Zabezpečenie spravodajskej komunikácie ezoterickými prostriedkami

Security Intelligence Esoteric Means of Communication

Bc. Monika Hanzenová

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. Monika HANZENOVÁ**
Osobní číslo:	**A11314**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Zabezpečení zpravodajské komunikace ezoterickými prostředky**

Zásady pro vypracování:

1. **Zpracujte informačně analytický materiál o použití ezoterických technik a technologií ke spravodajské ochraně kanálů spojení.**
2. **Analyzujte současné techniky a technologie používané ve spojovacím článku speciálních služeb.**
3. **Popište vývoj chemického a fyzikálního tajnopisu v budoucnosti.**
4. **Uveďte jiné formy a metody spojení pro budoucnost.**

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. **DOSKOČIL, František a Pavel ŽÁČEK. Průlom: agentem CIA uvnitř komunistické nomenklatury. Vyd. 2. Olomouc: Votobia, 2004, 285 s. ISBN 80-722-0208-1.**
4. **BOROVIČKA, V. Přísně tajné šifry. Vyd. 1. Praha: Naše vojsko, 1982, 315 s.**
5. **MELTON, H. Velká kniha o špionáži. Překlad Milan Hausner, Petr Kučera. Bratislava: Perfekt, 1997, 175 s. ISBN 80-804-6061-2.**
6. **ROEWER, Helmut, Stefan SCHÄFER a Matthias UHL. Encyklopedie tajných služeb ve 20. století. Vyd. 1. Praha: Euromedia Group – Knižní klub, 2006, 544 s. Universum (Euromedia Group). ISBN 80-242-1607-8.**
7. **JANEČEK, Jiří. Válka šifer: výhry a prohry československé vojenské rozvědky, 1939-1945. Olomouc: Votobia, 2001, 345 p. ISBN 80-719-8505-8.**
8. **VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. 1. vyd. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-000-1888-8.**
9. **SINGH, Simon. Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii. 2. vyd. v čes. jaz. Překlad Petr Koubský, Dita Eckhardtová. Praha: Dokořán, 2009, 382 s. Aliter, sv. 9. ISBN 978-802-5701-447.**

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

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

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

Ve Zlíně dne 8. února 2013

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Táto diplomová práca je informačne analytický materiál, ktorý pojednáva o použití steganografických techník a technológií v spravodajskej službe.

V úvode sú vysvetlené základné informácie o steganografii. Druhá kapitola prehľadne vysvetľuje a objasňuje všetky formy fyzikálneho, chemického a matematického tajnopisu, používaného v spravodajskej službe. Ďalej práca poukazuje na najnovší vývoj kvantovej kryptografie a chemického tajnopisu. Záver práce je zameraný na využitie skrytých kanálov k prenosu tajných správ.

V praktickej časti sú otestované a porovnané príklady steganografických voľne dostupných programov pre skrývanie súborov do obrázkov.

Kľúčové slová: steganografia, bezpečnosť, spravodajská služba, tajnopis, kryptografia, neviditeľný atrament, skryté kanály,

ABSTRACT

This diploma thesis acts as an information-analytical material about using steganography techniques and technologies in the intelligence service.

The introduction explain the basic information about steganography. Second chapter clearly explains and clarifies all forms of physical, chemical and mathematical secret code, which were used in the intelligence service. This thesis points the latest developments of quantum cryptography and chemical secret code. Conclusion is focused on using of cover channels to transmit secret messages.

The practical part talking about testing and comparing the steganography examples of free programs for hiding files within the image.

Keywords: steganography, security, intelligence, secret code, cryptography, invisible ink, hidden channels,

Poďakovanie:

Moje poďakovanie patrí JUDr. Vladimírovi Lauckému za pomoc pri vyhľadávaní doporučenej literatúry a za cenné pripomienky a rady pri vypracovávaní diplomovej práce.

Tiež ďakujem svojej rodine a priateľovi za veľkú podporu pri štúdiu na univerzite.

Motto:

„Nemohou oči jen samy přece poznat podstatu věcí;

Proto, co chybou je duch, to zde chybou nedávej očím“

Lukrecius

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

Tajné správy a tajnopis sú známe od dôb, ktoré sa spájajú s vynálezom písma v samom počiatku ľudskej civilizácie. Každá kultúra, skupina a epocha si so sebou priniesla alebo si vytvorila určitý systém ukrývania správy, v inej nevinnej správe, pred ostatnými. Používanie tohto jednoduchého a bezpečného spôsobu utajovania komunikácie pretrváva dodnes.

Steganografia je stará metóda ukrývania správ v obrázkoch, textu a objektoch. Zahrňuje obrovské množstvo metód tajnej komunikácie skrývajúcich samotnú skutočnosť, že k posielaniu utajenej správy dochádza.

Táto práca obsahuje prehľadný popis všetkých metód, ktoré sa využívali na zabezpečenie spravodajskej komunikácie. Predstavuje analyticko-informačný materiál o profesii, vybavení a technikách, ktoré boli vyvinuté pre rôzne spravodajské operácie a o ich vývoji.

Pri písaní vychádzam z predpokladu, že prostriedky spravodajskej komunikácie a moderná steganografia sú oblasti nie príliš známe bežným čitateľom a aj v našom študijnom obore sme sa s nimi stretli len okrajovo. Preto cítim potrebu na ne poukázať a objasniť ich. Najväčším problémom je nedostatok študijných materiálov, pretože mnohé technológie a techniky boli ešte donedávna utajované. Preto sa v práci snažím využiť všetky dostupné zdroje, pričom využívam aj cudzojazyčnú literatúru.

V dnešnej dobe je steganografia stále častejšie spájaná s vložením dát v nejakej podobe elektronického média. Dáta zo „skrýše“ alebo ak chcete zdrojového súboru sú skrývané na základe meniacich sa nevýznamných bitov z informácií vo verejnom alebo hostiteľskom súbore. Okrem prenosu utajovanej správy slúži steganografia k ochrane autorských práv či cenín. Aj to je dôvod prečo veľké množstvo úspešných svetových podnikov označujú steganografiu ako nový trh, perspektívny pre investíciu.

Diplomová práca je členená na 4 kapitoly v teoretickej časti a jednu kapitolu v časti praktickej.

Prvá kapitola objasňuje pojem steganografia a základné terminológie s ňou spojené. Úvodom druhej kapitoly sú uvedené základné pojmy používané v spravodajskej komunikácii a ďalej prehľadne a názorne rozdeľuje techniku tajnopisu na fyzikálnu, chemickú a matematickú. Tretia a Štvrtá kapitola ponúka čitateľovi prehľad o aktuálnom

vývoji tajnopisu a metód spojenia. Praktická časť diplomovej práci rieši oboznámenie čitateľa s vybranými voľne dostupnými steganografickými programami, ktoré umožňujú skrytie rôznych typov súboru do obrázka. Tieto programy sú testované a výsledky spracované do tabuliek.

I. TEORETICKÁ ČASŤ

1 STEGANOGRAFIA

V ďalekých dejinách Histiaeus, v snahe vymaniť sa z väzenia kráľa Daria, oholil otrokovi hlavu, na ktorú napísal tajnú správu. Otroka potom po opätovnom narastení vlasov poslal do Milétu aby odovzdal informáciu. [1] Tento príbeh je pokladaný za najstarší a najznámejší spôsob steganografie v dejinách ľudstva. Existuje veľké množstvo podobných historických príbehov, ktoré využívali zdĺhavejšie či kratšie spôsoby ukrytia správy. Tajné správy a tajnopis sú známe od dôb, ktoré sa spájajú s vynálezom písma v samom začiatku ľudskej civilizácie.

Steganografia, ktorá v preklade z gréčtiny znamená skryté písanie, predstavuje rôzne metódy tajnej komunikácie, ktorých cieľom je zakryť samotný fakt existencie správy, čím sa zväčšuje úroveň zabezpečenia. Je to stará metóda ukrývania správ v obrázkoch textu a objektoch. Narušiteľ by nemal ani len tušiť, že sa nejaká správa prenáša. Najdokonalejší spôsob utajenia komunikácie, predstavuje spojenie steganografie s kryptografiou, kedy aj v prípade, že sa prenos informácií nepodarí utajiť, narušiteľ nie je schopný správu rozlúštiť. [2]

Teraz, keď bola táto staroveká technika aplikovaná na komunikačné systémy dnešnej doby, stala sa z nej veľmi efektívna forma nepostrehnuteľných správ. [3]

Tento obor zahrňuje veľké množstvo metód utajenej komunikácie, skrývajúcej samotnú skutočnosť, že dochádza k zasielaniu správ. Patrí sem neviditeľný atrament, mikrotečka, digitálny podpis, skryté kanály, širokopásmová komunikácia a využitie usporiadaní znakov, ktoré je odlišné od kryptografických metód. [2]

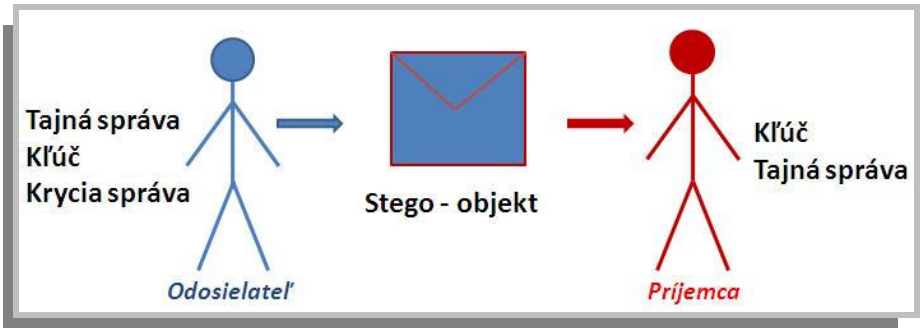
1.1 Základné rysy steganografie

- **bezpečnosť v nejasnosti** (Security through obscurity), predstavuje základnú funkciu steganografie, kedy je dôležité nedať najavo samotný fakt komunikácie. Nie je na pohľad jasné, že prenos informácií prebieha,
- **zastieranie** (Camouflage), pomáha v situácii, kde nepriateľ pozná spôsob použitej metódy, ale aj tak sa mu neoplatí skrytú informáciu hľadať, napríklad z dôvodu veľkého objemu dát, ktoré by musel prehľadať,

- **skrývanie umiestnenia vloženej informácie** (Hiding the location of the embedded information), umiestnenie utajovanej správy v napríklad texte by nemalo byť možné vyzistiť na základe žiadnej logickej operácie,
- **šírenie skrytej informácie** (Spreading the hidden information), na spoľahlivý prenos utajovanej správy je potrebné opakovanie skrytej informácie. Hlavne v prípadoch, kde nám môže správu vyrušiť šum alebo narušiteľ,
- **využívanie techník špecifických pre prostredie** (Techniques specific to the environment). Spôsob ukrytia informácií sa v závislosti na prostredí mení. [4]

1.2 Princíp

Obecný model steganografie je možné najlepšie a najzrozumiteľnejšie vyjadriť pomocou nasledujúceho obrázka.



Obrázok 1, Obecný model steganografie, [vlastný]

Základom utajenej komunikácie je fakt, že obaja, odosielateľ aj príjemca, musia poznať tajný kľúč, podľa ktorého budú správu ukrývať aj získavať. V závislosti na tom, akú tajnú správu potrebuje odosielateľ príjemcovi odovzdať, musí vymyslieť adekvátny krycí list. Následne na to túto tajnú správu zašifruje do listu vopred dohodnutým kľúčom. Tak vzniká stego objekt, ktorý je pripravený na poslanie. Keďže posielaný krycí list nevzbudzuje svojim obsahom žiadne podozrenie, príjemca ho dostane a rozlúšti pomocou kľúča. [5]

1.3 Tajný a verejný kľúč

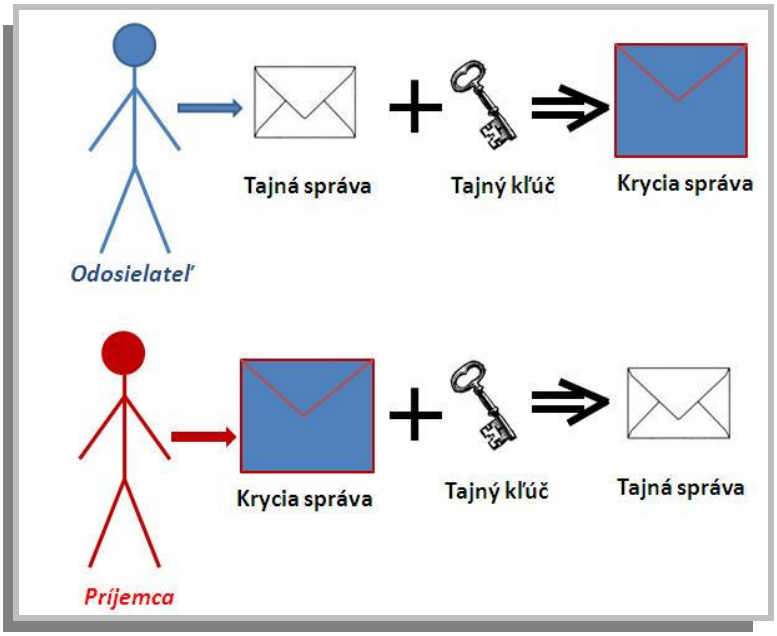
Tento typ ukrývania informácií je veľmi odolný voči odhaleniu, pretože využíva princípy kryptografie s tajným kľúčom a navyše je informácia ukrytá v krycej správe. Vďaka tomu

je ukrytá správa veľmi ťažko odhaliteľná, a pokiaľ je odhalená tak je veľmi ťažko rozlúštiteľná.

1.3.1 Čistá steganografia

Medzi najstaršie steganografické metódy patrí ukrytie správy bez využitia kľúča. To znamená, že na utajovanú správu nie je použitá žiadna šifrovacia metóda. Informácia je jednoducho uložená, ukrytá, v čistej forme. Čistá steganografia predstavuje vizuálne ukrytie správy. Príkladom je neviditeľný atrament, vypichovanie dier do textu, kde pozícia dier nesie jednotlivé kombinácie písmen skrytého textu, alebo úprava textu. [5]

1.3.2 Steganografia s tajným kľúčom

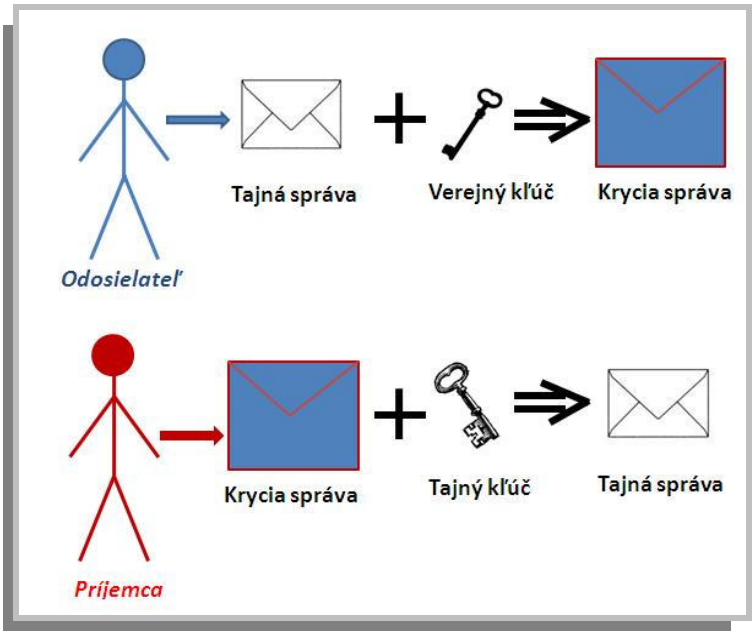


Obrázok 2, Steganografia s tajným kľúčom. [vlastný]

Odosielateľ zašifruje tajnú správu tajným kľúčom a potom ju vloží do krycej správy takým spôsobom, na ktorom sa vopred s príjemcom dohodli.

Príjemca musí najskôr získať tajnú správu z krycej správy v závislosti na tom, aký typ ukrytia bol použitý. Potom získanú správu dešifruje tým istým tajným kľúčom, ktorým bola zašifrovaná odosielateľom. [5]

1.3.3 Steganografia s verejným kľúčom



Obrázok 3, Steganografia s verejným kľúčom. [vlastný]

Steganografia s verejným kľúčom využíva dva rôzne kľúče. Odosielateľ má verejný kľúč, ktorým zašifruje tajnú správu a potom je vloží do krycej správy.

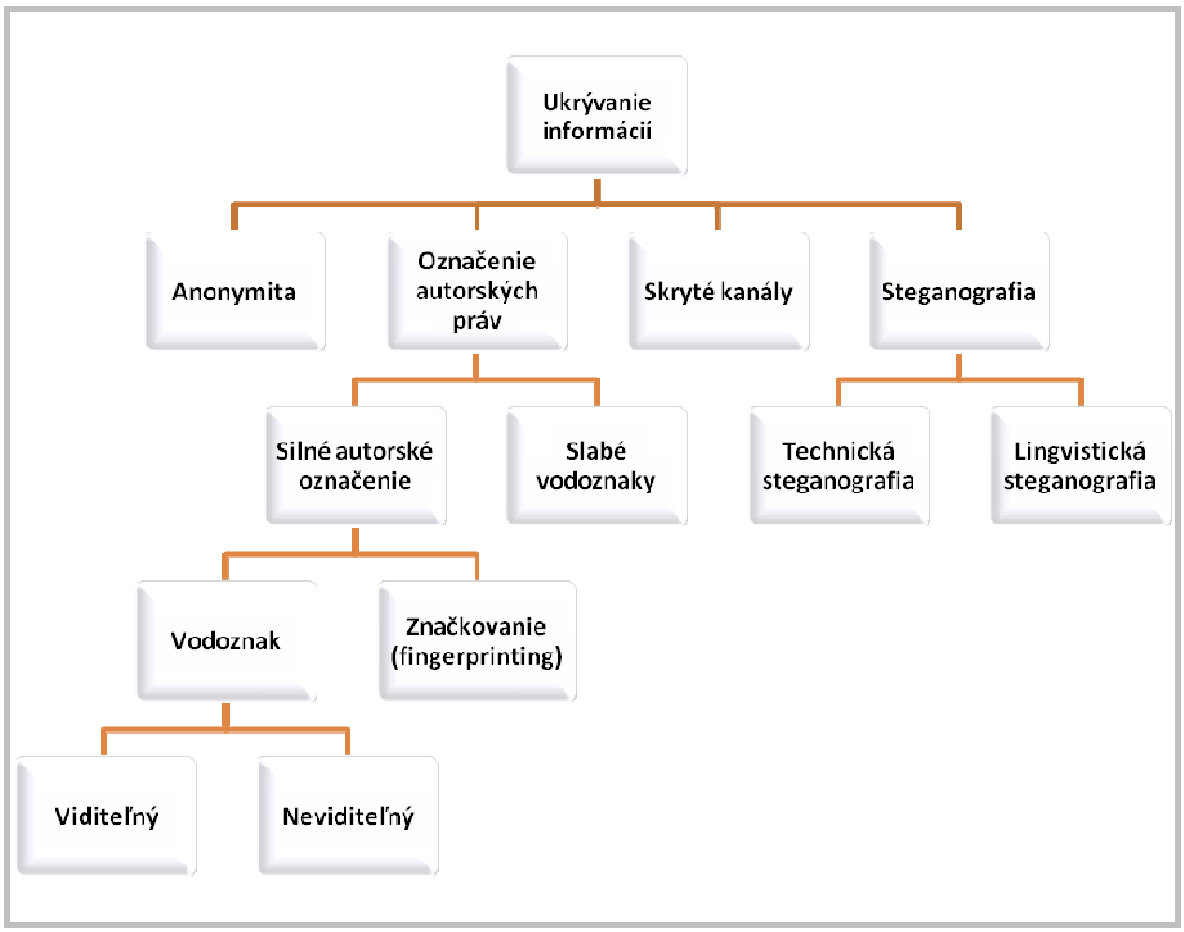
Prijímateľ dostane kryciu správu, z ktorej získa zašifrovanú správu a pomocou tajného kľúča ju dešifruje a získa správu tajnú. [5]

1.3.4 Prenos tajného kľúča

Najväčším a asi jediným problémom pri prenose informácií takýmto spôsobom, je doručiť príjemcovi správy tajný kľúč. Toto je možné uskutočniť viacerými spôsobmi. Buď sa použijú klasické steganografické či kryptografické metódy, alebo je možné celý proces úplne zaistiť proti odhaleniu spôsobom, ktorý využíva štyri pravdepodobnostné algoritmy. Tento spôsob vypočítava tajný kľúč zo správ, ktoré si odosielateľ s príjemcom navzájom posielajú. [5]

Obrázok 4, Známka ako úkryt. [6]

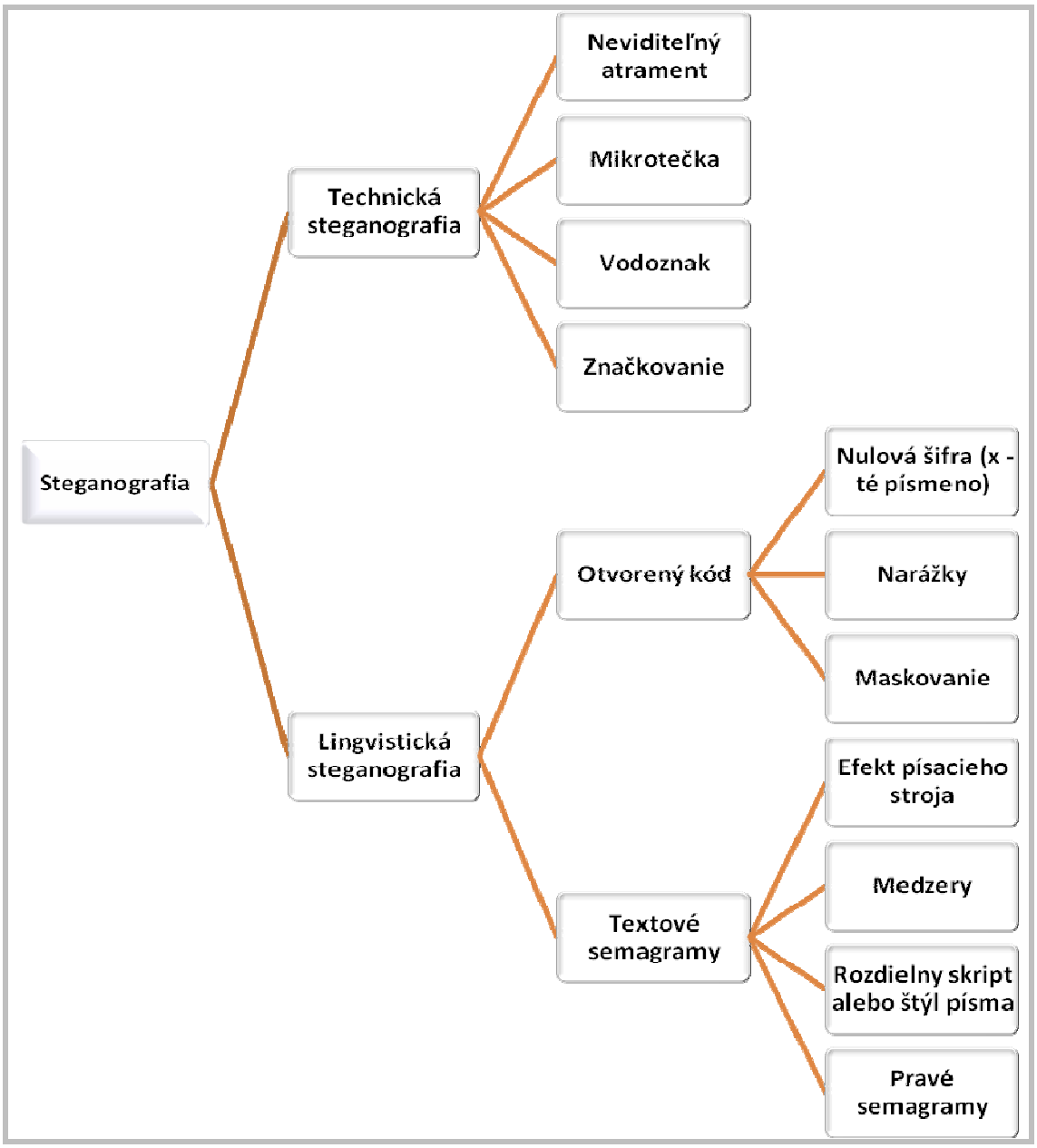
1.4 Rozdelenie steganografie



Obrázok 5, Schéma oblasti ukrývania informácií. [vlastný]

Steganografia sa v literatúrach obecne rozdeľuje podľa ukrývania správ, ktoré sa používali v histórii, do dvoch hlavných skupín:

- **technická steganografia** – správu fyzicky ukrýva pomocou rôznych technologických procesov,
- **lingvistická steganografia** – utajovaná správa predstavuje určité vopred dohodnuté znaky alebo slová v texte. [5], [2]



Obrázok 6, Schéma historického rozdelenia steganografie. [vlastný]

1.4.1 Lingvistická steganografia

Využíva písané slovo pre ukrytie tajnej správy bez viditeľného odlíšenia znakov. Základným princípom je ukrytie známok existencie pravej správy. Je dôležité aby samotný text dával zmysel, bol nenápadný a nevyvolal zvýšenú pozornosť.

Otvorený kód kladie dôraz na pozíciu textu. Vo voľne čitateľnom nenápadnom texte je tajná správa, v podobe slov alebo písmen, skrytá na určitom mieste v texte horizontálne alebo vertikálne.

