívateľovi. Nevýhodou je veľká náročnosť na matematické operácie a tým pádom aj na výkon počítača. Konkrétnymi príkladmi asymetrického šifrovania sú šifry RSA, DSA a ElGamal.

Najznámejším a najviac používaným algoritmom zo spomínaných troch algoritmov asymetrického šifrovanie je algoritmus RSA. [1], [5]

2.2.1 RSA

RSA možno označiť za najznámejšiu šifru asymetrických kryptografických systémov. Väčšina asymetrických kryptografických systémov v praxi pracuje so správou zloženou z veľkých celých čísel, kde bezpečnosť daného algoritmu spočíva v zložitosti riešenia matematických operácií, výnimkou nie je ani šifra RSA.

RSA vynašli v roku 1978 Ron Rivest, Adi Shamir a Len Adleman. Základom tejto jednosmernej šifry, ktorej jednosmernosť vychádza z jednoduchosti výpočtu jednosmernej funkcie a zároveň zo zložitosti získať späť jej pôvodnú hodnotu, je rozklad na prvočísla. Prvočísla sú čísla, ktoré nemajú iných deliteľov ako seba samých a čísla 1. Napr. číslo 11 je prvočíslo, pretože ho žiadne čísla s výnimkou čísel 1 a 11 nedelia bezo zvyšku.

Pre vytvorenie verejného šifrovacieho kľúča „*N*“, je potrebné zvoliť si dve prvočísla „*p*“ a „*q*“, napr. *p = 17 159* a *q = 10 247*. Vynásobením týchto prvočísel dostaneme výsledok *N = 175 828 273*. Ak chce odosielateľ poslať šifrovanú správu, nájde si príjemcov verejný kľúč *N*, v našom prípade hodnotu *175 828 273*, vloží ju do všeobecnej podoby jednosmernej funkcie a správu zašifruje. Jednosmerná funkcia je navrhnutá tak, aby dešifrovanie správy prebiehalo pomocou prvočísel *p* a *q*, ktorých vynásobením dostaneme hodnotu *N*. *N* je teda verejný kľúč, ktorého hodnota je verejne známa, zatiaľ čo *p* a *q* tvoria prijímateľov súkromný kľúč. Útočník, ktorý chce šifru rozlúštiť, pozná ako každý iný hodnotu čísla *N*, k tomuto číslu sa snaží nájsť hodnoty prvočísel *p* a *q* tak, že sa bude snažiť vypočítať, ktoré čísla mu po vynásobení dajú hodnotu *N*, tento proces sa nazýva faktorizácia a je veľmi časovo náročný.

Číslo *N* je teda potrebné voliť dostatočne veľké, aby ho útočník nedokázal rozložiť na prvočísla a tým správu rozlúštiť. Ak by bolo *N* príliš malé, napr. by malo hodnotu 15, tak by pre každého bolo veľmi jednoduché previesť rozklad čísla 15 na prvočísla o hodnotách 3 a 5. Naopak ak by číslo *N* bolo dostatočne veľké a obsahovalo by prvočísla v rádoch 10^{165} alebo väčšie, je hľadanie prvočísel dostatočne náročné.

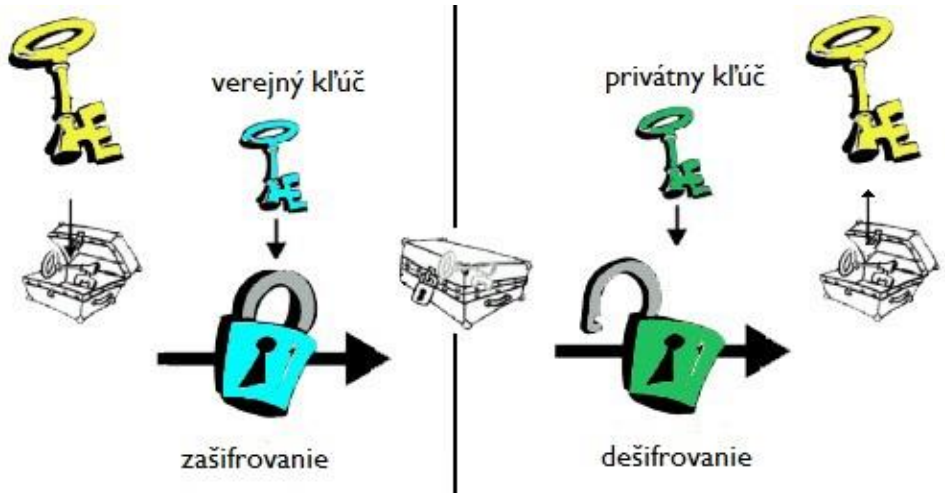
Hodnota N tak určuje veľkosť bloku aj kľúča, ktorá býva omnoho väčšia ako pri symetrických šifrách. Zatiaľ čo symetrické šifry majú klasickú veľkosť bloku 64 alebo 128

bitov, veľkosť bloku u RSA môže byť 640 bitov, 1024 bitov alebo dokonca až 2048 bitov. Keďže práca s algoritmom RSA zahŕňa veľké množstvo výpočtov s veľkými číslami, šifrovanie a dešifrovanie prebieha celkom pomaly. RSA sa teda priveľmi nepoužíva pre šifrovanie veľkých objemov dát, ale uplatnenie nachádza v práci s digitálnymi podpismi alebo v šifrovaní symetrických kľúčov. [1], [16]

2.3 Hybridné šifrovanie

Hybridné šifrovanie predstavuje kombináciu symetrického a asymetrického šifrovania. Asymetrické šifrovanie slúži pre prenos symetrického kľúča medzi obidvoma komunikujúcimi stranami, symetrický kľúč sa potom použije pre zašifrovanie konkrétnej správy pomocou symetrického algoritmu. Pri hybridnom šifrovaní sa využívajú výhody z obidvoch metód šifrovania, jedná sa o rýchlosť symetrického šifrovania a „použiteľnosť“ asymetrického šifrovania.

Odosielanie správy prebieha tak, že sa zvolí symetrický kľúč, ktorý odosielateľ zašifruje prostredníctvom verejného kľúča príjemcu a takto zašifrovaný kľúč mu pošle. Príjemca tak dostane asymetrickým algoritmom zašifrovaný symetrický kľúč, ktorý dešifruje vďaka svojmu súkromnému kľúču. Dešifrovaním získava samostatný symetrický kľúč, ktorý obaja účastníci komunikácie môžu použiť k šifrovaniu konkrétnej správy symetrickými algoritmami. Vďaka tomuto procesu zaniká problém distribúcie kľúča, ktorý je bežný pri symetrickom šifrovaní, a zároveň sa celý proces zrýchli, asymetrické šifrovanie je totiž pre dlhé správy veľmi pomalé. [13]



Obr. 18. Princíp hybridného šifrovania [13]

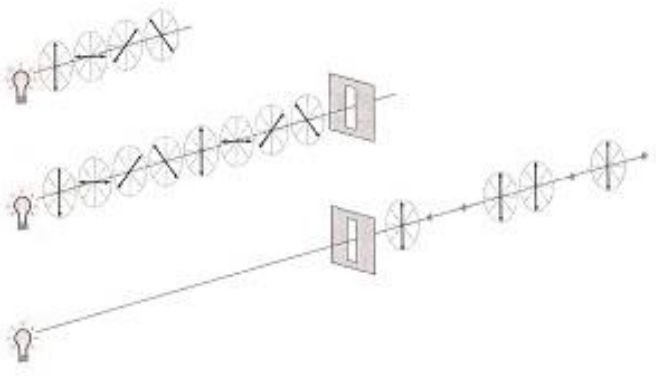
2.4 Kvantová kryptografia

Kvantovej kryptografii predchádzala myšlienka, ktorá sa zrodila v hlave študenta Kolumbijskej univerzity Stephena Wiesnera na konci 60. rokov 20. stor. Išlo o koncept kvantových bankoviek, ktoré by bolo úplne nemožné sfalšovať. Wiesnerove návrhy kvantových bankoviek nikdy neboli zrealizované kvôli tomu, že zatiaľ nebola vynájdená technológia umožňujúca zachytiť fotóny v určitom tvare na dostatočne dlhú dobu a aj keby taká technológia bola, bolo by príliš nákladné ju zaviesť. Wiesnerovej myšlienky sa chopil až jeho priateľ Charles Bennett, ktorý spolu s Gillesom Brassardom prišiel na to, že návrh kvantových peňazí je možné aplikovať na kryptografiu. [16]

Kvantová kryptografia sa nepoužíva na šifrovanie celého obsahu správy, ale rieši problém distribúcie šifrovacieho kľúča. Kľúč sa prenáša za pomoci kvantových stavov jednej častice, v tomto prípade fotónu. Ak sa niekto pokúsi odpočúvať komunikáciu, zmení sa stav častice a odpočúvanie bude odhalené. Kľúč, pri ktorom došlo k odhaleniu odpočúvania, sa jednoducho nepoužije. Z toho vyplýva, že kvantová kryptografia síce nedokáže zabrániť odpočúvaniu, ale dokáže hodnoverne zistiť, či k odpočúvaniu došlo.

Fungovanie kvantovej kryptografie si ukážeme na klasickej vzorovej situácii, kedy si chcú odosielateľ (označovaný ako Alica) s prijímateľom (typicky zvaný Bob) vymeniť kryptografický kľúč, avšak nepovolaná tretia osoba (Eva) chce ich tajný kľúč získať, aby mohla nerušene lúštiť ich ďalšiu šifrovanú komunikáciu. Binárny kľúč je tvorený náhodnou postupnosťou 0 a 1.

Pre názorný prenos kľúča sa používa usporiadanie lineárne polarizovaných fotónov. Je potrebné si uvedomiť, že keď fotón cestuje priestorom, tak vibruje. Uhol vibrácie je u každého fotónu iný aj za predpokladu, že fotóny letia rovnakým smerom. Spomínaný uhol vibrácie sa nazýva polarizácia fotónu. Pre zjednodušenie predpokladajme, že polarizácia fotónu sa môže vyskytovať iba v štyroch smeroch, a to: →, ↑, ↖, ↗. Ak fotónom umiestnime do cesty tzv. polarizačný filter orientovaný zvislo, tak ním prejdú všetky zvislo orientované fotóny, všetky vodorovne orientované fotóny budú zablokované a iba polovica uhlopriečne polarizovaných fotónov filtrom prejde a zmení sa na fotóny zvislé.

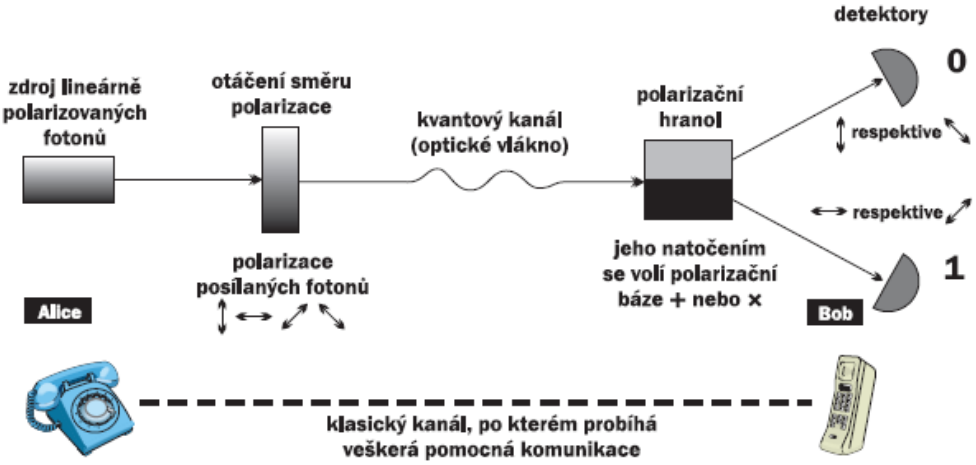


Obr. 19. Prechod polarizačných fotónov skrz zvislý filter [16]

Najskôr sa pred odosielaním správy odosielateľ a príjemca, teda Alica a Bob, dohodnú na dvoch na seba kolmých polarizačných schémach, ktoré budú používať. V prvej, tzv. rovnobežnej schéme, ktorá sa značí ako +, bude fotón s polarizáciou ↑ zastupovať 0 a fotón s polarizáciou → zastupovať 1. V druhej schéme, tzv. diagonálnej, ktorá sa znázorňuje ako ×, bude fotón s polarizáciou ↖ charakterizovať 0 a fotón s polarizáciou ↗ charakterizovať 1. Pri samotnom odosielaní správy Alica zvolí náhodnú postupnosť 0 a 1 a následne taktiež náhodne vyberie polarizačné schémy a podľa bitov charakterizovaných polarizačnými schémami otáča polarizáciu fotónov, ktoré posiela Bobovi, viď. tabuľka (Tab. 6).

Následne Bob nezávisle na Alici náhodne vyberie polarizačné bázy. Na základe týchto báz otáča svoj polarizačný filter, ktorý má na výstupe umiestnené dva detektory fotónov, jeden zodpovedá „0“ a druhý „1“. Niektoré fotóny majú tendenciu sa pri prenose stratiť, a tak ich detektor nie je schopný detekovať, nezostáva nič iné, iba tieto bity vynechať, viď. tabuľka (Tab. 7).

Nakoniec si Alica s Bobom prostredníctvom verejného kanálu povedia, aké polarizačné schémy použili a ponechajú si iba tie, v ktorých sa zhodli. Je potrebné si uvedomiť, že si prezradia iba polarizačné schémy, nie konkrétne natočenie fotónov, viď. tabuľka (Tab. 8).



Obr. 20. Princíp kvantovej kryptografie [17]

Ak chce Eva prenášaný kľúč zachytiť, musí zmerať polarizáciu fotónu prostredníctvom podobného zariadenia, aké používa Bob, a následne každý bit poslať Bobovi pomocou podobného zariadenia, aké používa Alica. Eva ale vôbec netuší, aké polarizačné schémy použila Alica a ak pre svoje meranie použije nesprávnu polarizačnú schému, vnesie do postupnosti bitov s určitou pravdepodobnosťou chybu. Napr. ak Eva natočí svoj polarizačný filter do tvaru + a zmeria prvý fotón polarizovaný do tvaru ↖, bude ho mylne považovať za fotón v tvare ↑ alebo → (je zrejmé, že 50% fotónov polarizovaných ↖ alebo ↗ prejde filtrom + a ich polarizácia sa zmení na zvislú ↑ alebo vodorovnú →, viď. obrázok (Obr. 19). Pokiaľ Eva určí polarizáciu fotónu v zvislom tvare, tak z jej hľadiska nastal úspech, pretože táto polarizácia taktiež predstavuje 0, naopak ak určí polarizáciu fotónu vo vodorovnom tvare, tak má problém, pretože symbol predstavuje 1. Eva má však iba jednu príležitosť k meraniu, pretože fotón je nedeliteľný a nemôže ho rozdeliť na dva rovnaké kusy a následne ho zmerať podľa oboch schém. Keďže Eva nemá možnosť porovnať si svoje polarizačné schémy s Alicou, nemôže si byť istá, či zachytila šifrovanú správu presne, a tým pádom nemá žiadnu nádej na jej dešifrovanie. Navyše ak Eva svojím meraním zmení polarizáciu fotónu ↖, ktorý vyslala Alica, na fotón v tvare ↑, Bob s Alicou by sa to pri kontrole bitov dozvedeli.

Kontrola prebieha tak, že Bob niektoré prenesené bity „obetuje“ a zverejní ich, aby si ich mohol spolu s Alicou porovnať a odhaliť tak prípadné rozdiely, ktoré by nastali pri odpočúvaní Evou. Obetované bity sa v danom kľúči nepoužijú, viď. tabuľka (Tab. 9)

Tab. 6. Kvantový prenos kryptografického kľúča - časť 1. Prenos na strane Alici [autor]

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Alicou náhodne zvolené bity														
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
Alicou náhodne zvolené polarizačné schémy														
↖	→	↗	↑	→	→	↑	↑	↗	↖	→	↗	↖	↖	→
Zodpovedajúce pootočenie polarizácie fotónov														

Tab. 7. Kvantový prenos kryptografického kľúča - časť 2. Kvantový prenos na strane Boba [autor]

+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
Bobom zvolené polarizačné schémy														
1		1		1	0	0	0		1	1	1		0	1
Detekované bity prijaté Bobom														

Tab. 8. Kvantový prenos kryptografického kľúča - časť 3. Verejná diskusia [autor]

+		×		+	×	×	+		+	×	×		×	+
Bob oznamuje schémy, v ktorých nameral fotóny														
		OK		OK			OK				OK		OK	OK
Zhoda zvolených schém														
		1		1			0				1		0	1
Prenesená postupnosť bitov														

Tab. 9. Kvantový prenos kryptografického kľúča - časť 4. Zisťovanie odpočúvania [autor]

				1									0	
Obetovanie bitov k odhaleniu Evy														
				OK									OK	
Potvrdenie obetovaných bitov Alicou														
		1					0				1			1
Zvyšné tajné bity zdieľané Alicou a Bobom - vygenerovaný kľúč														

Až v roku 1988 začal Bennett pracovať na konštrukcii prístroja, ktorý by umožňoval využitie kvantovej kryptografie v praxi. Na pomoc pre zostavenie prístroja si zamestnal aj študenta Johna Smollina. Až o rok neskôr sa pokúsili o prenos prvej správy zašifrovanej kvantovou kryptografiou. Po dlhom úsilí sa im podarilo poslať cez svetlotesnú miestnosť polarizované fotóny a potom ich zmerať pomocou + schémy a × schémy. Počítač zvaný Alica riadil vysielanie fotónov a počítač menom Bob vyhodnocoval každý jednotlivý fotón prostredníctvom polarizačných filtrov a detektorov. Následne Alica s Bobom prekonzultovali polarizačné schémy, ktoré sa zhodovali, vyradili fotóny, ktoré Bob zmeral nesprávnym polarizačným filtrom a dohodli sa na kľúči, ktorý sa skladal zo zostávajúcich fotónov.

Prenos fotónov na väčšie vzdialenosti ako je vzdialenosť jednej miestnosti je možný prostredníctvom optického vlákna. Ženevskí výskumníci v roku 1995 pomocou optického vlákna zostavili kvantovú kryptografiu na vzdialenosť 23 km, konkrétne týmto spôsobom spojili Ženevu s mestom Nyon. Neskôr skupina vedcov z Nového Mexika prišla na nápad vytvoriť systém kvantovej kryptografie, ktorý by mohol fotóny prenášať vzduchom prostredníctvom satelitov. Zatiaľ sa im podarilo preniesť kľúč prostredníctvom satelitov iba na vzdialenosť 1 km. Ak by sa však v blízkej budúcnosti podarilo zostaviť systémy kvantovej kryptografie, ktoré by fungovali na veľké vzdialenosti, vývoj v jednej oblasti šifier by sa zavŕšil a hľadanie súkromia by sa priblížilo k svojmu cieľu. [16], [17]

2.5 Hash algoritmy

Okrem symetrického a asymetrického šifrovania existuje ešte oblasť kryptografie, kde chceme dáta iba zašifrovať, ale už nikdy dešifrovať späť. Spomínanou vlastnosťou sa vyznačujú tzv. hash funkcie.

Hash možno charakterizovať aj ako miniatúrny odtlačok správy. Vzniká funkciou zvanou hashovanie, ktorej výhoda tkvie v tom, že zo zadaného veľkého množstva dát vracia omnoho menšiu veľkosť dát a to bez zmeny obsahu danej správy. Pri malej zmene správy na vstupe musí nastať veľká zmena hodnoty hashu na výstupe. Pri využití hash funkcie v kryptografii je dôležité, aby bola táto funkcia jednosmerná. Ak je známa hodnota hashu a tiež je známy pôvodný dokument, z ktorého bol hash vytvorený, je dôležité, aby bolo náročné vytvoriť iný dokument s rovnakou hashovacou hodnotou. Z uvedeného vyplývajú dôležité vlastnosti hash algoritmu:

- pre zhodné vstupné dáta musí byť výsledok hashu vždy rovnaký,
- hash funkcia musí byť jednosmerná, teda musí byť úplne nemožné z hashovej hodnoty odvodiť hodnotu pôvodnej správy,
- pri funkcii hash nesmie dochádzať ku kolízii, tzn. dva rôzne vstupné údaje nesmú dať rovnaký výsledok hash.