- maskovanie - text obsahuje slová, ktoré začínajú podobným znakom, ktorý má ale úplne iný význam, čím vznikajú rôzne metafory ako maskovací nástroj,
- narážky – je definované určité slovo, ktoré sa v texte správy nachádza,
- nulová šifra – tiež známe ako x-té písmeno, správu získava prepísaním každého x-tého znaku, každého slova alebo po značke, ktorý slúži ako ukazovateľ začiatku postupu.

Textové sémagramy využívajú grafické spracovanie textu.

- použitie medzier – frekvencia medzier alebo ich početnosť sú nositeľmi binárneho kódu,
- použitie efektu písacieho stroja – písmená vyrazené pri písaní môžu byť nepatrne hrubšie alebo tenšie, či mierne pod alebo nad líniou ostatných slov,
- použitie rozdielneho skriptu alebo štýlu písma – tým sa vytvára binárny kód v texte,
- použitie pravých sémagramov – obrázky v sebe ukrývajú tajnú správu, ktorá je bežným pozorovateľom nespozorovateľná. [5]

1.4.2 Technická steganografia

Na ukrývanie správy využíva technologické procesy. Historicky nie sú technologické procesy v steganografii nič nového. Vypichovanie dierok do papiera k označeniu písmen tvoriacich správu, správy písané pod voskom voskovej tabuľky, rôzne druhy neviditeľných atramentov, či tetovanie pod vlasmi postupne roky vývoja v steganografii vystriedali za

pixely, mikrotečky, či vodoznaky. O týchto všetkých technológiách ukrývania informácií sa podrobnejšie zmieňujem v ďalších kapitolách mojej práce. [5]

1.5 Stegoanalýza

Steganografia má uplatnenie nie len ako nástroj utajovania konverzácií ale je tiež nápomocná pri kontrolovaní podozrivých súbor. Stegoanalýza sa práve zaoberá odhaľovaním utajovaných správ a prípadne ich zneškodňovaním. Porovnáva vlastnosti nezmenených súborov so súbormi, ktoré obsahujú pridané, vložené skryté informácie. [29] Takéto informácie môžeme na základe stegoanalýzy získavať z rôznych médií ako textov, obrazov či audio súborov, pričom sa využívajú dva druhy útokov:

- **získanie kódového slova a dát,**
- **zničenie skrytej informácie.**

Každá metóda steganografie ukrýva informácie rôznymi spôsobmi, preto pokiaľ nepoznáme použitú metódu, je odhalenie utajovanej správy veľmi náročné. Našťastie, alebo nanešťastie existujú nástroje, ktoré generujú typické charakteristiky, podľa ktorých sa dá použitý spôsob rozoznať. Potom už len stačí porovnať originálny obraz s obrazom nesúcim kódové slovo, čo nám vlastne umožní odhaliť kľúčové slovo.

Z pohľadu stegoanalýzy rozlišujeme dve skupiny metód steganografie:

a) **Obrázky ako oblasť pôsobnosti.**

Metódy image domain pracujú na bitovej fáze. Ide o jednoduché systémy pracujúce na princípe zmeny najmenej významných bitov súborov. Ako príklad tohto typu nástroja môžeme uviesť programy: StegoDos, Hide and Seek, Noise Storm a veľa ďalších. [5]

b) **Transformácia ako oblasť pôsobnosti.**

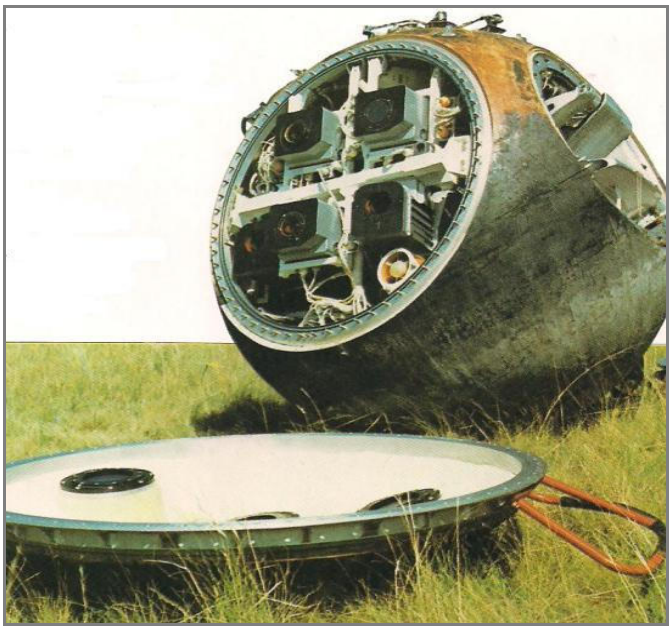
Metódy transform domain pracujú na priamej transformácii dát, akou je napríklad zmena svietivosti. Príkladom tohto typu sú: PictureMarc, SureSign. [5]

1.6 Aplikácie steganografie

Pojem steganografia sa často stretáva s nesprávnym pochopením u ľudí, ktorí nemajú dostatočné informácie o tejto oblasti a spájajú si využívanie steganografie iba s nezákonnou činnosťou spravodajských služieb. Samozrejme by bolo klamstvo tvrdiť, že

tieto techniky boli využité vždy iba v súlade so zákonmi, avšak je dôležité aby sme steganografiu chápali ako spôsob, ktorý nám napomáha práve takéto nezákonné praktiky odhaliť. A tiež umožňuje významné posilnenie bezpečnosti a práv spoločnosti. [2] Za hlavné oblasti aplikácie skrývania informácií by sme mohli označiť nasledovné:

- nenápadná komunikácia pre armádne a spravodajské služby,
- techniky pre anonymnú komunikáciu na webe, z dôvodu obmedzenia slobody prejavu na internete niektorých vlád,
- plány napríklad elektronických volieb využívajú metód anonymnej komunikácie,
- rozposielanie spamov (nevyžiadaných správ), pri marketingových akciách, sa deje pomocou techník falšovania elektronickej pošty, aby sa vyhli reakciám pobúrených užívateľov,
- ochrana autorských práv vo forme digitálnych vodoznakov,
- marketingové využitie, prostredníctvom vloženia informácii o produkte napríklad do hudby,
- priemyselná špionáž,
- zločinci napríklad využívajú pre komunikáciu hacknuté telefónne ústredne veľkých spoločností alebo priamo verejné internetové stránky kde vložia skrytý text, ktorý je bežnému čitateľovi neviditeľný. Takýto spôsob komunikácie vraj využívali, podľa článku uverejnenom 5. Januára 2001 v denníku USA Today, aj Bin Ládin a iné teroristické skupiny, ktoré ukrývajú pokyny pre teroristické činnosti v športových konverzačných skupinách a iných WWW serveroch. [2]



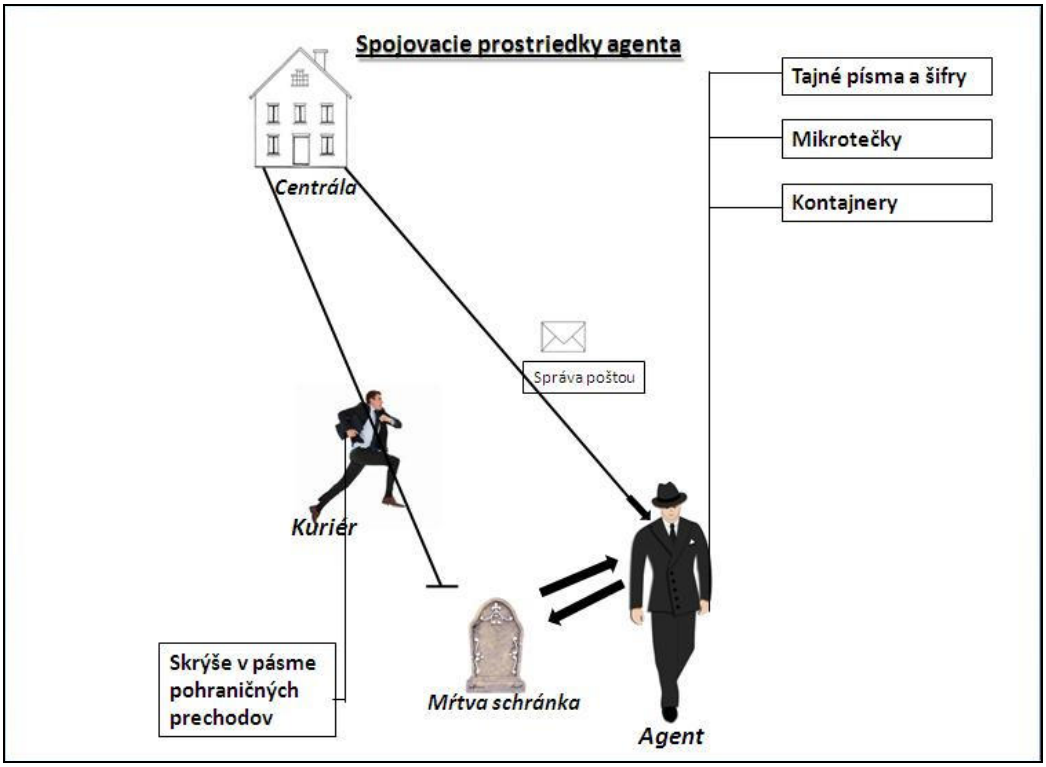
Obrázok 7, Špionážny košík zo satelitu. [6]

2 DOTERAJŠIE TECHNIKY A TECHNOLÓGIE POUŽÍVANÉ V SPOJOVACOM ČLÁNKU ŠPECIÁLNYCH SLUŽIEB

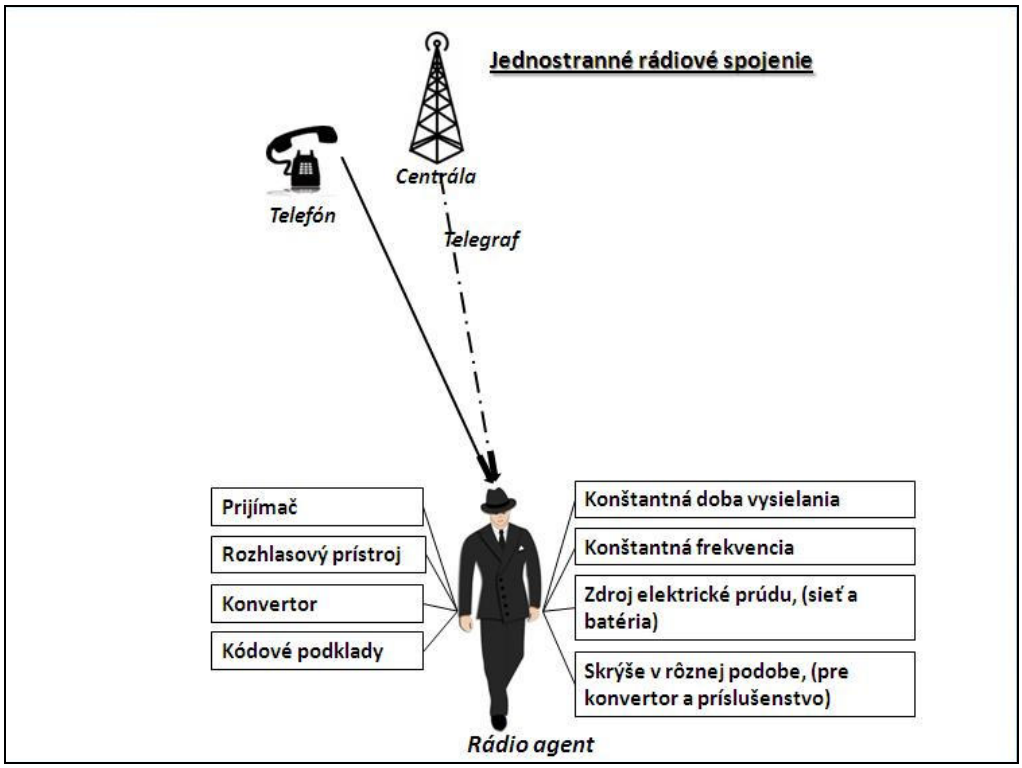
Techniku tajnej služby, ktorá sa používala v časoch druhej svetovej vojny a v rokoch po nej môžeme rozdeliť do 4 komplexov:

- **technika slúžiaca k tajnému získavaniu informácií**,
- **technika spojovacieho systému tajnej služby,**
- **technika slúžiaca tajnej službe k vykonávaniu analýz,**
- **teroristická sabotážna a diverzná technika.**

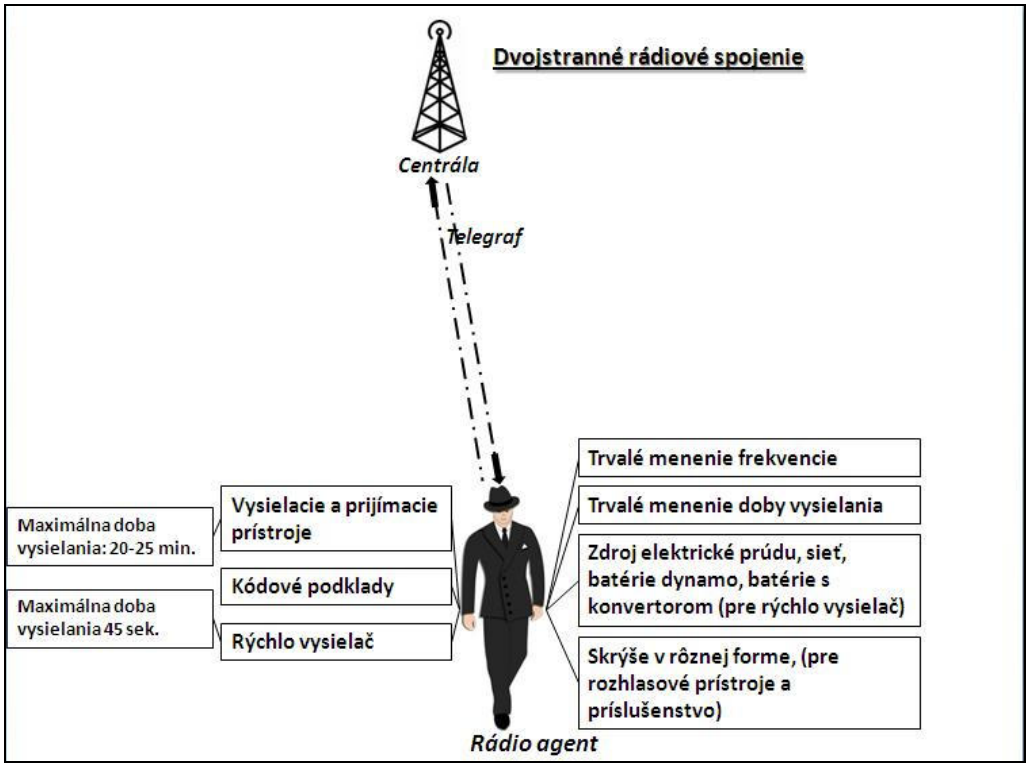
Tajné služby využívali rôzne technológie, techniky a postupy k zaisteniu prenosu informácií v časoch po druhej svetovej vojne. Nasledujúce obrázky by mali slúžiť pre predstavu čitateľa ako to celé fungovalo. [7]



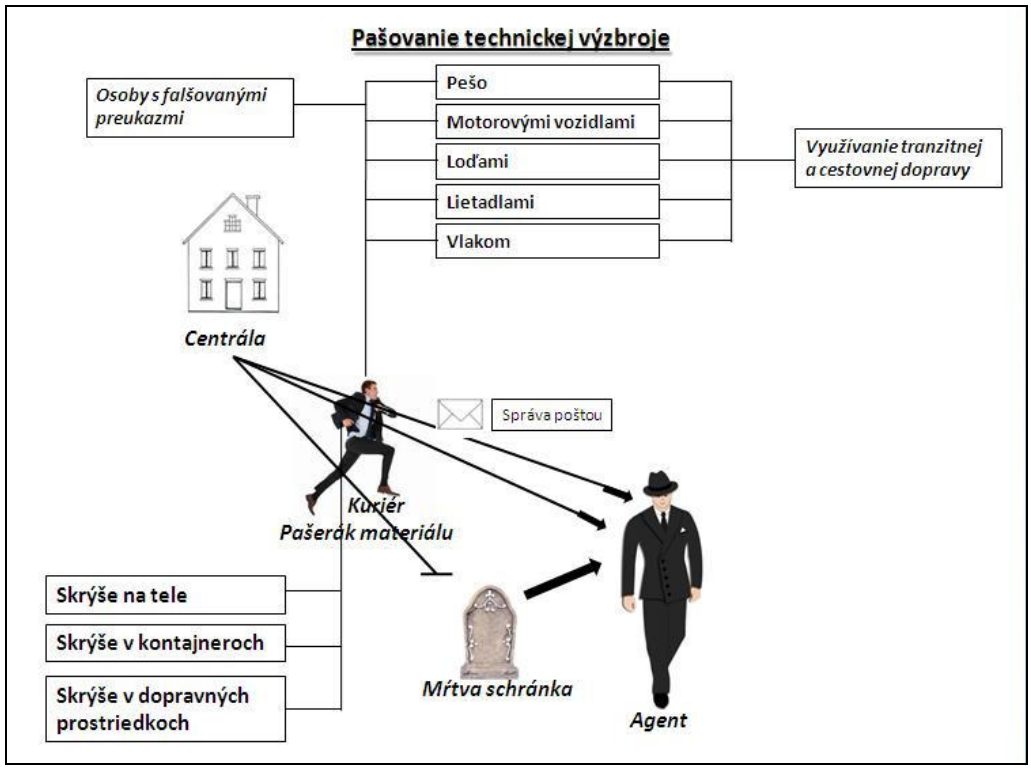
Obrázok 8, Spojovacie prostriedky agenta. [vlastný]



Obrázok 9, Jednostranné rádiové spojenie. [vlastný]



Obrázok 10, Dvojstranné rádiové spojenie. [vlastný]



Obrázok 11, Pašovanie technickej výzbroje. [vlastný]

2.1 Základná terminológia

2.1.1 Spravodajská služba

Obecné označenie pre civilné a vojenské rozviedkové a kontrarozviedkové organizácie. Spravodajská služba zhromažďuje a vyhodnocuje informácie, bežne nezistiteľné. Využíva operatívnu techniku a tajných spolupracovníkov k vykonávaniu konšpiratívnej činnosti. Môžeme medzi ňu zahrnúť aj špeciálne policajné útvary zaoberajúce sa zhromažďovaním a analýzou informácií o organizovanom zločine. [8]

2.1.2 Špeciálne služby

V spravodajskej terminológii, hlavne v bývalých komunistických štátoch, ide o označenie všetkých vojenských aj civilných spravodajských služieb. Označovali si sa tak aj bezpečnostné služby, ktoré sa odlišovali od bežnej policajnej činnosti.

Patria sem civilné a vojenské rozviedky a kontrarozviedky, špeciálne protidrogové a protiteroristické jednotky ale aj bezpečnostné služby vykonávajúce ochranu vládnych predstaviteľov, budov a iné. [8]

2.1.3 Mŕtva schránka

Považujem za potrebné, v prípade ak píšem o technikách a technológiách používaných v spojovacom článku, spomenúť termín, ktorý je neoddeliteľnou súčasťou procesu predávania informácií.

Mŕtva schránka sa používala v spravodajskej praxi ako prostriedok spojenia. Predstavuje starostlivo vybrané a upravené miesto k predávaniu utajovaných správ, inštrukcií a materiálov. Budovala sa na verejných miestach akými sú otvory v skalách, diery v stromoch, splachovacie nádrže na verejných záchodoch. Utajované správy a materiály sa do týchto skrýš ukladali v nádobách prezývaných kontajnery, ktoré mali chrániť tajnopisy pred poveternostným vplyvom a náhodným poškodením. Nešlo pritom o nič zložitejšie ako krabičky od cigariet alebo plechovky.

Časové rozpätie od vloženia správy do schránky a jej vybratie sa pohybovalo okolo desiatok minút, nie dlhšie, pričom každá schránka sa z bezpečnostného hľadiska používala iba na krátku dobu a pre jedného agenta. [8]

František Doskočil v krátkom dokumentárnom filme „Akce průlom“ popisuje mŕtvu schránku Americkej CIA, pre ktorú pracoval ako tajný špión, ktorá bola vytvorená z kameňa. Špión presne vedel kam musí kladivkom udrieť aby sa kameň roztvoril a tým získal krycie listy a všetky potrebné tajné materiály.

[9]

Obrázok 12, Mŕtva schránka. [6]

2.1.4 Spojenie

Spojenie zaisťuje bežnú komunikáciu v rámci spravodajských služieb. Jeho hlavnou funkciou je styk centrál s detašovanými pracoviskami a rezidenturami, pričom sa využívajú konšpiratívne postupy. Na detašované pracoviská sa vysiela kuriér alebo posielajú zakódované správy, ako je možné vidieť v obrázkoch na začiatku kapitoly, v akciách sa používajú vopred dohodnuté heslá. [8]

2.1.5 Rádiové spojenie

Je to druh neosobného spojenia spolupracovníkov rozviedky prostredníctvom rádiového vysielania. Spojenie môže prebiehať jednosmerne alebo obojsmerne. Jednosmerné spojenie funguje tak, že centrála vysiela v určitú, vopred dohodnutú hodinu radu čísiel začínajúce kódom agenta. Agent správu prijíma na prijímači a následne ju dešifruje. Časť z vysielania neslúži na komunikáciu ale iba na zmätenie protivníka. Veľkou nevýhodou jednosmerného spojenia je práve jednosmernosť, čím neumožňuje spätnú väzbu od agenta. Aj vďaka tomu je tento druh spojenia považovaný za bezpečný a z tohto dôvodu sa využíva dodnes. [8]

Agenti vo vopred dohodnutom čase, napríklad každý utorok a štvrtok v rovnakom čase, dostávali inštrukcie. Prvá pätica čísiel im oznamovala či ide o správu živú alebo mŕtvu. Pokiaľ išlo o správu živú, agent si musel opísať všetky čísla, použiť falošné odčítanie, použiť šifrovacie a dešifrovacie tabuľky, rozšifrovať text a riadiť sa inštrukciami. [9]

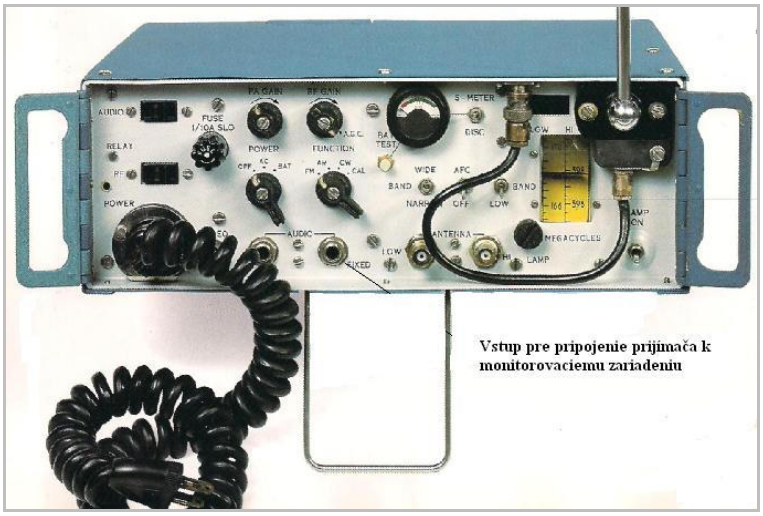
Obojsmerné rádiové spojenie využíva obe cesty spojenia. Centrála vysiela správy a agent odpovedá z vlastnej rádiostanice, čím sa dostáva do veľkého nebezpečenstva. Preto sa tento typ využíval iba v krajných prípadoch.

Moderná technika funguje tak, že reláciu pripraví vopred a pošle ju v zlomku sekundy pomocou smerovej antény s úzkym zväzkom vĺn a nízkym výkon cez komunikačnú družicu. Internet dnes umožňuje úplne iné spojenia cez satelity. [8]

Obrázok 13, Rádiostanica v kufríku. [6]

2.1.5.1 Princíp rádiového spojenia

Signál, ktorý je počuteľný ľudským uchom sa mikrofónom premení na elektrické napätie. Toto napätie je možné napäťovo alebo výkonovo zosilniť a pomocou reproduktoru späť preniesť na zvuk, ktorý je pre človeka počuteľný. Základom rádiového prenosu sú vysokofrekvenčné kmity, ktoré sa dokážu účinne šíriť priestorom. Tieto kmity sa nazývajú nosný kmitočet, sú ovplyvňované počuteľným nízkofrekvenčným signálom z mikrofónu a privedené do antény, ktorá zaistí ich šírenie do priestoru. Následne prijímacia anténa zachytí modulovanú nosnú vlnu a v prijímači sa vyberie signál požadovaného kmitočtu, ktorý sa zosilnie. Prebehne oddelenie nízkofrekvenčného hovorového spektra od vysokofrekvenčnej nosnej vlny a tento nízkofrekvenčný signál sa zosilnie a prevedie reproduktorom na počuteľný. [10]



Obrázok 14, prenosná prijímacia stanica. [6]

2.1.6 Nomenklatúra

Po rozhovore s mojím spolužiakom o tejto práci, som zistila, že im tento výraz nie je známy, preto som sa ho rozhodla vysvetliť. Nomenklatúra predstavovala kategórie osôb, v rámci tejto práci Sovietskeho zväzu a ďalších krajín východného bloku, ktorí zastávali rôzne kľúčové administratívne pozície vo všetkých oblastiach činnosti týchto krajín.