Hash algoritmy majú v kryptografii hneď niekoľko využití. Používajú sa napr. pri uložení hesiel do systému. Užívateľ zadá nové heslo do systému, napr. „heslo006“, pomocou algoritmu sa toto heslo zašifruje na nejakú nečitateľnú hodnotu, napr. „w.*3_2q“, ktorá sa uloží do systému. Keďže je algoritmus šifrovania stále rovnaký, to isté zadané heslo sa vždy zašifruje na rovnakú hodnotu. Potom stačí, ak si užívateľ zapamätá heslo, ktoré zadával do systému, tj. „heslo006“. Po zadaní tohto hesla systém daný vstup zašifruje a vyjde mu rovnaký výsledok ako ten, ktorý si uložil, teda „w.*3_2q“. Výhodou uloženia hesiel do systému pomocou algoritmu hash je, že systém nemusí poznať heslo užívateľa, ale stačí poznať iba jeho zašifrovanú hodnotu. Minimálna dĺžka hash funkcie je 64 bitov a táto dĺžka úplne postačuje, lebo systém nechráni heslá iba pomocou hash algoritmov, ale aj prístupovými právami k súboru s uloženými heslami. Odporučeným štandardom je dĺžka 160 bitov, ktorá sa používa aj pre digitálne podpisy.

Ďalšie využitie hash algoritmov spočíva v porovnávaní textov, pri ktorom sa snažíme zistiť, či je daný text pôvodný. Zjednodušene povedané, pomocou hash algoritmu dokážeme otestovať integritu textu. S veľmi vysokou pravdepodobnosťou sa totiž môžeme spoľahnúť na to, že ak majú dve správy rovnaký hash, sú rovnaké. Integrita dát sa zisťuje napr. pri prenose a to tak, že pred prenosom sa spočíta hash, po prenose taktiež a ak sa hashe po porovnaní rovnajú, tak sa dáta preniesli správne.

Keď chceme overiť autenticitu dát, tzn. informáciu o autorovi textu, pridáme pred výpočtom hashu vygenerované tajné dáta. Tým sa hovorí kľúč, soľ alebo heslo. Soľ sa pridáva na začiatok, do prostriedku alebo na koniec dát. Nevytvára sa tak odtlačok samotných dát, ale dát „osolených“. Vygenerované tajné dáta sa môžu pridávať aj prostredníctvom algoritmov, ktoré pracujú tak, že pripoja k vstupným dátam zadaným prostredníctvom užívateľa heslo a až takto zaheslované dáta použijú ako vstup hash funkcie. Takéto algoritmy sa nazývajú MAC (Message Authenticity Code) a špeciálnym príkladom tohto typu algoritmov je HMAC (Hash Message Authenticity Code), kde sa k

vstupným dátam pridá heslo zašifrované pomocou hash funkcie a výsledok sa ešte raz zahashuje. Tento princíp sa používa napr. v protokole IPsec pre overenie celistvosti a pôvodu bloku dát.

Medzi najstaršie hashovacie algoritmy sa zaraďuje algoritmus MD5. Vymyslel ho v roku 1991 Ron Rivest. Keďže sa pred niekoľkými rokmi objavili možnosti získania kolíznych dokumentov, v súčasnosti sa MD5 nepovažuje za bezpečný hashovací algoritmus. Pri tomto druhu algoritmu je možné získať aj časti hesiel prostredníctvom tzv. rainbow tables, čo sú tabuľky, v ktorých sa nachádzajú rôzne kombinácie hesiel s ich odtlačkami. [6]

SHA-1 predstavuje novší algoritmus. Je síce založený na princípe MD5, ale je dlhší, jeho dĺžka predstavuje 160 bitov, zatiaľ čo MD5 má dĺžku iba 128 bitov. Nie je znevážený takým spôsobom ako algoritmus MD5, ale je iba otázkou času, kedy jeho prelomenie nastane.

Obr. 21. Využitie hash algoritmu SHA-1 [autor]

V súčasnej dobe je v oblasti hashových algoritmov najlepší SHA-2. Spomínaný algoritmus sa vyskytuje v dvoch možných variantoch: SHA-256 a SHA-512, kde číslo za pomlčkou predstavuje dĺžku odtlačku v bitoch. Algoritmy SHA-2 sú opäť založené na podobných princípoch ako MD5 a SHA-1, ale sú o ešte niečo väčšie a dlhšie. V súčasnosti sú tieto algoritmy považované za celkom bezpečné.

Pre výber hashovacích algoritmov sa vyhlasujú verejné súťaže. Posledná takáto súťaž sa konala 2. 9. 2012, kedy bol americkým Národným inštitútom pre štandardy a technológie (NIST) vyhlásený víťaz súťaže algoritmus SHA-3. Tento algoritmus už nie je založený na

obdobných princípoch ako predchádzajúce algoritmy, ale pre svoju novotu nie je doposiaľ implementovaný v bežných kryptografických systémoch. [18]

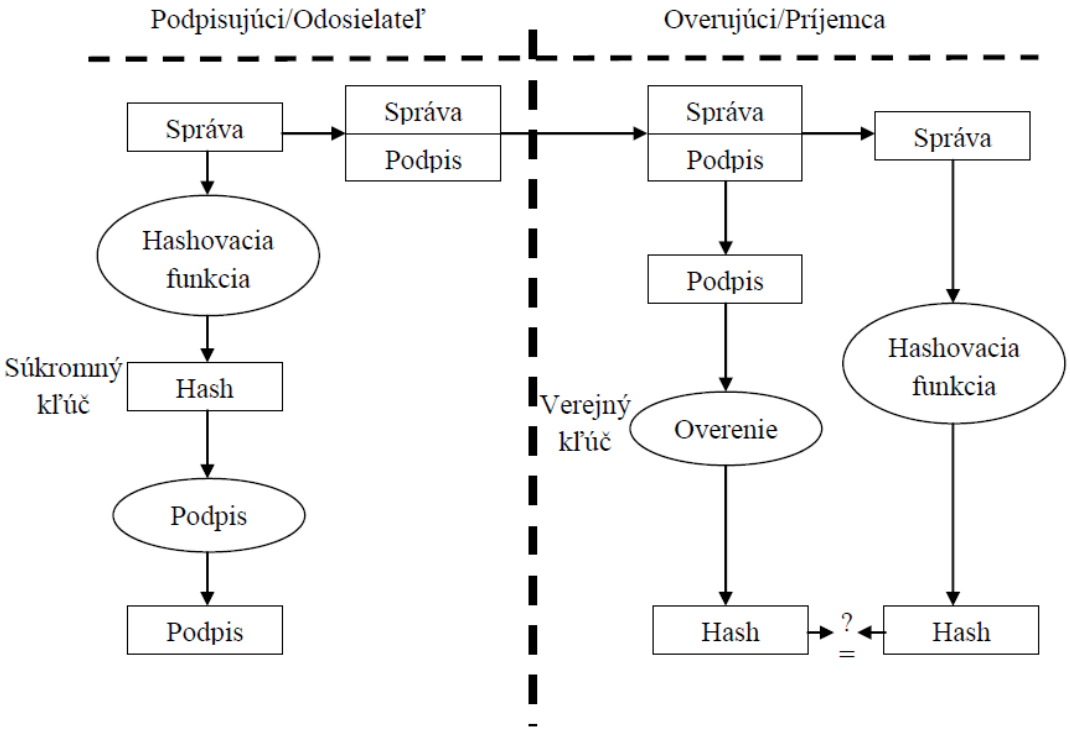
2.6 Elektronický podpis

Elektronický podpis správy má rovnakú funkciu ako klasický podpis s tým rozdielom, že sa ním podpisujú elektronické dáta. Elektronický podpis je ale výhodnejší v tom, že zaisťuje integritu dát a zároveň identifikuje odosielateľa správy príjemcovi. Jedná sa o kryptografický reťazec, ktorého hodnota vyplýva z obsahu správy a od samotného odosielateľa.

Elektronické podpisy využívajú pre svoje účely asymetrické algoritmy, ako napr. RSA algoritmus alebo El Gamal. Z podkapitoly o asymetrickom šifrovaní sme sa dozvedeli, že verejný kľúč slúži k šifrovaniu a súkromný kľúč k dešifrovaniu správ. Avšak tento proces je uplatniteľný aj naopak, čiže súkromný kľúč sa použije k šifrovaniu správ, zatiaľ čo verejný kľúč je použiteľný pre dešifrovanie správ. Spomenutý proces šifrovania neposkytuje žiadnu bezpečnosť, no na druhej strane umožňuje overiť autorstvo. Z uvedeného vyplýva, že každý užívateľ má svoj vlastný súkromný kľúč, ktorý môže používať jedine on sám a použitie tohto kľúča jednoznačne identifikuje užívateľa. Pochopiteľne u každého užívateľa existuje ešte zodpovedajúci verejný kľúč. Verejný kľúč pozná každý a prostredníctvom neho je možné si overiť, či bol použitý zodpovedajúci súkromný kľúč, ktorého podobu je nemožné zistiť. Práve informácia o použití súkromného kľúča dáva príjemcovi možnosť preveriť pôvod správy a tiež neporušiteľnosť správy, resp. dát. Zároveň u odosielateľa dochádza k odbúraniu obavy, že by jeho súkromný podpisový kľúč eventuálne niekto napodobnil prostredníctvom kľúča verejného, resp. overovacieho.

Samotné spracovanie asymetrického šifrovania, ktoré je používané pri elektronickom podpisovaní, je náročné na výpočtovú kapacitu. V tejto situácii prichádza na pomoc hashová funkcia, vďaka ktorej sa obsah správy upraví do skrátenej hashovej podoby. Následne sa zo zahashovanej správy pomocou súkromného kľúča vytvorí podpis, ktorý sa pripojí k pôvodnej správe a takto sa odošle príjemcovi. Príjemca si overí podpis a vzápätí aj prijatú správu. Podpis si overí pomocou asymetrického verejného kľúča, kde výsledkom overenia by mala byť hodnota zahashovanej správy. Napokon na pôvodnú správu aplikuje hashovaciu funkciu, ktorej výsledkom je hash. Ak sa hash zhoduje s hodnotou

zahashovanej správy, je zrejmé, že podpis je pravý a dokument nebol pri prenose zmenený, naopak, ak sa nezhoduje, je podpis falošný alebo bol dokument pri prenose zmenený.



Obr. 22. Princíp elektronického podpisu [1]

So slovným spojením elektronický podpis sa viaže termín digitálny podpis. Digitálny podpis je v podstate typický elektronický podpis, ku ktorému sa ešte navyše pripája tzv. digitálny certifikát zaisťujúci identitu odosielateľa. Tým je vlastne zabezpečené zviazanie podpisu s konkrétnou osobou. V systéme verejných kľúčov totiž môže nastať situácia, kedy sa nejaká konkrétna osoba bude vydávať za niekoho iného. Predpokladajme existenciu dvoch užívateľov, užívateľa A a užívateľa B. Užívateľ A sa pokúsi obísť systém tým, že vydáva svoj súkromný kľúč za súkromný kľúč užívateľa B. V takejto situácii by všetci ostatní používali verejný kľúč používateľa A k zašifrovaniu správ, ktoré majú byť adresované užívateľovi B. Zašifrovanú správu by potom prijal používateľ A a nie používateľ B. Navyše by mohol užívateľ A podpisovať svojím súkromným kľúčom správy, o ktorých by si ostatní mysleli, že ich podpísal a zároveň vytvoril užívateľ B. Takýmto útokom by sa malo predchádzať pomocou využívania certifikačných autorít a zavedením infraštruktúry verejných kľúčov (Public Key Infrastructures, PKI). [1]

Infraštruktúra verejného kľúča slúži k tomu, aby každý odosielateľ nemusel svoj vlastný verejný kľúč doručovať zvlášť každej osobe, s ktorou chce komunikovať. V tejto

infraštruktúre sú zahrnuté aj osoby používajúce elektronický podpis, certifikačné autority (CA) a registračné autority (RA). Certifikačné autority vydávajú a spravujú digitálne certifikáty. Registračná autorita plní úlohy spojené s prevzatím verejného kľúča od svojich klientov, overovaním zhody osobných údajov klientov, posielaním žiadostí certifikačnej autority o vydanie certifikátu verejného kľúča, odovzdaním klientskeho certifikátu a odovzdaním certifikátu verejného kľúča klientom. Certifikát obsahuje identifikačné údaje o vlastníkovi verejného kľúča, verejný kľúč, údaje o CA, ktorá certifikát vydala, informáciu o dobe platnosti certifikátu a napokon elektronický podpis certifikátu vytvorený pomocou tajného kľúča CA. [19]

2.7 Eliptické krivky

Kryptografia založená na eliptických krivkách (Elliptic Curve Cryptography, ECC) je moderný trend v oblasti asymetrickej kryptografie, ktorý v mnohých smeroch prináša lepšie výsledky ako ostatné nesymetrické algoritmy. Využitie eliptických kriviek v oblasti kryptografie sa prvýkrát vyskytlo v roku 1985 a navrhli ho nezávisle od seba Victor Miller a Neal Koblitz.

Ako je už spomenuté, jedná sa o oblasť asymetrickej kryptografie, a teda ide o analógiu systémov s verejným kľúčom, kde sa využíva aritmetika založená na operácii s bodmi na eliptickej krivke. Pri práci s algoritmami definovanými nad eliptickou krivkou sa hierarchicky zvolia dva typy algebraických štruktúr, konečné teleso a eliptická krivka, ktorá reprezentuje skupinu bodov, nad ktorou je vlastný asymetrický algoritmus definovaný. Na voľbe obidvoch týchto algebraických štruktúr výrazne závisí bezpečnosť a efektívnosť kryptosystému. Spomínané štruktúry spolu úzko súvisia.

Základ bezpečnosti eliptických algoritmov tkvie v náročnosti riešenia úlohy diskrétneho logaritmu pre eliptické krivky. Táto úloha má v súčasnosti omnoho zložitejšie riešenie ako úloha klasického diskrétneho logaritmu. Pre tento typ algoritmov nie sú známe žiadne subexponenciálne algoritmy, najlepšie algoritmy majú úplne exponenciálny charakter. Algoritmy založené na eliptických krivkách umožňujú konštruovať omnoho kratšiu dĺžku kľúčov ako asymetrické algoritmy a to aj pri zachovaní rovnakej úrovne bezpečnosti. Táto skutočnosť je výhodná hlavne pre implementáciu algoritmov s menšími nárokmi na pamäť, ďalšia výhoda spočíva vo výrazne väčšej rýchlosti eliptických kryptosystémov. Aj napriek všetkým týmto výhodám sa eliptické krivky zaraďujú k veľmi mladým kryptosystémom na

rozdiel od RSA alebo DSA a z dôvodu nedostatočného štúdia tejto problematiky v minulých desaťročiach sú tieto staršie kryptosystémy stále preferované. [20]

Tab. 10. Porovnanie dĺžky kľúčov rôznych kryptosystémov [20]

Blokové šifry	RSA/DL	Eliptické krivky
56	417	105
64	682	120
80	1464	149
86	1881	161
...	...	...
109	4047	206

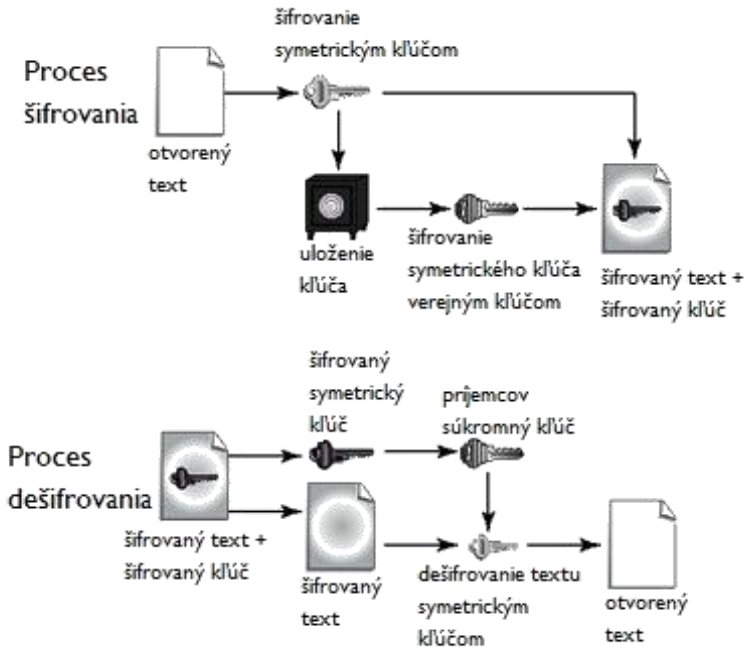
2.8 Šifrovací program PGP

Philip Zimmermann bol presvedčený, že každý človek má právo na také súkromie, aké poskytuje RSA algoritmus, a tak vďaka jeho znalostiam z počítačovej sféry vytvoril lacný a výkonný program, ktorý fungoval aj na obvyklom osobnom počítači. Tento program, ktorý je vhodný aj pre bežného používateľa bez znalostí kryptografie, nazval „Celkom dobré súkromie“ (Pretty Good Privacy, PGP).

Koncom 80. rokov 20. stor. sa Zimmermann pustil do spracovania svojho programu a postupne skompletizoval balíček šifrovacieho softwaru. Šifrovanie a následné dešifrovanie správ šifrou RSA vyžaduje množstvo matematických operácií a teda proces šifrovania a dešifrovania dlhšej správy môže na osobnom počítači trvať aj niekoľko minút. Ak chce však odosielateľ posielať denne 100 správ, nemôže si dovoliť stráviť pri odosielaní každej správy niekoľko minút, preto sa Philip Zimmerman predovšetkým zaoberal zrýchlením kryptografického procesu. Zrýchlenie procesu vymyslel tak, že spojil asymetrické šifrovanie RSA so starším symetrickým šifrovaním. Klasické symetrické šifrovanie je totiž rovnako bezpečné ako asymetrické, a dokonca je omnoho rýchlejšie na prevedenie, trpí však problémom distribúcie kľúčov. Problém distribúcie kľúčov sa odstráni pomocou šifry RSA, ktorú je možné použiť k zašifrovaniu symetrického kľúča.

Uskutočnenie šifrovania pomocou softvéru PGP funguje tak, že odosielateľ najskôr zašifruje správu prostredníctvom symetrickej šifry IDEA (viď. podkapitola 2.1 Symetrické šifrovanie). Lenže k šifrovaniu pomocou algoritmu IDEA je potrebné zvoliť kľúč, aby

mohol príjemca správu dešifrovať. Pre distribúciu tohto kľúča si odosielateľ vyhľadá príjemcov verejný kľúč pre RSA, ktorý použije pre zašifrovanie kľúča k šifre IDEA. Takže príjemca tak od odosielateľa prijme samotnú zašifrovanú správu šifrou IDEA a ešte aj kľúč k tejto správe zašifrovaný pomocou asymetrickej šifry RSA. Úlohou príjemcu je potom použiť svoj súkromný kľúč RSA k dešifrovaniu kľúča a napokon týmto kľúčom dešifruje vlastnú správu. Tým sa vyriešil problém s rýchlosťou, pretože správa, ktorá môže obsahovať veľké množstvo informácií, je zašifrovaná rýchlou symetrickou šifrou IDEA a pomalý algoritmus RSA sa použije na zašifrovanie symetrického kľúča, ktorý pozostáva z omnoho menšieho množstva informácií ako obsahuje posielaná správa.



Obr. 23. Šifrovací systém PGP [21]

Po vyriešení situácie s rýchlosťou Zimmermann zaradil do PGP ešte mnoho ďalších užitočných vlastností, medzi ktoré patrí aj generovanie kľúčov. Pred použitím algoritmu RSA musí odosielateľ vytvoriť dvojicu kľúčov, jeden súkromný a k nemu prislúchajúci verejný kľúč. Vytváranie kľúčov je celkom zložitá záležitosť, pretože vyžaduje vyhľadanie dvojice obrovských prvočísel. Jednoduchým pohybom myši sa program pustí do práce a vygeneruje dvojicu súkromného a verejného kľúča používateľa. Pohybom myši sa vloží do procesu náhodný faktor, ktorý program potrebuje na zaistenie toho, aby mal každý užívateľ svoju vlastnú dvojicu prvočísel a z toho plynúci svoj vlastný jedinečný súkromný a verejný kľúč. Konkrétny používateľ potom len svoj verejný kľúč zverejní.