2.2 Chemický tajnopis

Chemický tajnopis predstavuje spôsob zabezpečenia spravodajskej komunikácie, ktorý k zaisteniu utajenia využíva rôzne chemické látky a technológie založené na chemických princípoch. V tejto podkapitole sú spomenuté chemické spôsoby zabezpečenia komunikácie, ktoré sa používali, a niektoré z nich sa aj stále používajú, v spravodajských službách.

2.2.1 Tajný atrament

V spravodajskej praxi predstavuje neviditeľný atrament jeden zo spôsobov tajnopisu, maskovaného odovzdávania inštrukcií a správ. Neviditeľné atramenty, tiež nazývané sympatetické sa radia medzi základné steganografické metódy.

Ich použitie zaisťuje, že napísaný text nie je bežným okom viditeľný. Pričom príjemca správy musí vedieť akým spôsobom si má text prečítať.

Forma neviditeľného písma bola používaná ešte v druhej svetovej vojne. Zdroje neviditeľného písma boli bežné potraviny akými sú ocot, mlieko a rôzne ovocné šťavy. Ku sfarbeniu dochádza tepelným rozkladom organických látok, čiže zahrievaním. Neskôr už bolo možné bežné zdroje veľmi ľahké odhaliť, preto sa začali používať chemické atramenty, ktoré už neboli organického pôvodu ale zviditeľňovali sa tiež zahriatím. Tretia skupina využíva chemické reakcie ku zviditeľneniu písma. Funguje to tak, že sa písmo napíše určitou bezfarebnou chemickou látkou, ktorá sa po reakcii s inou látkou viditeľne sfarbí. František Doskočil v už spomínanom dokumentárnom filme popisuje tajnopisný papier CIA, ktorý bolo potrebné celý namočiť do vody, aby sa tajná správa stala čitateľnou. [9]

Následne sa začali vytvárať aj správy, ktoré bolo možné zviditeľniť iba v laboratórií pomocou ultrafialových alebo infračervených žiarení. [1]

Tieto spôsoby sa však onedlho prestali používať, pretože boli vynájdené univerzálne vývojky, ktoré dokázali rozpoznať miesta vlhčené pri písaní podľa zmien na povrchu vlákien papiera. Dnes sa podobná metóda používa pri výrobe bankoviek. [2]

Obrázok 15, Tajné písmo na vreckovke. [6]

Dokonalý neviditeľný atrament predstavuje taký atrament, ktorý bude reagovať iba s jednou chemikáliou. [2]

Po výbere látky neviditeľného atramentu musíme venovať pozornosť aj voľbe papiera. Tvrdý papier je pre písanie neviditeľnej správy vhodnejší, pretože ho atrament lepšie

vtiahne a nie sú na ňom viditeľné stopy po písaní. Tiež je vhodné po napísaní utajovanej správy papier popísať viditeľnými informáciami, pretože je potom papier menej nápadný a písaním sa vyrovná. Spravodajské správy sa zvykli písať do listov, kníh či časopisov. K predávaniu takto vytvorených textov sa využívala pošta, osobný alebo sprostredkovaný styk vo forme mŕtvych schránok. Pre prípad zachytenia neviditeľného textu sa obsah správy zvykol zašifrovať. Dnes sa neviditeľné atramenty používajú len veľmi málo. [3], [8], [11]

Tabuľka 1, Neviditeľné atramenty. [4], [vlastný]

Typ atramentu	Neviditeľná látka	Zviditeľnenie	Sfarbenie
Organické kvapaliny	Moč	ľahké zahriatie	dohneda
	Mlieko		
	ovocná šťava		
	Ocot		
Chemické látky	nasýtený roztok dusičnanu draselného	Zahriatie	papier zuhoľnatie
	chlorid kobalnatý		jasne modré
Chemické látky	síran železnatý	chemická reakcia s kyanidom sodným	tmavo modré
Fyzikálne látky	kyselina salicylová	ultrafialové žiarenie	fialové

Obrázok 16, Fľaštička s tajným atramentom. [6]

2.2.2 Latentný obraz

Latentné písmo je v spravodajských službách výraz, používaný pre chemicky vytvárané tajné písma. [12] Takzvaná latentná fotografia, tajné mikropísmo vytvárané fotochemickou cestou, je zdokonalený tajnopis. Vo všeobecnosti ide o okom nezbadateľne nanesené texty, ktoré sa nám opticky zjavia po špeciálnom chemickom spracovaní. [7]

Na to, aby latentný obraz vznikol potrebujeme aby bol fotografický materiál vystavený pôsobeniu svetla, poprípade röntgenovému žiareniu v rádiografii. Potom pôsobením vývojky dochádza k stmavnutiu materiálu v miestach, kde bol osvetlený.

Deje sa tak kvôli zmene kryštálov halogenidu striebra vo významných častiach materiálu. Obraz spočiatku nie je viditeľný pretože častice striebra sú príliš malé, avšak ak sa k ploche priblíži vývojka, prenikne časticou striebra a obraz zviditeľní. [13]

2.2.3 Karbónový papier

Karbóny sú špeciálne prostriedky pre zhotovenie chemického suchého tajnopisu, používané ako kopírovacie papiere. Ako nosič tajnej správy sa použil buď ľubovoľný alebo špeciálny papier, na ktorý sa položil karbón a ceruzkou alebo špicatým predmetom sa napísala správa, nakreslil obrázok alebo situácia. Karbón sa následne zničil, spravidla spálil. Na čistý papier, na ktorom bola pomocou karbónu nanesená správa, sa potom napísal neškodný text, spravidla rodinného charakteru a odoslal sa na kryciu adresu v zahraničí. Cez karbón bolo možné text písať aj do časopisov, kníh alebo tlače. Centrála príslušnej rozviedky potom tajnopis vyvolala pomocou vývojky, čo je špeciálna chemická látka reagujúca na karbón, alebo pomocou zahriatia napríklad žehličkou. Spravodajcovia alebo spolupracovníci spravodajskej služby si vyrábali karbóny sami, alebo im ich hotové dávali centrály. Chemické zloženie karbónov sa menilo, z toho dôvodu sa ich všetky rozviedky a kontrarozviedky snažili získať k chemickej analýze. Karbóny používali takmer všetky rozviedky ale úplne nerozbitné karbóny mala západonemecká rozviedka BND a tiež francúzska DGSE. V súčasnosti význam karbónov pre účely spravodajskej komunikácie poklesol. [8], [12]

2.2.3.1 Postup

V knihe Průlom autori Doskočil a Žáček naskenovali inštrukcie CIA pre písanie tajnopisu z jednej z prvých mŕtvych schránok.

„Inštrukcia k písaniu tajných správ pre nás, používaných karbón pre tajné písmo.

1. *Všeobecné poznámky*

Tajný karbón je čistý list papiera, ktorý bol nasýtení zvláštnou chemickou látkou, takže použitím tlaku ceruzky, veľmi malé množstvo chemickej zlúčeniny sa prenesie z karbónu na list papiera, s ktorým je karbón v styku. Prenos chemickej zlúčeniny sa vykoná bez ohľadu od toho, ktorá stránka karbónu je v styku s papierom, na ktorý prenášame tajnú správu. Karbón postačí k napísaniu veľa tajných správ: Je nutné ale zaobchádzať s karbónom opatrne, nesmie sa zašpiniť alebo pokrčiť. Karbón má byť uschovaný v bezpečnom a suchom mieste. Musíte byť opatrný aby ste nezamenil karbón s inými papiermi.

Než sa pokúsite napísať Vašu prvú tajnú správu používajte vopred pripravené krycie listy. Prečítajte si nasledujúci návod veľmi dôkladne. Je dôležité aby ste vopred cvičili tento spôsob nasledujúcim spôsobom: Položte listy papiera, podľa vyobrazenia, ale namiesto krycieho listu a karbónu, použite čistý papier. Cvičte písanie s nie príliš ostrou ceruzkou a používajte rôzne tlaky keď píšete. Pozrite sa na papier, ktorý používate namiesto krycieho listu proti svetlu. K tomuto účelu držte list papiera vo výške očí, takže svetlo lampy naň šikmo dopadá a odrazí sa. Ako to je znázornené v priloženej kresbe. Otáčajte papier mierne nahor a dole a preskúšajte obe strany, keď zistíte, že môžete rozoznať nátlaky vzniknuté ceruzkou na tomto liste, zničte túto stránku. Pokračujte vo Vašich pokusoch, až nájdete tlak, ktorý nezanechá žiadne viditeľné odtlačky na krycom liste. Použite tento tlak k písaní skutočnej tajnej správy.

2. *Príprava tajnej správy*

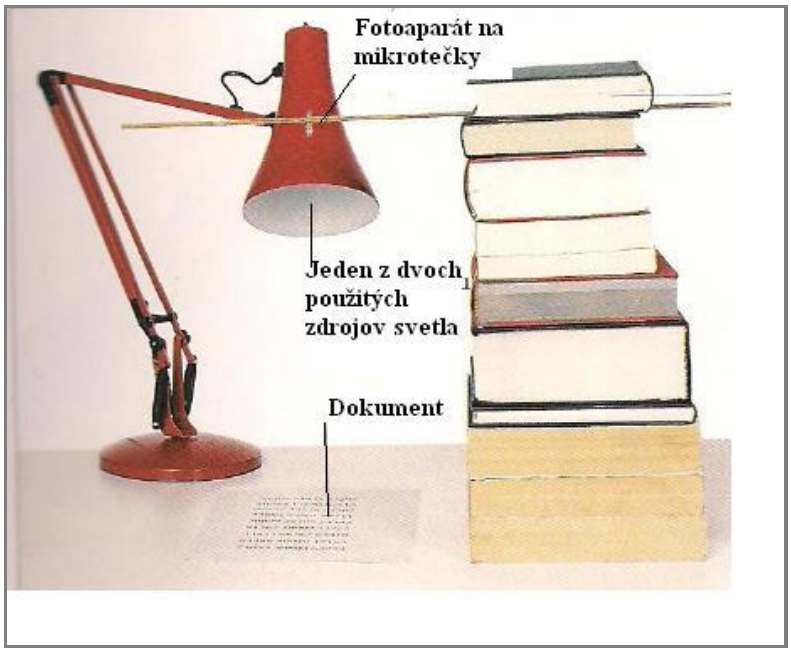
Prvý krok je pripraviť vašu správu a zašifrovať ju podľa priloženého návodu. Vaša zašifrovaná správa musí byť vždy na opačnej strane listu, ktorý obsahuje viditeľné písmo. Zoberte vopred napísaný krycí list a dôkladne čistou, bielou vreckovkou otrite prázdnu stránku listu – tú stránku, ktorá bude obsahovať Vaše tajné písmo. Otrite čistú stránku, vždy jedným smerom zo všetkých štyroch strán (otáčajte pritom papier). Potom postupuje nasledovne:

- *Položte čistý list papiera na čistú, tvrdú podložku, nalepte na sklo,*
- *Na tento list položte stránku z jedného z vopred pripravených krycích listov. Viditeľné písmo tohto listu bude zospodu.*
- *Položte karbón na tento list krycieho listu.* [14]

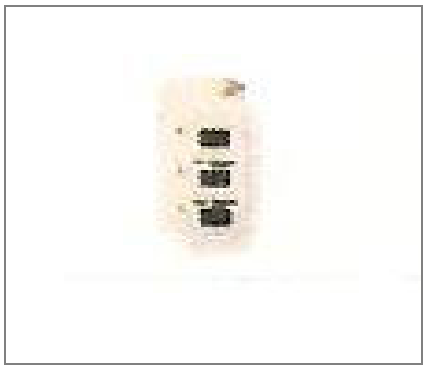
2.2.4 Mikrotečka

Technológie na skrývanie utajovaných správ sa neustále zlepšovali, dôkazom čoho je vynález prevratnej technológie nazývaný mikrotečka.

V encyklopédii tajných služieb je mikrotečka definovaná ako fotografia zmenšená na veľkosť miniatúrneho bodu. Ide v podstate o veľmi malý fotografický negatív, ktorý môže byť v meradle až 1:200. Špeciálnym fotografickým zariadením je fotografia zmenšená na veľkosť 0,5mm^2 až 12mm^2. Tento negatív v sebe dokáže skrývať až niekoľko strán formátu A4, ktoré sú optickými prístrojmi zmenšené až na neskutočnú veľkosť špendlíkovej hlavičky. Predpokladom vyhotovenia kvalitnej mikrotečky je technicky zdatný, vycvičený a odborne vybavený agent. [8], [15]



Obrázok 17, Použitie fotoaparátu na mikrotečky. [6]



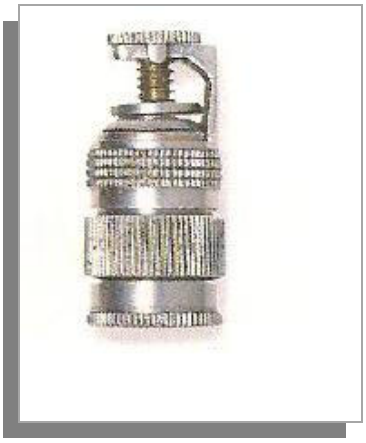
Obrázok 18, Zväčšené mikrotečky. [6]

Aj napriek tomu, že boli také malé, mikrotečky boli už v časoch vojny schopné skryť enormné objemy dát vrátane kresieb a fotografií. Takýmto spôsobom mohli byť ukryté napríklad plány lietadiel, či letísk. Výhodou tejto technológie je, že krycia správa, ktorá slúži ako nosič utajenej informácie nemusí byť vôbec rozsiahla, poprípade môže byť mikrotečka k príjemcovi dopravená samostatne. V prusko-francúzskej vojne sa posielali správy v tomto formáte prostredníctvom holubov, v inej vojne boli zas prepravované v náušniciach, v nosných dierkach alebo za nechtami agentov.

Mikrotečky sa však bežne ukrývali pod známku, do lepu na okraji obálky, alebo v listoch písaných na stroji na horný okraj interpunkčných znamienok. [16]

Táto technológia bola veľmi účinná pretože správy ani nebolo nutné šifrovať, či skrývať, boli jednoducho také malé, že na seba neupútavali pozornosť. Detekovať ich bolo možné aktiváciou pomocou neutrónov a na prečítanie bola potrebná lupa alebo pri menších rozmeroch čítačka, či mikroskop. [2], [5], [7], [16]

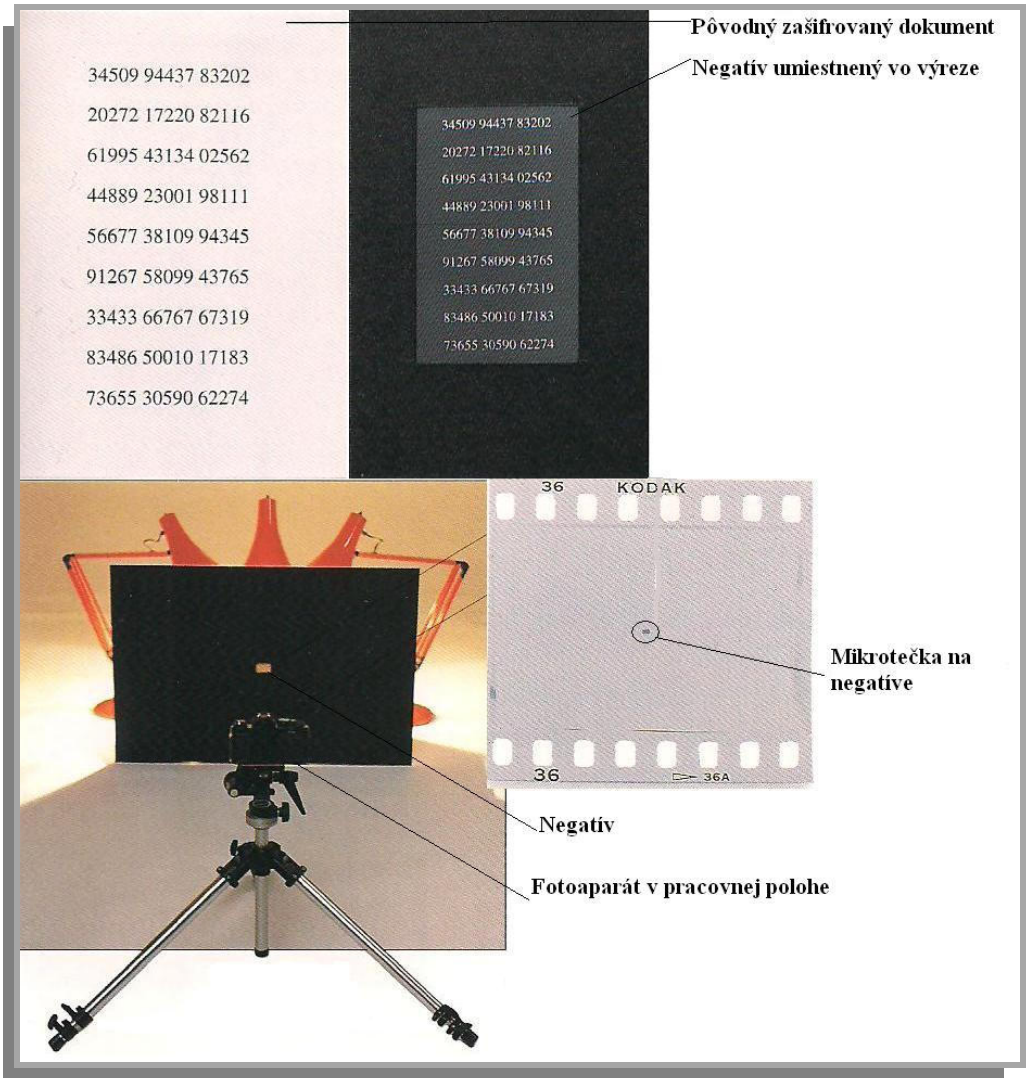
Obrázok 19, Čítačka mikrotečky. [6]



Obrázok 20, Fotoaparát na mikrotečky. [6]

2.2.4.1 Postup

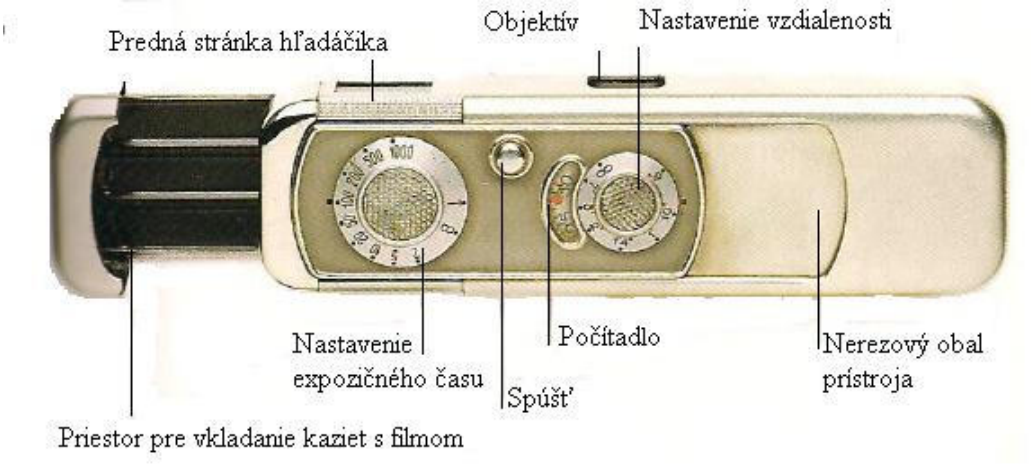
Mikrotečku je možné zostrojiť pomocou kvalitného fotografického prístroja na kinofilm 35 mm. Britská metóda výroby používa čiernobiely film s vysokým stupňom citlivosti. Utajovaný dokument sa vyfotografuje tak, aby zaplnil celé okienko filmu. Negatív z vyvolaného filmu sa umiestni do výrezu v čiernom kartóne. Kartón sa zozadu osvieti a vyfotografuje s objektívom s ohniskovou vzdialenosťou 50 mm, zo vzdialenosti 127 cm. Výsledný čierny obrázok na bielom pozadí má veľkosť 1 mm. [6]



Obrázok 21, Výroba mikrotečky. [6]

2.2.5 Fotoaparáty Minox

Najrozšírenejšie fotoaparáty vo svete špionáže do začiatku 90. rokov boli miniatúrne prístroje značky Minox. Mali vynikajúce konštrukčné riešenie a dokonalú prispôsobivosť, ktorými umožňovali agentovi ideálne tajné snímkovanie. Dokázali fotografovať budovy, či kopírovať dokumenty. Vyrábali sa aj Minoxy nezávislé na batérii, tie mohli zostať nepoužívané neobmedzene dlhú dobu a vždy boli pripravené k použitiu. [6]



Obrázok 22, fotoaparát Minox. [6]

2.3 Fyzikálny tajnopis

Fyzikálny tajnopis predstavuje ďalší spôsob spravodajského zabezpečenia, ktorý využíva fyzikálne princípy k utajeniu komunikácie. V tejto kapitole uvádzam rôzne techniky fyzikálneho tajného písania správ, používaného spravodajskou službou.

2.3.1 Suché pero

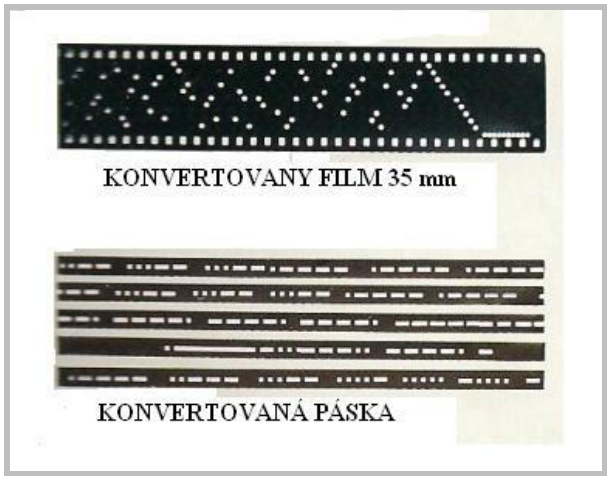
Ide o prostriedok výroby tajnopisu fyzikálnou cestou, ktorý sa vykonával vyrytím do papierového podkladu. Po vyrytí sa nosič tajnopisu uhladil, aby neboli vidieť vyryté stopy. K tomu slúžilo hladítko z kože. Cez tajnú správu sa napísal takzvaný rodinný list, ktorý nevzbudzoval pozornosť. Centrála rozviedky tajnopis nevyvolávala ale si ho prečítala pomocou UV lampy, kremíkovej lampy, alebo pod šikmým svetlom. Problémom bolo, že takto napísaná správa sa musela uchovávať v kontajneroch, pretože by sa riskovalo, že neznáma osoba ju naplní atramentom. Ďalší problém mohol nastať ak by sa stopa príliš dôsledne uhladila, čo by znemožňovalo jej čitateľnosť. V takomto prípade rozviedka tajnú správu čítala röntgenom. [12]

2.3.2 Magnetická stopa

S rozvojom technológií, predovšetkým magnetofónovej techniky začali západonemecká, americká ale aj iné rozviedky používať magnetofónové pásky ako nosiče pokynov pre svoju agentúru umiestnenú vo svete, predovšetkým vo východnej Európe. Princíp spočíval

v tom, že agent získal magnetofónovú pásku, na ktorej bola nahraná populárna hudba, väčšinou vo východnej Európe nedostupná. Súčasťou tejto pásky bola aj spravodajská správa zapracovaná na zvláštnej stope pásky. Na prehranie utajovanej správy slúžil špeciálny magnetofón, ktorým si agent informáciu vypočul a následne pásku zničil. Problém bol v tom, že agenti väčšinou pokyn na zničenie kazety nesplnili. Práve kvôli zahraničnej, vo Východnej Európe nedostupnej hudbe, si agenti pásky nechávali, či si ich dokonca požičiavali. [12]

Okrem magnetofónovej pásky mohla byť správa zaznamenaná aj na všeobecne používaný 35 mm fotografický film.



Obrázok 23, Pásky pre zhlukový prenos. [6]

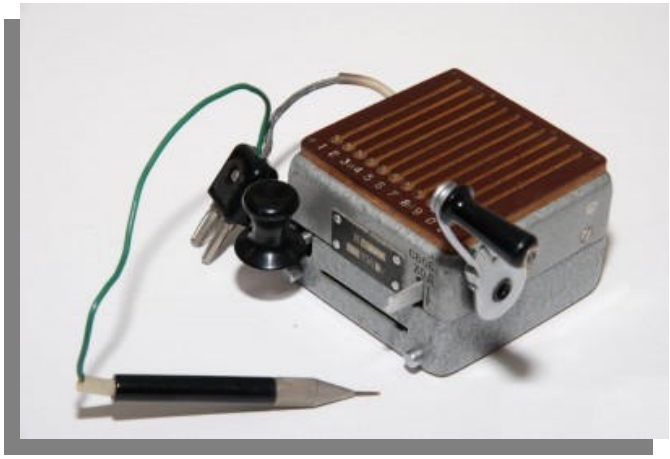
2.3.3 Rýchlospoj

Rýchlospoj predstavoval rýchlovysielač, ktorý nebolo možné zamerať. Bol využívaný hlavne u CIA.

Rýchlo vysielač je mechanické zariadenie, ktoré dokázalo vysielať správy na krátkych vlnách takou rýchlosťou a s minimálnym vyžarovaním, že bolo pre každú rádiovú kontrarozviedku nemožné vysielač zamerať. Spojenie sa väčšinou uskutočňovalo v teréne daného štátu, v miestach, kde bola ľahká kontrola proti sledovaniu. Spojenie väčšinou obstarával pracovník rezidentury príslušného štátu sediaci v diplomatickom aute. Spojenie sa medzi ním a agentom, sediacim tiež v aute, vykonávalo vo veľmi krátkom čase. Išlo zhruba o 30 sekúnd až 60 sekúnd, pričom vzdialenosť nepresahovala 2 kilometre. [12] Prístroj obsahoval voliaci kotúč s troma tlačidlami, ktorými sa manipulovalo. Po potočení prvým tlačidlom, bolo možné nahovoriť celú utajovanú správu, pričom mohla mať rozsah

až dvoch strán. Voliaci kotúč sám automaticky preniesol zakódované slová elektromagnetizáciou na oceľový pásik nachádzajúci sa vo vnútri aparátu. To spôsobilo zhustenie správy na oceľovom pásiku do Morseových znakov. Následne sa potočilo druhým tlačidlom, čo spôsobilo rozsvietenie magického zeleného oka. To znamenalo, že krátke vlny sú nasmerované na konkrétny prijímač. Už len stačilo otočiť tretím tlačidlom aby sa znaky z oceľového pásika vyslali k príjemcovi. [7], [17]

Toto zariadenie umožňovalo vysielanie zašifrovanej správy rýchlosťou až 900 znakov za minútu, Čo bolo dostatočne rýchlo na to, aby správu nezachytil protivník. Tento spôsob spojenia bol mimoriadne bezpečný. [12]



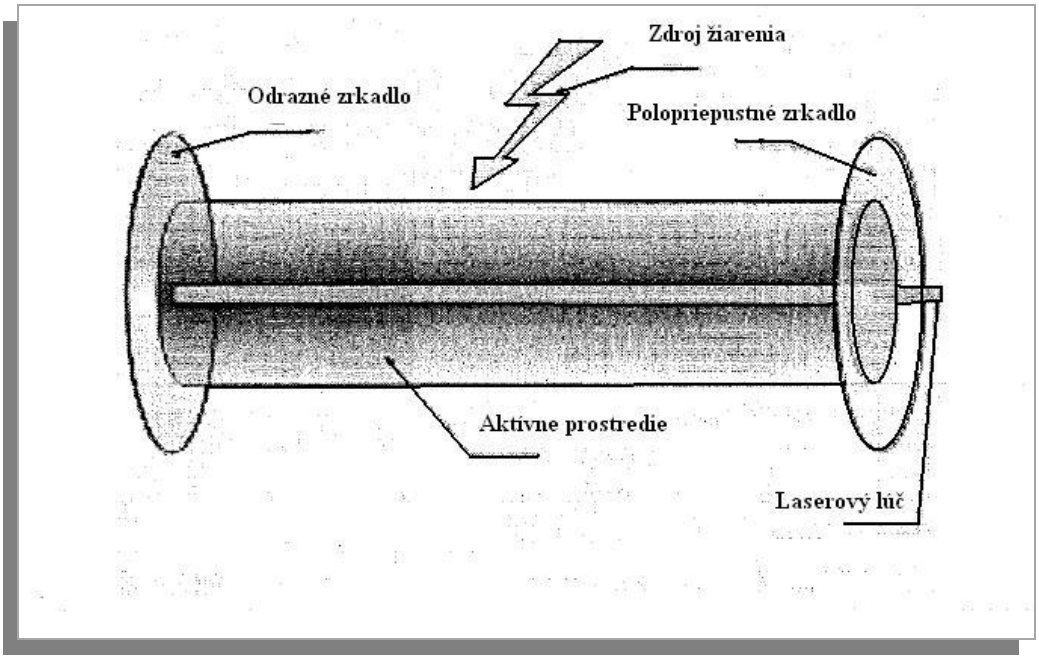
Obrázok 24, Kóder R350. [6]

2.3.4 Rádioizotopy

Tajná správa bola napísaná špeciálnym perom naplneným rádioizotopovou látkou, ktorá fungovala na princípe takzvaného bezpečného žiarenia. Fungovalo to tak, že agent týmto špeciálnym perom napísal tajnú správu na nosič, ktorý prekryl bežným nepopísaným listom. Rozviedka správu vyvolala špeciálnou technikou, vytvorenou na princípe geigerovho počítača. Vo väčšine prípadov agent ani netušil, že pracuje s bezpečným rádioizotopom pretože by to s najväčšou pravdepodobnosťou odmietol. [12]

2.3.5 Laserová technika

Laserové odpočúvanie je spôsob diaľkového odpočúvania hovorov využívajúci laserové lúče pre snímanie vibrácií stien alebo okenných tabúl. Laser je zosilňovač svetla pomocou stimulovanej emisie žiarení, ktorý využíva zákony kvantovej mechaniky a termodynamiky. [18]

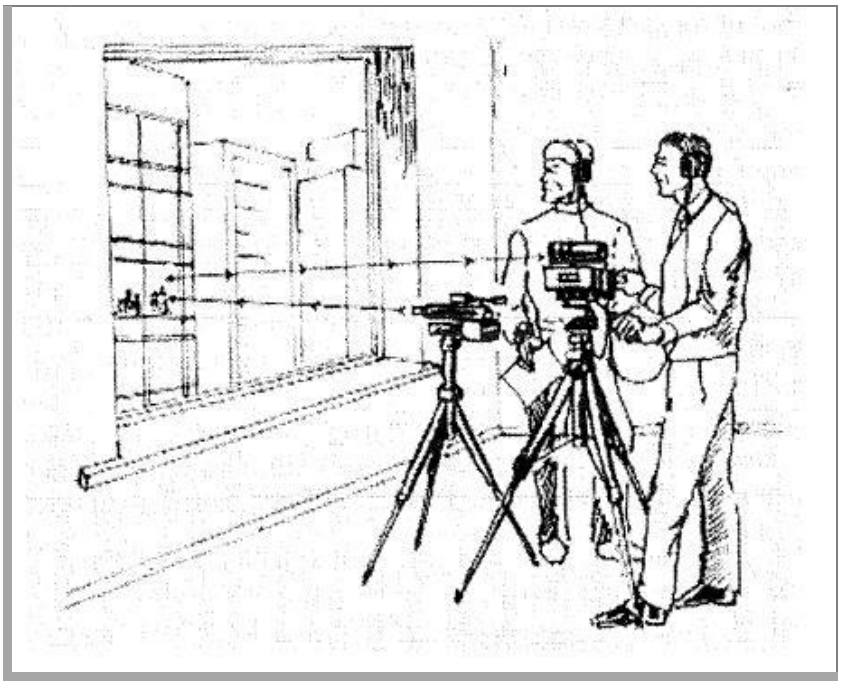


Obrázok 25, Konštrukcia laseru. [18]

Laserový zdroj žiarenia obsahuje iba jednu vlnovú dĺžku a ide iba jedným smerom. Preto vyžaruje ostrý lúč s typickou farbou. Využíva infračervené laserové zdroje alebo ultrafialové. Laserová odpočúvacia súprava sa skladá z vysielacej jednotky s optickým zameriavačom, kvalitného zosilňovača a ekvalizéra. V praxi je aplikácia laserového odpočúvania veľmi náročná, pretože spoľahlivé výsledky nie sú schopné odolávať vplyvom prostredia z rušnej ulice. Hlavnou výhodou tohto zariadenia je jeho odolnosť proti poveternostným podmienkam, dokonalá presnosť a kvalita nahrávky. [18]

2.3.5.1 Postup

Vysielač laserového lúča zameriame na okennú tabulu alebo rezonančnú plochu v odpočúvanej miestnosti. Z hovoreného hlasu vznikajú frekvencie, tie rozochvejú rezonančné plochy v miestnosti a následne sa namodulujú na odrazený laserový lúč, ktorý oknom opustí odpočúvanú miestnosť. Z tohto lúča prijímač vytvorí hlasovú informáciu. [18]



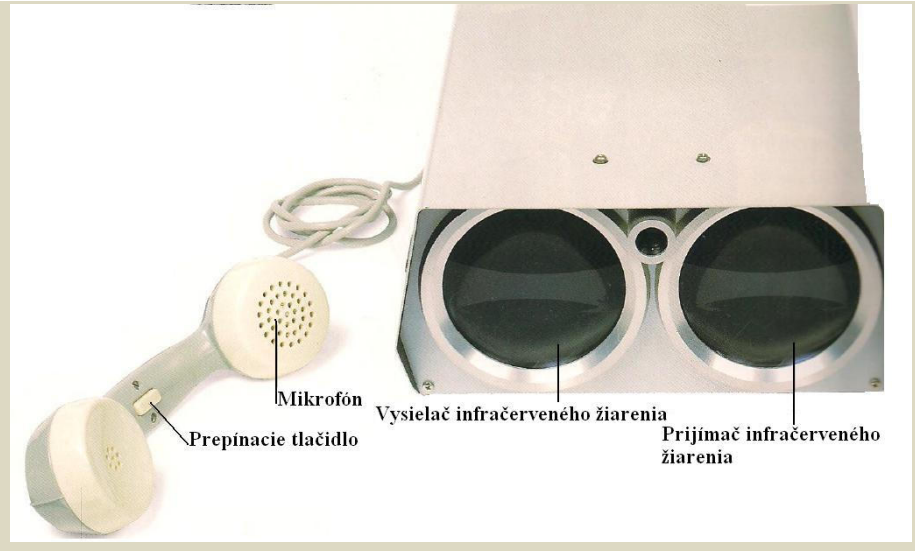
Obrázok 26, Použitie laserového odpočúvania v praxi. [18]

2.3.5.2 Šumový generátor

Šumová ochrana proti odpočúvaniu predstavuje mechanické zašumenie miest, na ktorých by bolo možné snímať zvuky. Na toto slúži šumový generátor, ktorý obsahuje procesor slúžiaci na automatické vyhodnotenie zvukov z miestnosti, aby púšťal iba takú úroveň zašumenia, ktorá je nevyhnutná v závislosti na hlasitosti konverzácie. [18]

2.3.6 Infračervené žiarenie

Komunikácia prostredníctvom infračervených lúčov sa využívala na vysielanie a príjem fonických správ na vzdialenosti väčšie ako 3km, medzi agentom a riadiacim dôstojníkom. Umožňuje vysielať správy cez deň aj v noci. Tento spôsob komunikácie je obzvlášť vhodný pre mestské oblasti. Jeho najväčšou nevýhodou je znižovanie výkonu v hmle alebo daždi. Dôležité je aby infračervenému lúču nestála v ceste žiadna prekážka. [6] Toto zariadenie bolo a stále je veľmi ťažko odhaliteľné.

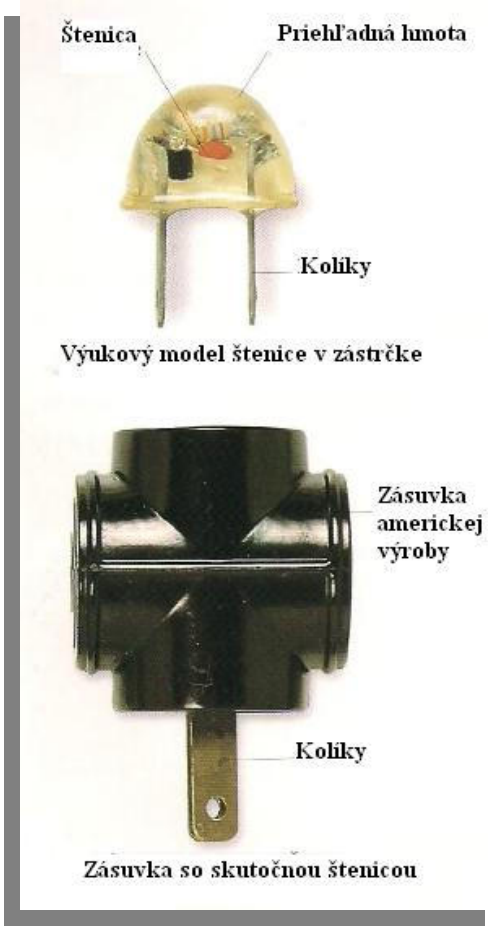


Obrázok 27, Infračervený komunikačný prístroj. [6]

2.3.7 Odpočúvacie zariadenia

Spravodajské služby vynakladajú obrovské úsilie, aby disponovali technickými zariadeniami, ktoré im umožnia odpočúvať konverzáciu protivníka. Toto umožňuje celá škála techniky od miniatúrnych mikrofónov, cez vysielače a magnetofóny, až po tiché kladivo. Je dôležité, aby mal prenášaný signál dostatočnú silu a bol primerane odrušený kvôli protivníkovým detektorom. V súčasnej dobe je technika natoľko pokročilá, že dokáže prenášať digitalizovaný zvuk iba vo vopred stanovenom časovom intervale. Nasledujúci obrázok (Obr.28), predstavuje miniatúrne odpočúvacie zariadenie, schopné odpočúvania cez stenu, ktoré vzhľadom k plastovej konštrukcii nie je možné odhaliť s detektorom kovov. [6]

Obrázok 28, Zariadenie k odpočúvaniu cez stenu. [6]



Obrázok 29, Prvá miniatúrna štenica. [6]

2.4 Matematický tajnopis

Kryptografická ochrana predstavuje dôležitú časť procesu ochrany komunikácie.

2.4.1 Legislatívna úprava kryptografickej ochrany

O kryptografickej ochrane hovorí zákon č. 412/2005 o ochrane utajovaných informácií a o bezpečnostnej spôsobilosti.

Podľa hlavy VIII sa za kryptografický materiál považuje kryptografický prostriedok, materiál k zaisteniu jeho funkcie alebo kryptografický dokument. Kryptografické prostriedky a kryptografické pracoviská, slúžiace pre kryptografickú ochranu utajovaných informácii, musia byť certifikované.

Orgán štátu, právnická osoba a podnikajúca fyzická osoba, ktoré vykonávajú fyzickú ochranu, musia viesť evidencie kryptografického materiálu, pracovníkov kryptografickej

ochrany, prevádzkovej obsluhy kryptografických prostriedkom a kuriérov kryptografického materiálu.

K výkonu kryptografickej ochrany je oprávnený pracovník kryptografickej ochrany, ktorý je poverený zodpovednou osobou, je držiteľom platného osvedčenia fyzickej osoby a je tiež držiteľom osvedčenia o zvláštnej odbornej spôsobilosti.

Prevádzkovú obsluhu kryptografického prostriedku môže vykonávať osoba, ktorá je poverená zodpovednou obsluhou, splňuje podmienky prístupu k utajovanej informácii a je k obsluhe zaškolená.

Prepravu kryptografického materiálu zaisťuje kuriér kryptografického materiálu, ktorý bol k preprave poverený zodpovednou osobou, je držiteľom platného osvedčenia fyzickej osoby a bol k preprave zaškolený.

Distribúciu a evidenciu kryptografického materiálu Českej republiky, kryptografického materiálu Európskej únie a kryptografického materiálu distribuovaného na základe medzinárodnej zmluvy zaisťuje Úrad. Distribúciu a evidenciu kryptografického materiálu Organizácie Severoatlantickej zmluvy a kryptografického materiálu pre vojenské účely zaisťuje Ministerstvo obrany.

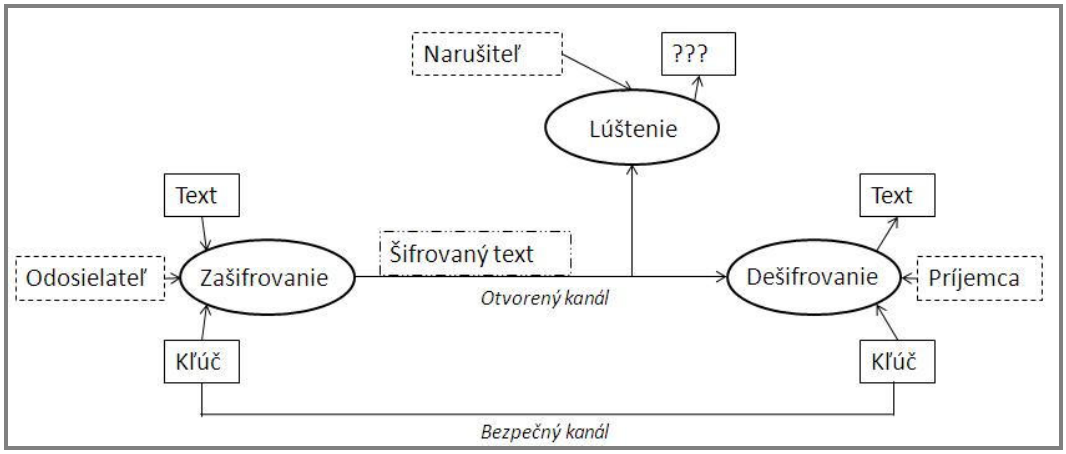
Podmienky evidencie, manipulácie a kontroly kryptografického materiálu v Českej republike zahrňujúci predovšetkým možnosť zriadenia účtov pre kryptografický materiál v orgánoch štátu alebo u podnikateľa, vedenie evidencií, kontrolnej funkcie, povinností držiteľov kryptografického materiálu voči Úradu alebo Ministerstva obrany a zaistenie kuriérnej služby pre kryptografický materiál Európskej únie upravuje bezpečnostný štandard.

Utajované informácie stupne utajenia Prísne tajné, Tajné alebo Dôverné sa pred únikom kompromitujúcim vyžarovaním zaisťujú zabezpečením elektrických a elektronických zariadení zabezpečenej oblasti alebo objektu. Overovanie spôsobilosti elektrických a elektronických zaradení zabezpečenej oblasti alebo objektu k ochrane pred únikom utajovanej informácie kompromitujúcim vyžarovaním zaisťuje Úrad pri certifikácii informačného systému alebo kryptografického prostriedku, pri schvaľovaní projektu bezpečnosti komunikačného systému, alebo na základe odôvodnenej písomnej žiadosti orgánu štátu alebo podnikateľa v súvislosti s ochranou utajovaných informácií.

K vykonávaniu merania zariadení, zabezpečenej oblasti alebo objektu, ktoré sú prevádzkované alebo užívané spravodajskými službami, sú oprávnené spravodajské služby. V týchto prípadoch nie je vyžadované uzavretie zmluvy.

Pri vykonávaní meraní sú spravodajské služby povinné dodržiavať ustanovenia tohto zákona, prevádzacích právnych predpisov a bezpečnostných štandardov Úradu. [19]

2.4.2 Základný princíp kryptografickej ochrany

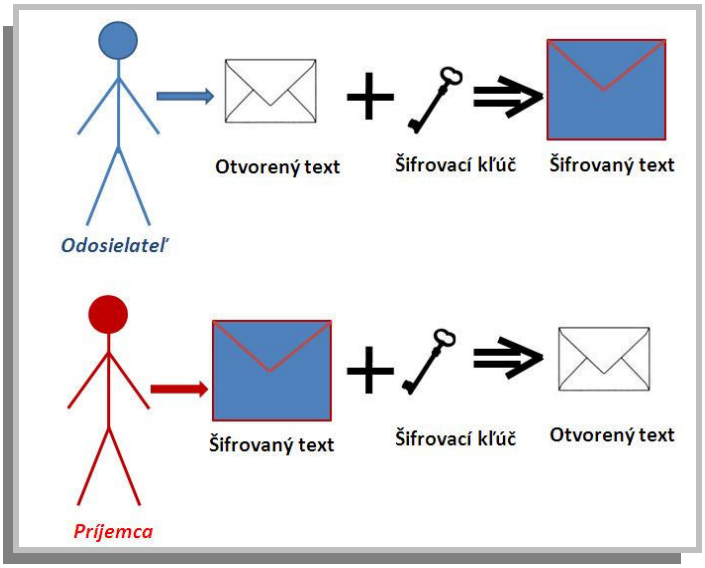


Obrázok 30, Základné schéma komunikácie pomocou šifier. [vlastný]

Na princípe predchádzajúceho obrázka funguje celý systém kryptografickej ochrany. Text správy, ktorý chce odosielateľ poslať príjemcovi sa zašifruje pomocou kľúča. Kľúč si odosielateľ s príjemcom vymenili prostredníctvom bezpečného kanála. Zašifrovaný text sa pošle cez otvorený kanál príjemcovi. V tejto fáze má priestor narušiteľ, ktorý by správu mohol odchytiť a pokiaľ by poznal kľúč tak aj odšifrovať. Príjemca zašifrovanú správu dostane a pomocou kľúča, si ju dešifruje.

Symetrická kryptografia

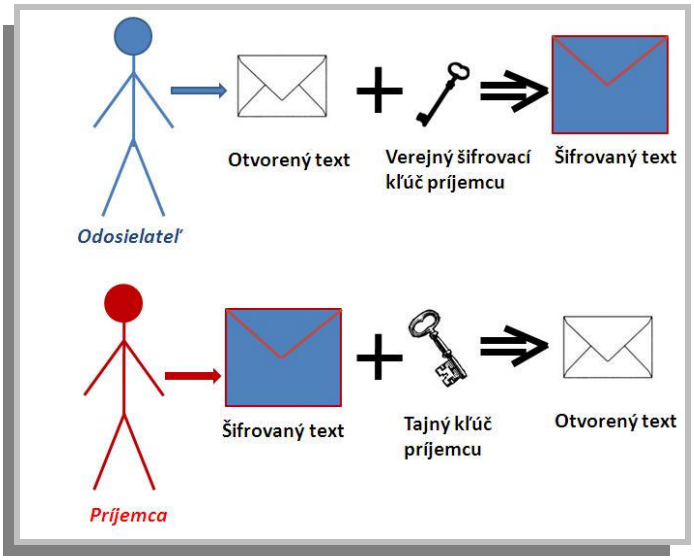
Symetrická kryptografia je šifrovací algoritmus, ktorý na zašifrovanie aj dešifrovanie správy používa rovnaký šifrovací kľúč. Nevýhodou tohto algoritmu je fakt, že šifrovací kľúč si odosielateľ a príjemca musia nejakým spôsobom povedať, čo býva hlavným kameňom úrazu. [5]



Obrázok 31, princíp symetrickej kryptografie. [vlastný]

Asymetrická kryptografia

Kryptografia s verejným kľúčom, ako je asymetrická kryptografia tiež nazývaná, predstavuje šifrovací algoritmus, ktorý využíva na zašifrovanie a odšifrovanie rozdielne kľúče. Tým pádom tu odpadá problém prenosu kľúča. Asymetrická kryptografia funguje tak, že odosielateľ zašifruje otvorený text verejným šifrovacím kľúčom príjemcu a pošle zašifrovanú správu po verejnom kanály. Príjemca dostane zašifrovanú správu, ktorú je možné dešifrovať iba jeho vlastným tajným šifrovacím kľúčom. [6]



Obrázok 32, Princíp asymetrickej kryptografie. [vlastný]

Základné rozdelenie šifrových systémov

- Substitúcia,
- Transpozícia,
- Kódová kniha.

Substitučné šifry spočívajú v zámene použitej abecedy textu, ktorý šifrujeme, za znaky šifrovej abecedy. K prevodu otvoreného textu na šifrovaný text sa používa jedna šifrovacia abeceda pre celý text alebo sa môže použiť pre každé písmeno otvoreného textu, iná šifrovacia abeceda. Príkladom tohto šifrového systému môže byť napríklad Caesarová šifra. [7], [20]

Transpozičné šifry spočívajú v zamiešaní poradia písmen v otvorenom texte. Písmená sa preskupujú podľa presne stanovených pravidiel. [8]

Kódová kniha predstavuje slovník, v ktorom sú slová alebo vety otvoreného textu nahradzované kódmi. Jedná sa prevažne o štvoricu alebo päticu písmen alebo čísiel. K tomu, aby sme zamedzili odhaleniu najpoužívanejších fráz, niektoré kódové knihy obsahujú pre často používané slová viacero kódových skupín. [9]

2.4.3 Šifrovacie bločky na jedno použitie

V tridsiatich rokoch prijali moderné spravodajské služby systém komunikácie používajúci šifrovacie bločky na jedno použitie. Na Slovensku sa tomuto spôsobu šifrovania hovorí prešifrovacie zošity. V porovnaní s ostatnými spôsobmi šifrovania, je tento spôsob najbezpečnejší, pretože tento šifrovací bloček majú k dispozícii iba odosielateľ tajnej informácie a prijímateľ. Prešifrovací zošit je celý zaliatí do fólie. K odhaleniu kľúča je nutné fóliu mechanicky poškodiť, čím sa zaistí to, aby si odosielateľ bol istý, že už bol bloček jeden krát použitý. Pokiaľ sa dodrží pravidlo, že bude každá strana šifrovacieho bločku použitá iba jeden krát a následne na to zničená, bude tento šifrovací kód nerozlúštiteľný. [16]

Začiatkom vojny mali Rusi týchto jednorazových bločkov nedostatok, preto ich v jednom čase rozposlali na viaceré miesta. Americký kryptoanalytik sa dostal k jednému z týchto bločkov. Ten obsahoval kód pre najčastejšie používané slová : „hláskuj“ a „koniec hláskovania“, ktoré sa používali pred a po skončení hláskovania slova, ktoré nebolo

v kódovacom bločku. Na základe toho skúmaním zistil, že použili bločky viackrát a bol schopný dešifrovať niektoré správy. [16]

So šifrovacími blokmi bol spojený aj výraz **Indikátorová skupina.** Ide o nešifrovanú skupinu znakov zo šifrovacieho bloku, slúžiaca k tomu, aby príjemca vedel, na ktorom mieste je potrebné správu priložiť k bloku na začatie dešifrovania. [16]

Bolo veľmi dôležité aby sa k šifrovacím blokom nedostala nepovolaná osoba, preto sa občas bločky vydávali v miniatúrnej podobe a schovávali napríklad na dno zapaľovača alebo do iných predmetov, ktoré nevzbudzovali pozornosť.