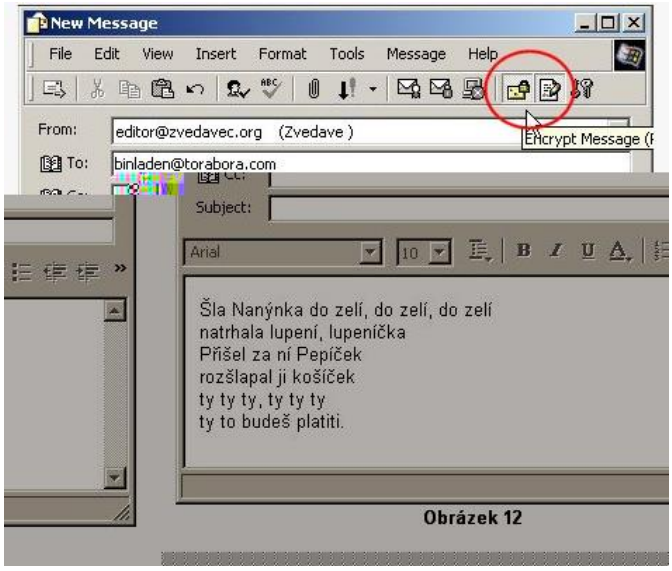
PGP je možné aplikovať aj na digitálny podpis e-mailov. Klasický e-mail neobsahuje žiadny podpis, a preto je úplne nemožné overiť pravého autora elektronickej správy. Digitálny podpis je už síce spomínaný v podkapitole o elektronickom podpise, ale pripomeňme si ešte jeho dôležitosť na konkrétnom príklade. Banka prijme od svojho klienta e-mail, v ktorom dáva príkaz, že sa majú všetky jeho peniaze previesť na iný súkromný účet. A tu nastáva problém v pochybnosti banky, či je prijatý e-mail skutočne od konkrétneho klienta. E-mail totiž mohol byť napísaný zločincom, ktorý si chce cudzie peniaze previesť na svoj vlastný účet. Ak chce teda odosielateľ poslať správu príjemcovi, musí si uvedomiť možnosti, ktoré sa mu naskytujú - buď chce zašifrovať správu verejným kľúčom, aby zaistil súkromie, alebo ju zašifruje vlastným súkromným kľúčom, čím zaručí jej autorstvo. Najlepším východiskom je použitie obidvoch možností. Čiže odosielateľ najskôr zašifruje správu svojím súkromným kľúčom, tento úkon predstavuje odosielateľov podpis, a potom takto zašifrovanú správu opäť zašifruje, ale tentokrát prostredníctvom príjemcovho verejného kľúča. Po prijatí správy príjemca najskôr rozlúšti pomocou svojho súkromného kľúča obsah správy a nakoniec za pomoci použitia verejného kľúča odosielateľa si príjemca overí autorstvo správy, či správa nepochádza od podvodníka.

Zimmermann vyvinul svoj projekt do podoby, kde sú všetky vyššie spomínané úkony zahrnuté v jednom programe PGP a dejú sa automaticky. Vďaka tomu nie je potrebné, aby používatelia programu disponovali zložitými znalosťami matematiky. Pri použití PGP sa najskôr k zašifrovaniu pôvodnej správy použije šifra IDEA, nasleduje použitie šifry RSA pre zašifrovanie súkromného kľúča a napokon sa do správy vloží digitálny podpis. V praxi to funguje nasledovne. Ak chce odosielateľ poslať správu, napíše svoj e-mail a vyberie voľbu PGP z menu počítača. Po uvedení mena príjemcu do programu, PGP vyhľadá verejný kľúč príjemcu a automaticky správu zašifruje. Zároveň prevedie všetky potrebné činnosti spojené s digitálnym podpisom správy. Pri prijatí správy príjemca vyberie voľbu PGP, následne program dešifruje správu a napokon overí autora.

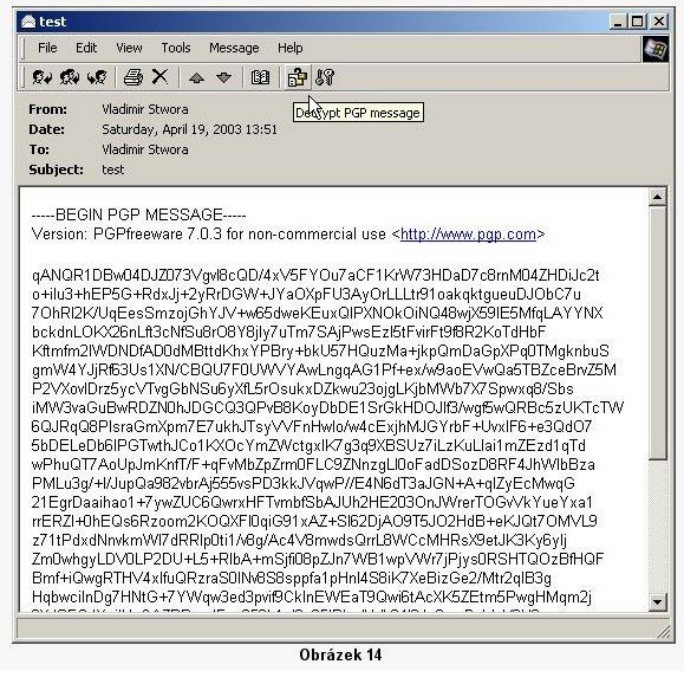
V roku 1991 Zimmermann poprosil svojho priateľa, aby PGP umiestnil na internet, kde si mohol každý tento softvér stiahnuť zdarma. Zimmermann sa tým postavil pred dva zásadné problémy. Prvým problémom bolo, že algoritmus RSA, ktorý je vlastne jadrom celého programu, je patentovaný produkt. Na základe patentového zákona by musel Zimmermann získať licenciu od RSA Data Security, Inc. Tento problém však ignoroval a dúfal, že mu dá spoločnosť povolenie zadarmo, lebo podľa jeho mienky nekonkuruje RSA Data Security,

Inc. Vážnejším problémom však bolo to, že Zimmermann musel čeliť vyšetrovaniu colných úradov USA, ktoré sa snažili dokázať, že zverejnením algoritmu umožnil šírenie PGP do celého sveta a tým porušil vývozné predpisy Spojených štátov.

Až v roku 1996 úrad amerického generálneho prokurátora stiahol žalobu, a zároveň sa Zimmermann dohodol s RSA a získal povolenie, ktoré odstránilo problém s patentom. Program PGP sa stal legitímnym produktom a Zimmermann bol od obvinenia oslobodený. V súčasnosti je ešte stále možné si stiahnuť softvér PGP z internetu zdarma. [16]



Obr. 24. Pôvodný obsah emailu pre adresáta [22]



Obr. 25. Zašifrovaný obsah textu pre adresáta [22]

3 LEGISLATÍVA ČR SPOJENÁ S KRYPTOGRAFIOU

Kryptografickou ochranou sa v ČR zaoberá zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v jeho druhej časti s názvom Ochrana utajovaných informací, a to predovšetkým v Hlave VIII, a vyhláška č. 432/2011 Sb. o zajištění kryptografické ochrany utajovaných informací.

V ČR existuje legislatíva, ktorá sa venuje aj certifikácii kryptografických prostriedkov a kryptografických pracovísk. Túto oblasť certifikácie upravuje Hlava IX druhej časti uvedeného zákon č. 412/2005 Sb. a vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.

3.1 Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

Tento zákon bol prijatý dňa 21. 9. 2005 s účinnosťou od 1. 1. 2006. Podľa § 2 písm. a) tohto zákona je utajovanou informáciou „informácia v akejkoľvek podobe zaznamenaná na akomkoľvek nosiči označená v súlade s týmto zákonom, ktorej vyzradenie alebo zneužitie môže spôsobiť ujmu záujmu Českej republiky alebo môže byť pre tento záujem nevýhodné, a ktorá je uvedená v zoznamu utajovaných informácií“. Z uvedeného vyplýva, že utajované informácie sa musia chrániť pred nepovolanými osobami. Ustanovenie § 5 zákona pojednáva o druhoch zaistenia ochrany utajovaných informácií, medzi ktoré patrí aj kryptografická ochrana. Okrem nej môže byť ochrana utajovaných informácií zaistená aj prostredníctvom personálnej bezpečnosti, priemyselnej bezpečnosti, administratívnej bezpečnosti, fyzickej bezpečnosti a bezpečnosti informačných alebo komunikačných systémov. Podľa § 5 písm. f) tohto zákona kryptografickú ochranu tvorí „systém opatrení na ochranu utajovaných informácií použitím kryptografických metód a kryptografických materiálov pri spracovaní, prenose alebo ukladaní utajovaných informácií“.

V zákone sa ešte spomína, že kryptografické prostriedky sú zahrnuté v tzv. komunikačnom systéme, ktorý nakladá s utajovanými informáciami a zaisťuje prenos utajovaných informácií medzi koncovými používateľmi. Tento komunikačný systém zahŕňa okrem kryptografických prostriedkov aj koncové komunikačné zariadenia, prenosové prostredie, obsluhu a prevádzkové podmienky a postupy. Kryptografická ochrana sa využíva aj na ochranu pri prenose taktickej informácie. Pojem taktická informácia sa na základe tohto

zákona chápe ako utajovaná informácia, ktorá sa vyznačuje krátkou dobou trvania dôvodu utajenia.

Poverenie fyzickej osoby na výkon kryptografickej ochrany je povinnosťou zodpovednej osoby. Zo zákona taktiež vyplývajú povinnosti orgánu štátu, právnických osôb a podnikajúcich fyzických osôb, ktoré majú prístup k utajovanej informácii. Ich povinnosťou je používať len certifikovaný prostriedok pre kryptografickú ochranu a využívať kryptografické pracovisko na účely, na ktoré bolo certifikáciou určené.

Národní bezpečnostní úřad (NBÚ) zaisťuje činnosť Národního střediska pro distribuci kryptografického materiálu, prevádza certifikáciu kryptografického prostriedku, kryptografického pracoviska a tieniacej komory. Ďalej zaisťuje výskum, vývoj a výrobu národných kryptografických prostriedkov, vyvíja a schvaľuje národné šifrové algoritmy, vytvára národnú politiku kryptografickej ochrany a okrem toho disponuje ešte mnohými ďalšími oprávneniami. [23]

3.1.1 Hlava VIII - Kryptografická ochrana

V zákone č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti je v jeho druhej časti kryptografickej ochrane venovaná celá Hlava VIII, ktorá je ohraničená ustanoveniami § 37 - § 45.

Ustanovenie § 37 definuje kryptografický materiál nasledovne: „Kryptografickým materiálom je kryptografický prostriedok, materiál k zaisteniu jeho funkcie alebo kryptografický dokument“. Ďalej toto ustanovenie hovorí o nutnosti certifikácie kryptografických prostriedkov, ktoré sa používajú pre kryptografickú ochranu utajovaných informácií. Certifikácia by mala byť vykonávaná prostredníctvom NBÚ. Odsek 3 tohto ustanovenia definuje kryptografické pracovisko: „Kryptografickým pracoviskom je pracovisko určené na výrobu alebo testovanie materiálu na zaistenie funkcie kryptografického prostriedku, ukladanie kryptografického materiálu alebo na distribúciu a evidenciu kryptografického materiálu alebo na výrobu a testovanie kryptografických prostriedkov“. Ďalej uvádza skutočnosť, že je nutné, aby kryptografické pracovisko spĺňalo bezpečnostné štandardy a že musí byť schválené bezpečnostným riaditeľom alebo inou zodpovednou osobou ešte pred jeho samotným uvedením do prevádzky. Kryptografické pracovisko musí byť ešte pred schválením do prevádzky bezpečnostným riaditeľom alebo zodpovednou osobou certifikované NBÚ. Znenie § 37 tiež ustanovuje, že orgán štátu alebo

osoby vykonávajúce kryptografickú ochranu sú povinné viesť evidenciu kryptografického materiálu, pracovníkov kryptografickej ochrany, prevádzkovej obsluhy kryptografických prostriedkov a kuriérov kryptografického materiálu.

Ustanovenie § 37a pojednáva o kontrolovanej kryptografickej položke, ktorou sa rozumie neutajované zariadenie alebo súčasť tohto zariadenia, ktoré slúži na ochranu informácií pri ich spracovaní alebo prenose a ktoré využíva kryptografické metódy. Na základe žiadosti NBÚ kontrolovanú kryptografickú položku schváli a zaradí ju do zoznamu kontrolovaných kryptografických položiek, pokiaľ je to v súlade so zámermi ČR v oblasti zaisťovania ochrany utajovaných informácií.

Znenie § 38 popisuje výkon kryptografickej ochrany. Za výkon kryptografickej ochrany možno považovať bezpečnostnú správu kryptografickej ochrany, obsluhu kryptografického prostriedku a napokon výrobu kryptografického prostriedku alebo materiálu. Pracovník kryptografickej ochrany prevádza výkon kryptografickej ochrany. Pracovník musí byť k výkonu poverený zodpovednou osobou alebo osobou ňou poverenou, musí vlastniť platné osvedčenie fyzickej osoby a musí mať osvedčenie o špeciálnej odbornej spôsobilosti pracovníka kryptografickej ochrany.

Ustanovenie § 39 pojednáva o špeciálnej odbornej spôsobilosti pracovníka kryptografickej ochrany a skúške špeciálnej odbornej spôsobilosti. Pracovník kryptografickej ochrany musí byť znalý predpisov z oblasti kryptografickej ochrany utajovaných informácií a musí byť schopný ich aplikovať. Jeho znalosti a schopnosti overuje NBÚ prostredníctvom skúšky odbornej spôsobilosti.

Prevádzkovou obsluhou kryptografického prostriedku sa zaoberá ustanovenie § 40. „Prevádzkovou obsluhou kryptografického prostriedku sa rozumie výkon užívateľských funkcií kryptografického prostriedku.“ Osoba, ktorá takúto obsluhu prevádza, musí k nej byť poverená zodpovednou osobou, musí spĺňať podmienky prístupu k utajovanej informácii a musí byť k takejto obsluhe zaškolená.

Znenie § 41 popisuje manipuláciu s kryptografickým materiálom a kontrolovanou kryptografickou položkou. Manipuláciou s kryptografickým materiálom sa rozumie „spôsob prenášania, prepravy, zapožičiavania, ukladania alebo iného nakladania s ním, vrátane jeho vyraďovania“. Manipulácia a evidencia kryptografického materiálu musí byť vykonávaná takým spôsobom, ktorý zaručuje jeho ochranu.

Nasledujúce ustanovenie sa zaoberá prepravou kryptografického materiálu a vývozom kryptografického prostriedku. Prepravu kryptografického materiálu zabezpečuje kuriér kryptografického materiálu, ktorý musí byť k preprave poverený zodpovednou osobou, musí byť držiteľom platného osvedčenia fyzickej osoby a musí byť zaškolený k preprave. NBÚ vydáva povolenie na vývoz certifikovaného kryptografického prostriedku z územia ČR. Toto povolenie sa vydáva na základe písomnej žiadosti, kde je uvedený vývoz konkrétneho kryptografického prostriedku a účel jeho vývozu.

Znenie § 43 hovorí o kompromitácii kryptografického materiálu, ktorou sa rozumie „nakladanie s kryptografickým materiálom, ktoré spôsobilo alebo mi mohlo spôsobiť porušenie ochrany utajovanej informácie“. Kompromitácia kryptografického materiálu musí byť bezodkladne oznámená NBÚ.

Ustanovenie § 43a určuje, že distribúciu a evidenciu kryptografického materiálu ČR zaisťuje NBÚ a Ministerstvo obrany. NBÚ zaisťuje distribúciu a evidenciu kryptografického materiálu EÚ a kryptografického materiálu distribuovaného na základe medzinárodnej zmluvy. Ministerstvo obrany zaisťuje distribúciu a evidenciu kryptografického materiálu Organizácie Severoatlantickej zmluvy a kryptografického materiálu na vojenské účely. Podmienky evidencie a manipulácie kryptografického materiálu upraví bezpečnostný štandard.

Znenie § 44 hovorí o tom, čo upravuje vykonávací právny predpis č. 432/2011 Sb. a nakoniec ustanovenie § 45 popisuje kompromitujúce vyžarovanie. „Ochranou utajovaných informácií stupňa utajenia Prísne tajné, Tajné alebo Dôverné pred ich únikom kompromitujúcim vyžarovaním je zabezpečenie elektrických a elektronických zariadení zabezpečenej oblasti alebo objektu“. Ochrana utajovanej informácie pred únikom kompromitujúcim vyžarovaním môže byť zabezpečená pomocou tieniacej komory, ktorá ale musí byť certifikovaná NBÚ. Spôsobilosť elektrických a elektronických zariadení overuje NBÚ pri certifikácii informačného systému alebo kryptografického prostriedku. Spravodajské služby sú oprávnené k vykonávaniu merania spomínaných zariadení, zabezpečenej oblasti alebo objektu. [23]

3.1.2 Hlava IX - Certifikácia

V druhej časti zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti sa Hlava IX venuje certifikácii. Niektoré ustanovenia tejto hlavy sa venujú certifikácii v oblasti kryptografie.

Táto hlava začína spoločným ustanovením popisujúcim certifikáciu ako postup, ktorým NBÚ overuje spôsobilosť technického prostriedku, informačného systému, kryptografického prostriedku, kryptografického pracoviska a tieniacej komory na ochranu utajovaných skutočností a na nakladanie s nimi. Ak NBÚ spôsobilosť zistí, príslušné certifikáty vydá. Spoločné ustanovenie popisuje obsah certifikátov informačného systému, kryptografického prostriedku, kryptografického pracoviska a tieniacej komory. Tieto certifikáty musia obsahovať evidenčné číslo, identifikáciu držiteľa certifikátu, dátum vydania a dobu platnosti certifikátu, odtlačok úradnej pečiatky NBÚ a podpis oprávneného zástupcu NBÚ. Certifikáty kryptografického prostriedku a tieniacej komory ešte obsahujú identifikáciu kryptografického prostriedku, resp. tieniacej komory, identifikáciu výrobcu kryptografického prostriedku (tieniacej komory) a stupeň utajenia utajovaných informácií. Certifikát kryptografického pracoviska navyše obsahuje identifikáciu tohto pracoviska, rozsah jeho spôsobilosti a jeho príslušnú kategóriu. NBÚ rozhoduje o zániku platnosti certifikátu, proti tomuto rozhodnutiu nie je možné sa odvolať. Prílohou certifikátu informačného systému, kryptografického prostriedku, kryptografického pracoviska alebo tieniacej komory je certifikačná správa, ktorej obsahom je zásada a konkrétne podmienky ich prevádzkovania. Pri overovaní spôsobilosti informačného systému, kryptografického prostriedku, kryptografického pracoviska alebo tieniacej komory, ktoré majú byť prevádzkované prostredníctvom spravodajských služieb a ktoré z dôvodu utajenia NBÚ nemôže vykonávať, sú k vykonávaniu jednotlivých úloh oprávnené práve spomínané spravodajské služby.

Ustanovenie § 49 podrobne popisuje žiadosť o certifikáciu kryptografického prostriedku a platnosť certifikátu kryptografického prostriedku, § 50 sa venuje žiadosti o certifikáciu kryptografického pracoviska a platnosti certifikátu kryptografického pracoviska a § 51 poskytuje podrobné informácie o žiadosti o certifikáciu tieniacej komory a platnosť certifikátu tieniacej komory. Napokon ustanovenie § 53 popisuje, čo upravuje vykonávací právny predpis č. 525/2005 Sb. [23]

3.2 Vyhláška č. 432/2011 Sb. o zajištění kryptografické ochrany utajovaných informací

Vyhláška č. 432/2011 Sb. o zajištění kryptografické ochrany utajovaných informací zo dňa 16. 12. 2011 nadobudla účinnosť 1. 1. 2012.

Vyhláška vymedzuje nasledujúce pojmy:

a) kryptografická zásielka - rozumie sa ňou „kryptografický materiál vybavený k preprave, prepravovaný alebo doručený adresátovi na miesto určenia do ukončenia jej prepravy a jej overenia“,

b) preprava kryptografickej zásielky - ide o „jej dopravenie mimo objekt orgánu štátu, právnickej osoby alebo podnikajúcej fyzickej osoby za účelom jej doručenia adresátovi“,

c) prenášanie kryptografického materiálu - jedná sa o „jeho prepravovanie mimo objekt orgánu štátu, právnickej osoby alebo podnikajúcej fyzickej osoby, ktorého cieľom nie je jeho doručenie“,

d) kryptografický dokument – je ním „listina alebo iný nosič informácií obsahujúci utajované informácie kryptografickej ochrany“,

e) kryptografický prostriedok - vyhláška určuje ako „hardwarový alebo softwarový produkt určený ku kryptografickej ochrane“,

f) kryptografický kľúč – ide o „utajovaný premenný parameter nevyhnutný k jednoznačnému zašifrovaniu a odšifrovaniu dát“,

g) kľúčový materiál – rozumie sa ním „kryptografický kľúč na nosiči“,

h) heslový materiál – jedná sa o „utajovaný znakový reťazec na nosiči, z ktorého je odvodzovaný kryptografický kľúč alebo ktorý je použitý k autentizácii“,

i) materiál k zaisteniu funkcie kryptografického prostriedku – predstavuje „kľúčový materiál a heslový materiál pre kryptografickú operáciu“.

Vyhláška ďalej ustanovuje podrobnosti zaisťovania odbornej skúšky a nachádzajú sa tu informácie o tom, čo má obsahovať odborná skúška, jej organizácia a vykonanie, čo má byť obsahom osvedčenia o špeciálnej odbornej spôsobilosti pracovníka kryptografickej ochrany a čo je obsahom žiadosti o uzavretie zmluvy k vykonaniu odbornej skúšky.

Vyhláška definuje aj minimálne požiadavky na zaistenie bezpečnostnej správy kryptografickej ochrany. Bezpečnostnú správu vyhláška vymedzuje ako „plnenie opatrení v oblasti personálnej, administratívnej a fyzickej bezpečnosti a bezpečnosti informačných alebo komunikačných systémov pri zaisťovaní kryptografickej ochrany“.

Obsahom vyhlášky sú aj podrobné informácie o zaisťovaní prevádzky kryptografického prostriedku, ktoré pojednávajú o inštalácii a obsluhe kryptografického prostriedku a o výrobe a používaní materiálu k zaisteniu funkcie kryptografického prostriedku. Ďalej je v nej popísaný spôsob zaškoľovania a vzor potvrdenia pracovníka prevádzkovej obsluhy kryptografického prostriedku a kuriéra kryptografického materiálu. Vyhláška hovorí aj o označovaní kryptografického materiálu. Pri označovaní materiálu k zaisteniu funkcie kryptografického prostriedku sa na daný materiál poznačí stupeň utajenia. Kľúčový materiál a kryptografický dokument v listinnej podobe sa označia slovom „KRYPTO“. Okrem označovania sa vykonávací právny predpis venuje aj náležitostiam kryptografického dokumentu v listinnej a nelistinnej podobe a spôsobu vedenia evidencie. Vymenúva druhy a náležitosti administratívnych pomôcok kryptografickej ochrany.

Časť vyhlášky popisuje požiadavky na spôsob a prostriedky spojené s manipuláciou s kryptografickým materiálom. Konkrétne sa jedná o evidenciu kryptografického prostriedku, kryptografického materiálu a dokumentu. Ďalej ide o vyhotovenie kryptografického dokumentu v listinnej podobe a zaznamenávanie poznámok, ktoré obsahujú utajované informácie kryptografickej ochrany na nosič utajovaných informácií. Vyhláška v tejto časti popisuje náležitosti týkajúce sa opisu, kópie, prekladu a výpisu z kryptografického dokumentu. Ak sa jedná o stupeň utajenia Prísne tajné alebo Tajné, vyhotovujú sa na základe písomného súhlasu pôvodcu tohto dokumentu a ak sa jedná o dokument stupňa utajenia Dôverné alebo Vyhradené, vydávajú sa so súhlasom vedúceho zamestnanca.

Kryptografický prostriedok sa odosiela v obale, ktorý by mal byť zabezpečený proti neoprávnenému použitiu. Materiál k zaisteniu funkcie kryptografického prostriedku sa odosiela v dvoch obaloch:

- vo vnútornom, aby neumožňoval získanie informácie o jeho obsahu,
- a vo vonkajšom, ktorý predstavuje prenosnú schránku.

Kryptografický dokument v listinnej podobe sa odosiela v dvoch obálkach a kryptografický dokument v nelistinnej podobe sa odosiela ako príloha kryptografického dokumentu v listinnej podobe. Kryptografický dokument možno preniesť aj elektronickou cestou.

Pri príjme kryptografickej zásielky sa poverený pracovník zodpovedný za prevzatie kuriérovi podpíše a odtlačí pečiatku. Pri zistení vady sa hneď pri prijatí zásielky spíše záznam o poškodení kryptografickej zásielky. Preprava kryptografického materiálu sa vykonáva ako preprava kryptografickej zásielky za pomoci kuriéra kryptografického materiálu. Tieto zásielky nemožno prepravovať prostredníctvom verejných dopravných prostriedkov. Ku každej kryptografickej zásielke, ktorá obsahuje kryptografický materiál alebo prostriedok, sa vyhotovuje sprievodný list. Kryptografický materiál stupňa utajenia Prísne tajné, Tajné a Dôverné prepravuje kuriér za doprovodu najmenej 1 osoby.

Kryptografický materiál sa prenáša v zalepenej obálke alebo uzavretom obale a vyznačuje sa slovom „KRYPTO“. Táto skutočnosť neplatí pre obálku alebo obal obsahujúci heslový materiál, lebo heslový materiál sa neoznačuje slovom „KRYPTO“. Prenos kryptografického materiálu zabezpečuje pracovník kryptografickej ochrany.

Kryptografický materiál sa ukladá do úschovného objektu v zabezpečenej oblasti. Úschovným objektom môžu byť všetky druhy trezorov alebo kovových skríň, ktoré musia byť uzamykateľné. Prenosovou schránkou je nejaký druh aktovky, kufra, kufríka, kuriérneho vaku alebo prenosnej bezpečnostnej schránky. Vyžaduje sa, aby na účely prenosu bola prenosná schránka zabezpečená proti neoprávnenej manipulácii s jej obsahom. Zabezpečenie môže byť vykonané napr. uzamknutím mechanickým alebo kódovým zámkom, pečatením alebo plombovaním.

Uložený kryptografický dokument je možné zapožičať pracovníkovi kryptografickej ochrany na nevyhnutne nutnú dobu. Zapožičanie dokumentu sa zaznamenáva do knihy zapožičaní. Zapožičané dokumenty sa po uplynutí 6 mesiacov vždy predkladajú ku kontrole poverenej osobe. Podmienky týkajúce sa vyraďovania kryptografického materiálu ustanovujú bezpečnostné štandardy, príslušné vykonanie vyraďovania zaisťuje zodpovedná osoba alebo ňou poverený pracovník kryptografickej ochrany. Vyhláška upravuje, čo musí obsahovať žiadosť o udelenie povolenia pre vývoz certifikovaného kryptografického prostriedku z územia ČR.

Kategóriou kryptografického pracoviska sa podľa vyhlášky rozumie „označenie úrovne spôsobilosti kryptografického pracoviska zaistiť ochranu utajovanej informácie z oblasti kryptografickej ochrany podľa najvyššieho stupňa utajenia utajovanej informácie, ktorá sa v ňom ukladá alebo spracováva, a podľa toho, či vstupom na kryptografické pracovisko dochádza (trieda I) alebo nedochádza (trieda II) k zoznámeniu sa s utajovanou informáciou“. Kryptografické pracoviská sa zaraďujú do kategórií:

a) Prísne tajné, triedy I alebo II,
b) Tajné, triedy I alebo II,
c) Dôverné, triedy I alebo II,
d) Vyhradené, triedy I alebo II. [24]

3.3 Vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací

Vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací zo dňa 14. 12. 2005 nadobudla účinnosť dňa 1. 1. 2006 a odvtedy bola novelizovaná vyhláškou č. 434/2011 Sb.

Vyhláška ustanovuje, čo má byť obsahom žiadosti o certifikáciu kryptografického prostriedku, žiadosti o certifikáciu kryptografického pracoviska a čo má byť obsahom opakovanej žiadosti o certifikáciu kryptografického prostriedku alebo opakovanej žiadosti o certifikáciu kryptografického pracoviska.

Ustanovenie § 5 vyhlášky popisuje dokumentáciu, ktorá sa predkladá pri priebehu vykonávania certifikácie kryptografického prostriedku. Bezpečnostný štandard poskytnutý žiadateľovi stanovuje zoznam, formu a obsah dokumentácie. Uvedené ustanovenie predkladá aj obsah spomínanej dokumentácie. Znenie § 6 popisuje dokumentáciu potrebnú na vykonanie certifikácie kryptografického pracoviska. Jedná sa o dokumentáciu zabezpečenia prostredníctvom fyzickej bezpečnosti kryptografického pracoviska a o dokumentáciu prevádzkovo-bezpečnostného zabezpečenia kryptografického pracoviska.

Vzory certifikátu kryptografického prostriedku a certifikátu kryptografického pracoviska sú uvedené v prílohe č. 1 a 2 tejto vyhlášky a prikladám ich do prílohy mojej diplomovej

práce. Prílohami oboch typov certifikátov je tzv. certifikačná správa, ktorej obsah je vymedzený v ustanoveniach § 7 a § 8 vyhlášky.

Vyhláška ustanovuje spôsob a podmienky vykonania certifikácie kryptografického prostriedku a kryptografického pracoviska. Rozsah, spôsob a poradie vykonania certifikácie stanovuje NBÚ. Certifikácia sa delí na etapy, ktoré uskutočňujú odborné pracoviská NBÚ, orgánu štátu, právnickej osoby alebo podnikajúcej fyzickej osoby. Podľa výsledkov hodnotenia etáp vydá NBÚ potrebné rozhodnutie. Jednotlivé etapy, ktoré prispievajú k rozhodovaniu NBÚ, sú popísané v ustanoveniach § 9 a § 10. [25]

4 MOŽNOSTI OCHRANY UTAJOVANÝCH INFORMÁCIÍ A KNOW HOW Z TECHNICKÉHO HĽADISKA

Zo zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti je zrejmé, že kryptografická ochrana patrí medzi prostriedky ochrany utajovaných informácií. Utajované informácie sú informácie, na ktorých utajení má záujem nejaká fyzická osoba alebo právnická osoba, ktorou môže byť inštitúcia, príp. štát. Snahou týchto osôb je utajenie informácie z dôvodu, že pri jej zneužití môže vzniknúť nejaká ujma. Subjekt chráni informácie mnohými opatreniami, aby utajenie bolo zachované a nepovolaná osoba sa s takouto informáciou nezoznámila.

Pomocou prostriedkov kryptografickej ochrany sa chráni aj tzv. know-how, z angl. „vedieť ako“. Jedná sa o súbor technicko-ekonomických znalostí, metód a postupov, ktoré sa získavajú vo výrobnom procese, výskume, vývoji, príp. v ďalších procesoch. Tento súbor umožňuje dosiahnuť vysoký stupeň kvality, akosti, bezporuchovej prevádzky, efektívnych postupov, atď. Know-how býva predmetom obchodných rokovaní a spravidla sa utajuje. [26]

Hlavnou úlohou kryptografických opatrení zaisťovaných kryptografickými prostriedkami je zabránenie nepovolanej osobe zoznámiť sa s obsahom utajovanej informácie alebo know-how. Do skupiny kryptografických prostriedkov možno zaradiť aj špeciálne technické prostriedky, ktorých úlohou je znemožniť realizáciu technických zariadení určených k odpočúvaniu. Jedná sa o šifrátory, zaistenie miestností proti úniku informácií, generátory šumu a ďalšie technické prostriedky určené k ochrane telefónnych, počítačových a ďalších liniek a sietí. [27]

Obr. 26. Mobilné GSM odpočúvanie

[28]

4.1 Generátory šumu

Pojem šum sa v teórii informácie prezentuje ako falošná informácia alebo tzv. dezinformácia. Šum sa delí na niekoľko typov a vyskytuje sa pri všetkých fyzikálnych veličinách. Šum môže byť napr. akustický, elektrický, pneumatický, kvantový, atď. Šum možno deliť aj podľa farby. Názvy farieb pre rôzne typy šumu boli vytvorené ako približná analógia medzi ich frekvenčným spektrom a spektrom farebného svetla. Teda spektrum ružového šumu zodpovedá spektru svetla s ružovým odtieňom, atď. Podľa farby šumy delíme na biely šum, ružový šum, hnedý (červený) šum, modrý (azúrový) šum, purpurový (fialový) šum, šedý šum, oranžový šum, zelený šum a čierny šum. [29]

V teórii šumov sa vyskytuje pojem Brownov pohyb, ktorý predstavuje vnútorný mechanický šum. Tento pohyb spôsobujú nevyvážené dynamické sily, ktoré sú zapríčinené náhodnými vplyvmi molekúl na malé čiastočky okolia. Nazýva sa tiež náhodný šum a ide v podstate o jav, ktorý sa vyskytuje vo všetkých systémoch. Tento pohyb teoreticky popísal v roku 1905 Albert Einstein. [30]

Generátor šumu sa využíva ako spôsob ochrany pred odpočúvaním miestnosti, v ktorej prebieha rozhovor. Pri klasickom rozhovore hovorené slovo spôsobuje tlakové vlny, ktoré rozochvievajú okná, steny a tiež predmety nachádzajúce sa v miestnosti. Z týchto rozochvených predmetov je potom možné prostredníctvom odpočúvania zachytiť hovorené slovo. Generátor šumu sa využíva práve na to, aby nebolo možné hovorené slovo prostredníctvom rozochvených predmetov zachytiť. Tieto generátory vydávajú akustický signál, ktorý rozochvené predmety zašumí. To znamená, že k ich frekvencii chvenia pridá frekvenciu šumu. Dôsledkom toho je skutočnosť, že nie je možné z týchto predmetov zachytiť hovorené slovo z rozhovoru v danej miestnosti. Generátory šumu sa inštalujú na okná, steny, žalúzie alebo tapety. Vhodné je nainštalovať generátory šumu s akustickými meničmi.

Rozoznávame dva typy šumových generátorov:

1. Analógový šumový generátor - produkuje pomerne vyrovnaný biely šum, pri ktorom môže na veľmi spodnom konci spektra prevládať šum ružový. Obvod je tvorený predzosilovačom, po ktorom nasleduje integračný článok (dolná prepusť), ktorý urobí z bieleho šumu ružový šum. Tento integračný článok nie je čistý

integrátor, býva ešte trochu frekvenčne korigovaný, pretože nie je potrebný podzvukový ani nadzvukový šum.

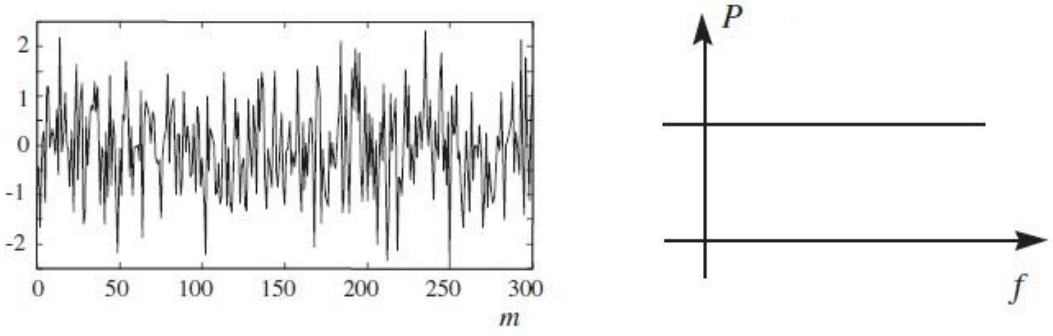
2. Digitálny šumový generátor - produkuje pseudonáhodný signál, teda signál, ktorý je predvídateľný (popísaný matematickou funkciou), ale vykazuje isté známky náhodnosti. Tento pseudonáhodný signál vzniká na špeciálne zapojených posuvných registroch, resp. logických integrovaných obvodoch. Jedná sa o nepravidelnú sériu obdĺžnikových impulzov. Z ich výstupov prechádza odoberaný signál taktiež mnohými filtrami typu dolnej prepusti. Keď sa pustí nahlas, je v ňom počuť kovové strojové zafarbenie. [29], [31]

Obr. 27. Šumový generátor SNG [32]

4.1.1 Biely šum

Pri šumových generátoroch sa najčastejšie využíva biely šum. Biely šum je náhodný signál s konštantnou spektrálnou hustotou, tzn. nezávisí na kmitočte. Signál ma rovnaký výkon v akomkoľvek pásme totožnej šírky. Napr. pásmo široké 20Hz má medzi 40Hz a 60Hz rovnaký výkon ako pásmo medzi 4000Hz a 4020Hz. [31]

Biely šum, ktorý má charakter náhodného šumu prechádzajúceho všetkými frekvenciami, na ktorých má totožný výkon v rozsahu ±∞, by nutne potreboval nekonečný výkon, a preto sa jedná iba o teoretický koncept. Z praktického hľadiska je v praxi vhodné ho ohraničiť určitým frekvenčným pásmom s plochým spektrom, ktoré pokrýva frekvenčný rozsah komunikačného systému, a z toho dôvodu sa bielemu šumu tiež pripisuje názov „širokopásmový šum“. Napr. každé ploché spektrum so šírkou rovnajúcou sa alebo väčšou ako 10kHz, ktoré sa nachádza v audiosystémoch so šírkou pásma 10kHz, možno považovať za biely šum. [33]



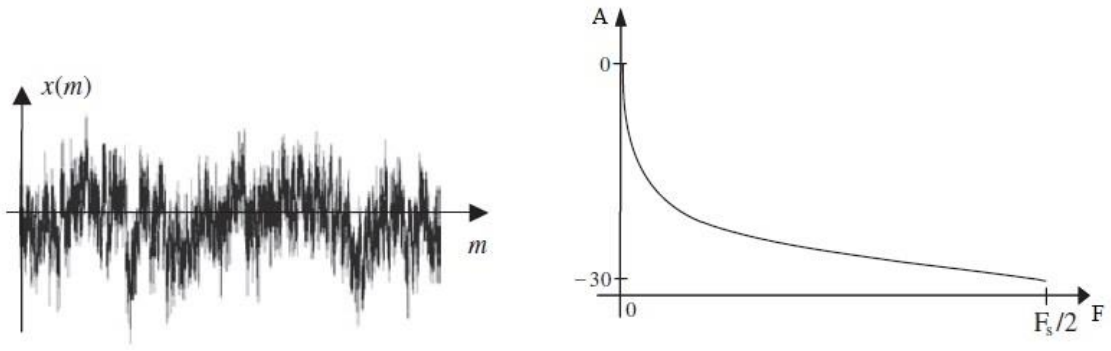
Obr. 28. Časový priebeh bieleho šumu, výkonové spektrum [33]

4.1.2 Ružový šum

Ružový šum sa v niektorých literatúrach vyskytuje pod pojmom „1/f šum“ alebo tiež „kmitajúci šum“. Jeho frekvenčný rozsah je charakterizovaný tak, že výkonová frekvenčná hustota je priamo úmerná prevrátenej hodnote frekvencie. [31]

Ružový šum sa objavuje pri nízkych kmitočtoch, tzn. do 100Hz. Tento kmitajúci šum môže byť v praxi prítomný iba vo vymedzenom frekvenčnom pásme. Prakticky je biely šum silnejší ako ružový, ale až nad určitou frekvenciou, ktorá sa označuje ako frekvenčný zlom. Ani po uskutočnených meraniach na frekvencii 10-7Hz nebola zistená spodná hranica frekvencie ružového šumu a šum bol prítomný aj pri takto nízkych frekvenciách.

Mnoho fyzikov a vedcov zastáva názor, že tento šum je všadeprítomný. Možno povedať, že všeobecná teória šumu nie je zatiaľ úplne vypracovaná do konca a zaoberá sa ňou veľa vedcov po celom svete. [34]



Obr. 29. Signál ružového šumu, amplitúdové spektrum [33]

4.2 Rádiový analyzátor

Cieľom rádiových analyzátorov je odhaliť rádiové odpočúvacie prostriedky umiestnené v záujmových priestoroch, resp. miestnostiach. Všetky rádiové frekvencie, aktívne v danom čase a v danej oblasti, sa zapíšu do pamäte týchto rádiových prostriedkov. Následne prebehne skenovanie rádiového spektra, pri ktorom sa porovnáva skutočný stav s pamäťou analyzátora. Pri objavení nezhody, zamerajú frekvenciu nového vysielača a umožnia počúvanie nového signálu, príp. ukážu približnú vzdialenosť vysielača od prijímača, ktorá predstavuje silu poľa.

Existuje niekoľko typov rádiových analyzátorov, rozdiel medzi nimi je v šírke pásma, ktoré dokážu kontrolovať, a v rýchlosti tejto kontroly. Analyzátory sa žiaľ vyznačujú aj niekoľkými nevýhodami. Medzi nevýhody patrí pomerne vysoká náročnosť na obsluhu, pretože niektoré analyzátory môže obsluhovať iba zaškolená osoba a iné vyžadujú prácu špecialistu. Avšak základný problém tkvie v množstve rádiových signálov aktívnych najmä vo veľkých mestách, ako je napr. Londýn, ktorý ich má aktívnych cez 600, alebo Praha cez 200. Nie všetky rušivé frekvencie pochádzajú z odpočúvania (napr. záchranka, polícia), a preto je potrebné dbať na citlivosť nastavenia, ktoré je dôležité pre správnu činnosť rádiového analyzátora a pre zamedzenie vzniku zbytočných obáv.

V súčasnosti niektoré spoločnosti vyvíjajú rádiové analyzátory, ktoré budú fungovať na princípe prepojenia s internetom, čím sa zaistí ich správa na diaľku. Vďaka tomuto spôsobu bude možné „privolať“ špecialistu rýchlo do ktorejkoľvek kancelárie kdekoľvek na svete. [28]

Obr. 30. Rádiový pamäťový analyzátor MRA 5 [35]

4.3 Tieniace komory - Faradayova klietka

Tieniace komory tienené prostredníctvom Faradayovej klietky slúžia na ochranu miestností pred tzv. kompromitujúcim vyžarovaním. Kompromitujúce vyžarovanie sa vytvára prostredníctvom elektronických a elektromechanických zariadení, ktoré sa používajú na spracovanie informácií. Ak je toto vyžarovanie nejakým spôsobom zachytené a následne analyzované, môže vyzradiť informáciu, ktorá mala pôvodne zostať utajená. Pre problematiku súvisiacu s kompromitujúcim vyžarovaním sa v SR používa pojem „ochrana pred nežiaducim elektromagnetickým vyžarovaním“ (NEV). [36]

Z uvedeného môžeme odvodiť definíciu kompromitujúceho vyžarovania, ktorú NBÚ ČR popisuje ako elektromagnetické, akustické alebo optické vyžarovanie elektrických zariadení, elektronických zariadení a informačných systémov, ktoré môže zapríčiniť únik utajovanej informácie.