Využívali sa tiež **klamné čísla**. Vložením takzvaného klamača došlo k posunu čísiel a tým pádom bolo nemožné pre narušiteľa správu dešifrovať. Navyše slúžili ako dôkaz, že zašifrovanú správu poslal naozaj odosielateľ. Toto využívali hlavne Američania kvôli našej spravodajskej službe. [14]

2.4.3.1 Postup

Pre odoslanie šifrovanej správy pomocou jednorazového šifrovacieho bloku, musí najskôr odosielateľ previesť každé slovo tajnej správy, pomocou kódovacieho slovníka, na skupiny štvorciferných čísiel. Pokiaľ je napríklad prvé slovo našej správy slovo obrana, ktorá má priradené číslo 3765 a prvá skupina čísiel v šifrovacom bloku je 1196, použije sa Fibonacciho metóda, vďaka ktorej vznikne číslo 4851. Táto metóda spočítava čísla bez toho, že by čísla väčšie ako 9 prenášala dopredu. Tým vlastne vzniká dvojité zašifrovanie. [16] Klamač bolo napríklad číslo 0, ktoré sa pred falošným odčítaním vložilo vždy na iné miesto v texte, na začiatku správy. Tým došlo k posunu všetkých čísiel a po dešifrovaní správy k nezmyselným informáciám. [14]

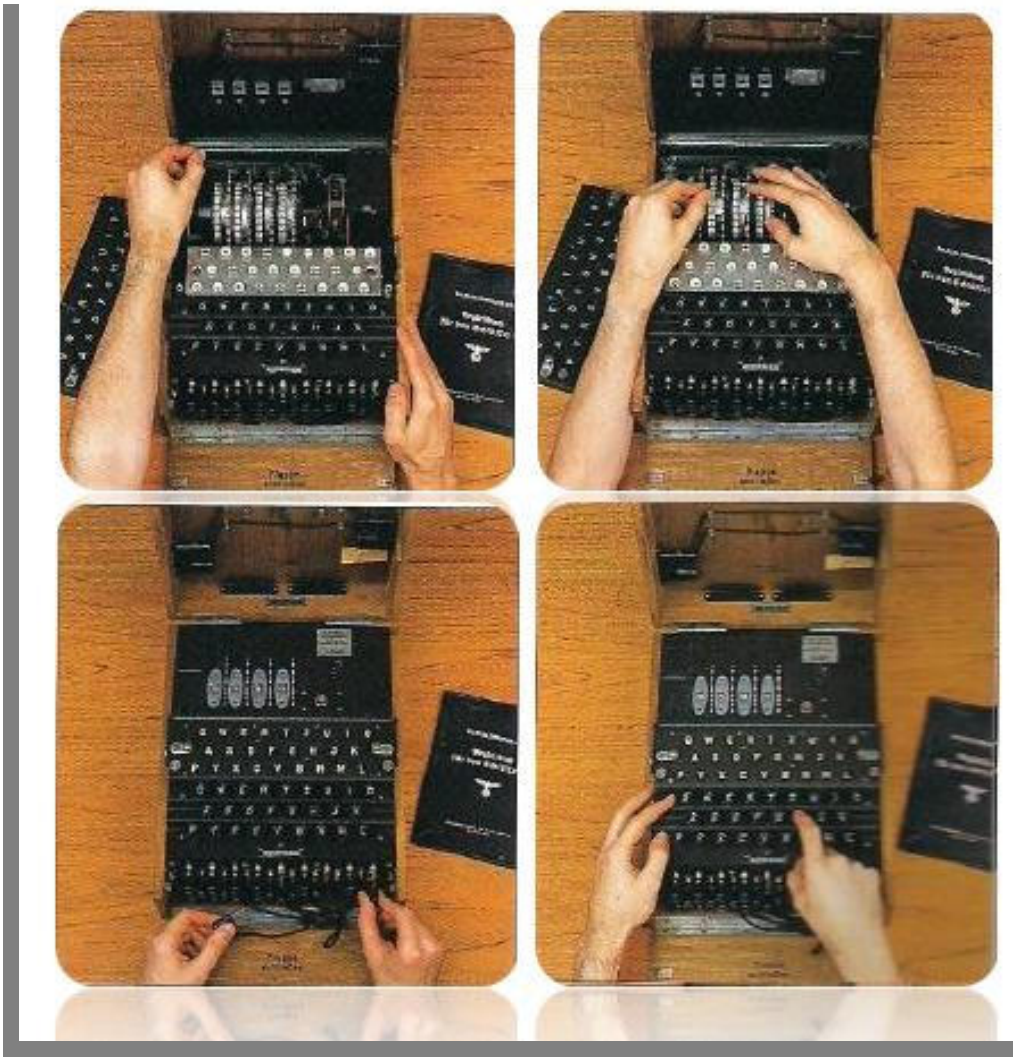
2.4.4 Enigma

Nemecký elektromechanický prístroj na šifrovanie a dešifrovanie správ bol skonštruovaný v roku 1923. Každé písmeno sa zašifrovalo samostatne prostredníctvom radou spojení a rotorov. Nemci v priebehu vojny Enigmu neustále zdokonaľovali a zvyšovali zložitosť šifier. Vznikali rôzne typy prístroja, ktoré sa navzájom od seba líšili v závislosti na tom, v ktorých nemeckých organizáciách, armáde, bezpečnostných a spravodajských službách či diplomatickom zbore mali byť použité. [6]

Obrázok 33, Nemecký šifrovací stroj Enigma. [6]

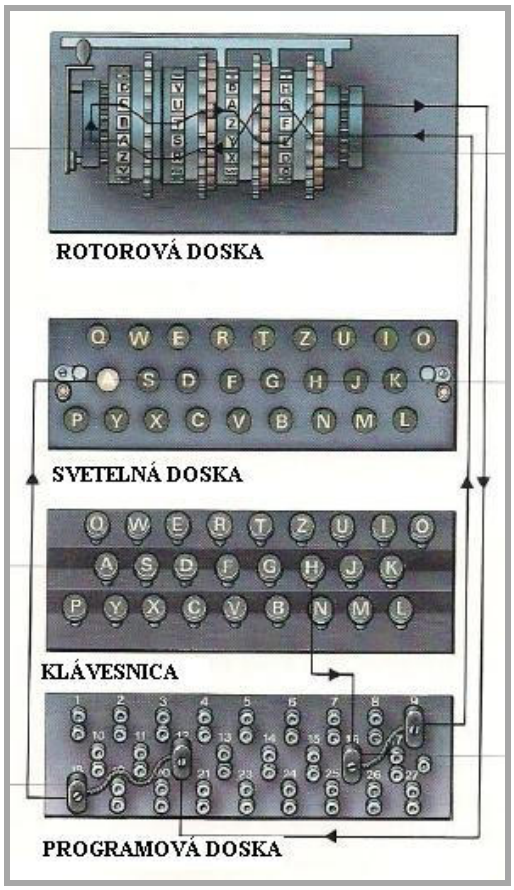
2.4.4.1 Mechanizmus Enigmy

Zložitosť Enigmy závisela na spôsobe nastavenia stroja. Na rotorový valec sa umiestňovali abecedné rotory v akomkoľvek poradí a tiež vnútorné vedenie v každom rotore sa mohlo nastaviť do akejkoľvek pozície. Určenie šifry záviselo na počiatočnom nastavení rotorov. Do programovej dosky sa vkladali zástrčky tiež v akejkoľvek kombinácii. Všetky nastavenia prístroja sa pravidelne obmieňali. [6]



Obrázok 34, Mechanizmus Enigmy1. [6]

- Posunutím páčky sa uvoľnia rotory, tie sa vyberú z prístroja a pozmení sa prstencové nastavenie. Potom sa rotory vrátia naspäť do prístroja.
- Písmená rotorov je možné vidieť v okienkach krytu. Rotor sa bude točiť, až kým sa písmenka nenastavia podľa aktuálnych inštrukcii.
- Keď sú písmenká v základnom aktuálnom nastavení zaklapne sa kryt a nastaví sa spojenie na programovej doske. Dvojice písmen spoja zástrčky podľa šifrovacej knihy operátora.
- Operátor si náhodne vyberie 4 písmenká, ktoré napíše dvakrát. Táto osem písmenková šifra slúži ako označenie správy. Potom sa na tieto 4 písmenka nastavia rotory. [6]



Obrázok 35, Mechanizmus Enigmy2 [6]

Na obrázku operátor stlačil písmeno H. To dalo impulz na elektrický signál, ktorý vedie k číslu 16 a odtiaľ na číslo 9. Signál z čísla 9 prechádza rotorovou doskou, kde sa niekoľkokrát zmení. Zmenený signál sa vracia do programovej dosky, do čísla 12 a odtiaľ do čísla 18. Nakoniec signál vedie do svetelnej dosky, kde dopadá na písmeno A, ktoré sa vzápätí rozsvieti. Rozsvietené písmeno predstavuje začiatok zašifrovanej správy. [6]

2.4.5 Fialka

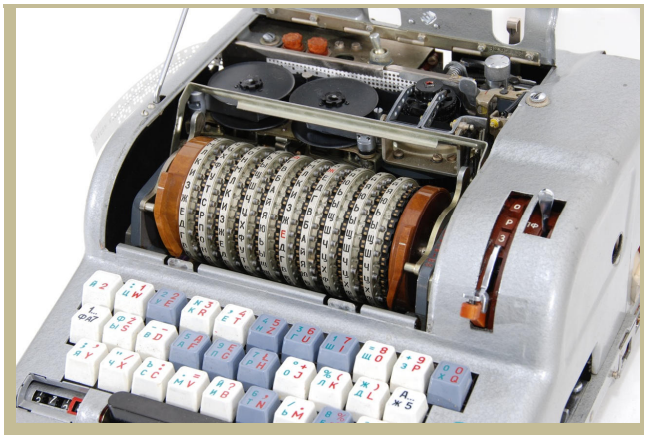
Fialka je šifrovací stroj, ktorý bol vyvinutý ZSSR krátko po druhej svetovej vojne a bol najpoužívanejším strojom Varšavskej zmluvy až do roku 1990. Každá krajina Varšavskej zmluvy mala svoju vlastnú prispôsobenú verziu pre miestny jazyk. Stroj, ktorý používal šifry postupu Fialka mal označenie M-125.

Konštrukcia tohto šifrovacieho stroja bola z väčšej časti založená na stroji Enigma. Rovnako ako Enigma používa celý rad kódovaných kolies na zakódovanie písmen písaných

na klávesnici. S každým stlačením klávesnice sa koleso otočí do novej polohy, čím efektívne mení substitúciou každé písmeno zadané na klávesnici.

Rusi sa však pri konštruovaní Fialky poučili z mnohých chýb Enigmy.

Skôr než vyjde výstup na panel lampy, stroj vytlačí kódovaný list priamo na dierne pásky. V rovnakom čase môže udrieť list na tú istú papierovú pásku v 5-bitovom digitálnom kóde. Okrem toho Fialka obsahuje vysielač papierových pások, ktorý môže byť použitý na prenos alebo kópiu záznamov. [21]



Obrázok 36, Ruský šifrovací stroj Fialka. [21]

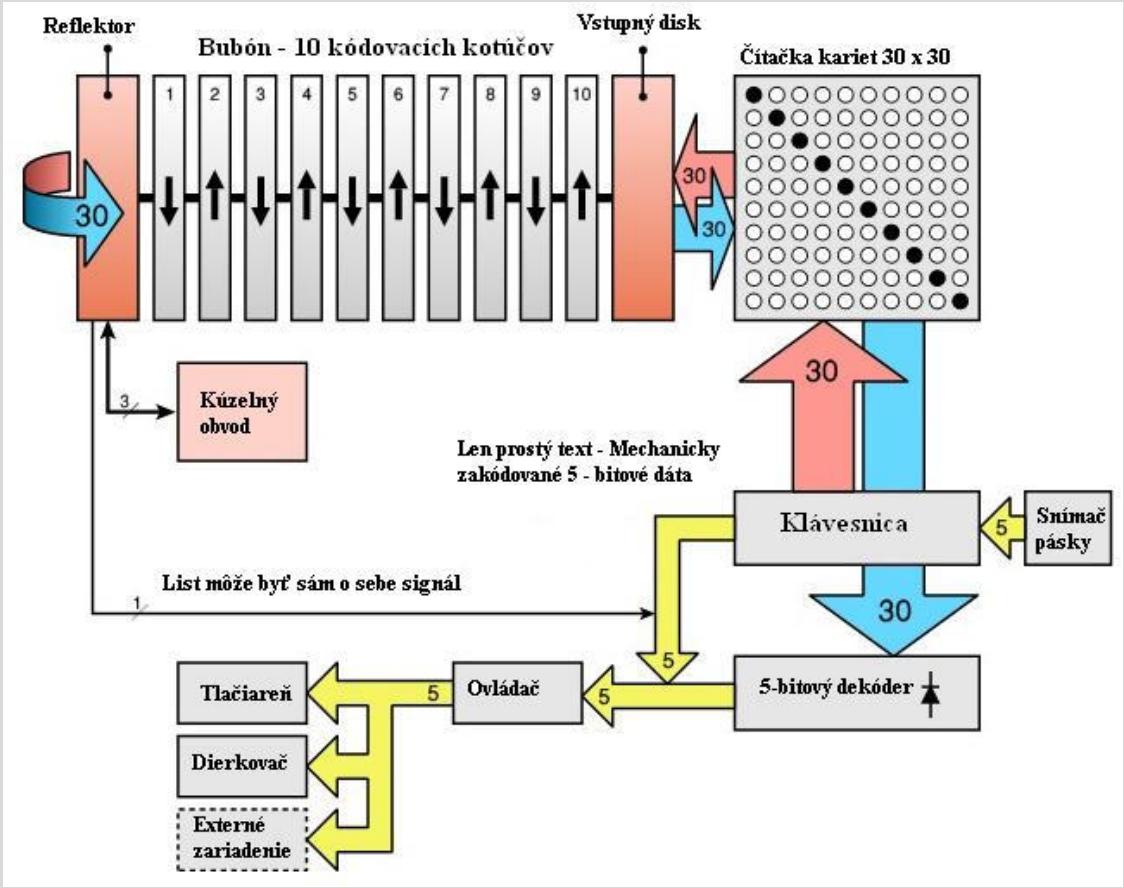
2.4.5.1 Mechanizmus Fialky

Stlačením písmena na klávesnici sa vyšle elektrický prúd do čítačky kariet, ktorá sa chová podobne ako konektor dosky u Enigmy. Z čítačky kariet prechádza signál na vstupný disk odkiaľ putuje ďalej do bubna. Na konci bubna sa signál odráža a prechádza znovu cez vstupný disk, čítačku až do klávesnice, úplne rovnako ako v mechanizme Enigmy. Tam ich diódová matica prevedie na 5 bitovú vzorku.5 bitové dáta sú použité na pohon tlačiarne aj dierkovača.

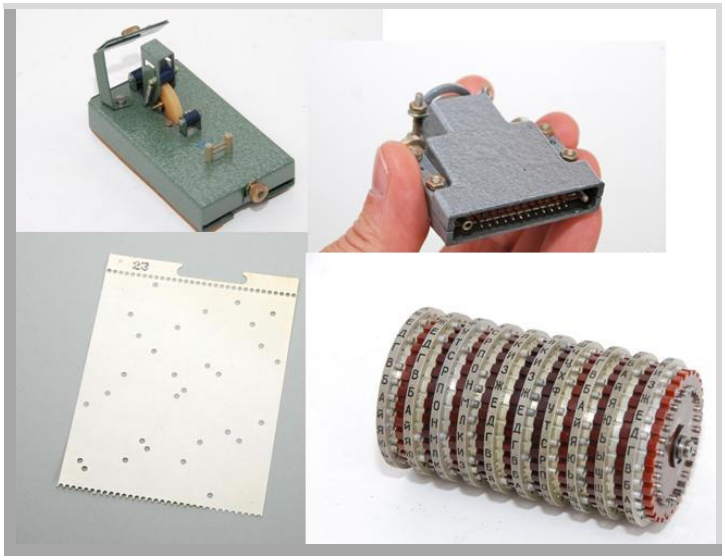
Okrem riadenia jedného z 30 prepínačov obsahuje klávesnica aj mechanický 5 bitový kódovač, produkujúci digitálny kód totožný z predchádzajúcim. Tento kód sa používa, pokiaľ je Fialka nastavená ako štandardný ďalekopis. Vďaka tomu je možné aby bol list zakódovaný sám do seba.

Ďalšie tri drôty od reflektora sú zapracované do kúzelného obvodu, používajúci inteligentný rotačný princíp, ktorý zapríčiní aby Fialka čiastočne strácala vzájomnosti. [21]

Zvyšných 26 kontaktov je prepojených v párach presne ako u Enigmy.



Obrázok 37, Blokové schéma základného mechanizmu Fialky. [21],[vlastný]



Obrázok 38, Zariadenia Fialky: krém pre lepiacu papierovú pásku, testovací zariadenie, karta, kotúč. [21]

Tabuľka 2, Porovnanie šifrovacieho stroja Fialka s Enigmou. [vlastný]

Fialka	Enigma
10 kotúčov	3-4 kotúče
väčšia frekvencia kotúčov	menšia frekvencia kotúčov
priľahlé kolesá sa pohybujú v opačných smeroch	priľahlé kolesá sa pohybujú v rovnakých smeroch
zapojenie kolies je možné zmeniť priamo na poli	
stĺpcové dierne štítky ako náhrada konektoru dosky	konektory dosky
list môže byť zakódovaný do seba	list nemôže byť nikdy zakódovaný do seba

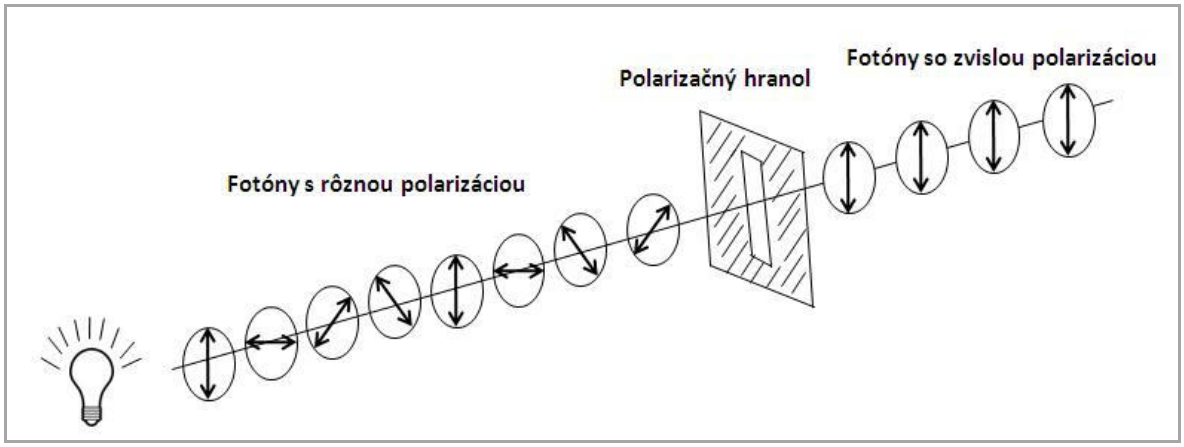
3 VÝVOJ CHEMICKÉHO A FYZIKÁLNEHO TAJNOPISU

3.1 Kvantová kryptografia

Potreba neustáleho hľadania a vytvárania neprelomiteľných šifier priniesla objav v modernej fyzike. Nová forma šifrovania je úplne odlišná od doterajších metód šifrovania. Vojtech Hála píše v článku týždenníka Aldebaran Bulletin, že kvantová kryptografia ponúka nepodmienenú bezpečnosť, to znamená absolútne utajenie zaručené prírodnými zákonmi. Tento článok bol však napísaný v roku 2005, čo bolo niekoľko rokov predtým ako sa ukázalo že aj tento spôsob šifrovania nie je sto percentne spoľahlivý.

3.1.1 Princíp

Celá teória kvantovej kryptografie vychádza z fyziky fotónov. Keď fotón cestuje priestorom, tak vibruje, pričom uhol vibrácie je u každého fotónu iný. Uhol vibrácie predstavuje polarizáciu fotónov. Tu sa nám zobrazuje prvá zaujímavá vlastnosť kvantového sveta, ktorou je náhodnosť. Aby sme si teóriu kvantovej fyziky zjednodušili, predpokladáme, že fotóny majú iba 4 rôzne polarizácie. Postavením polarizačného filtru do cesty fotónom umožníme, aby sa lúč svetla skladal iba z fotónov s rovnakou polarizáciou v závislosti od filtra.



Obrázok 39, Prechádzanie fotónov cez polarizačný filter. [vlastný]

Avšak ak máme uhlopriečne polarizované fotóny a zvislý polarizačný filter, dochádzka k takzvanej kvantovej dileme, pretože v takomto prípade bude náhodne vybraná polovica fotónov zablokovaná, zatiaľ čo druhá náhodne vybraná polovica filtrom prejde a zmení sa

ich polarizácia na zvislú. To isté platí aj naopak. Na tomto je založený celý princíp kvantovej kryptografie. [22]

K prenosu informácií sa teda používajú 4 polarizácie fotónov predstavujúce bitové hodnoty 1 a 0 a dve bázy prenosu. Rovnobežná báza tiež nazývaná plus schéma posiela fotón s polarizáciou zvislou ako zástupcu bitovej hodnoty 1 a s polarizáciou vodorovnou predstavujúcou hodnotu 0. Diagonálna alebo x báza posiela fotóny s polarizáciami šikmými do oboch strán. [22]

Obrázok 40, Reprezentácia bitov pomocou fotónov polarizovaných v 4 rovinách. [vlastný]

Pri prenose informácií to funguje nasledovne. Odosielateľ chce odoslať informáciu prenesenú do bitových hodnôt, pričom má k dispozícii dva filtre - dve bázy (+, x). Ak chce odosielateľ poslať informáciu napríklad v podobe: 1101, môže to urobiť tak, že nastaví filter podľa plusovej schémy, vtedy hodnotu 1 predstavuje zvislá polarizácia fotónu, potom zmení filter podľa x-ovej schémy a druhú jednotku vyšle šikmou polarizáciou fotónu z ľavého horného rohu smerom k pravému dolnému rohu, ako je naznačené v predchádzajúcom obrázku. Potom môžeme napríklad ponechať x – ovú schému a následnú 0 preniesť šikmou polarizáciou fotónu z pravého horného rohu smerom k ľavému dolnému rohu. Následne nastavíme filter do plusovej schémy a poslednú jednotku prenesieme zvislou polarizáciou fotónu. Toto sa dá spraviť rôznymi spôsobmi zmeny filtrov. Pokiaľ by sa narušiteľ snažil zachytiť správu, potrebuje rozpoznať polarizáciu každého fotónu. Ak by chcel zmerať polarizáciu fotónu, musí sa vždy

rozhodnúť ako orientovať polarizačný filter. Vzhľadom k tomu, že narušiteľ nemôže vedieť aké filtre použil odosielateľ, jeho voľba bude náhodná, a v tom prípade mylná. Navyše, keď narušiteľ zachytí vyslaný fotón a zle určí filter spôsobí, že k príjemcovi sa buď fotón nedostane, pretože cez filter neprejde alebo sa zmení jeho polarizácia na základe princípu, ktorý som uviedla vyššie. A toto je signál pre obe strany vymieňajúce si správu, že sú odpočúvané treťou osobou.

V roku 1989 bol prvý krát použitý prístroj využívajúci kvantovú kryptografiu, ktorý bol zostrojený Charlesom Benettom a Johnom Smolinom. Prístroj vtedy preniesol polarizované fotóny medzi dvoma počítačmi vzdialenými 30 cm. Dnes už je to možné v rozpätí stoviek kilometrov. K meraniu polarizácie fotónov sa využívajú kryštály $CaCO_3$ a k prenášaniu fotónov slúžia optické vlákna. [22]

3.1.2 Kvantový protokol výmeny kľúča

Tento skvelý šifrovací systém narazil na problém, až keď bolo potrebné vymyslieť ako dopraviť kľúč, podľa ktorého prijímateľ vedel rozpoznať ktorý filter kedy použiť.

Vtedy Charles Benett a Gillesi Brassard, ktorí kvantovú fyziku aplikovali na kryptografiu vymysleli Kvantový protokol výmeny kľúča, ktorý má označenie BB84.

I. Odosielateľ generuje fotóny, ktoré sú náhodne polarizované, rovnomerne rozložené medzi 4 možné roviny. Odosiela ich kvantovým kanálom príjemcovi. Počet týchto odoslaných fotónov by mal presiahnuť dvojnásobok počtu bitov tajnej správy, ktorá má byť poslaná.

II. Príjemca meria prichádzajúce fotóny, pričom náhodne strieda plusovú a x – ovú bázu. Konkrétne hodnoty polarizácie si však necháva pre seba.

III. Odosielateľ oznámi príjemcovi verejným kanálom poradie báz, v ktorom boli fotóny polarizované, ale konkrétne hodnoty polarizácie si nechá pre seba.

IV. Príjemca si zaznačí všetky hodnoty polarizácií, ktoré meral so správnym filtrom. Tieto bity tvoria šifrovací kľúč.

V. Príjemca odosielateľovi cez verejný kanál oznámi, ktoré fotóny meral správnou schémou. Odosielateľ vie, s akou polarizáciou tieto fotóny posielal, preto pozná všetky bity šifrovacieho kľúča.

VI. V poslednom kroku je potrebné obetovať niekoľko bitov z kľúča na zistenie či linka nebola odpočúvaná. Príjemca s odosielateľom si ich povedia a porovnajú. Pokiaľ sa všetky zhodujú môžeme predpokladať, že prenos nie je odpočúvaný. [23]

Čím viac bitov si odosielateľ s príjemcom vymenia, tým je väčšia šanca odhalenia narušiteľa. Ak porovnáme 32 bitov je šanca 99,99%, že narušiteľa odhalíme.