Vo svete sa s definíciou kompromitujúceho vyžarovania spája termín TEMPEST. V súvislosti s týmto termínom vznikajú činnosti určené k zisťovaniu a skúmaniu kompromitujúceho elektromagnetického vyžarovania, konkrétne sa jedná o neúmyselne vyžiarené elektromagnetické signály, na základe ktorých je možné odhaliť obsah spracovanej informácie.

Elektronické zariadenia sú kvôli svojej konštrukcii a použitej technológii náchylné na vonkajšie rušenie a tiež samy vyžarujú elektromagnetickú energiu, teda rušenie. Vyžarovaná energia elektronických zariadení, ktoré sú súčasťou informačných systémov, v sebe môže niesť spracovávanú informáciu. Preto je potrebné tieto informačné systémy chrániť. [37]

Priestory, v ktorých sa nachádzajú informačné systémy, sa často chránia elektromagnetickým tienením, využívaným v tzv. tieniacich komorách. Tieniace komory sú zariadenia slúžiace k zamedzeniu úniku elektromagnetického žiarenia z priestorov komory. Popritom zabraňujú vstupu vonkajšieho zariadenia, resp. rušenia do priestorov komory. Využitie komory má dvojaký charakter, jednak zaisťuje priestory pred elektronickými odpočúvaniami (mobilné telefóny, signály z počítačov, odpočúvacie zariadenia) a ešte aj prispieva k ochrane elektronických zariadení vo vnútri komory (dátové centrá, ochrana pred elektromagnetickým žiarením, atď.). Tieniace komory možno zaviesť do novostavieb alebo už do existujúcich priestorov.

Obr. 31. Tieniaca komora [38]

Najčastejšie využívaný princíp v oblasti tieniacich komôr je založený na Faradayovej klietke. Faradayova klietka pracuje tak, že elektrický náboj je sústredený iba na povrchu vodiča a nie v jeho objeme. Tým pádom vo vnútri vodiča, resp. vo vnútri Faradayovej klietky nepôsobí žiadne elektromagnetické pole alebo elektrické pole, z čoho vyplýva úplná elektromagnetická izolácia od okolitých priestorov. [38]

Pred zavedením Faradayovej klietky sa vyberie najviac vyhovujúci priestor v danom objekte. Následne sa vykonajú úpravy spojené s elektroinštaláciou, ktoré prebiehajú privedením jedného napájacieho kábla a odstránením všetkých ostatných pripojení ako sú PC a telefóny. Na dané vedenie sa pripojí sieťový filter. Na steny danej miestnosti sa nainštaluje sieť tvorená piezomeničmi, aby sa zamedzilo prípadnému kontaktnému snímaniu informácií z plášťa miestnosti. Na sieť piezomeničov sa nalepí špeciálna medená fólia. Existujú rôzne druhy týchto fólií, napr. ak je požiadavka na nižšiu tieniacu účinnosť, postačí inštalácia metalizovaných tapiet. Naopak pri požiadavke na vysoký tieniaci účinok sa použije konštrukcia pozinkovaných plechov. Fólia sa pokryje omietkou. Do okien sú umiestnené špeciálne pokované sklá a na dvere sa nalepí samolepiaca fólia, pričom sa môžu použiť aj špeciálne dvere a zárubne. Miestnosť treba uzemniť. Zmeria sa výsledný útlm, ktorý sa porovná s požadovaným útlmom. Ak je to potrebné, nainštaluje sa ešte jedna vrstva fólie. Napokon sa dokončia ostatné interiérové úpravy a do miestnosti sa zavedie rádiový analyzátor a generátor šumu. [39], [40]

Obr. 32. Využitie tieniacich komôr v dátových centrách, pri ochrane dôverných dát a v miestnosti pre jednanie s utajením [41]

4.4 Technika na ochranu komunikačných médií

Doteraz sme sa v predošlých podkapitolách zaoberali ochranou miestností proti prípadnému odpočúvaniu, no rovnako vzniká potreba chrániť v súčasnosti stále viac populárne informačné a komunikačné technológie (ICT), pretože prostredníctvom nich sa čoraz častejšie prenášajú citlivé informácie a v dôsledku toho vzrastá potreba tieto ICT zabezpečovať proti odpočúvaniu neautorizovanými osobami.

V dnešnej dobe si už mnoho ľudí nevie svoju existenciu predstaviť bez používania mobilných komunikačných prostriedkov ako sú mobilné telefóny, osobné komunikátory a pod. Vďaka ich nízkej cene a jednoduchosti ovládania si ich obľúbili všetky vrstvy obyvateľstva a využívajú ich pre súkromné a aj pre služobné potreby. Zariadenia disponujú veľmi užívateľsky príjemným prostredím a umožňujú vykonávať prenos hlasu, textových správ, obrazových a dátových informácií. Tieto mobilné komunikačné technológie majú schopnosť prispievať k zefektívneniu a k zrýchleniu práce. Naproti tomu, ako väčšina nových technológií, tak aj ICT so sebou prinášajú riziká zneužitia. Najväčšie riziko predstavuje jednoduchá možnosť odpočúvania a monitorovania komunikačnej prevádzky. Najúčinnejší spôsob zamedzenia odpočúvaniu prenášaných informácií je šifrovanie. [42]

K ochrane GSM komunikácie pred odpočúvaním sa používa niekoľko spôsobov. Celkom rozšíreným spôsobom sú hardwarové šifrovacie prístroje používajúce k zašifrovaniu telefónnej konverzácie špeciálne kódy, ktoré zabránia neautorizovanej osobe dekódovať dáta. Autorizovaná osoba totiž disponuje rovnakým zariadením a dohodnutým dešifrovacím kľúčom. Okrem hardwarových šifrovacích prístrojov sa k ochrane dát používa aj software v podobe špeciálnej aplikácie, ktorá sa nahrá do mobilného telefónu. Táto aplikácia sa postará o zašifrovanie a následné dešifrovanie dát. Výhodou je, že nie je

potrebné externé zariadenie a tým vzniká nenápadnosť používania. Obidve komunikujúce strany musia disponovať rovnakým softwarovým vybavením. [31]

Niekoľko svetových výrobcov sa postaralo o vývoj špeciálnych mobilných telefónov, ktoré sú vybavené kryptovacím zariadením. Všeobecný princíp fungovania šifrovacích GSM telefónov spočíva v digitalizovaní informácie, jej následnom zašifrovaní a nakoniec odoslaní z prístroja v dátovej podobe. Na strane príjemcu dochádza k rozšifrovaniu informácie a z digitálnej podoby sa z nej spätne vyvinie akustická informácia. Niektoré zariadenia tohto typu kontrolujú aj to, či má príjemca rovnaké zariadenie ako odosielateľ a teda, či je možné kryptovaný hovor uskutočniť. Kontroluje sa aj oprávnenosť osoby, ktorá chce hovor uskutočniť, a to prostredníctvom ACCESS kódu užívateľa, ktorým sú telefóny vybavené. [28]

V prípade prenosu utajovaných informácií prostredníctvom ICT je povinnosť ochrany takto prenášaných informácií ustanovená zákonom. Pre ochranu utajovaných informácií sa používajú iba certifikované zariadenia. Prvým a zároveň jediným certifikovaným prostriedkom v ČR bol mobilný GSM telefón nórskej proveniencie NSK 200. V roku 2008 NBÚ certifikoval zariadenie švédskej spoločnosti Sectra Communication AB s názvom Tiger®XS, ktorý umožňoval šifrovanie hlasových a dátových komunikácií. Tiger®XS je sieťovo nezávislý osobný hlasový a dátový šifrátor, ktorý v štandardnej verzii umožňuje šifrovanie hlasu, šifrovanie dátových prenosov a šifrovanie krátkych textových správ. Tento prostriedok je primárne určený pre použitie vo vládnych a bezpečnostných orgánoch. [42]

Obr. 33. Šifrovací GSM telefón Tiger®XS [42]

5 ZABEZPEČENIE DOHĽADOVÝCH A POPLACHOVÝCH PRIJÍMACÍCH CENTIER

Dohľadové a poplachové prijímacie centrum (DPPC), z angl. „Alarm Receiving Centre“ (ARC), je stredisko, do ktorého sa predávajú informácie nesúce v sebe údaje o stave jedného alebo viacerých poplachových systémov nachádzajúcich sa v stráženom objekte. Stredisko DPPC disponuje stálou a trvalou obsluhou a tým zabezpečuje neustály vzdialený dohľad nad majetkom a ochranou užívateľov. V niektorých literatúrach sa uvádza názov „pult centralizovanej ochrany“, tento názov je však už podľa normy ČSN EN 50518 neplatný. [43]

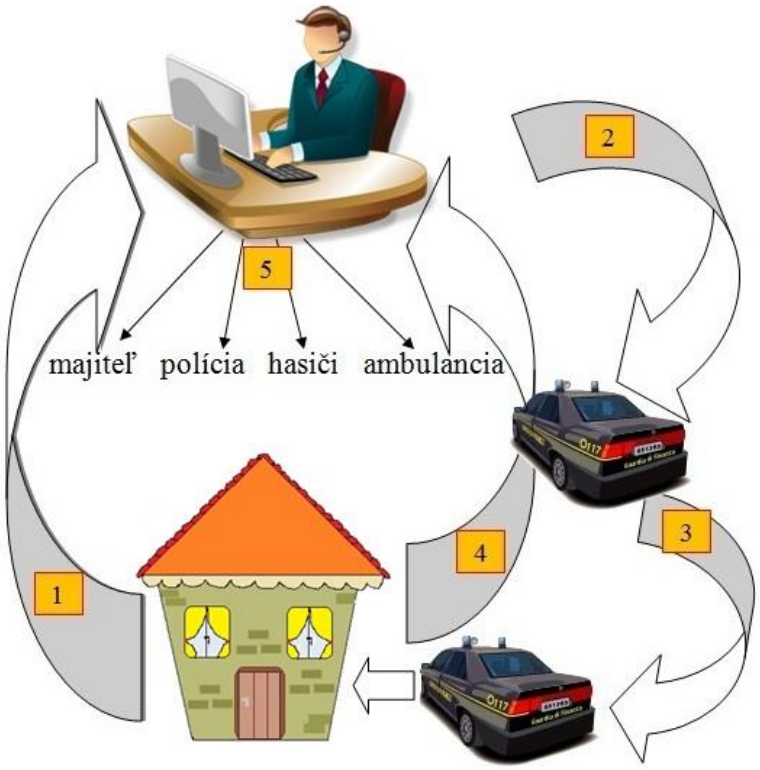
Obr. 34. Pracovisko DPPC [44]

Pri zabezpečení DPPC je dôležité chrániť komunikáciu vo vnútri objektu DPPC, aby bolo detekované akékoľvek rušenie zvonku v súlade s normou EN 50136-1. Ďalej je potrebné v rámci DPPC chrániť dáta z monitorovaných systémov zákazníkov, ktoré môžu o klientoch prezradiť veľmi citlivé údaje typu, kedy sa klient nachádza doma a naopak, kedy doma nebýva atď. Žiaducou podmienkou pri spracovaní informácií je zachovávanie bezpečnosti uloženia informácií týkajúcich sa zákazníkov, archivácia týchto informácií a poskytovanie chráneného sprístupnenia dát zákazníkom. Z uvedeného plynie skutočnosť, že DPPC musí zaviesť a dodržiavať ochranné opatrenia zaisťujúce nedotknuteľnosť zákazníckych údajov pred nepriateľskými činmi alebo vplyvmi. Okrem zabezpečenia priestorov DPPC je vhodné

chrániť aj prenos správ medzi stráženým objektom a dispečingom DPPC, kde sa uvedená komunikácia chráni šifrovaním.

5.1 Princíp DPPC

DPPC pracuje na princípe napojenia poplachových zabezpečovacích a tiesňových systémov na dispečing prijímacieho poplachového centra. Z ústredne strážených objektov sú vyslané správy o stave týchto objektov, ktoré operátor DPPC prijme a následne vyhodnotí. Operátor vzápätí vyhľadá najbližšiu zásahovú jednotku, ktorú skontaktuje a vyšle ju na miesto napadnutia. Ďalším krokom je zaistenie bezpečnosti prostredníctvom vykonania zásahu v narušenom objekte. V prípade potreby môže informovať aj políciu, resp. inú zložku integrovaného záchranného systému. Nakoniec informuje klienta o stave jeho majetku. [45]



Obr. 35. Princíp činnosti DPPC [autor]

Obrázok (Obr. 35) poukazuje na fakt, že činnosť DPPC je možné zhrnúť do piatich stručných bodov:

1. Signál o napadnutí objektu.

2. Operátor vysiela zásahovú skupinu.
3. Vykonanie zásahu na mieste.
4. Spätná informácia operátorovi o stave.
5. Informovanie klienta, príp. niektorej zo zložiek integrovaného záchranného systému.

Na DPPC sa je možné napojiť niekoľkými spôsobmi a to najmä prostredníctvom:

- telefónnej siete (JTS),
- mobilnej siete (GSM, GPRS, SMS),
- rádiového prenosu,
- internetu,
- kombinovaného prenosu (kombinácia dvoch druhov prenosu, napr. JTS a rádiový spoj, alebo JTS a GSM). [43]

5.2 Správy na DPPC

Správy sa vysielajú z bezpečnostného systému, ktorý je nainštalovaný vo vzdialenom objekte. Z objektu sa môžu vysielať rozličné typy a adresy správ, ktoré sú definované vhodným programom a následne prijaté na DPPC. Jedná sa o nasledujúce typy správ:

1. Poplachové správy - považujú sa za najdôležitejšie informácie prenášané z poplachových zabezpečovacích a tiesňových systémov a sú z hľadiska prenosu prioritné. Software nachádzajúci sa na DPPC zobrazí napadnuté miesto a umiestnenie detektora, ktorý hlási poplach. Súčasťou poplachových správ je tzv. „panik poplach“, ktorý zobrazuje ohrozenie zdravia alebo života. Poplachy môžu byť typu sabotážneho, požiarneho, pohybového a otrasového.
2. Poruchové správy – pokladajú sa hneď za poplachovými správami za druhé najdôležitejšie prenášané informácie. Majú za úlohu informovať pracovníka DPPC o poruchách bezpečnostného systému. Jedná sa o poruchy napájania, záložného zdroja, sirény, výpadok telefónnej linky. Operátor po prijatí poruchovej správy informuje obsluhu bezpečnostného systému, príp. servisného technika.

3. Testovacie správy - vo vopred určených časových intervaloch bezpečnostný systém informuje DPPC správou „Automatický test“, ktorá značí funkčnosť prenosovej trasy.
4. Ostatné správy - majú iba informačný charakter, niektoré SBS ich nepoužívajú. Môže ísť o správy typu aktivácia/deaktivácia bezpečnostného systému, odomknutie/uzamknutie dverí, práce technika atď.

Software na DPPC rozoznáva typy správ farebným odlíšením a akustickou signalizáciou. Navyše software ukladá a stráži správy, ktorými dispečer na prijatie poplachu reaguje. Tieto správy sa nazývajú „operátorské správy“. [46]

5.2.1 Prenos správy na DPPC a prenosové formáty

Prenosové správy sa programujú v ústredniach alebo komunikátoroch poplachových zabezpečovacích a tiesňových systémov. Ide vlastne o „kódovanú“ správu, ktorú bezpečnostný systém posiela po prenosovej trase do DPPC. Po prijatí správy na DPPC sa správa preloží, resp. dekóduje a vzápätí sa zobrazí na monitore operátora DPPC. DPPC potvrdí bezpečnostnému systému prijatie tejto informácie. Prenosové formáty sa delia na:

- Pulzné formáty: formát 3+1, 3+1 - rozšírený, 3+2, 4+1, 4+1 - rozšírený, 4+2, 4+2 - rozšírený, 4+3, formáty s paritou.
- Tónové formáty: Contact ID, DTMF.
- Modemové formáty: SIA.

Pulzné formáty využívajú určitý počet pulzov pre prenos jednotlivých správ v určitom čase. Medzi najrozšírenejšie pulzné formáty v ČR patrí formát 4+2, kde prvé štyri čísla označujú číslo objektu a ďalšie dve čísla predstavujú kód správy. Tento pulzný formát sa vysiela po analógovej linke. Prenosové rýchlosti analógových formátov môžu byť 1200, 2400, 4600 bit/s a záleží iba na type DPPC, s akým formátom a rýchlosťou dokáže pracovať.

Medzi tónové formáty sa zaraďuje Contact ID a DTMF. Tónové formáty pracujú s tónmi určitej frekvencie, kde sa každej číslici priraďuje dvojica takýchto tónov, ktorých je maximálne 16. Vďaka tomu sa skráti doba vytáčania a spojenie s volanou stanicou.

Posledným druhom prenosových formátov sú modemové formáty SIA. SIA formáty sú schopné v celkom krátkom časovom intervale preniesť viac informácií naraz, i keď je

väčšinou potrebné preniesť iba jednu informáciu z bezpečnostného systému, ale zato veľmi dôležitú. SIA pracuje na princípe tzv. full-duplex prenosu, tzn. že dáta sa prenášajú oboma smermi, v tomto prípade aj z DPPC do bezpečnostného systému. Komunikácia pripomína bežné modemy pre telefónne linky, teda až na prenosovú rýchlosť. [47]

Prenos správy na DPPC (telefónny):

1. Vznik udalosti na poplachovom systéme určenej pre prenos na DPPC.
2. Komunikátor ústredne poplachového systému sa pripojí na telefónnu linku a následne ústredňa vytočí číslo na DPPC.
3. Po druhom zazvonení sa na DPPC zdvihne linka.
4. DPPC pískne handshake, jedná sa o signál určitej frekvencie a dĺžky potvrdzujúci ústredni, že DPPC je pripravené prijať dáta a že prenosová cesta je priechodná.
5. Ústredňa pošle dáta na DPPC. Tónovo alebo pulzne prenášaná správa obsahuje číslo objektu a kód udalosti.
6. Podľa DPPC môže ústredňa poslať dáta znovu pre overenie.
7. DPPC potvrdí príjem písknutím kissoff, je to signál určitej frekvencie a dĺžky potvrdzujúci ústredni poplachového systému, že DPPC prijalo bezchybné dáta.
8. Ak ústredňa posiela ďalšie správy o stave stráženého objektu, potom komunikácia pokračuje akciou č. 5. Naopak, ak ústredňa nemá ďalšie správy pre posielanie údajov na DPPC, tak ukončí komunikáciu zavesením linky.
9. Po akcii č. 7 dôjde na strane DPPC k dekódovaniu dát a na monitore dispečingu sa zobrazí názov objektu a udalosť, ktorá bola prijatá. [43]

5.2.2 Šifrovaný prenos

Pri odosielaní správy zo stráženého objektu objektovým zariadením môže byť použité šifrovanie správ. Objektové zariadenie, resp. bezpečnostný systém musí oznámiť použitie AES šifrovania pri odosielaní správ. Pre šifrovanie správ sa používa metóda šifrovania po blokoch, viď. podkapitola 2.1.2 Blokové šifry. Spracovanie šifrovaných správ je pre prijímače dohľadového centra povinné.

V prípade použitia šifrovania správ sa šifrované správy označujú hviezdičkou. Šifrovanie je použité na časti správy ako sú dáta, časová značka a doplňujúce znaky. Prvý znak šifrovania sa označuje ako „[" v dátovej časti správy a končí pred posledným znakom správy „<CR>". Šifrovaná časť správy je označená farebne:

<LF><*crc16*><0*LLL*>

<„id protokolu*"><*seq*><R*rcvr*><L*pref*><#idk>[<*pad*>|...*data*...][x…data…]<*časová značka*>**

<CR>

Objektové zariadenia väčšinou používajú súkromné šifrovacie kľúče, ktoré majú dĺžku 128, 192 alebo 256 bitov. Tieto kľúče musí byť objektové zariadenie schopné uchovávať. Použitý kľúč musí byť rovnaký pre obidve strany komunikácie, ako pre objektové zariadenie, tak aj pre prijímač na strane DPPC. Musí byť rovnaký nie len obsah, ale aj dĺžka kľúča.

Prijímač DPPC musí vedieť pracovať so všetkými troma typmi šifrovacích kľúčov. Prijímač musí byť schopný spracovávať aj nešifrované správy. Každý port prijímacieho centra musí vedieť prijať a následne spracovať šifrované správy, pri ktorých bol použitý najmenej jeden šifrovací kľúč určený pre objektové zariadenie. Existuje možnosť použitia viacerých kľúčov s individuálnym využitím pre jednotlivé objekty alebo skupiny objektov.

Pre vytváranie súkromných a skupinových kľúčov je najvhodnejším spôsobom použitia pseudonáhodný proces. Potom sa z kľúča vytvorí postupnosť núl a jednotiek. Použitie nejakej slovnej frázy (binárne vyjadrenej v ASCII) je nezodpovedné.

Každý byte v šifrovanej časti správy je zakódovaný do dvoch ASCII znakov (0-9, A-F), ktoré vyjadrujú hexadecimálnu hodnotu šifrovaného bytu. [48]

5.3 Normy súvisiace s dohľadovými a poplachovými prijímacími centrami

DPPC upravuje v ČR súbor noriem ČSN EN 50518, ktorý pripravila technická komisia CENELEC (Európsky výbor pre normalizáciu v elektrotechnike). Súbor noriem sa vzťahuje na dohľadové a poplachové prijímacie centrá, ktoré slúžia k monitorovaniu, príjmu a spracovaniu signálov vyžadujúcich odozvu v prípade mimoriadnej udalosti.

Norma definuje poplachové prijímacie centrum (ARC) ako „centrum s trvalou obsluhou, do ktorého sú podávané informácie týkajúce sa stavu jedného alebo viacerých poplachových systémov".

Norma pozostáva z 3 častí:

- ČSN EN 50518-1 Umiestnenie a konštrukčné požiadavky
- ČSN EN 50518-2 Požiadavky na technické riešenie
- ČSN EN 50518-3 Pracovné postupy a požiadavky na prevádzku

5.3.1 ČSN EN 50518-1 Umiestnenie a konštrukčné požiadavky

Norma bola schválená dňa 1. 12. 2010 a účinnosť nadobudla dňa 1. 1. 2011. Táto časť normy stanovuje minimálne požiadavky na návrh, konštrukciu a funkčné zariadenia pre budovy, v ktorých sa uskutočňuje monitorovanie, príjem a spracovanie (poplachových) signálov generovaných poplachovými systémami pre zaistenie bezpečia a zabezpečenia. Požiadavky sa vzťahujú na prípady diaľkovej konfigurácie, v ktorých sú prenášané informácie z viacerých systémov do jedného alebo viacerých poplachových prijímacích centier. Okrem toho sa požiadavky vzťahujú aj na prípady jedného centra, ktoré je určené pre monitorovanie a spracovanie poplachov generovaných jedným alebo viacerými poplachovými systémami.

Norma opisuje voľbu miesta situovania DPPC, kde ide o miesto s nízkym rizikom požiaru, výbuchu, zaplavenia, vandalizmu a nebezpečenstva, ktoré hrozí z rôznych iných miest. Ak DPPC zdieľa objekt s inými užívateľmi tohto objektu, musí byť od zvyšku budovy oddelené fyzickou bariérou pozostávajúcou zo stien, podláh, stropov a nevyhnutných otvorov. Prvým krokom pri voľbe umiestnenia musí byť posúdenie rizík.

Ďalšia časť normy popisuje stavebné riešenie DPPC. Konštrukcia DPPC musí byť odolná proti útoku strelnou zbraňou, proti požiaru, chránená proti blesku. Norma presne stanovuje, aké príslušenstvo sa má v centre nachádzať, aké otvory je povolené v konštrukcii DPPC použiť. V norme sú podrobne popísané požiadavky na vstupnú predsieň, jej rozmery, požiadavky na dvere vo vstupnej predsieni, uzamykateľný systém dverí. Uzamykací mechanizmus v norme charakterizujú požiadavky ako na elektromechanický zámok, tak aj na mechanický zámok. V stavebnom riešení sa neopomínajú skutočnosti spojené s núdzovým východom a s ním súvisiace požiadavky na dvere. Norma opisuje odolnosť

zasklených plôch proti fyzickému útoku a proti priestrelu. Ventilácia má presne stanovenú kvalitu vzduchu, použitie filtrov, hladinu hluku v DPPC a otvory ventilačných systémov, ktoré musia byť chránené vzduchotesnými klapkami a je možné ich uzamknúť. Norma definuje požiadavky na technologické otvory v obvodovom plášti, ktoré slúžia pre všetky káble a potrubia. Napokon sa v stavebných prvkoch určujú požiadavky na manipulačné okienko.

Poplachové systémy DPPC tvoria ďalšiu časť normy, v ktorej sa nachádza ustanovenie, že elektronická detekcia pre všetky základné časti DPPC sa musí týkať udalostí ako sú útok zvonku, požiar, vchod/východ, plyn, detekcia rušenia v komunikačných zariadeniach, tieseň (prepadnutie), monitorovanie bezpečnosti personálu, signály bezpečnostných systémov, dohľad pomocou CCTV. Pre každú z uvedených udalostí sú v norme stanovené konkrétne požiadavky a uvedené príslušne normy. Ak pre niektorú z udalostí neexistuje príslušná norma, tak sa vykonáva údržba pre zaistenie trvalej spoľahlivosti na základe smerníc výrobcu.

Posledná kapitola normy popisuje napájanie elektrickým prúdom. Obsahom kapitoly je obmedzenie a spresnenie použitia sieťového napájania, ktoré musí byť použité ako hlavný zdroj, musí byť zaistený dostatočný príkon pre napájanie všetkých zariadení a napájacie káble musia byť chránené proti mechanickému poškodeniu a proti požiaru. Kapitola obsahuje aj informácie o záložnom zdroji napájania, záložnom akumulátore a pohotovostných generátoroch. [49]

5.3.2 ČSN EN 50518-2 Požiadavky na technické riešenie

Norma bola schválená 1. 8. 2011 a účinná je od 1. 9. 2011. Ide o časť normy EN 50518, ktorá stanovuje technické požiadavky týkajúce sa DPPC. Ďalej zahŕňa funkčné kritériá a overovanie výkonnosti.

Norma stanovuje požiadavky na výkonnosť, ktorú musia zaisťovať poplachové prijímacie zariadenia. Doba medzi časom prijatia výstupného signálu z komunikátora prijímacieho centra do indikačného zariadenia a časom začiatku zásahu dispečera musí splňovať nasledovné výkonnostné kritériá:

- v prípade tiesňových poplachov: 30s pri 80% prijatých signálov a 60s pri 98,5% prijatých signálov,

- v prípade ostatných poplachov: 90s pri 80% prijatých signálov a 180s pri 98,5% prijatých signálov.

Ďalšia časť normy sa venuje požiadavkám na komunikáciu, kde sa vyžaduje, aby DPPC disponovalo zariadeniami na záznam vonkajšej komunikácie s príslušným časovým údajom a dátumom tak, aby bolo možné komunikáciu obnoviť, zobraziť, znovu prehrať a uchovať po dobu najmenej troch mesiacov.

Požiadavky na príjem signálov určujú, že každý signál musí byť samostatne identifikovateľný a musí byť zaznamenaný, taktiež prípadné zásahy dispečera musia byť zaznamenané.

Pre pravidelné testovanie všetkých zariadení DPPC musia existovať dokumentované postupy. Zariadenia musia byť synchronizované so svetovým časom (UTC) najmenej každých 24 hodín. V norme sú definované zariadenia, pre ktoré treba vykonávať každodenné testy a pre ktoré je potreba vykonať týždenné testy.

Časť normy sa venuje údajom, kde je nutné upriamiť pozornosť na európsku smernicu o ochrane osobných údajov. Obsahom tejto časti normy je popis údajov o zákazníkovi, údajov o vonkajšej komunikácii DPPC a záznamov zásahov dispečera. Údaje o klientovi a záznamy zákrokov dispečera sa uchovávajú po dobu najmenej dvoch rokov a uchovávanie údajov o vonkajšej komunikácii DPPC sa musí uskutočňovať najmenej po dobu troch mesiacov.

V prípade vyradenia DPPC z činnosti musí byť vypracovaný núdzový plán pre vysporiadanie sa s následkami. V norme je ustanovené, čo musí núdzový plán obsahovať a sú v nej tiež uvedené príklady udalostí, ktoré musia byť brané do úvahy pri vytváraní núdzového plánu. [50]

5.3.3 ČSN EN 50518-3 Pracovné postupy a požiadavky na prevádzku

Norma ČSN EN 50518-3 bola schválená 1. 1. 2012 a jej účinnosť sa datuje od 1. 2. 2012. Táto časť normy EN 50518 stanovuje minimálne postupy a požiadavky na prevádzku DPPC.

Vyžaduje sa, aby DPPC bolo nepretržite obsadené najmenej dvoma dispečermi. Personál musí byť preverený a musí absolvovať bezpečnostné preverenie registru trestov štátnym

orgánom. Všetci dispečeri musia absolvovať výcvik zaisťujúci minimálnu spôsobilosť na vykonanie konkrétnych úloh, ktorý musí byť zdokumentovaný.

Predpisy pre prevádzkové postupy obsahujú postupy pre testovanie, vstup a odchod z DPPC, správu databáz, prevádzkovú kontinuitu a núdzové stavy, evakuačné postupy a napokon spracovanie signálov. Pri správe databáz musí byť systém správy databáz udržovaný v priestoroch prijímacieho centra, ktoré ukladá, organizuje, riadi, spravuje a umožňuje presuny všetkých klientskych údajov. DPPC musí zaviesť a dodržiavať ochranné opatrenia zaisťujúce nedotknuteľnosť zákazníckych údajov pred nepriateľskými činmi alebo vplyvmi. Navyše musia byť stanovené a zaznamenávané postupy pre všetkých zamestnancov, ako bezpečne zachádzať so všetkými dôvernými informáciami, ku ktorým majú prístup. Spomínané predpisy musia byť dostupné všetkým dispečerom.

Norma stanovuje povinnosť že každoročne musí byť prevádzaný audit zhody. Vedenie DPPC sa musí postarať o odstránenie všetkých nezhôd. DPPC musí mať ďalej zdokumentovaný postup pre prijímanie a spracovávanie sťažností zákazníkov.

Posledná časť normy ČSN EN 50518-3 sa týka údajov. Norma určuje povinnosť ustanovenia zdokumentovaných postupov definujúcich ukladanie, ochranu, oprávnené premiestňovanie, dobu platnosti a nakladanie s údajmi. Pre elektronicky ukladané údaje platí, že musia byť bezpečne archivované a musia byť zavedené zálohovacie postupy. Pri potrebe zmazania údajov dôvernej povahy ich odstránenie musí byť prevedené v súlade s normou EN 15713. [51]

II. PRAKTICKÁ ČASŤ

6 PROBLÉMY PRI REALIZÁCII TOHTO DRUHU OCHRANY

Realizácia tohto druhu ochrany neprináša iba samé výhody a prednosti, ale vyplýva z nej aj množstvo nevýhod a problémov, ktoré je potrebné riešiť, resp. im nejakým spôsobom predchádzať. Riešenia na mnohé problémy sa nachádzajú v predpisoch príslušných noriem a v legislatíve.

6.1 Problémy spojené s realizáciou kryptografickej ochrany

Problémy pri uskutočňovaní kryptografickej ochrany sa viažu najmä na skutočnosť, že jej realizáciu a manipuláciu s kryptografickými prostriedkami a kryptografickým materiálom povoľuje Národný bezpečnostný úrad a že kryptografickú ochranu musia vykonávať zamestnanci, ktorí sú riadne zaškolení.

Bezpečnostnú správu kryptografickej ochrany, obsluhu a výrobu kryptografického prostriedku alebo výrobu kryptografického materiálu na zaistenie funkcie kryptografického prostriedku môže vykonávať iba pracovník, ktorý je držiteľom platného osvedčenia alebo vlastní osvedčenie o špeciálnej odbornej spôsobilosti pracovníka kryptografickej ochrany. Obsahom pojmu špeciálna odborná spôsobilosť je znalosť predpisov z oblasti kryptografickej ochrany utajovaných informácií a schopnosť ich aplikácie. Tieto znalosti overuje NBÚ skúškou špeciálnej odbornej spôsobilosti.

Osoba, ktorá uskutočňuje výkon užívateľských funkcií kryptografického prostriedku, musí spĺňať podmienky prístupu k utajovanej informácii a musí byť k obsluhe kryptografického prostriedku zaškolená. Zásadnou podmienkou, ktorej splnením fyzická osoba získa prístup k utajovanej informácii, je, že spomínaná fyzická osoba tento prístup nevyhnutne potrebuje na výkon svojej funkcie. Fyzická osoba musí byť držiteľom oznámenia o splnení podmienok pre prístup k utajovanej informácii, pričom toto oznámenie sa vydá iba osobe, ktorá je spôsobilá na právne úkony, spĺňa vekový limit minimálne 18 rokov a je bezúhonná.

Držiteľom platného osvedčenia fyzickej osoby musí byť taktiež kuriér kryptografického materiálu, ktorý chce vykonávať jeho prepravu, a musí byť k tejto preprave zaškolený. Zaškolenie kuriéra kryptografického materiálu zaisťuje bezpečnostný správca kryptografickej ochrany. Vývoz certifikovaného kryptografického materiálu z územia Českej republiky sa smie uskutočniť iba na základe povolenia NBÚ.

Pri ochrane utajovaných informácií je potrebné zabezpečiť elektrické a elektronické zariadenia, aby nedošlo k úniku utajovanej informácie prostredníctvom kompromitujúceho vyžarovania. Ak je na ochranu utajovanej informácie pred únikom kompromitujúcim vyžarovaním použitá tieniaca komora, musí byť certifikovaná NBÚ. Čo sa týka certifikácie, povinnosťou právnickej osoby, podnikajúcej fyzickej osoby a orgánu štátu je používať na kryptografickú ochranu iba prostriedky certifikované NBÚ a používať kryptografické pracovisko iba na ten účel, na ktorý bolo certifikované a schválené do prevádzky.

Ďalej je povinnosťou právnickej osoby a podnikajúcej fyzickej osoby, ktoré majú prístup k utajovanej informácii, a orgánu štátu viesť evidenciu kryptografického materiálu, evidenciu pracovníkov kryptografickej ochrany, evidenciu prevádzkovej obsluhy kryptografického prostriedku, evidenciu kuriérov kryptografického materiálu a evidenciu prípadov neoprávneného nakladania s utajovanou informáciou. [23]

Na mieste, kde sa uskutočňuje výkon kryptografickej ochrany, musí byť prostredníctvom zodpovednej osoby určená bezpečnostná správa, v ktorej je zahrnutá personálna, fyzická a administratívna bezpečnosť a bezpečnosť informačných alebo komunikačných systémov pri zaisťovaní kryptografickej ochrany.

Výroba materiálu na zaistenie funkcie kryptografického prostriedku musí byť vykonaná povereným pracovníkom špeciálnej obsluhy kryptografického prostriedku, ktorý musí byť držiteľom platného osvedčenia o špeciálnej odbornej spôsobilosti, v ktorom je uvedené oprávnenie na výrobu materiálov zaisťujúcich funkciu kryptografického prostriedku.

Kryptografický dokument je možné preniesť elektronickou cestou iba za predpokladu splnenia konkrétnych podmienok. Jednou z podmienok je, aby bol elektronický prenos kryptografického dokumentu zaznamenaný v tomto dokumente a v jednacom protokole. Ďalšou podmienkou je zaznamenanie manipulácie s kryptografickým dokumentom v priebehu elektronického prenosu. Pri odoslanom výtlačku kryptografického dokumentu sa v zázname pre uloženie do riadku „Vypravil" zapíše „odoslané automaticky", meno a priezvisko odosielateľa. Prijatie kryptografického dokumentu sa zaznamená do evidencie odoslaných a prijatých správ elektronického prenosu a uvedie sa doň dátum a čas prijatia, meno a priezvisko príjemcu. Prijatý dokument musí byť bezodkladne predaný poverenému pracovníkovi k zaevidovaniu.

Pri príjme kryptografickej zásielky nastáva možnosť vzniku vady. V takejto situácii je potrebné informovať odosielateľa a spísať záznam o poškodení kryptografickej zásielky. Kryptografickú zásielku nemožno prepraviť verejnými dopravnými prostriedkami s výnimkou leteckej, námornej a vodnej prepravy. Prepravu zásielky je potrebné zaistiť tak, aby nedošlo k neoprávnenej manipulácii s jej obsahom. Kryptografický materiál je možné prenášať iba s písomným súhlasom zodpovednej osoby alebo s písomným súhlasom vedúceho zamestnanca, pričom písomný súhlas sa ukladá spoločne s kryptografickým materiálom.

Kryptografický dokument je možné zapožičať pracovníkovi kryptografickej ochrany iba so súhlasom zodpovednej osoby orgánu štátu, právnickej osoby alebo podnikajúcej fyzickej osoby alebo ňou povereného pracovníka kryptografickej ochrany. Vypožičané kryptografické dokumenty sa každých 6 mesiacov od zapožičania predkladajú poverenej osobe k vykonaniu fyzickej kontroly. [24]

6.2 Problémy spojené s realizáciou DPPC

Pomerne veľká nevýhoda spočíva vo vysokej cene za napojenie na DPPC a služby s ním spojené. Kým paušálne poplatky a výjazdy zásahových skupín by si ešte mohli bežní obyvatelia domu dovoliť, to však k samotnej službe nestačí. Monitorovaný objekt totiž musí mať nainštalované zabezpečovacie alebo monitorovacie zariadenie v súlade s platnými technickými normami, čo sa tiež prejaví na výslednej cene. Navyše je potrebné počítať so vstupnými poplatkami za pripojenie objektu na DPPC, ktoré môže byť napojené prostredníctvom telefónnej linky, mobilnej siete, rádiovej siete alebo internetu. Preto tieto služby väčšinou využívajú rôzne firmy a podniky, akými sú napr. zlatníctva, klenotníctva, banky a im podobné inštitúcie.

Samotná výstavba DPPC je tiež veľmi finančne náročná. Mnohé prvky súvisiace s výstavbou dohľadového centra totiž podliehajú mnohým podmienkam. Obvodový plášť budovy musí byť odolný proti fyzickým útokom. Vonkajšie steny, podlahy a stropy obvodového plášťa budovy sa väčšinou konštruujú zo železobetónu, liateho betónu a plnej ocele. Dvere a zasklené plochy plášťa musia poskytovať určitú odolnosť proti ručne vedenému útoku a proti útoku strelnou zbraňou. Plášť budovy musí byť odolný proti požiaru a blesku. Vstupnú predsieň musia tvoriť dvoje dvere, ktoré treba vybaviť

samouzavieracím a samouzamykateľným systémom. Dvere musia byť elektricky vzájomne viazané, aby nebolo možné ich otvoriť súčasne.

Budova DPPC musí byť vybavená poplachovým zabezpečovacím systémom stupňa zabezpečenia 3 podľa požiadaviek EN 50131-1. Ďalej musí byť vybavená poplachovým požiarnym systémom, ktorý musí obsahovať certifikované komponenty, akustickou alebo optickou signalizáciou, detekčným systémom detekujúcim minimálne oxid uhoľnatý a tiesňovými hlásičmi. Bezpečnosť personálu DPPC musí byť monitorovaná. Potrebné je tiež nainštalovať kamerový systém, prostredníctvom ktorého bude možné sledovanie všetkých prístupových ciest k budove a to v súlade so smernicou pre aplikáciu EN 50132-7. DPPC musí obsahovať aj záložné zdroje v prípade výpadku z napájania.

Vnútorný priestor DPPC musí byť v nepretržitej prevádzke a 24 hodín denne musí byť zaistená jeho obsluha. V DPPC musia byť stále prítomní aspoň dvaja dispečeri. Z toho dôvodu musí byť priestor vybavený toaletami a umyvárňami. Ideálne je, ak sú k dispozícii priestory na prípravu jedla a pitia.

DPPC musí obsahovať zariadenia, ktoré umožňujú zaznamenávanie vonkajšej komunikácie s časom a dátumom. Každý prijatý signál na DPPC musí byť samostatne identifikovateľný a automaticky zaznamenaný. Prijatý signál musí poskytovať informácie o identifikácii strážených priestorov, type signálu a o čase a dátume prijatia signálu.

V zriadenom DPPC musia byť vykonávané každodenné testy, kde je denne kontrolovaná správna funkčnosť komunikátora prijímacieho centra, indikačného zariadenia, komunikačných systémov a všetky prijaté a odoslané komunikačné linky. Okrem každodenných testov je potrebné vykonávať aj týždenné testy, pomocou ktorých je kontrolovaná správna funkčnosť poplachových systémov, elektrických napájacích zdrojov a zariadení pre núdzové osvetlenie.