3.1.3 Spoľahlivosť kvantovej kryptografie

Kvantová kryptografia je systém, ktorý zaručuje bezpečnosť správ tým, že maximálne sťažuje protivníkovi prečítať komunikáciu medzi odosielateľom a príjemcom. Navyše pokiaľ sa narušiteľ snaží odpočúvať komunikáciu, bude odhalený.

Tým prichádzame k prvému problému, ktorý môže nastať a to, že bude narušiteľ neustále linku blokovať. Komunikácia bude musieť byť neustále odkladaná alebo premiestňovaná na inú linku. To je však iba technický problém.

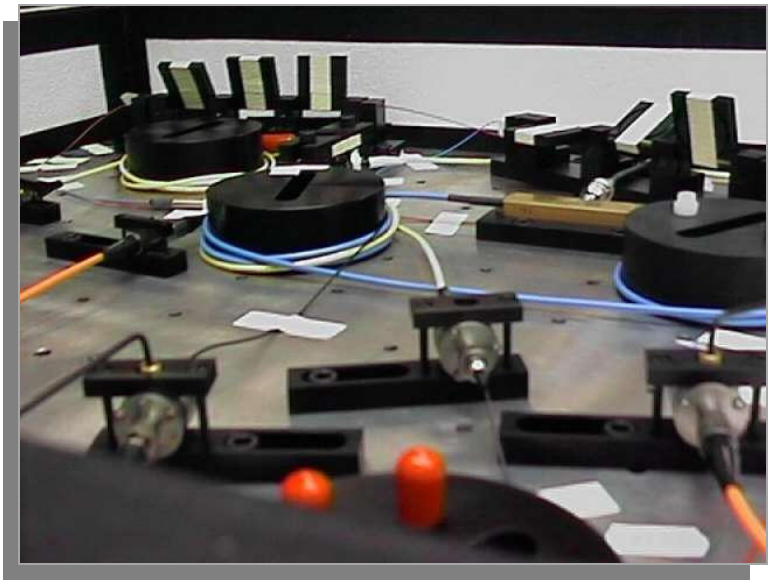
Druhým problémom predstavuje spôsob autentizácie. Pretože protokol nijako nerieši autentizáciu na verejnom kanále. Pri kontrole bitov si odosielateľ a príjemca nemôžu byť istí, že hovoria so správnym človekom.

V súvislosti s kvantovou kryptografiou sa spája aj výraz nepodmienená bezpečnosť. Predstavuje bezpečnosť, ktorá nie je podmienená žiadnymi predpokladmi na schopnosti a technické znalosti útočníka, pretože ani sila kvantových počítačov ani iných systémov nemôže porušiť prírodné zákony o ktoré sa tento princíp opiera.

V princípe neprelomiteľný spôsob šifrovania však skrýva slabé stránky v praktickom využití. Na významný nedostatok upozornili fyzici, ktorým sa podarilo skopírovať tajný kvantový kľúč bez odhalenia ich prítomnosti odosielateľom a príjemcom šifrovanej správy. Christian Kurtsiefer a jeho spolupracovníci v Národnej Univerzite v Singapure a výskumný tím z Univerzity v Trondheim v Nórsku našli cestu ako skryť narušiteľove odpočúvanie využitím slabosti jednofotónových detektorov, ktoré sú využívané vo väčšine komerčne dostupných kvanto – kryptografických prijímačoch. Princíp spočíva vo využití jasného svetla pre oslepenie štyroch fotodiód, ktoré príjemca používa k detekcii fotónov v každej zo štyroch rôznych polarizácii. Fotodiódy potom strácajú schopnosť detekcie jednotlivých fotónov a reagujú iba na intenzitu svetla. Prijímacia strana tak nemôže správne priraďovať polarizéry k jednotlivým meraniam, a pri neskoršom porovnávaní kľúča je znemožnené

odhaliť odpočúvanie narušiteľom. Vedci však dokážu aj tento problém vyriešiť. Jeden z návrhov vyslovil Vadim Makarov, ktorý vidí riešenie v malom jednofotónovom zdroji. Ten sa má uložiť pred prijímací detektor a prepínaním v náhodných intervaloch by sa malo zaručiť registrovanie individuálnych fotónov. Ak detektor opakovane zlyhá bude jasné, že prenos je odpočúvaný.

Kvantová kryptografia predstavuje ohromný skok v kryptografickom svete. Avšak ešte stále sa vyvíja a tým sa objavujú nové prekážky a problémy v dokonalo bezpečnom utajovanom prenose informácii. Jediná cesta k dokonalej realizácii kvantovej kryptografie predstavuje nezávislé testovanie. Na základe toho vykonávajú kvantoví hackeri veľmi užitočnú prácu. [22], [23], [24]



Obrázok 41, Machův-Zehnderův interferometr – vysielacia časť kvantového kryptografického aparátu. [25]

Obrázok 42, Kufrík s kvantovými trikmi. [24]

3.2 Neviditeľný atrament - nanočastice

Moderné technológie neviditeľných atramentov sa v posledných rokoch stále viac približujú bežnému užívateľovi. Dôkazom je aj neviditeľný atrament, ktorý v roku 2009 uviedol internetový denník MIT Technology Review.

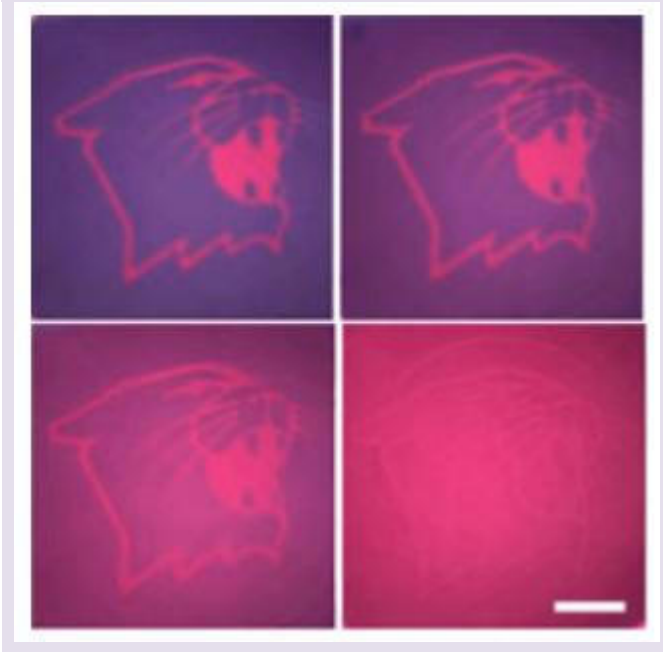
Prísne tajné mapy a správy, ktoré majú byť pre nežiaducu osobu neviditeľné, je možné zostrojiť pomocou nového atramentu z nanočastíc. Princíp spočíva v použití zlata a striebra nanočastice vloženej do tenkého pružného organického gélu, čím sa vytvorí samo-mazateľné médium.

Miznúci atrament využíva vlastností nanočastíc, ktoré majú schopnosť menenia farieb podľa toho ako sú navzájom od seba vzdialené. Pokiaľ sú nanočastice od seba dostatočne vzdialené ich sfarbenie je dočervena. Postupným približovaním sa častice zmenia na modré až sa nakoniec úplne vytratia, zneviditeľnia. Špeciálny molekulárny povlak pomáha zintenzívniť ultrafialové lúče, ktoré zabezpečujú viditeľnosť atramentu. Všetko závisí na intenzite dopadajúceho ultrafialového žiarenia. To pôsobí na nanočastice ako magnet, kedy sa k sebe približujú a vznikajú rôzne sfarbenia. Ak ultrafialové lúče prestanú žiariť na atrament, nanočastice sa vrátia do ich pôvodnej štruktúry a tým sa stanú neviditeľné. Funguje to ako molekulárne lepidlo, ktoré si môžete regulovať pomocou svetla.

Atrament má také vlastnosti, že pôsobením denného svetla alebo tepla zmizne v priebehu niekoľkých sekúnd. Preto sa zlatý atrament dá naprogramovať, aby napísaný text zmizol až

po ubehnutí takej krátkej doby, ktorá je potrebná bežnému čitateľovi na prečítanie správy. Film je možné vymazať a prepísať stokrát bez akejkoľvek zmeny v kvalite.

Správu, ktorá zmizne už nie je možné znovu nikdy prečítať, preto je tento spôsob neviditeľného atramentu veľkým objavom pre tajné a špeciálne služby. Ďalšie možné využitie sa predpokladá v cestovných lístkoch mestskej dopravy, kedy sa po vypršaní času jednoducho nápisy samé vytratia. [26]



Obrázok 43, Použitie atramentu z nanočastíc - po 9 hodinách sa úplne vytratí. [26]

3.3 Neviditeľný atrament - DNA

Kým DNA je známa ako základný stavebný kameň života, tieto veľké molekuly tiež majú potenciálne využitie v oblastiach bezpečnosti vo forme neviditeľného atramentu.

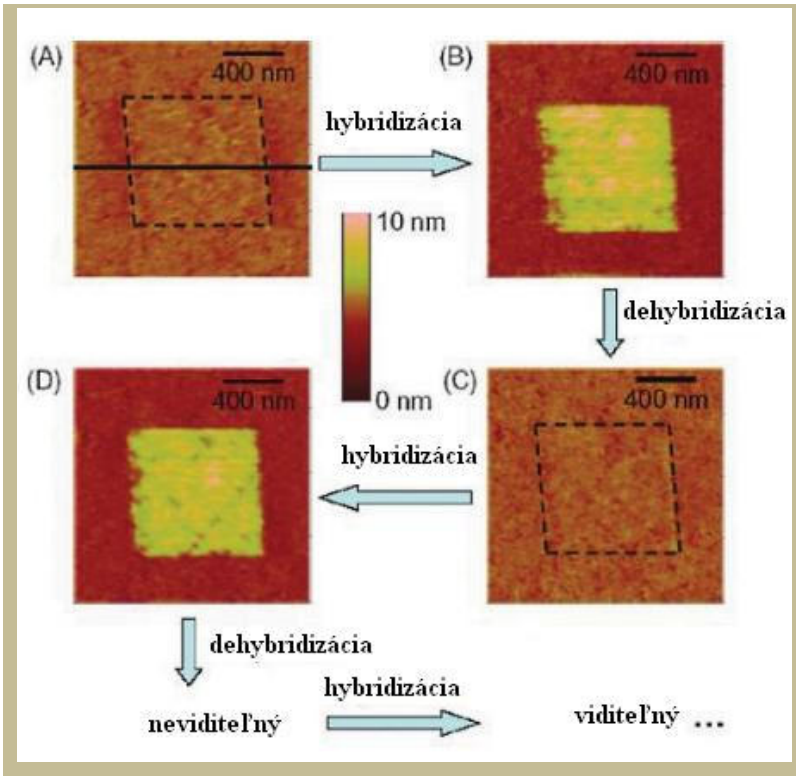
Na písanie s DNA ako s neviditeľným atramentom sa využíva nanolitografická technika zvaná nanografting. Využíva písanie nanoštruktúr pomocou mikroskopu atomárnych síl. Na rozdiel od ostatných nanolitografických techník, v ktorých sú nanoštruktúry písané na ploche, nanografting najskôr odstráni pôvodné molekuly v snímanej oblasti, a potom zapíše nové molekuly na ich mieste. Vedci pomocou tejto techniky najskôr pokryli zlatý povrch monovrstvou jednovláknovej molekuly DNA. Potom vložili rovnaký typ DNA s využitím nanograftingu do pozadia DNA. V tejto časti procesu je vzor DNA neviditeľný, pretože má

rovnakú hrúbku a chemické zloženie ako pozadie. Avšak DNA vložené pomocou tejto metódy sa líšia od normálneho DNA pozadia v tom, že majú tesnejšie baliace poradie. To spôsobuje, že je toto DNA citlivejšie na kríženie (hybridization).

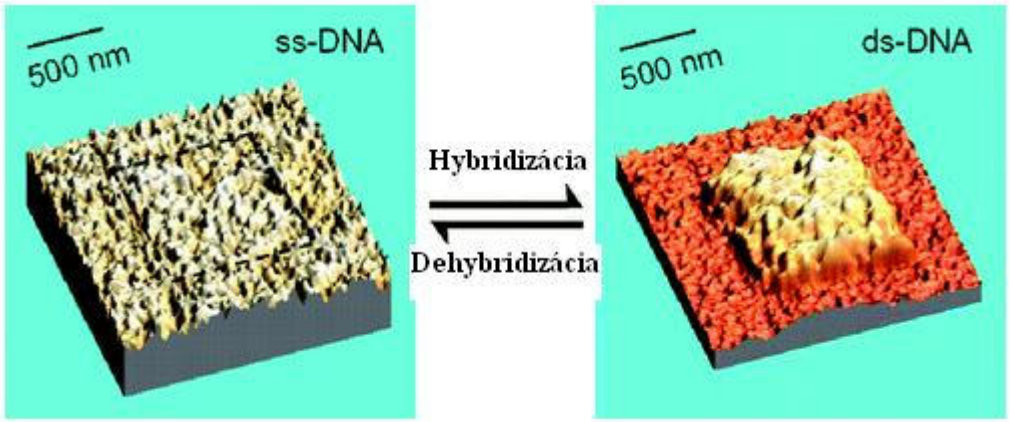
Čiže pôvodná stena DNA a vložené DNA s využitím nanograftingu sú na prvý pohľad rovnaké, avšak vedci zistili, že keď sa vykoná proces hybridizácie, doplnková DNA zvýši hrúbku nanograftingovej DNA omnoho dramatickejšie ako sa udeje na normálnej DNA. Tým sa stane vložená DNA viditeľnou.

Vykonaním dehybridizácie dokážu vedci vrátiť hrúbku do normálnej veľkosti a tým DNA opäť zneviditeľniť. Tento proces je možné zopakovať niekoľkokrát bez menšieho poškodenia viditeľnosti alebo neviditeľnosti.

Táto novinka predstavuje zaujímavý objav, ktorý by mohol byť použitý na manipuláciu biologických molekúl a vytváranie nových šifrovacích technológii. [27]



Obrázok 44, Proces hybridizácie a dehybridizácie v molekule DNA. [27]



Obrázok 45, Molekula DNA po procese zneviditeľnenia. [27]

3.4 Digitálna steganografia

Digitálna steganografia vychádza z klasickej steganografie s tým rozdielom, že je v nej umožnené skrývať všetko, čo je možné napísať v bitovej podobe (bitsream). Najčastejšie sa využíva ukrývanie súboru do obrázku, hudby alebo videa. [28]

3.4.1 Obrázková steganografia

Skrývanie dát do obrázkov je založené na nedokonalosti ľudského zraku. Do krycieho obrázku je možné ukryť akékoľvek dáta, ktoré sa dajú vložiť do bitového prúdu. Bežnému užívateľovi je dostupná celá rada programov pracujúcich na rôznych technikách ukrývania informácií:

- LSB (Least significant bit insertion),
- Maskovanie a filtrovanie,
- Algoritmy a transformácie.

Žiadna z týchto techník však nezaistí úplnú odolnosť vloženej správy voči manipulácií s obrázkom. [5]

LSB

Vzhľadom k tomu, že súbor vo formáte JPEG je kompaktný a nezhoršuje sa významne kvalita obrazu, je často používaný na internete. Tento formát používa diskrétnu kosínusovú transformáciu na identifikovanie 64 DCT koeficientov v blokoch 8x8 pixlov. Z týchto koeficientov sa najmenej významné bity používajú na vkladanie dát. Preto názov „Least

significant bit insertion", čo v preklade znamená vkladanie do najmenej významného bitu. [29]

Táto metóda využíva toho, že ľudské oko nie je schopné rozoznať nebadateľné zmeny v odtieňoch farby.

Princíp funguje tak, že pokiaľ máme obrázok s farebnou hĺbkou 24 bitov a chceme do neho ukryť písmeno „A", tak potrebujeme 8 najmenej významných bitov z obrázka, kam písmeno zapíšeme. Písmeno má v binárnej hodnote tvar: 10000011. Každý pixel sa skladá z 8 bitov červenej farby, 8 bitov zelenej farby a z 8 bitov modrej farby. Pokiaľ zoberieme posledný bit z každej farby budeme na zapísanie písmena do obrázku potrebovať 3 pixle. [5]

Tabuľka 3, Zmena bitov obrázka pri vložení písmena „A", [5]

Pixel	Červená	Zelená	Modrá	Obrázok
1.	10101010	10101010	10101010	Originálny
	1010101**1**	1010101**0**	1010101**0**	Stego
2.	11000011	01010100	10100010	Originálny
	1100001**0**	101010**0**	1010001**0**	Stego
3.	00000000	00000000	11111111	Originálny
	0000000**1**	0000000**1**	11111111	Stego

Zakódovanie správy pomocou LSB nie je veľmi bezpečné, preto sa odporúča pred vložením správy tajnú informáciu zašifrovať alebo správu rozložiť po obrázku pomocou generátora pseudonáhodných čísiel. Takto vložená správa bude vypadať ako náhodný šum a nebude vzbudzovať u narušiteľa pozornosť.

Moderné steganografické software využívajú rôzne techniky ukrývania informácií do obrázkov:

- Priama sekvencia,
- Frekvenčné skoky,
- Zošívanie.

Prvé dve metódy využívajú už spomínaný šum. A to buď pomocou fázovej modulácie dátového signálu sekvenciou pseudonáhodných čísiel u Priamej sekvencii, alebo rozdelením šírky frekvenčného pásma na niekoľko kanálov a preskokmi medzi nimi, ako sa deje v metóde Frekvenčných skokov.

Metóda Patchwork opakovane rozširuje po obrázku danú informáciu. Tento spôsob je dostatočne odolný proti poškodeniu obrázka a je ho ľahké dekódovať. Ideálne použitie tejto metódy je formou vodoznakov. [5]

3.4.2 Audio steganografia

Informácie je možné skryť aj do audio formátu. Existujú k tomu viaceré spôsoby.

Kódovanie na úrovni najnevýznamnejšieho bitu je metóda, ktorá pre ukrytie, podobne ako u obrázkovej steganografii, využíva najmenej významný bit. Kapacita pre ukrytie správy je asi 44 bps, pričom sa produkuje veľa šumu, čo je aj dôvodom slabej imunity voči skresleniu. Šum kanálu môže spôsobiť zničenie skrytej informácie.

Kódovanie fáze, tu dochádza k substitúcii fáze prvotného audiosegmentu s referenčnou fázou, ktorá reprezentuje dáta. Veľkou výhodou je, že pri tejto metóde nedochádza k vzniku audiošumu.

Rozšírenie v rámci spektra, na rozdiel od väčšiny komunikačných kanálov, pri tomto spôsobe sa zakódované dáta rozostierajú cez čo najväčšie frekvenčné spektrum.

Ukrytie dát do ozveny je metóda, kedy sú dáta vložené do audioformátu cez ozvenu. [5]

3.4.3 Digitálne vodoznaky

Existujú dve formy digitálnych vodoznakov: viditeľné a neviditeľné.

Viditeľné vodoznaky jednoducho vyznačujú autorské práva na pôvodnom obraze. Umožňuje použitie média ale zároveň ukazuje komu súbor patrí, alebo kde je možné získať o médiu viac informácií.

Neviditeľný vodoznak je prejavom steganografie slúžiacej na vloženie informácií o autorských právach do originálneho súboru, bez zmeny jeho vizuálnej reprezentácie. Vtedy rozoznávame neviditeľný vodoznak robustný, ktorý slúži k detekovaniu zneužitia média. Je navrhnutý aby odolával manipulácii médiom a to tak, že sa vykonáva zmena

formátu bitov pre vytvorenie rovnomerne rozloženého vzoru obrazových bodov, ľudským okom nerozoznateľné.

Neviditeľný krehký vodoznak sa nachádza napríklad na fotografických snímkach, ktorého úlohou je overenie autentickosti snímku. Vtedy sa vkladajú textové informácie do obrazu. Aj keď sa neviditeľný vodoznak nedá vizuálne identifikovať, objavuje sa tu vedomie existencie, ktoré je dostačujúce na odradenie potenciálnych narušiteľov autorských práv. [28], [29]

Samozrejme aj tento spôsob steganografie je možné obísť. Snímky obsahujúce digitálne vodoznaky sa môžu „očistiť“ jednoduchou konverziou súboru do iného formátu a späť do pôvodného formátu. Jedným z verejne dostupných nástrojov je program s názvom StirMark. [29]

3.4.4 Steganografia namiesto šifrovania

Jednou z možností ako využiť steganografiu na ukrytie digitálnych dát predstavuje spôsob, s ktorým prišiel Hassan Khan. Týmto spôsobom sa snaží vyhnúť šifrovaniu správy, pretože najbezpečnejšie ukryté informácie sú také, o ktorých sa nevie že vôbec existujú. Preto vynašiel metódu ukrytia dát na pevnom disku. Namiesto šifrovania sa kúsky citlivých dát rozhadzujú medzi fragmenty súborov na pevnom disku. Umožňuje zakódovať 20 megabajtov správy na 160 GB pevnom disku. Metóda využíva ako pevné disky dátové úložiská súborov v zoskupeniach s veľkým množstvom malých kúskov. Operačný systém ukladá tieto zhluky všade tam, kde je voľný priestor medzi fragmentami z iných súborov.

Software využíva kód, ktorý je závislý na tom, či sa sekvenčné zhluky nachádzajú na pevnom disku vedľa seba, čo zodpovedá binárnej 1, alebo na rôznych miestach, binárna 0. Tak ako sú poskladané fragmenty normálnych dát na disku, sa kódujú dáta tajné.

Technika funguje pokiaľ žiadny zo súbor na pevnom disku nie je upravený pred odovzdaním.

Na dekódovanie musí príjemca použiť rovnaký software. A tu sa stretávame s druhým nedostatkom, pretože si musia príjemca s odosielateľom navzájom predať špecializovaný software a samotný disk obsahujúci tajné informácie. [30]

Obrázok 46, Driver určený k ukrytiu dát. [30]

4 FORMY A METÓDY SPOJENIA PRE BUDÚCNOSŤ

4.1 Skryté kanály (Covert Channels)

V diele „Research Report: Covert Channels“ je pojem skrytý kanál vystihnutý veľmi jasne: „Skrytý kanál je komunikačný kanál, ktorý umožňuje proces k prenosu informácií takým spôsobom, ktorý porušuje systém jej bezpečnostnej politiky. [31]

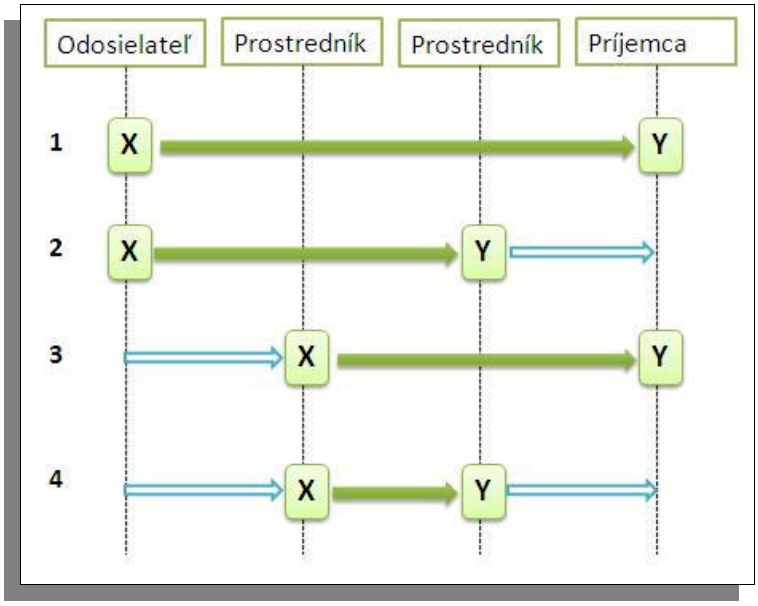
Skryté kanály predstavujú komunikačné cesty, ktoré sa používajú na prenos tajnej správy. Ich cieľom je utajiť samotnú existenciu komunikácie a preniesť správu spôsobom, ktorý na to nie je primárne určený.

Obrovské množstvo dát a veľké množstvo rôznych protokolov na internete predstavuje ideálnu príležitosť pre skrytú komunikáciu. Tak ako pri použití steganografie aj skryté kanály potrebujú nosiče, v ktorých sa ukrývajú prenášané dáta. V počítačových sieťach sa nachádzajú kanály, akými sú sieťové protokoly, využívané ako nosiče skrytých kanálov. Fakt, že skrytý kanál využíva také komunikačné cesty, ktoré na to ani zďaleka nie sú určené prispieva k tomu, aby odhalenie komunikácie bolo veľmi náročné a niekedy až takmer nemožné. [32], [33]

Ja opisujem skryté kanály ako spôsob prenosu tajných informácií špeciálnych alebo spravodajských služieb, existuje však mnoho aplikácií skrytých kanálov, ktoré sú škodlivej alebo nežiaducej povahy, a preto predstavujú reálnu hrozbu pre bezpečnosť siete.