Akákoľvek súčasť zariadenia, ktorá je zapojená do príjmu, zobrazenia alebo prenosu poplachového signálu, vrátanie napájania, musí disponovať záložným zariadením a postupom, ktorým môže byť toto zariadenie uvedené do prevádzky automaticky alebo dispečerom. Na opravu poškodeného zariadenia musí tiež existovať zdokumentovaný postup.

Počas prevádzky prijímacieho centra je potrebné dbať na ochranu osobných údajov. Nevyhnutné je to hlavne pri údajoch o zákazníkovi, pri údajoch o vonkajšej komunikácii

DPPC a pri záznamoch o zákrokoch dispečera. Celková výkonnosť poplachového systému musí byť v súlade s normami EN 50131-1 a EN 50136-1.

DPPC musí mať pripravený a vypracovaný núdzový plán pre jeho prípadné vyradenie z prevádzky. Pri spisovaní núdzového plánu sú brané do úvahy nasledujúce udalosti:

- zlyhanie schopnosti vykonávania úkonov,
- poruchy alebo poškodenie technickej infraštruktúry, komunikačného zariadenia alebo komunikačných okruhov,
- požiar, vrátane vystavenia ohňu v susedných objektoch,
- povodne alebo iné prieniky vody,
- poškodenie pri búrke, vrátane prepätia v dôsledku blesku pri dodávke elektriny a telefónneho vedenia,
- náraz vozidla, vrátane koľajových vozidiel a lietadiel,
- úmyselné poškodenie,
- zločinný útok, vyhrážanie bombou alebo iné situácie protiprávneho nátlaku.

V DPPC môže pracovať iba personál, ktorý bol pred nástupom do zamestnania v DPPC riadne preverený. Všetci zamestnanci a potenciálni zamestnanci musia byť preverení štátnym orgánom na základe registra trestov. Organizácia prevádzkujúca DPPC musí umožniť svojmu personálu absolvovanie potrebného výcviku, ktorý pokrýva teoretické a praktické znalosti stanovené pre DPPC.

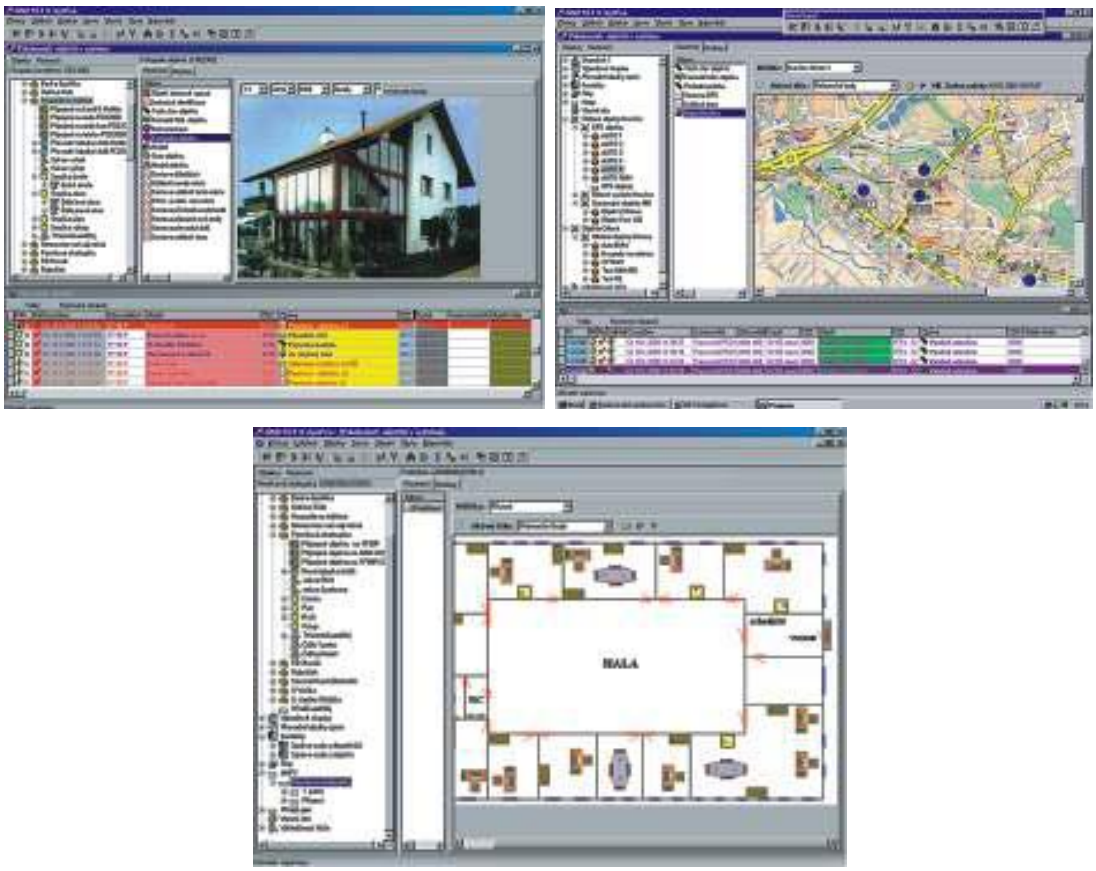
Súčasťou dokumentovaných postupov dostupných všetkým dispečerom musí byť aj predpis pre vstup do DPPC. Predpis sa týka najmä identifikácie osôb požadujúcich sprístupnenie vchodu do priestorov prijímacieho centra. Pred povolením prístupu do DPPC musí byť vykonaná pozitívna identifikácia osôb vyžadujúcich toto povolenie. Prístup je potrebné riadiť zvnútra prostredníctvom dispečera počas celej doby prevádzky DPPC. Ďalej sa vyžaduje, aby bol vedený záznam o všetkých osobách, ktoré prijímacie centrum navštívili. Navyše je nutné, aby DPPC zaviedlo a dodržiavalo ochranné opatrenia zaisťujúce nedotknuteľnosť údajov týkajúcich sa klientov pred nepriateľskými činmi alebo vplyvmi. Organizácia prevádzkujúca DPPC musí disponovať stanovenými predpismi pre každého zamestnanca, ako má bezpečne zachádzať so všetkými dôvernými informáciami, ku

ktorým má prístup. Každému zákazníkovi, ktorý má pripojený poplachový systém k DPPC, musí byť pridelený individuálny a jednoznačne označený záznam. V DPPC musí byť zaistená dokumentácia, v ktorej sú stanovené postupy na ochranu, ukladanie, premiestňovanie a nakladanie s údajmi. Údaje elektronickej podoby musia byť bezpečne uložené a k týmto údajom musia byť zavedené postupy pre zálohovanie.

Pre DPPC musí byť vypracovaný detailný evakuačný plán zahŕňajúci čiastočnú a úplnú evakuáciu. Tento plán musí tiež obsahovať uvedenie do pôvodného stavu nasledujúce po evakuácii. Všetci zamestnanci musia disponovať inštrukciami a výcvikom pre núdzové postupy, ktorý musí byť zaznamenávaný.

Každý rok musí byť vykonaný audit zhody akreditovaným orgánom podľa EN 45011 alebo EN-ISO/IEC 17020.

DPPC musí disponovať špeciálnym softwarom, ktorý umožňuje spracovávať dáta, a moderným informačným systémom. [49], [50], [51]



Obr. 36. Príklad softwaru DPPC, monitorovací software NET-G [52]

7 POROVNANIE LEGISLATÍVY ČR A SR V OBLASTI KRYPTOGRAFIE A UTAJOVANÝCH INFORMÁCIÍ

Slovenským ekvivalentom už spomenutého českého zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní zbůsobilosti je zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

Zatiaľ čo v ČR vykonávacie právne predpisy v tejto oblasti predstavujú dve vyhlášky, konkrétne vyhláška č. 432/2011 Sb. o zajištění kryptografické ochrany utajovaných informací a vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, v slovenskej legislatíve je problematika kryptografie upravená len v jednom právnom predpise, vyhláške č. 340/2004 Z.z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií. Kým v českej legislatíve je certifikácia upravená samostatnou vyhláškou, v SR je zahrnutá v uvedenej vyhláške č. 340/2004 Z.z.

7.1 Zákonné ustanovenia

Slovenská legislatíva na český pojem utajovaná informácia používa termín utajovaná skutočnosť. Utajovaná skutočnosť je v ustanovení § 2 zákona č. 215/2004 Z.z. definovaná ako „informácia alebo vec určená pôvodcom utajovanej skutočnosti, ktorú vzhľadom na záujem Slovenskej republiky treba chrániť pred vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením a ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda Slovenskej republiky svojím nariadením.“

Zákony sa líšia aj v pojmoch týkajúcich sa kryptografie. Zatiaľ čo v ČR sa jedná o kryptografickú ochranu, v SR je ňou šifrová ochrana. Kým v slovenskom zákone sa definícia kryptografických pojmov nachádza v jeho prvej časti v § 2, v českom až v ôsmej hlave jeho prvej časti v § 37. V zákone č. 412/2005 Sb. sú definované pojmy ako kryptografický materiál, kryptografické prostriedky a kryptografické pracovisko, ktoré sú vysvetlené v tretej kapitole tejto práce. Slovenský zákon č. 215/2004 Z.z. vysvetľuje odlišné pojmy ako certifikačná autorita, digitálny certifikát, verejný podpisový kľúč, systém šifrovej ochrany informácií a prostriedok šifrovej ochrany informácií, ktoré § 2 charakterizuje nasledovne:

- Certifikačná autorita, ktorej povinnosťou je vydávanie a overovanie digitálnych certifikátov verejných kľúčov, ktoré sa používajú v asymetrických systémoch.
- Digitálny certifikát je podľa zákona elektronické potvrdenie plniace funkciu priradenia verejného podpisového kľúča k určitému subjektu a navyše potvrdzuje jeho identitu.
- Verejný podpisový kľúč je vlastne kryptografický kľúč, ktorý slúži na overenie elektronického podpisu.
- Systém šifrovej ochrany informácií je súbor prostriedkov šifrovej ochrany, ktorý sa používa na generovanie, distribúciu a likvidáciu šifrových materiálov po skončení ich platnosti.
- Prostriedkom šifrovej ochrany informácií je zariadenie stanovené k šifrovej ochrane informácií a šifrovým materiálom. [52]

Stupne utajenia utajovaných informácií, resp. skutočností sú v obidvoch štátoch rovnaké, jedná sa o utajenie stupňa:

a) prísne tajné (PT),

b) tajné (T),

c) dôverné (D),

d) vyhradené (V).

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní zbůsobilosti venuje kryptografickej ochrane v jeho druhej časti celú VIII. hlavu. Jednotlivé ustanovenia poskytujú informácie o kontrolovanej kryptografickej položke, výkone kryptografickej ochrany, špeciálnej odbornej spôsobilosti, prevádzkovej obsluhe kryptografického prostriedku, manipulácii s kryptografickým materiálom, preprave kryptografického materiálu a prostriedku, kompromitácii kryptografického materiálu, distribúcii a evidencii kryptografického materiálu, vykonávacích ustanoveniach a kompromitujúcom vyžarovaní. Slovenský zákon č. 215/2005 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov venuje šifrovej ochrane informácií celú svoju tretiu časť, v ktorej jednotlivé ustanovenia definujú pojmy ústredný šifrový orgán, rezortný šifrový orgán, certifikačná autorita a odborná spôsobilosť.

Ustanovenie § 65 slovenského zákona č. 215/2005 Z.z. sa zaoberá povinnosťami a oprávneniami ústredného šifrového orgánu, ktorý riadi a kontroluje činnosť ústredných orgánov štátnej správy v oblasti šifrovej ochrany informácií. Zamestnanci ústredného šifrového orgánu sú oprávnení vstupovať na pracoviská šifrových orgánov za účelom vykonávania kontroly bezpečnosti systémov a prostriedkov šifrovej ochrany informácií. Ústredný šifrový orgán môže zastaviť svojím rozhodnutím prevádzku systému alebo prostriedku šifrovej ochrany a to v prípade zistenia závažných nedostatkov na úseku šifrovej ochrany informácií. Po odstránení týchto nedostatkov ústredný šifrový orgán svojím písomným súhlasom môže obnoviť prevádzku systému alebo prostriedku šifrovej ochrany. Ďalšie ustanovenia informujú o skutočnosti, že rezortný šifrový orgán na zabezpečenie šifrovej ochrany informácií môže byť zriadený ako osobitné pracovisko a to pomocou vedúceho ústredného orgánu štátnej správy. Výkon funkcie certifikačnej autority je tiež zabezpečený ústredným šifrovým orgánom na ochranu utajovaných skutočností. Zamestnanec v oblasti šifrovej ochrany musí byť oprávnený na oboznamovanie sa s utajovanými skutočnosťami a taktiež musí spĺňať podmienky odbornej spôsobilosti.

Český zákon č. 412/2005 Sb. sa v jeho piatej časti v ustanoveniach § 137 a § 138 venuje povinnostiam a oprávneniam NBÚ ČR. V slovenskom zákone č. 215/2004 Z.z. sa povinnostiam a oprávneniam NBÚ SR venuje jeho štvrtá časť v ustanovení § 70 a šifrovou ochranou informácií sa konkrétne zaoberá ods. 1 písm. c). [23], [52]

Pre český NBÚ vyplýva zo zákona v oblasti kryptografie niekoľko povinností. Jedná sa o povinnosti spojené so zaisťovaním činnosti Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího vyzařování a Národního střediska pro bezpečnost informačních systémů. NBÚ taktiež vykonáva certifikáciu technického prostriedku, informačného systému, kryptografického prostriedku, kryptografického pracoviska a tieniacej komory. Okrem toho plní aj funkciu výskumu, vývoja a výroby národných kryptografických prostriedkov, vyvíja a schvaľuje národné šifrové algoritmy a vytvára národnú politiku kryptografickej ochrany. NBÚ je oprávnený viesť evidenciu pracovníkov kryptografickej ochrany, kuriérov kryptografického materiálu a evidenciu fyzických osôb, ktoré vlastnia osvedčenie o špeciálnej odbornej spôsobilosti. Disponuje aj kompetenciou viesť certifikačný spis informačného systému, kryptografického prostriedku, pracoviska a tieniacej komory, zoznam kontrolovaných kryptografických položiek a dokumentáciu pre vykonávanie činností. NBÚ má oprávnenie

uzatvárať zmluvy s orgánom štátu alebo podnikateľom na vykonávanie čiastočných úloh pri certifikácii kryptografických prostriedkov, kryptografického pracoviska a tieniacich komôr. Zmluvy môže uzatvárať aj na činnosti spojené s vykonávaním školenia špeciálnej odbornej spôsobilosti pracovníkov kryptografickej ochrany, so zisťovaním možnosti výskytu kompromitujúceho vyžarovania tam, kde sa utajované informácie budú vyskytovať, a s prevádzaním výroby kryptografických prostriedkov. [23]

Obr. 37. Znak NBÚ ČR [53]

Obr. 38. Sídlo NBÚ ČR [53]

Pôsobnosť NBÚ SR sa v slovenskom zákone č. 215/2004 Z.z. delí na jednotlivé úseky. Konkrétne sa jedná o úsek:

a) ochrany utajovaných skutočností,

b) ochrany zahraničných informácií,

c) šifrovej ochrany informácií,

d) vnútornej ochrany.

Pôsobnosť NBÚ na úseku šifrovej ochrany informácií súvisí s plnením funkcie ústredného šifrového orgánu SR, vypracovávaním koncepcie rozvoja šifrovej ochrany informácií a

ustanovením zásad šifrovej ochrany informácií. NBÚ má oprávnenie certifikovať alebo overovať a uznávať zahraničné certifikáty a tiež schvaľovať do prevádzky metódy, systémy a prostriedky šifrovej ochrany informácií. Ďalej kontroluje bezpečnosť šifrovej ochrany informácií a určuje podmienky týkajúce sa zamestnancov, ako je výber zamestnancov, ich odborná príprava, vydávanie a odnímanie osvedčenia na prácu. Rozhoduje o rozsahu a spôsobe využívania informačného systému šifrovej ochrany informácií a o rozsahu, spôsobe a podmienkach správy systémov šifrovej ochrany informácií a výroby šifrových materiálov. Zaoberá sa výskumom a vývojom v oblastiach kryptológie a výroby prostriedkov šifrovej ochrany informácií. NBÚ vykonáva znaleckú činnosť, vedie rôzne evidencie, ktoré súvisia so šifrovou ochranou informácií, plní funkciu gestora vládneho a zahraničného spojenia a gestora zabezpečovania prostriedkov šifrovej ochrany informácií, vydáva bezpečnostné štandardy pre oblasť šifrovej ochrany informácií a pre ochranu pred nežiaducim elektromagnetickým vyžarovaním technických prostriedkov a prostriedkov šifrovej ochrany informácií. [52]

Obr. 39. Znak NBÚ SR [54]

Obr. 40. Sídlo NBÚ SR [55]

7.2 Ustanovenia vykonávacích právnych predpisov

V českej legislatíve tieto ustanovenia obsahujú dve už spomenuté vyhlášky č. 432/2011 Sb. a č. 525/2005 Sb., ktorých obsah je podrobnejšie priblížený v tretej kapitole o legislatíve ČR spojenej s kryptografiou. Slovenská vyhláška č. 340/2004 Z.z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií, nadobudla účinnosť dňa 1. 6. 2004.

Vyhláška sa podrobne venuje certifikácii a schvaľovaniu systémov a prostriedkov šifrovej ochrany informácií do prevádzky, ich použitiu, nasadeniu, preprave, evidencii a používaniu šifrových materiálov. Popisuje podrobnosti o vedení evidencií zamestnancov v oblasti šifrovej ochrany a overovaní ich odbornej spôsobilosti a pojednáva o náležitostiach zriaďovania rezortného šifrového orgánu.

V ustanovení § 2 vyhláška definuje certifikáciu prostriedkov ako overovanie a osvedčovanie spôsobilosti prostriedku chrániť utajované skutočnosti, ktorá má byť v súlade s bezpečnostným štandardom pre systémy a prostriedky šifrovej ochrany informácií a tiež s bezpečnostným štandardom na ochranu pred nežiaducim elektromagnetickým vyžarovaním.

Znenie § 3 popisuje skutočnosť, že schvaľovanie prostriedkov do prevádzky je možné iba na základe príslušného certifikátu vydaného úradom alebo vedúcim a musí byť splnená podmienka prevádzky prostriedku v chránenom priestore a v priestore, ktorý zodpovedá bezpečnostnému štandardu na ochranu pred nežiaducim elektromagnetickým vyžarovaním.

Vyhláška pojednáva o používaní a preprave prostriedkov, pričom prostriedky možno používať iba za predpokladu, ak sú riadne certifikované a schválené do prevádzky a ich používanie je umožnené iba v súlade s návodom na obsluhu a pravidlami na ich používanie. Prepravu prostriedkov smú vykonávať iba osoby oprávnené na prepravu utajovaných skutočností, ktorých si určí vedúci. Prijaté zásielky s prostriedkami môže otvoriť len adresovaný príjemca na pracovisku šifrového orgánu. Zariadenia ustanovené na šifrovú ochranu informácií a šifrové materiály určené do týchto zariadení sa prepravujú a ukladajú oddelene.

Rezortný šifrový orgán vedie centrálnu evidenciu všetkých prostriedkov a jedenkrát do roka vykonáva ich fyzickú inventarizáciu. Ustanovenie § 6 vyhlášky č. 340/2004 Z.z. opisuje používanie šifrových materiálov, ktoré definuje ako „heslá, kľúče, premenné parametre kryptografických algoritmov označené podľa druhu prostriedku a stupňa ochrany

utajovaných skutočností.'' Šifrové materiály je možné používať iba v prípade, ak sú v súlade s pravidlami na používanie prostriedku.

Znenie § 7 pojednáva o odbornej spôsobilosti zamestnanca, ktorá sa preukazuje znalosťou právnych predpisov a interných predpisov o ochrane utajovaných skutočností. Ak by zamestnanec preukázal záujem o prácu s prostriedkom, musí disponovať znalosťami návodu na obsluhu daného prostriedku, pravidiel na jeho používanie a musí vedieť vykonať praktickú obsluhu prostriedku. Odbornú prípravu na získanie odbornej spôsobilosti vykonáva NBÚ a rezortný šifrový orgán.

Vyhláška popisuje, aké náležitosti musí obsahovať evidencia zamestnancov na úseku šifrovej ochrany informácií a aké náležitosti musí obsahovať žiadosť vedúceho o súhlas ústredného šifrového orgánu na zriadenie rezortného šifrového orgánu.

Rezortný šifrový orgán sa zruší, ak sa skončila potreba šifrovej ochrany informácií v ústrednom orgáne štátnej správy, ak došlo k zániku, príp. zrušeniu ústredného orgánu štátnej správy alebo ak by došlo k zlúčeniu ústredného orgánu štátnej správy s ústredným orgánom štátnej správy, ktorá má zriadený rezortný šifrový orgán. [56]

ZÁVER

Cieľom mojej diplomovej práce bolo poskytnúť čitateľovi informácie o technologických možnostiach kryptografickej ochrany. Problematiku týkajúcu sa kryptografie som sa usilovala zachytiť už od jej skorých počiatkov až po jej súčasné moderné metódy.

Na začiatku práce som sa snažila uviesť čitateľa do témy definovaním základných pojmov týkajúcich sa kryptografie a vysvetlením princípu šifrovania. Následne som sa stručne venovala histórii šifrovania, ktorú som si rozdelila do jednotlivých období, počínajúc dávnym starovekom a končiac obdobím 2. sv. vojny.

V ďalšej kapitole som sa zaoberala súčasnými metódami kryptografie. Postupovala som v nej podľa základného rozdelenia kryptografie, ktoré pozostáva zo symetrického šifrovania, asymetrického šifrovania a hybridného šifrovania. Ďalej som považovala za dôležité v tejto kapitole aspoň okrajovo spomenúť kvantovú kryptografiu a eliptické krivky. Neopomenula som ani vysvetlenie pojmov ako hash algoritmy, elektronický podpis a program na šifrovanie emailov PGP.

Popri opise kryptografických metód bolo mojím zámerom popísať túto problematiku aj z pohľadu utajovaných informácií a know-how. Touto problematikou sa zaoberá legislatíva ČR, ktorá sa venuje kryptografii v zákone č. 412/2005 Sb. a v dvoch s ním súvisiacich vyhláškach č. 432/2011 Sb. a č. 525/2005 Sb. Kryptografia chráni utajované informácie pomocou rôznych prostriedkov, ktoré som v práci postupne popísala. Do tejto skupiny prostriedkov sa zaraďujú najmä generátory šumu využívajúce najčastejšie biely a ružový šum, rádiové analyzátory, tieniace komory pracujúce na princípe Faradayovej klietky a v neposlednom rade aj technika na ochranu GSM komunikácií. Kryptografia sa používa aj v dohľadových a poplachových prijímacích centrách, v ktorých vzniká prevádzkovateľom povinnosť chrániť a uchovávať citlivé údaje o ich zákazníkoch.

V druhej časti diplomovej práce bolo mojou snahou priblížiť problémy týkajúce sa dohľadových a poplachových prijímacích centier, medzi ktoré patrí najmä ich drahá výstavba a nákladné napojenie objektu na DPPC. Pri poskytovaní kryptografickej ochrany sa vyskytujú aj problémy súvisiace so získaním povolenia z NBÚ a so zaškolením a bezpečnostným preverením personálu. V poslednej kapitole som pozornosť čitateľa upriamila na porovnanie legislatívy ČR a SR.

SUMMARY

A goal of my diploma work was to provide the reader with information about the technological possibilities of cryptographic protection. I tried to capture the issue related to cryptography from its early beginnings to its current modern methods.

At the beginning of the work, I tried to put the reader into the topic by defining the basic concepts of cryptography and explains the principles of encryption. Then I was devoted to history of cryptography briefly, which I divided into individual periods, beginning with ancient and ending World War II.

In the next chapter I dealt with current methods of cryptography. I proceeded in it according the basic division of cryptography, which consists of symmetric encryption, asymmetric encryption and hybrid encryption. Next, in this chapter I considered it important to mention quantum cryptography and elliptic curve at least marginally. I did not forget or explanation of terms such as hash algorithms, electronic signature and email encryption program PGP.

In addition to the description of cryptographic methods my intention was to describe this issue also from the perspective of classified information and know-how. This issue is addressed in the legislation of the Czech Republic, which deals with cryptography in law no. 412/2005 Sb. and in two related edicts no. 432/2011 Sb. and no. 525/2005 Sb. Cryptography protects classified information by various facilities, which I described in the work gradually. In this group of facilities are classified especially noise generators using the most white and pink noise, radio analyzers, shielding chambers working on the principle of Faraday cage and last but not least the technology to protect GSM communications. Cryptography is also used in alarm receiving centers, where the operators are obliged to protect and preserve the sensitive data about their customers.

In the second part of the diploma work my effort was to bring problems related to alarm receiving centers, including mainly their expensive construction and costly connection an object to ARC. In providing cryptographic protection there are also problems associated with obtaining a permit from NBÚ and staff training and security verification. In the last chapter, I drew attention of the reader to comparison legislation of the Czech and Slovak Republic.

ZOZNAM POUŽITEJ LITERATÚRY

[1] PIPER, Fred a Sean MURPHY. *Kryptografie.* 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.

[2] VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. 1. vyd. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-000-1888-8.

[3] *Invisible ink* [online]. [cit. 2013-02-18]. Obrázok vo formáte jpg. Dostupné z: http://3.bp.blogspot.com/_5kSia53SdlI/TE_fxmQjYuI/AAAAAAAABA8/jhxzbdZMNis/s320/invisible_ink.gif

[4] *La steganografia: l'arte della comunicazione del Nuovo Ordine Mondiale* [online]. 2007 [cit. 2013-02-18]. Obrázok vo formáte jpg. Dostupné z: http://etleboro.com/picture_library/_Graphics_D5_37_7.jpg

[5] HANŽL, Tomáš, Radek PELÁNEK a Ondřej VÝBORNÝ. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi.* Vyd. 1. Praha: Portál, 2007, 198 s. Oko. ISBN 978-807-3671-969.

[6] JAŠEK, Roman. *Informační a datová bezpečnost.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-731-8456-7.

[7] ZELENKA, Josef. *Ochrana dat: kryptologie.* Vyd. 1. Hradec Králové: Gaudeamus, 2003, 198 s. ISBN 80-704-1737-4.

[8] *ATBASH (Hebrew) cipher* [online]. 2004 [cit. 2013-02-19]. Obrázok vo formáte gif. Dostupné z: http://www.borderschess.org/Atbash.gif

[9] *Telegraf* [online]. [cit. 2013-02-20]. Obrázok vo formáte jpg. Dostupné z: http://www.national-geographic.cz/wp-content/uploads/2012/09/samuel_morse_telegraph-320x229.jpg

[10] *Rádio* [online]. [cit. 2013-02-21]. Obrázok vo formáte jpg. Dostupné z: http://1.bp.blogspot.com/-H5FLQ6ywcE4/Tc18PX8wa_I/AAAAAAAAAKg/Cs8vrYMKwGc/s1600/OldRadio.jpg

[11] *German Enigma machine* [online]. [cit. 2013-02-22]. Obrázok vo formáte jpg. Dostupné z: http://www.ilord.com/enigma.html

[12] JANEČEK, Jiří. *Válka šifer: výhry a prohry československé vojenské rozvědky*, 1939-1945. Olomouc: Votobia, 2001, 345 p. ISBN 80-719-8505-8.

[13] UŘIČÁŘ, Peter. *Základy šifrování* [online]. [cit. 2013-03-13]. Dostupné z: http://www.vrstevnice.com/akce/grandaction/vskola/3semestr/site/sifrovani.pdf

[14] HÁLA, Vojtěch. *Kvantová kryptografie* [online]. 2005 [cit. 2013-03-19]. ISSN 1214-1674. Dostupné z: http://www.aldebaran.cz/bulletin/2005_14_kry.php

[15] LÓRENCZ, Róbert. *Bezpečnost: 7. Proudové šifry, blokové šifry, DES, 3DES, AES, operační módy* [online]. [cit. 2013-03-21]. Dostupné z: https://edux.fit.cvut.cz/oppa/BI-BEZ/prednasky/bez7.pdf

[16] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. Praha: Dokořán, 2003, 382 s. ISBN 80-865-6918-7.

[17] DUŠEK, Miloslav, Ondřej HADERKA a Martin HENDRYCH. *Foton jako důvěryhodný kurýr: Co je to kvantová kryptografie* [online]. 1998 [cit. 2013-03-26]. Dostupné z: http://muj.optol.cz/dusek/clanky/krypto.pdf

[18] *Přísně tajné šifry: Hash a snadné ověření pravosti zpráv a odhalení zbytečností* [online]. 2012 [cit. 2013-03-30]. Dostupné z: http://m.ihned.cz/c1-58446560-zaklady-kryptografie-hashovaci-funkce

[19] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Teoretický základ elektronického podpisu* [online]. ©2012 [cit. 2013-04-01]. Dostupné z: http://www.nbusr.sk/sk/elektronicky-podpis/elektronicky-podpis/teoreticky-zaklad-elektronickeho-podpisu.html

[20] OCHODKOVÁ, Eliška. *Přínos teorie eliptických křivek k řešení moderních kryptografických systému* [online]. [cit. 2013-03-04]. Dostupné z: http://www.cs.vsb.cz/arg/workshop/files/ecc_eli.pdf

[21] *Chapter 8: Cryptography Standards* [online]. ©2009-2013 [cit. 2013-03-03]. Dostupné z: http://flylib.com/books/en/4.213.1.89/1/

[22] STWORA, Vladimír. *Jak na to: PGP* [online]. 2003 [cit. 2013-03-04]. Obrázok vo formáte jpg. Dostupné z: http://www.zvedavec.org/techpor/2003/04/568-jak-na-to-pgp.htm

[23] ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky.* 2005, částka 143/2005. Dostupné také z: http://www.zakonyprolidi.cz/cs/2005-412

[24] ČESKO. Vyhláška č. 432 ze dne 16. prosince 2011 o zajištění kryptografické ochrany utajovaných informací. In: *Sbírka zákonů České republiky.* 2011, částka 150/2011. Dostupné také z: http://www.zakonyprolidi.cz/cs/2011-432

[25] ČESKO. Vyhláška č. 525 ze dne 14. prosince 2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. In: *Sbírka zákonů České republiky.* 2005, částka 179/2005. Dostupné z: http://www.zakonyprolidi.cz/cs/2005-525

[26] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II.* Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.

[27] BRABEC, František. *Bezpečnost pro firmu, úřad, občana.* 1.vyd. Praha: Public History, 2001, 400 s. ISBN 80-864-4504-6.

[28] KUČERA, František. *Mobilní odposlechy – jak fungují a lze se jim bránit?* [online]. ©2012 [cit. 2013-04-15]. Dostupné z: http://www.svetandroida.cz/mobilni-odposlechy-jak-funguji-a-lze-se-jim-branit-201201

[29] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie*. (prednáška) Zlín: UTB, 2011

[30] *Noise in MEMS* [online]. 2010 [cit. 2013-04-22]. Dostupné z: http://iopscience.iop.org/0957-0233/21/1/012001/pdf/0957-0233_21_1_012001.pdf

[31] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 223 s. ISBN 978-80-7318-762-0.

[32] *Inteligentní šumový generátor SNG* [online]. [cit. 2013-04-12]. Dostupné z: http://www.odposlechy.com/inteligentni-sumovy-generator-sng

[33] VASEGHI, Saeed V. *Advanced digital signal processing and noise reduction*. 4th ed. Chichester: John Wiley, 2008, xxx, 514 s. ISBN 978-0-470-75406-1. Dostupné z: http://metro-natshar-31-71.brain.net.pk/articles/0470754060.pdf

[34] KOGAN, Sh. *Electronic noise and fluctuations in solids.* New York, NY, USA: Cambridge University Press, 1996, xviii, 354 p. ISBN 978-0-521-46034-7. Dostupné z: http://www.google.sk/books?id=s5tupGCMzBYC&printsec=frontcover&hl=sk%23v=onepage&q&f=false#v=onepage&q&f=false

[35] *Radiový paměťový analyzátor MRA 5* [online]. [cit. 2013-04-12]. Dostupné z: http://www.odposlechy.com/radiovy-pametovy-analyzator-mra-5

[36] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Nežiaduce elektromagnetické vyžarovanie* [online]. ©2012 [cit. 2013-04-22]. Dostupné z: http://www.nbusr.sk/sk/oblasti-bezpecnosti/informacna-bezpecnost/neziaduce-elektromagneticke-vyzarovanie.html

[37] *Věstník Národního bezpečnostního úřadu* [online]. Praha: Národní bezpečnostní úřad ČR, 1999- [cit. 2013-04-16]. ISSN 1212-7086. Dostupné z: http://www.nbu.cz/download/nodeid-554/

[38] TECHNISERV. *Elektromagneticky stíněný prostor Faradayova klec, stíněné komory* [online]. [cit. 2013-04-16]. Dostupné z: http://www.stinene-komory.cz/index.php

[39] ALIBABA. *Technika na ochranu informácií* [online]. 2012 [cit. 2013-04-16]. Dostupné z: http://www.alibaba.sk/component/k2/item/175-technika-na-ochranu-informácií.html

[40] PROBIN. *Stíněné komory - Faradayovy klece* [online]. ©2008-2013 [cit. 2013-04-16]. Dostupné z: http://www.probin.cz/cz/faradayovy-klece

[41] TECHNISERV. *Stíněné komory* [online]. [cit. 2013-04-16]. Dostupné z: http://www.stinene-komory.cz/stinene-komory.php

[42] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Osobní šifrátory* [online]. 18.02.2009 [cit. 2013-04-17]. Dostupné z: http://www.nbu.cz/cs/aktuality/590-osobni-sifratory/

[43] DRGA, Rudolf. *Elektronické bezpečnostní systémy*. (prednáška) Zlín: UTB, 2010

[44] *Integrovaný bezpečnostní systém ve Zlíně* [online]. 2009 [cit. 2013-04-18]. Obrázok vo formáte jpg. Dostupné z: http://trilobit.fai.utb.cz/Data/Articles/kladnicek_trilobit1_soubory/image015.jpg

[45] IDNES. *Jak se dnes můžete ochránit aneb kolik stojí bezpečí* [online]. 17.3.2008. ©1999 – 2013 [cit. 2013-04-18]. Dostupné z: http://finance.idnes.cz/jak-se-dnes-muzete-ochranit-aneb-kolik-stoji-bezpeci-fyd-/podnikani.aspx?c=A080317_085509_firmy_rady_fib

[46] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.

[47] BENEŠ, David. *Pult centrální ochrany NAM Global - výuková skripta*. Orlová: NAM system, 2008, 174 s. ISBN 978-80-254-1436-1.

[48] TSECURITY. Aplikace protokolu SIA DC-09 [online]. [cit. 2013-04-19]. Dostupné z: http://www.t-security.cz/image/TI_SIA_DC09.pdf

[49] ČSN EN 50518-1 (334599). *Dohledová a poplachová přijímací centra - Část 1: Umístění a konstrukční požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

[50] ČSN EN 50518-2 (334599*). Dohledová a poplachová přijímací centra - Část 2: Technické požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

[51] ČSN EN 50518-3 (334599). *Dohledová a poplachová přijímací centra - Část 3: Pracovní postupy a požadavky na provoz.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012.

[52] X. INFORMAČNÍ OBČASNÍK SPOLEČNOSTI NAM, a. s. *NAMák: Monitorovací software NET-G* [online]. 2001 [cit. 2013-05-04]. Dostupné z: http://www.nam.cz/download/namak/10.pdf

[52] SLOVENSKO. Zákon č. 215 zo dňa 11. marca 2004 o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. IN: *Zbierka zákonov Slovenskej republiky.* 2004, čiastka 93/2004. Dostupné tiež z: http://www.nbusr.sk/ipublisher/files/nbusr.sk/informace-pro-verejnost/informacie/215_2004.pdf

[53] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. [online]. [cit. 2013-05-06]. Obrázok vo formáte jpg. Dostupné z: http://www.nbu.cz/cs/

[54] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD. *Znak NBÚ* [online]. [cit. 2013-05-06]. Obrázok vo formáte jpg. Dostupné z: http://ep.nbusr.sk/kca/pictures/nbu_znak.jpg

[55] IPRAVDA. *Budova NBÚ* [online]. [cit. 2013-05-06]. Obrázok vo formáte jpg. Dostupné z: http://ipravda.sk/res/2011/09/05/thumbs/123812-budova-nbu-clanok.jpg

[56] SLOVENSKO. Vyhláška č. 340 zo dňa 10. mája 2004 ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií. In: *Zbierka zákonov Slovenskej republiky*. 2004, čiastka 141/2004. Dostupné z: http://www.nbusr.sk/ipublisher/files/nbusr.sk/informace-pro-verejnost/informacie/339_2004.pdf

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ARC	Alarm Receiving Centre (poplachové prijímacie centrum)
ASCII	American Standard Code for Information Interchange (americký štandardný kód pre výmenu informácií)
CA	Certifikačná Autorita
CBC	Cipher Block Chaining (reťazenie šifrových blokov)
CCTV	Closed-circuit television (uzavretý televízny okruh)
CENELEC	European Committee for Electrotechnical Standardization
CFB	Cipher Feedback mode (módy spätnej väzby)
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DPPC	Dohľadové a poplachové prijímacie centrum
DTMF	Dual-tone multi-frequency signaling
ECB	Electronic code book (elektronická kódová kniha)
ECC	Elliptic Curve Cryptography (eliptické krivky)
GSM	Global System for Mobile Communications (Globálny systém mobilných komunikácií)
GPRS	General Packet Radio Service (Univerzálna paketová rádiová služba)
HMAC	Hash Message Authenticity Code (hašovaný autentifikačný kód správ)
ICT	Information and Communications Technology (Informačné a komunikačné technológie)
IDEA	International Data Encryption Algorithm
IPsec	Internet Protocol Security
JTS	Jednotná telefónna sieť

MAC	Message Authenticity Code (Autentifikačný kód správy)
MD5	Message-Digest algorithm 5 (kryptografická hašová funkcia)
MNO	Ministerstvo národnej obrany
NBÚ	Národný bezpečnostný úrad
NEV	Nežiaduce elektromagnetické vyžarovanie
PGP	Pretty Good Privacy (veľmi dobré súkromie)
PKI	Public Key Infrastructures (infraštruktúra verejných kľúčov)
RA	Registračná autorita
RAM	Random Access Memory (pamäť s priamym prístupom)
RSA	Iniciály autorov algoritmu Rivest, Shamir, Adleman
SBS	Súkromná bezpečnostná služba
SMS	Short Message Service (krátka textová správa)
SHA	Secure Hash Alogithm (hašová funkcia)
SIA	Digitálny komunikačný formát pre alarmové systémy
SP	Substitúcia + pripočítanie
ST	Substitúcia + transpozícia
STP	Substitúcia + transpozícia + pripočítanie
STT	Substitúcia + transpozícia + transpozícia
TTS	Transpozícia + transpozícia + substitúcia
UTC	Coordinated Universal Time (svetový čas)
VRÚ	Vojenská rádiová ústredňa
XOR	Exclusive OR (exkluzívny súčet, binárna logická operácia)

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: CERTIFIKÁT KRYPTOGRAFICKÉHO PROSTRIEDKU

Příloha č. 1 k vyhlášce č. 525/2005 Sb.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49
150 06 Praha 56

Národní bezpečnostní úřad vydává podle § 46 zákona č. 412/2005 Sb.,
o ochraně utajovaných informací a o bezpečnostní způsobilosti

CERTIFIKÁT

kryptografického prostředku

Evidenční číslo: .....

.....
(název, typové označení kryptografického prostředku)

Identifikace držitele certifikátu

Obchodní firma /jméno a příjmení/název orgánu státu:
IČ:
Sídlo/trvalý pobyt/místo podnikání:

Identifikace výrobce kryptografického prostředku

Obchodní firma /název orgánu státu:
IČ:
Sídlo/trvalý pobyt/ místo podnikání:

kterým se potvrzuje způsobilost kryptografického prostředku pro ochranu utajovaných informací do a včetně stupně utajení

.....

Platnost certifikátu od:

Platnost certifikátu do:

Datum vydání certifikátu:

Otisk úředního razítka

Přílohy: (např. certifikační zpráva)

Podpis oprávněného zástupce

Príloha 1. Certifikát kryptografického prostriedku [25]

PRÍLOHA P II: CERTIFIKÁT KRYPTOGRAFICKÉHO PRACOVISKA

Příloha č. 2 k vyhlášce č. 525/2005 Sb.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49
150 06 Praha 56

Národní bezpečnostní úřad vydává podle § 46 zákona č. 412/2005 Sb.,
o ochraně utajovaných informací a o bezpečnostní způsobilosti

CERTIFIKÁT

kryptografického pracoviště

Evidenční číslo: .....

.....
(označení kryptografického pracoviště)

Identifikace držitele certifikátu:

Obchodní firma/jméno a příjmení /název orgánu státu:
IČ:
Sídlo/trvalý pobyt/místo podnikání:

Identifikace kryptografického pracoviště:

Specifikace (umístění, kategorie):

kterým se potvrzuje způsobilost kryptografického pracoviště k provádění činnosti kryptografické ochrany v rozsahu

.....
(specifikace vykonávaných činností)

Platnost certifikátu od:

Platnost certifikátu do:

Datum vydání certifikátu:

Otisk úředního razítka

Přílohy: (např. certifikační zpráva)

Podpis oprávněného zástupce

Príloha 2. Certifikát kryptografického pracoviska [25]