Základné delenie skrytých kanálov podľa kódovania rozdeľuje tento spôsob tajnej komunikácie na:

- Skladovacie kanály zahŕňajú priame alebo nepriame písanie hodnôt objektu odosielateľom a priame alebo nepriame čítanie hodnôt objektu príjemcom,
- Časové kanály zahŕňajú signalizáciu odosielateľovej informácie tým, že moduluje využívania zdrojov v priebehu času tak, aby ju príjemca mohol spozorovať a dekódovať. [33]



Obrázok 47, Schéma komunikácie v skrytom kanály. [33]

Obrázok ukazuje 4 rôzne spôsoby komunikácie prostredníctvom skrytého kanála, v závislosti na tom, aké postavenie v prenose informácii majú účastníci. Tí môžu vystupovať ako prijímateľ a odosielateľ, alebo ako prostredníci, ktorí prenášané informácie menia. [33]

V prvom prípade môže odosielateľ ľubovoľne manipulovať s kanálom, napríklad maximalizovať kapacitu koryta, má nad ním plnú kontrolu.

V druhom prípade príjemca zaujal pozíciu prostredníka. Týmto spôsobom sa môže zvýšiť utajenie komunikácie v skrytom kanále, pretože príjemca figuruje ako bežný prijímateľ zjavného kanálu.

Odosielateľ tiež môže zvoliť pozíciu prostredníka. Môže tak jednať v prípade, že nemôže skrytý kanál vytvoriť alebo nechce figurovať ako aktívny odosielateľ dát kvôli väčšiemu riziku odhalenia.

Najobťažnejšie ale tiež asi aj najnerizikovejšie je pre odosielateľa a prijímateľa, ak majú súčasne obaja postavenie prostredníka. V tomto prípade musí príjemca v postavení prostredníka nájsť vhodný uzol v ceste toku dát, kde sa pripojí. Po získaní potrebných skrytých dát by mal odstrániť z nosiča všetky tieto informácia, aby u skutočného príjemcu nevzbudil podozrenie. [32], [33]

Podľa správania sa rozdeľujú kanály v závislosti na tom ako je nosný protokol využívaný pre posielania dát, na:

- Aktívny kanál si generuje vlastnú dopravu. Tento typ je jednoduchší, pretože prenos dát nie je závislý na sieťovej prevádzke, avšak je tu riziko ľahšieho odhalenia odosielateľa.
- Pasívny kanál závisí na doprave vygenerovanej inými procesmi. Prenos závisí na výskyte vhodných nosičov, ale je oveľa bezpečnejší. [31], [32]

Podľa cesty, ktorá leží medzi odosielateľom a prijímateľom, na:

- Priama cesta umožňuje odosielateľovi komunikovať priamo s príjemcom,
- Nepriama cesta sa deje pomocou prostredných uzlov, čím zaisťuje väčšie utajenie komunikácie,
- Rozšírená cesta využíva rozdelenie dát na viacej častí, pričom ich následne posiela rôznymi cestami k príjemcovi. Tento spôsob je najbezpečnejší. [31]

4.1.1 Techniky ukrývania dát

Techník na ukrývanie prenosu dát pomocou skrytých kanálov je veľké množstvo. Ja sa pokúsim poskytnúť iba stručný prehľad aspoň tých základných, pretože to nie je hlavná oblasť zamerania mojej práce.

- Nevyužité hlavičky paketov,
- Rozšírenie hlavičky a výplň,
- IP identifikácia a zarovnanie,
- Pole adresy,
- Pole dĺžky paketu,
- Kontrolné súčty,
- Časovanie a frekvencia paketov,
- Tunelovanie,
- Triedenie a strata paketov,

- Pole identifikácie v IPv4,
- http protokol,
- Počiatočné číslo sekvencie v TCP protokole,
- DNS. [33]

4.1.2 Iný druh skrytého kanálu

V [2] píše autorka o type skrytého kanálu, ktorý predstavuje elektromagnetické žiarenie vydávané počítačom. Na ochranu proti takémuto neoprávnenému zachytávaniu žiarenia sa v dnešnej dobe v špeciálnych službách používajú chránené počítače alebo špeciálne vybavené komory, ktoré takéto žiarenia neprepúšťajú.

Toto žiarenie má schopnosť vyzradiť tajné informácie, nachádzajúce sa v počítači. Upravený televízny prijímač by mal byť schopný preniesť videosignál z monitorov a LCD displejov až na vzdialenosť stoviek metrov. Na základe toho je možné vytvoriť vírus, ktorý bude naprogramovaný tak, aby prehľadal harddisk počítača a skrytým kanálom tajne vyslal citlivé informácie. Podľa autorky by tento spôsob mohol byť aplikovaný na ochranu autorských práv, kedy by software pri práci tajne vysielal svoje licenčné číslo a detekčné vozy by signály prijímali a porovnávali zhodu v týchto číslach, čím by zistili či nie je software používaný viacerými počítačmi. [2]

II. PRAKTICKÁ ČASŤ

5 STEGANOGRAFICKÝ PROGRAM

Pre ukrytie tajných informácií do digitálnych dát existuje nespočetné množstvo verejne dostupných programov, ktoré ponúkajú široký výber rôznych spôsobov ukrývania dát, so zameraním skrývania do obrázkov, zvukových súborov, či videí.

5.1 Zničenie súboru

Zničiť takýmto spôsobom upravené súbory, v podobe obrázka, je možné veľmi jednoducho. Ak máme obrázok, v ktorom je tajná správa uložená pomocou metódy LSB, je jej zničenie možné ak jednoducho vynulujeme najmenej významné bity. Inak všeobecne sa dá obrázok s tajnou informáciou zničiť prevodom do formátu so stratovou kompresiou. Alebo jednoducho stačí obrázok orezať alebo iným spôsobom upraviť. Preto je dôležité aby obrázok skrývajúci tajný súbor, nebol nijakým spôsobom nápadný. Pokiaľ narušiteľ nemá podozrenie, že obrázok niečo skrýva, nebude s ním pracovať.

V prípade ukrývania veľmi veľkého súboru, dochádza k obrovskému nárastu veľkosti obrázka, čo môže mať za následok upútanie pozornosti narušiteľa. Preto je vhodnejšie ukrývať len malé súbory, alebo ich rozložiť do viacerých obrázkov.

5.2 S-tools 4

S- tools je steganografický nástroj, ktorý je možné inštalovať na operačný systém Windows. Je schopný ukrývať do obrázkov formátu BMP, GIF a WAV. Tento program využíva metódu LSB, čiže využíva najmenej významné bity na ukladanie tajných súborov.

Je schopný ukryť rôzne typy súboru, ako doc., pdf., BMP, GIF a iné. S-tools sa snaží znížením počtom farieb obrázka ukryť informáciu tak, aby zaistil zachovanie čo najväčšieho počtu detailov obrazu.

Program využíva heslo zadané osobou, ktorá súbor ukrýva. Na základe tohto hesla a pseudo-generátora náhodných čísiel vyberie pozíciu v obrázku, kde tajné informácie ukryje.

Program S-tools 4 ponúka možnosť nastavenia si základných vlastností skrytia súboru do obrázka, či zvuku.

5.2.1 Testovanie programu

Program je voľne stiahnuteľný z internetu. Nie je potrebné ho inštalovať a ani nezaberie veľa miesta. Obsluha v ňom je pritom veľmi jednoduchá. V 5 jednoduchých krokoch je každý užívateľ schopný ukryť akýkoľvek súbor do obrázku vo formáte BMP, GIF a WAV.

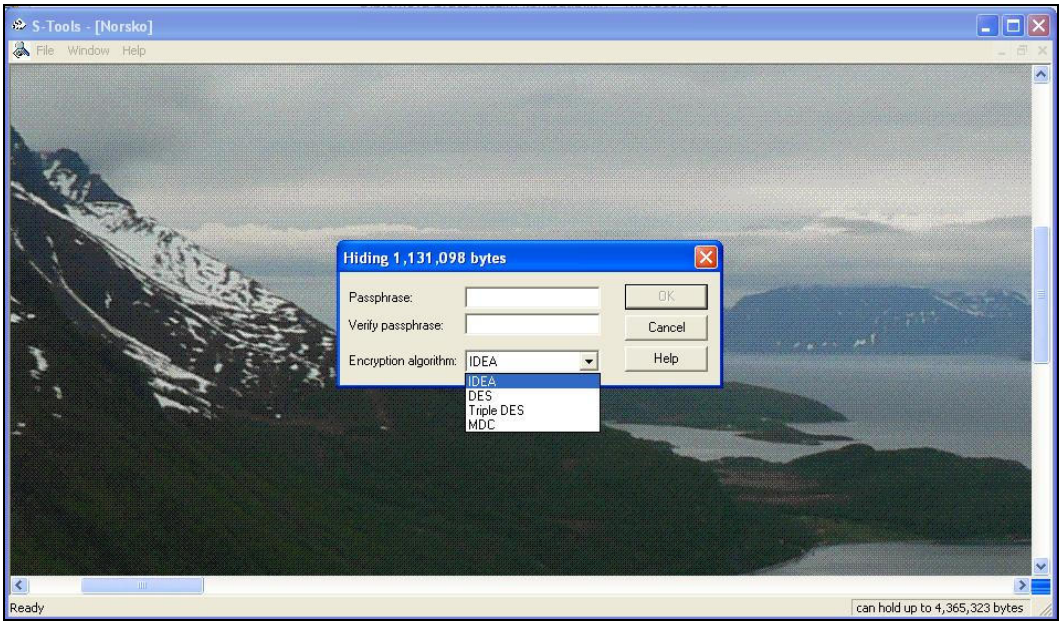
Po spustení programu, sa objaví nasledujúce okno (Obr.48)

Obrázok 48, Úvodné okno v programe S-tools4. [vlastný]

Obrázok vo vhodnom formáte sa do programu vloží jednoduchým premiestnením z užívateľského rozhrania na plochu okna Actions.

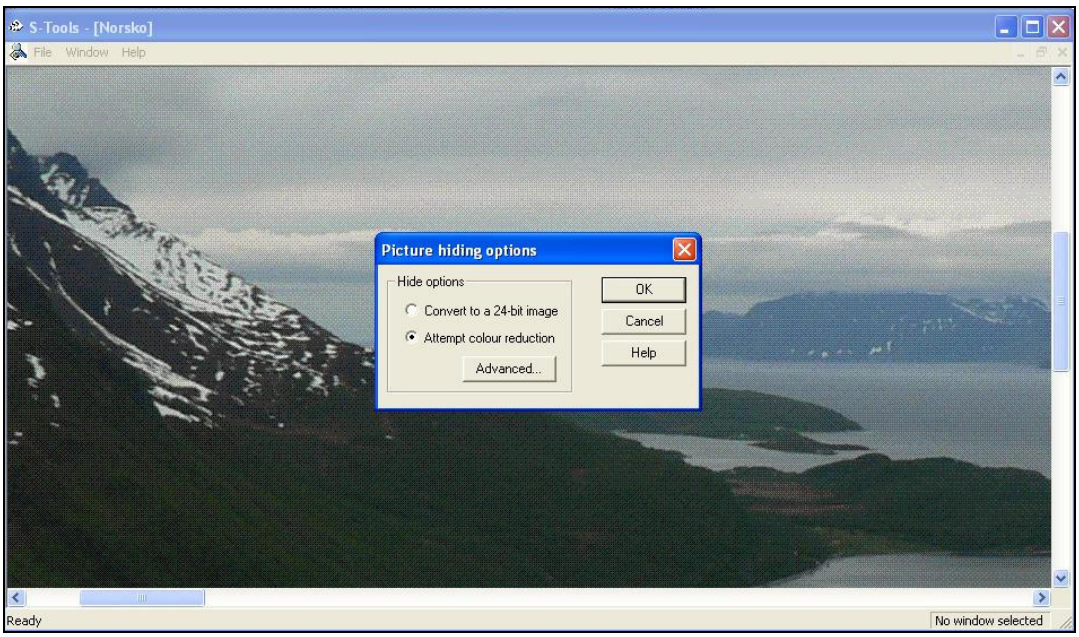
Ďalším premiestnením súboru z užívateľského rozhrania na plochu obrázka, sa súbor vo vhodnom formáte skryje. Kapacita veľkosti skrývaného súboru závisí na veľkosti obrázka. Čím väčší obrázok do programu vložíme, tým nám poskytuje väčší priestor pre skrývaný objekt.

Následne sa objaví okno na zadanie a overenie hesla, a výber šifrovacieho algoritmu. Program umožňuje výber zo 4 šifrovacích algoritmov.



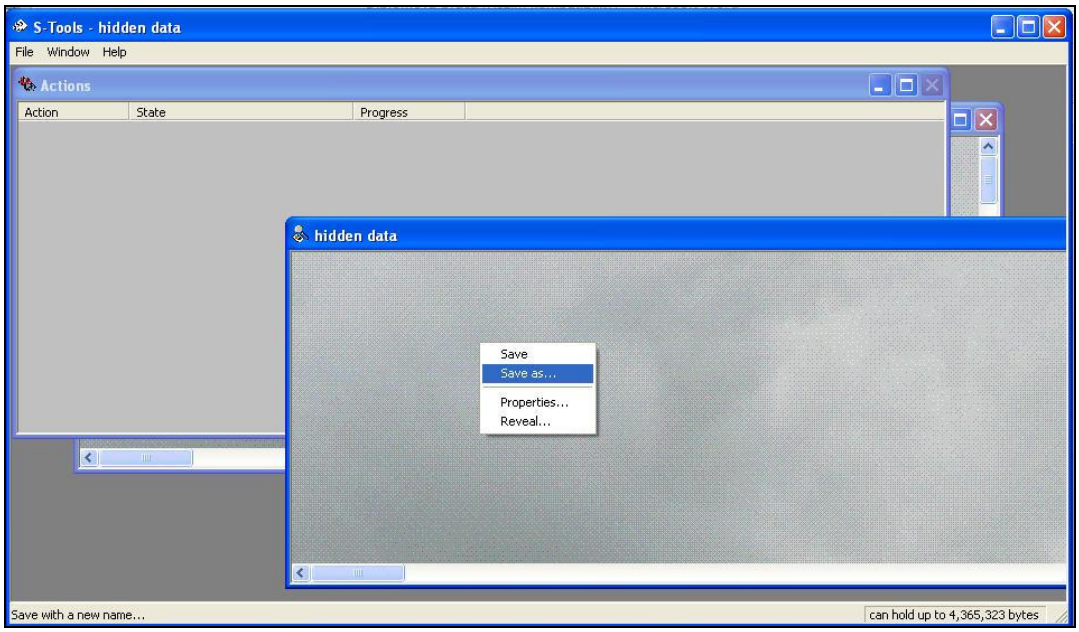
Obrázok 49, Zadanie hesla a výber šifry. [vlastný]

Program umožňuje výber medzi ukrytím do 24 bitového obrázka alebo obrázka s redukciou farieb. Toto nastavenie umožňuje znížiť jeho veľkosť. V prípade redukcie farieb si užívateľ môže vybrať, akým spôsobom bude redukcia farieb prebiehať.

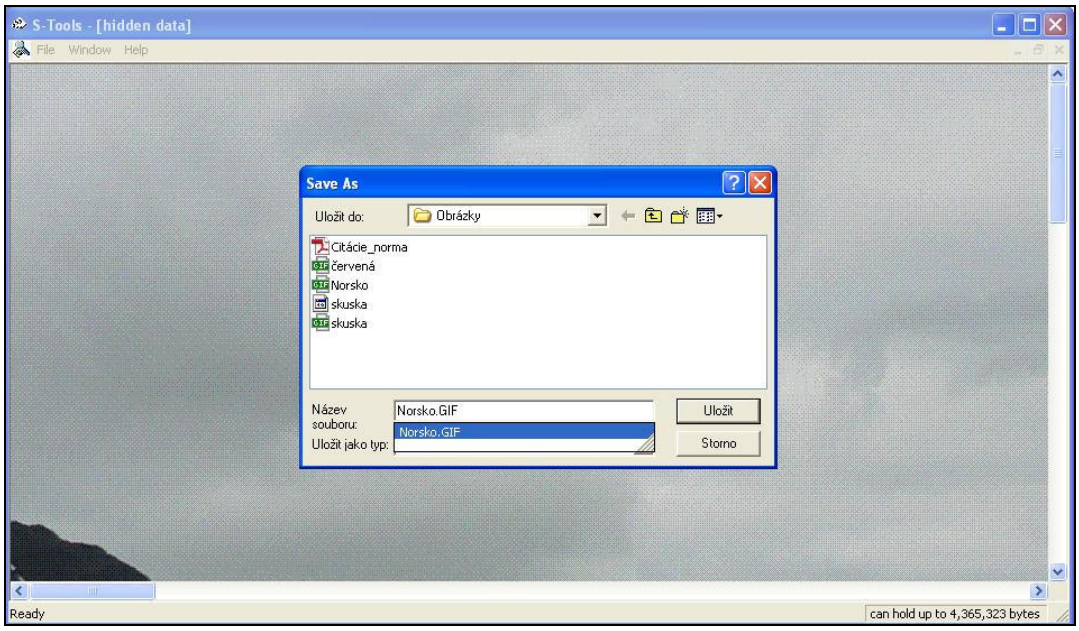


Obrázok 50, Výber redukcie farieb. [vlastný]

Ukrytie súboru trvá niekoľko sekúnd v závislosti na veľkosti skrývaného dokumentu. Potom už len stačí pomocou pravého tlačidla myši uložiť súbor s príslušnou koncovkou, ktorú program podporuje.

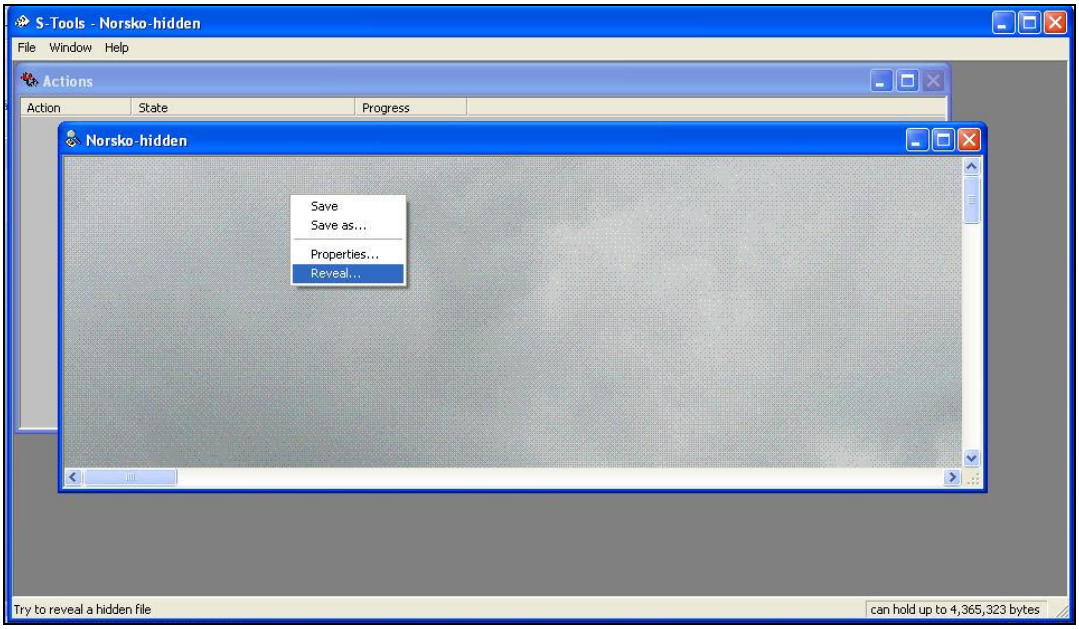


Obrázok 51, Uloženie. [vlastný]



Obrázok 52, Uloženie 2. [vlastný]

Príjemca utajovanej komunikácie si otvorí obrázok so skrytým súborom v programe S-tools4. Kliknutím pravým tlačidlom myši sa objaví nástroj Reveal, ktorý umožňuje odobrať skrývaný súbor z obrázka. Príjemca musí poznať heslo súboru a typ šifrovania. Pri ukladaní dokumentu musí byť súbor uložený s príslušnou koncovkou typu súboru. Inak bude dokument nečitateľný.



Obrázok 53, Výber skrývaného dokumentu. [vlastný]

Tento steganografický program je veľmi jednoduchý nástroj pre skrývanie do obrázka alebo zvukového súboru. Výsledný obrázok je k nerozoznaniu od pôvodného. Jedinou indíciou k odhaleniu obrázka, ktorý v sebe skrýva súbor je jeho veľkosť. Tieto obrázky majú omnoho väčšiu veľkosť v závislosti na veľkosti skrývaného súboru, preto je vhodnejšie ukrývať dokumenty s menším objemom.

Obrázok 54, Porovnanie originálnej fotografie s fotografiou, v ktorej je ukrytý súbor. [vlastný]

Tabuľka 4, Porovnanie typu súboru a spôsob šifrovania. [vlastný]

Test	*Obrázok*	*Šifrovanie*	*Typ*	*Šírka [pixel]*	*Výška [pixel]*	*Veľkosť [B]*
1.	**Originálny obrázok**	-	**GIF**	**7363**	**1581**	**2 054 964**
	Skrývaný súbor	-	**PDF**	**-**	**-**	**1 189 299**
	Obrázok so skrytým súborom	IDEA	GIF	7363	1581	***6180291***
			BMP	7363	1581	**11643562**
		DES	GIF	7363	1581	***6183671***
			BMP	7363	1581	**11643562**
		TRIPLE DES	GIF	7363	1581	***6182881***
			BMP	7363	1581	**11643562**
		MDC	GIF	7363	1581	***6182691***
			BMP	7363	1581	**11643562**
2.	**Originálny obrázok**	-	**BMP**	**2304**	**1728**	**11943990**
	Skrývaný súbor	-	**docx**	**-**	**-**	**14 065**
	Obrázok so skrytým súborom	IDEA	GIF	nejde	nejde	***nejde***
			BMP	2304	1728	**11943990**
		DES	GIF	nejde	nejde	***nejde***
			BMP	2304	1728	**11943990**
		TRIPLE DES	GIF	nejde	nejde	***nejde***
			BMP	2304	1728	**11943990**
		MDC	GIF	nejde	nejde	***nejde***
			BMP	2304	1728	**11943990**

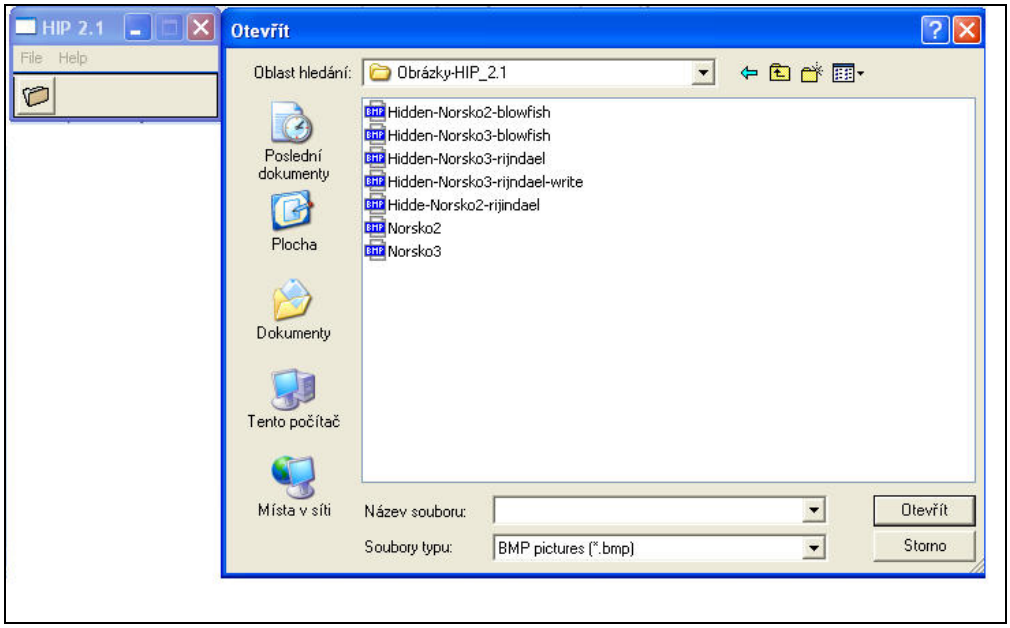
Po otestovaní programu s rôznymi typmi súboru som zistila, že pokiaľ je obrázok, do ktorého chceme skrývať súbor, typu BMP, jeho veľkosť sa po vložení dokumentu nemení. Nevýhodou však je príliš veľká veľkosť obrázka, čo môže vzbudzovať podozrenie u narušiteľa. U tohto typu obrázka po vložení súboru nie je možné zmeniť jeho formát na GIF. Naopak pri type súboru formátu GIF je veľkosť obrázka so súborom podstatne menšia ale líši sa od veľkosti pôvodného obrázka v závislosti na použitom šifrovaní. Pôvodný obrázok typu GIF je možné po ukrytí súboru uložiť ako formát BMP.

5.3 HIP 2.1

Hide In Picture je program určený na maskovanie súborov. Mal by podporovať formáty GIF a BMP, ale mne sa podarilo v tomto programe pracovať iba s formátom BMP. Steganografický program umožňuje skryť ľubovoľný súbor do obrázku, je verejne dostupný a pracovanie s ním je veľmi jednoduché a prehľadné.

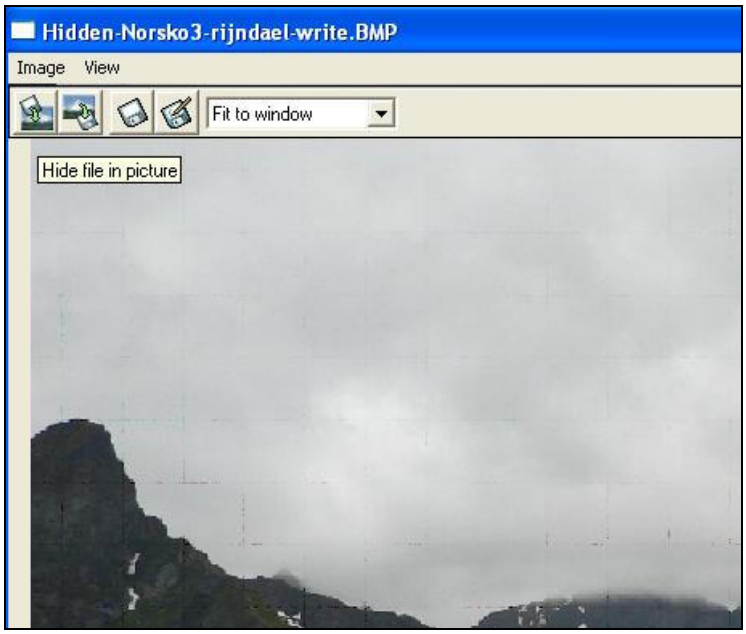
5.3.1 Testovanie súboru

Po otvorení programu je, ako v predchádzajúcom programe, doň potrebné vložiť obrázok, do ktorého budeme skrývať súbor. Tento program podporuje iba obrázky formátu BMP.



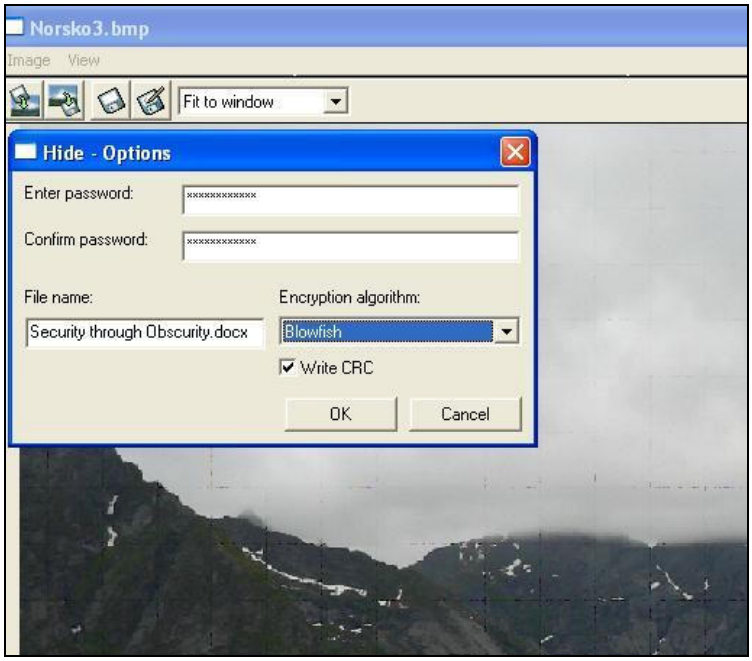
Obrázok 55, Vloženie obrázka. [vlastný]

Kliknutím na okno s nápisom „Hide file in picture“ vyberieme skrývaný súbor.



Obrázok 56, Výber skrývaného súboru. [vlastný]

Program HIP 2.1 nám po zadaní kryptovacieho hesla umožňuje výber medzi dvoma šifrovacími algoritmami, Blowfish a Rijndael.



Obrázok 57, Výber skrývaného súboru 2. [vlastný]

Príjemca získa ukrývaný súbor kliknutím na tlačidlo „Retrieve file from Picture“ a zadaním správneho hesla. V tomto programe nemusí príjemca vedieť použitý typ šifrovacieho algoritmu.

Tabuľka 5, Porovnanie typu súboru a spôsob šifrovania. [vlastný]

Test	*Obrázok*	*Šifrovanie*	*Typ*	*Šírka [pixel]*	*Výška [pixel]*	*Veľkosť [B]*
1.	**Originálny obrázok**	**-**	**BMP**	**2304**	**1728**	**11 943 990**
	Skrývaný súbor	**-**	**PDF**	**-**	**-**	**1 189 299**
	Obrázok so skrytým súborom	Blowfish	BMP	2304	1728	**11943990**
		Rijndael	BMP	2304	1728	**11943990**
2.	**Originálny obrázok**	**-**	**BMP**	**1087**	**714**	**2330550**
	Skrývaný súbor	**-**	**docx**	**-**	**-**	**14 065**
	Obrázok so skrytým súborom	Blowfish	BMP	1087	714	**2330550**
		Rijndael	BMP	1087	714	**2330550**

Keďže program Hide In Picture podporuje iba súbory typu BMP, ich veľkosť a vlastnosti sa po vložení súboru nijakým spôsobom nezmenili.

Pri porovnaní pôvodného obrázka s obrázkom skrývajúcim tajný súbor nie je vidieť známky žiadnej zmeny.

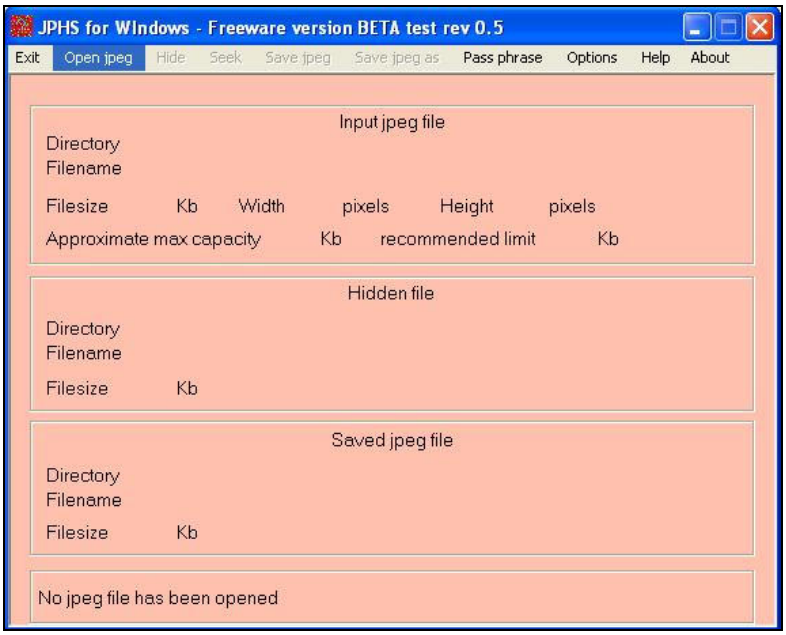
Obrázok 58, Porovnanie originálnej fotografie s fotografiou, v ktorej je ukrytý súbor. [vlastný]

5.4 JP Hide and Seek

JPHS jednoduchý steganografický program, ktorý dokáže ukryť rôzne súbory, dokumenty, videá alebo zvukové nahrávky primeranej veľkosti do obrázku formátu JPEG. Obrázok formátu JPEG dokáže v sebe ukryť súbory o veľkosti asi 10% z jeho celkového objemu dát. Program funguje na šifrovacom algoritme Blowfish ako základ generátora pseudonáhodných čísiel. To, do akej časti obrázka sa bude skrývaný súbor ukladať, závisí na hesle, ktoré si zvolíme pre ukrytie dát. Skrytý súbor je ovplyvnený náhodným šumom, ktorý sa pridáva k vizuálnej stránke.

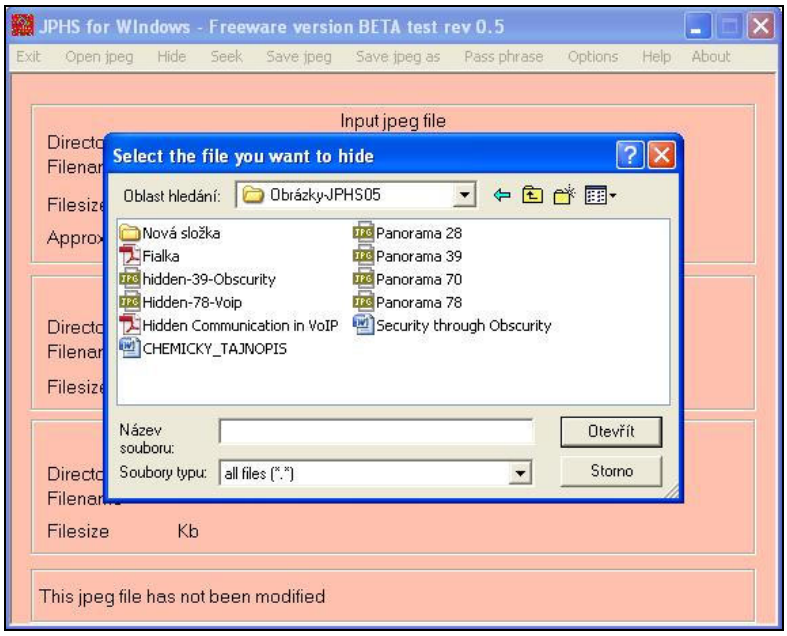
5.4.1 Testovanie

Úvodné okno programu JPHS05 obsahuje základné informácie o vkladanom obrázku, skrývanom súbore a výslednom obrázku obsahujúcom skrytý súbor. V kolónke vyhradenej pre základný obrázok sa nachádza presné vymedzenie veľkosti skrývaného súboru, ktorú nesmie prekročiť. Pre vloženie základného obrázka, ktorý musí byť vo formáte JPEG, stačí kliknúť na položku Open jpeg a súbor vybrať.



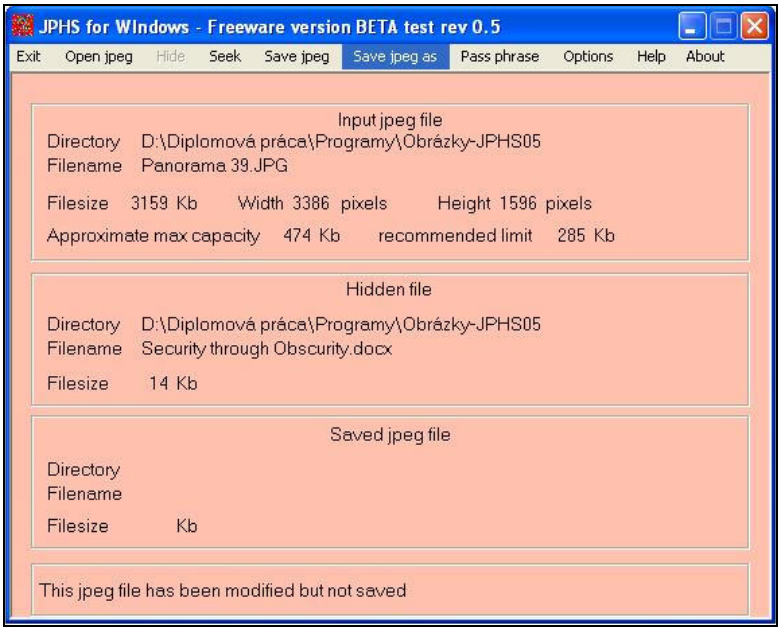
Obrázok 59, Vloženie obrázka. [vlastný]

Pre vloženie skrývaného súboru je potrebné kliknúť na položku Hide a po zadaní hesla súbor vybrať.



Obrázok 60, Výber skrývaného súboru. [vlastný]

Potom už len stačí súbor uložiť a poslať príjemcovi alebo zavesiť na webovú stránku, tak aby obrázok nevzbudil podozrenie.



Obrázok 61, Uloženie súboru. [vlastný]

Tabuľka 6, Porovnanie ukrývania pri rôznych veľkostí súborov. [vlastný]

Test	*Obrázok*	*Šifrovanie*	*Typ*	*Šírka [pixel]*	*Výška [pixel]*	*Veľkosť [B]*	*Povolená maximálna veľkosť skrývaného súboru [B]*
1.	**Originálny obrázok**	**-**	**JPG**	**9304**	**1601**	**10 406 981**	-
	Skrývaný súbor	**-**	**PDF**	**-**	**-**	**790 009**	**915 000**
	Obrázok so skrytým súborom	Blowfish	JPG	9304	1601	**10 078 784**	-
2.	**Originálny obrázok**	**-**	**JPG**	**3386**	**1596**	**3 234 118**	-
	Skrývaný súbor	**-**	**docx**	**-**	**-**	**14 065**	**285 000**
	Obrázok so skrytým súborom	Blowfish	JPG	3386	1596	**3 061 842**	-

Program JP Hide and Seek je z užívateľského hľadiska veľmi prehľadný a jednoduchý. Obsahuje iba jeden šifrovací algoritmus, Blowfish a podporuje iba jeden formát úvodného obrázka JPG, čím nedáva užívateľovi právo výberu.

Pre ukrytie do obrázka vyhradzuje presný objem dát, v závislosti na veľkosti úvodného obrázka, ktorý je v porovnaní s predošlými programami omnoho menší. Zaujímavé je, že výsledný obrázok so skrytým súborom, sa od úvodného líši iba nepatrne, a to veľmi malým objemom dát, pričom obrázok so skrývaným súborom je menší ako ten pôvodný.

Obrázok 62, Porovnanie originálnej fotografie s fotografiou, v ktorej je ukrytý súbor. [vlastný]

ZÁVER

Diplomová práca ukazuje históriu a súčasnosť steganografie ako nástroje na zabezpečenie spravodajskej komunikácie. Hoci sa zdá, že steganografia už v súčasnom svete prakticky nemá priestor, nie je to tak. Steganografia si neprestajne zachováva veľkú dôležitosť. Na rozdiel od hoci aj neprelomiteľnej, ale viditeľnej správy totiž nepriťahuje žiadnu neželanú pozornosť. Faktom je, že utajovanie správ, či už šifrou, alebo dômyselným úkrytom, je s ľudstvom už odnepamäti. Vek počítačov však toto odvetvie zmenil na nepoznanie a pozdvihol na takú úroveň, o ktorej sa prvým priekopníkom týchto metód určite ani nesnívalo.

Prostriedkov, ktoré využívali a stále využívajú spravodajské služby je nespočetné množstvo. V práci som tajnopis rozdelila na chemický, fyzikálny a matematický. Mojím cieľom bolo čitateľovi aspoň stručne priblížiť základné princípy týchto druhov tajnopisu, popísať ich vývoj, poukázať na iné formy a metódy spojenia, a myslím, že sa mi to podarilo.

Získať informácie nebolo jednoduché, ale samotné spracovanie bolo veľmi zaujímavé, pretože mi každé nové informácie priniesli ďalšie nezodpovedané otázky. Postupným, náročným štúdiom a zisťovaním informácií z kníh a dokumentárnych filmov som prenikla do hĺbky tejto zaujímavej, pritom neznámej oblasti. Tieto techniky sa dostali do úzadia, no znovu sa vynárajú a budú sa využívať v nových podobách stále častejšie, pretože šifrovanie a kryptografia, ktorá sa dnes využíva na utajenie informácií, sa ukazuje ako prekonateľné. Vždy sa nájde skôr, či neskôr niekto, kto šifru prelomí. Pokiaľ protistrana o komunikácii nevie, nevzbudzuje u neho pozornosť, nemá teda dôvod niečo skúmať alebo narúšať.

Techniky a technológie, ktoré v práci uvádzam môžu slúžiť a bohužiaľ pravdepodobne aj niekedy slúžia ako nástroj pre kriminálnu činnosť. Z tohto hľadiska je potrebné skúmať tieto spôsoby, aby v prípade, že sa dostanú do zlých rúk, nenarobili veľké škody. Steganografiu je nutné považovať za dvojsečný meč v závislosti na tom, kto ju používa. Preto pokladám za dôležité uviesť, že utajenie komunikácie by malo slúžiť pre nás, pre ľudstvo, a nie proti nám.

Prínos diplomovej práce je samotná práca, pretože táto tematika sa pri štúdiu nášho oboru vyskytuje len veľmi zriedka a okrajovo, preto som napísala tento informačný materiál,

ktorý pomôže študentom Univerzity Tomáše Bati ale aj študentom z iných univerzít oboznámiť sa s touto problematikou.

ZÁVER V ANGLIČTINE

Diploma thesis shows the history and present of Steganography as a instruments to provide intelligence communications. Although it seems that the Steganography in the modern world has practically no space, but it is not the true. Steganography can continually maintained great importance. Unlike even unsurpassable, but visible message does not attract any unwanted attention. The fact is that the secrecy of messages, either encryption or sophisticated hideaway, it has always been for humanity. Age of computers, however, the industry has changed beyond recognition, and was raised to a level on which the early pioneers of these methods will surely never dreamed of.

Means which are used to and still are using by the intelligence services are countless. I divided secret code into the chemical, physical and mathematical at my work. My aim was to bring to the reader at least briefly the basic principles of these species of secret codes, describe their development, pointed out other forms and methods of connection, and I think I was succeeded.

To get information was not very easy, but the process itself was very interesting, because any new information brought to me a new unanswered questions. By gradual, intensive study and survey of information from books and documentaries I penetrated deep into this exciting, unfamiliar area. These techniques were relegated to second place, but they are re-emerge and will be used in new forms, more often, because encryption and cryptography, which are today used for confidentiality of information seems to be surmountable. There is always sooner or later someone who will break the cipher. If the counterparty does not know about communication, does not inspire him with attention, therefore, has no reason to anything consider or disturb.

Techniques and technologies, which I present in my work, can serve and unfortunately probably also sometimes used to serve as a tool for criminal activity. In this respect, it is necessary to examine these methods because, if they get into the wrong hands, they did not do much damage. Steganography is necessary to considered as a double-edged sword, depending on who is using it. Therefore I considers very important to note that the confidentiality of communications should serve to us, to the humanity and not against to us. The contribution of this thesis is the work itself, because this theme is during our study

occurs very rarely and marginally, so I wrote this factsheet to help students of Tomas Bata University as well as students from other universities to become familiar with this issue.

ZOZNAM POUŽITEJ LITERATÚRY

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

[2] Steganografie. RYŠÁNKOVÁ, Alžběta. Kryptologie - Univerzita Hradec Králové [online]. [cit. 2013-02-28]. Dostupné z: http://kryptologie.uhk.cz/81.htm

[3] Steganografie: Zprávy ukryté ve špičkové technologii. Symantec [online]. 30.4.2002 [cit. 2013-02-28]. Dostupné z: http://www.symantec.com/region/cz/resources/Steganography.html

[4] Information Hiding: A Survey. PETITCOLAS, Fabien A.P., Ross J. ANDERSON a Markus G. KUHN. Gray-World [online]. July 1999 [cit. 2013-02-28]. Dostupné z: http://gray-world.net/pl/papers/petitcolas99information.pdf

[5] STEGANOGRAFIE. BĚLONOHÝ, Roman, Filip JEŽEK, Pavel VANČÁK a Radana VLAČIHOVSKÁ. Kryptologie: Univerzita Hradec Králové [online]. [cit. 2013-02-28]. Dostupné z: http://kryptologie.uhk.cz/82.htm

[6] MELTON, H. Velká kniha o špionáži. Překlad Milan Hausner, Petr Kučera. Bratislava: Perfekt, 1997, 175 s. ISBN 80-804-6061-2.

[7] CHARISIUS, Albrecht a Julius MADER. Tajná služba bez masky. Vyd. 1. Překlad Zdeněk Lahoda. Praha: Naše vojsko, 1974, 599 s. Fakta a svědectví, sv. 55.

[8] CHURAŇ, Milan. Encyklopedie špionáže: ze zákulisí tajných služeb, zejména Státní bezpečnosti. 2., přepracované a aktualizované vyd. Praha: Libri, 2000, 431 p. ISBN 80-727-7020-9.

[9] Tajné akce STB: Akce Průlom [Video]. 2009 [cit. 05.04.2013]. Dostupné z: http://www.ceskatelevize.cz/porady/10209991308-tajne-akce%20stb/409235100221018/video/

[10] DVOŘÁČEK, Petr. spojení v PO [pdf]. Frýdek - Místek, 2002 [cit. 07.04.2013]. Dostupné z: http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/030/cs/sys/resource/PDF/radiove-spojeni.pdf

[11] HANŽL, Tomáš, Radek PELÁNEK a Ondřej VÝBORNÝ. Šifry a hry s nimi: kolektivní outdoorové hry se šiframi. Vyd. 1. Praha: Portál, 2007, s. 85-94. ISBN 9788073671969.

[12] LAUCKÝ, Vladimír. SPECIÁLNI TECHNOLOGIE KOMERČNÍ BEZPEČNOSTI: Přednášky. Zlín, 2012.

[13] Latentní obraz. WIKIPEDIE [online]. [2012], 11.3.2013 [cit. 2013-04-18]. Dostupné z: http://cs.wikipedia.org/wiki/Latentní_obraz

[14] DOSKOČIL, František a Pavel ŽÁČEK. Průlom: agentem CIA uvnitř komunistické nomenklatury. Olomouc: Votobia, 2004, 285 s., xxxii s. obr. příl. ISBN 80-722-0208-1.

[15] ROEWER, Helmut, Stefan SCHÄFER a Matthias UHL. Encyklopedie tajných služeb ve 20. století. Vyd. 1. Praha: Euromedia Group - Knižní klub, 2006, 544 s. Universum (Euromedia Group). ISBN 80-242-1607-8.

[16] WRIGHT, Peter, Paul GREENGRASS a Matthias UHL. Lovec špionů. Vyd. 1. Překlad Jan Klíma. Praha: NLN, Nakladatelství Lidové noviny, 1997, 351 s. Universum (Euromedia Group). ISBN 80-710-6180-8.

[17] SMITH, Michael. Britské tajné služby. 1. vyd. Překlad Roman Marhold. Praha: Ivo Železný, 1998, 323 s. ISBN 80-237-3556-X.

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

[19] Česká republika. ZÁKON o ochraně utajovaných informací a bezpečnostní způsobilosti. In: http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/. 2005

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

[21] REUVERS, Paul a Marc SIMONS. Crypto Museum [online]. 2009, 18.April 2013 [cit. 2013-04-18]. Dostupné z: http://www.cryptomuseum.com/index.htm

[22] SINGH, Simon. Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii. 1. vyd. v českém jazyce. Překlad Petr Koubský, Dita Eckhardtová. Praha: Dokořán, 2003, 382 s. ISBN 80-865-6918-7.

[23] HÁLA, Vojtěch. Kvantová kryptografie. ALDEBARAN BULLETIN [online]. 2005, 3(2005), č. 14 [cit. 2013-03-20]. Dostupné z: http://www.aldebaran.cz/bulletin/2005_14_kry.php

[24] CARTLIDGE, Edwin. Hackers steal quantum code. Physicsworld [online]. 2011, June 2011 [cit. 2013-03-27]. Dostupné z: http://physicsworld.com/cws/article/news/2011/jun/17/hackers-steal-quantum-code

[25] Kvantová kryptografie. DUŠEK, Miloslav. Muj.optol [online]. [] [cit. 2013-04-18]. Dostupné z: http://muj.optol.cz/dusek/predn/kokt/krypt.htm

[26] PATEL, Prachi. New Type of Disappearing Ink: Nanoparticle inks that fade away in hours could be ideal for secure communications. MIT Technology Review [online]. 2009 [cit. 2013-04-18]. Dostupné z: http://www.technologyreview.com/news/415056/new-type-of-disappearing-ink/

[27] ZYGA, Lisa. DNA as invisible ink can reversibly hide patterns. PHYS.ORG [online]. 2012 [cit. 2013-04-18]. Dostupné z: http://phys.org/news/2012-01-dna-invisible-ink-reversibly-patterns.html

[28] Digitální steganografie [online]. České Budějovice, 2009 [cit. 2013-04-19]. Dostupné z: http://theses.cz/id/5y5kip/downloadPraceContent_adipIdno_11124. Diplomová práce. JIHOČESKÁ UNIVERZITA.

[29] WEISS, Max. Principles of Steganography [online]. [] [cit. 20.03.2013]. Dostupné z: http://www.math.ucsd.edu/~crypto/Projects/MaxWeiss/steganography.pdf

MARKS, Paul. Covert hard drive fragmentation embeds a spy's secrets.

[30] NewScientist [online]. 2011, issue 2809 [cit. 2013-04-19]. Dostupné z: http://www.newscientist.com/article/mg21028095.200-covert-hard-drive-fragmentation-embeds-a-spys-secrets.html

[31] SMEETS, Marc a Matthijs KOOT. Covert Channels [online]. Amsterdam, 2006 [cit. 2013-04-19]. Dostupné z: http://www.bandwidthco.com/whitepapers/netforensics/tcpip/covert/Covert%20Channels%20Research%20Report.pdf. Research Report. University of Amsterdam.

[32] DRAGOUN, Tomáš. Implementace skrytých kanálů v IPv6 [online]. Brno, 2012 [cit. 2013-04-19]. Dostupné z: http://is.muni.cz/th/359251/fi_b/bc.pdf. BAKALÁŘSKÁ PRÁCE. MASARYKOVA UNIVERZITA.

[33] ZANDER, SEBASTIAN, GRENVILLE ARMITAGE a PHILIP BRANCH. A SURVEY OF COVERT CHANNELS AND COUNTERMEASURES IN COMPUTER NETWORK PROTOCOLS. IEEE COMMUNICATIONS SOCIETY [online]. 2007, VOLUME 9, NO. 3 [cit. 2013-04-19]. Dostupné z: http://caia.swin.edu.au/cv/szander/publications/szander-ieee-comst07.pdf

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

BMP Bit Mapped Picture.

CIA Central Intelligence Agency.

DNA Deoxyribonucleic Acid.

DNS Domain Name Server.

GIF Graphic Interchange Format.

HIP Hide in Picture.

JPEG Joint Photographic Experts Group.

JPHS JP Hide and Seek.

LCD Liquid Crystal Display.

LSB Význam třetí zkratky.

PDF Portable Document Format.

TCP Transmission Control Protocol.

UV Ultraviolet.

WAV Waveform Audio Format.

ZSSR Zväz Sovietskych Socialistických Republík.

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK