POLITICKÝ A PRÁVNY RÁMEC KRYPTOGRAFICKÝCH APLIKÁCIÍ

Bc. Martina Čičelová, Bc. Miroslav Kolárik, Bc. David Mečíř,
Bc. Tomáš Halajčík, Bc. Tomáš Králik, Bc. Jozef Vlk

Obsah

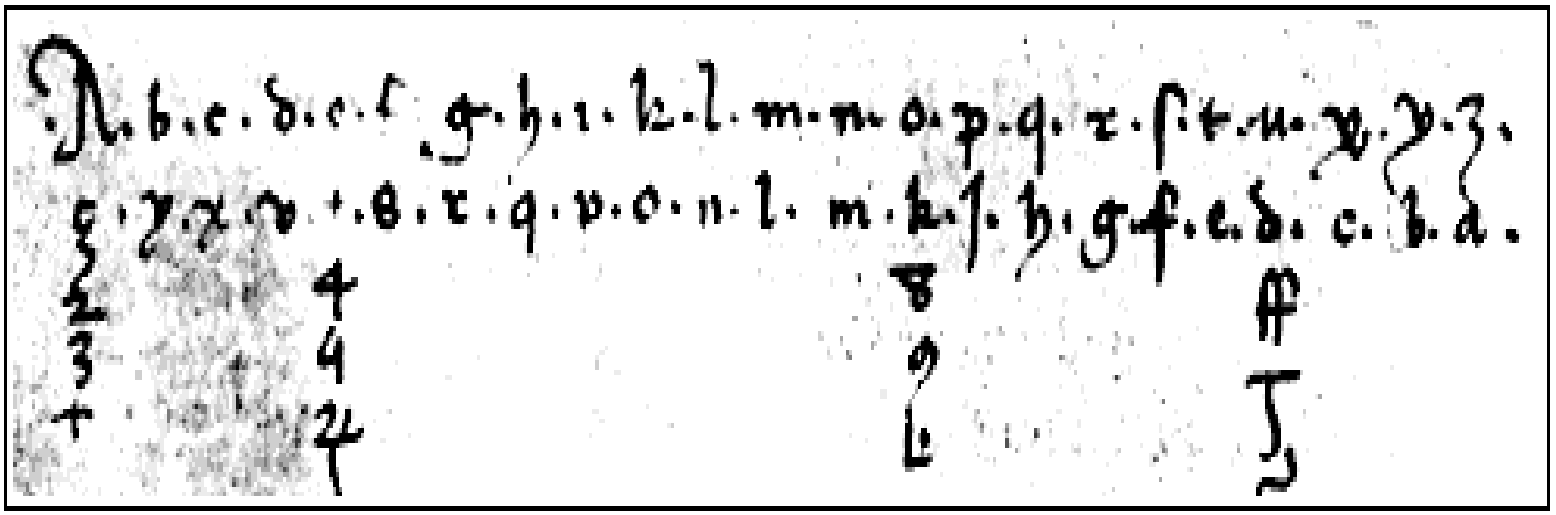
- História kryptografie
- EÚ (informatická bezpečnosť a ochrana pred cyber-útokmy)
- Slovenská republika (šifrovanie a utajovanie informácií)
- Česká republika (šifrovanie a utajovanie informácií)
- Medzinárodný prieskum šifrovacej politiky

História kryptografie - okolo 1860 p.n.l.

- Sesostris III., egyptský faraón a významný panovník strednej ríše vydal v rámci bezpečnostných opatrení pri jednaní so vzdialenými ríšami listinu Thraankh gris („Šedá líška“). Jedným z jej ustanovení bolo povinné používanie neštandardných hieroglyfických symbolov pri pohybe poslov cez nebezpečné Nubijské územia.

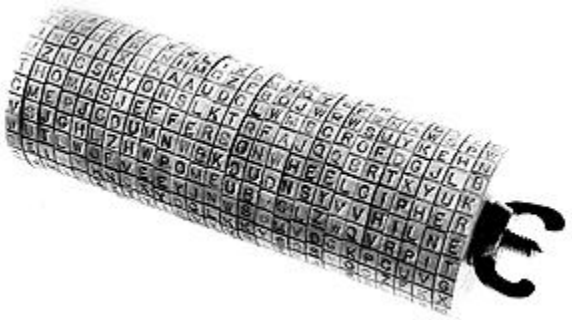
História kryptografie – r. 1401

- Doposiaľ najstaršiu známu západnú homofónnu šifru zostavil vojvoda Simeone de Crema z Mantovy.



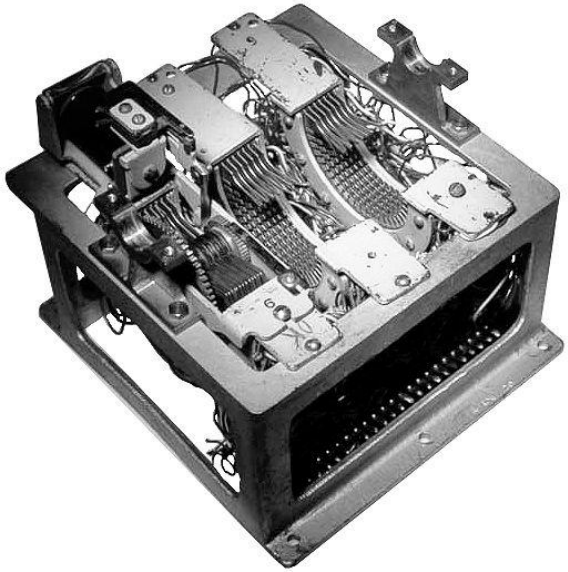
História kryptografie – r. 1790

- Americký minister zahraničných vecí Thomas Jefferson vynašiel mechanický šifrátor, ktorému sa hovorí Jeffersenov valec. Pozostáva z 26 rovnakých koliesok, ktoré sú nasunuté na spoločnú os a tak vytvárajú valec. Na obvode jednotlivých koliesok sú napísané všetky písmená abecedy v rozhádzanom poradí. Pri šifrovaní sa jednotlivé kolieska proti sebe otáčajú tak, že nakoniec dávajú vo zvolenom riadku na obvode valca požadovanú správu. Šifrovaný text sa prečíta z riadku nasledujúceho, alebo z iného vybraného z 26 možných. Kolieska boli číslované a mohli byť menené alebo poprehadzované.



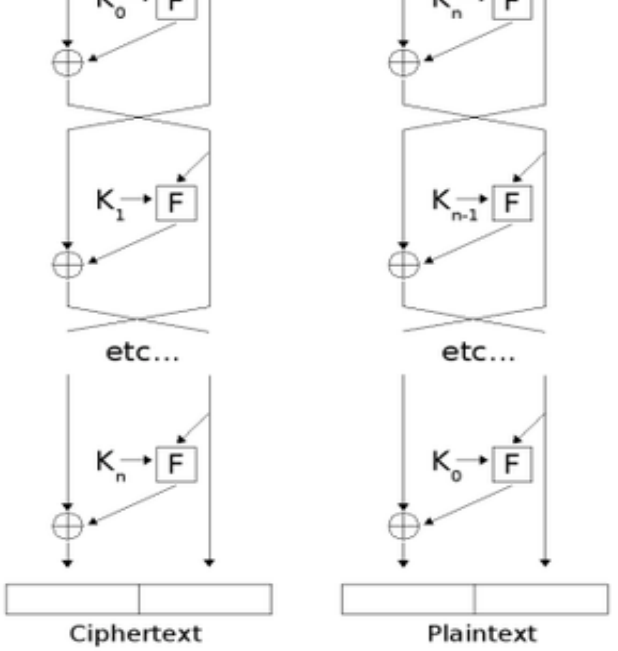
História kryptografie – r. 1937

- Japonská vláda začala používať šifrovací stroj PURPLE. Jeho šifra bola rozlúštená americkým tímom na čele s Williamom F. Friedmanom. Princíp Purple bol odlišný od nemeckej Enigmy, nebol založený na rotoroch, ale využíval telefonické súčiastky.



História kryptografie – r. 1970

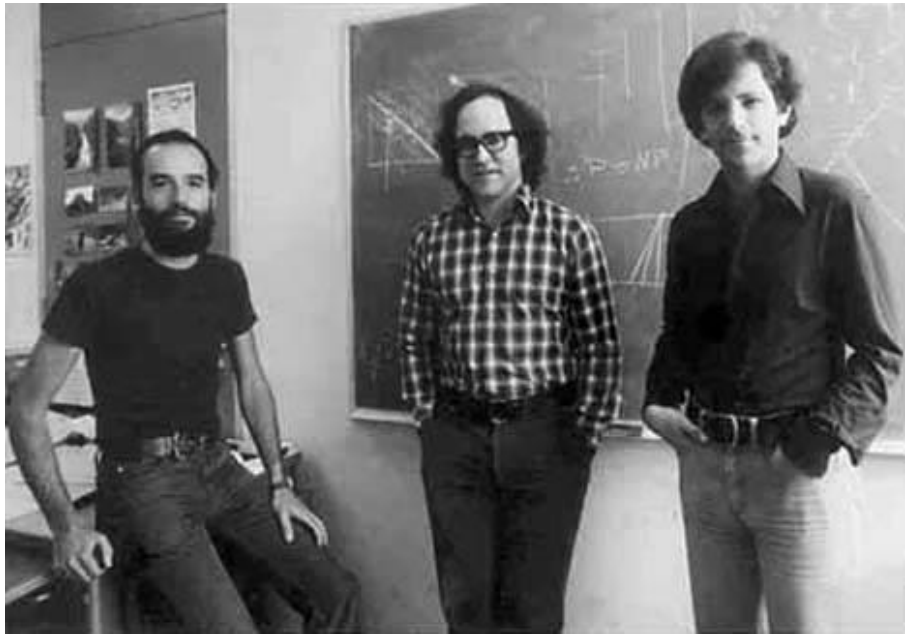
- Horst Feistel viedol výskumný projekt v IBM Watson Research Lab, ktorý počas šesťdesiatych rokov vyvíjal šifru LUCIFER. Táto šifra neskôr inšpirovala americký štandard DES a ďalšie šifry označované ako šifry Feistelovského typu.



Feistel Cipher

História kryptografie – r. 1977

- Inšpirovaní Diffie-Hellmanovou štúdiou oznámili Ronald L. Rivest, Adi Shamir a Leonard M. Adleman (z počítačového laboratória Massachusetts Institute of Technology) objav prvého konkrétneho kryptosystému s verejným kľúčom. Systém je založený na probléme faktorizácie veľkých čísel a dodnes je neoficiálnym svetovým priemyselným štandardom.



Európska Únia - ENISA

- sídli na gréckom ostrove Kréta v meste Heraklion
- poskytuje poradenstvo v oblasti bezpečnosti a komunikačných sietí a informačných systémov a analýzy dát
- podporuje zvyšovanie vedomia a spolupráce orgánov EÚ s členskými štátmi

Európska Únia - ENISA

- *RIADIACA RADA*
- *SKUPINA PSG (Permanent Stakeholders Group)*
- *Výkonný riaditeľ*

Európska Únia - ENISA

- zhromažďuje príslušné informácie na analýzu súčasných a vznikajúcich nebezpečenstiev, a poskytuje výsledky analýzy členským štátom a Komisii;
- poskytuje poradenstvo a prípadne podporu v rámci svojich cieľov Európskemu parlamentu, Komisii a príslušným európskym a vnútroštátnym orgánom;
- posilňuje spoluprácu medzi rôznymi subjektmi v sektore (napr. konzultácie,
  siete);

Európska Únia - ENISA

- uľahčuje spoluprácu medzi Komisiou a členskými štátmi v rozvoju spoločných metód k predchádzaniu bezpečnostných problémov;
- prispieva k zvyšovaniu povedomia a dostupnosť rýchle, objektívne a komplexné informácie o sieti a otázky bezpečnosti informácií pre všetkých užívateľov.
- pomáha Komisii a členským štátom v ich dialógu s priemyslom, adresuje problémy súvisiace s bezpečnosťou v oblasti hardware a softvérových produktov;

Európska Únia - ENISA

- sleduje vývoj noriem pre bezpečnostné produkty a služby a podporuje posúdenia rizika a riadiace činnosti;
- prispieva k úsiliu spoločenstva spolupracovať s tretími krajinami a medzinárodnými organizáciami na podporu globálneho spoločného prístupu k bezpečnosti;
- dáva vlastné závery, usmernenia a rady.

Európska Únia - ENISA

Žiadosti o radu a pomoc od agentúry by mali byť adresované výkonnému riadeteľovi a spravádzané ifnromáciami, ktoré objasňujú otázku, ktorá sa bude riešiť.

Tieto žiadosti môžu byť zo strany Európskeho parlamentu, Komisie alebo príslušných orgánov menovaných členským štátom.

Európska Únia - ENISA

- ***"Network"*** sa odkazuje na prenosové systémy a prípadne aj spojovacie alebo smerovanie zariadenia a iné prostriedky, ktoré umožňujú prenos signálov po drôte, rádiovými, optickými alebo inými el.magnetickými prostriedkami, vrátane satelitných sietí, pevných a mobilných pozemských sietí, pre rozhlasové a televízne vysielanie, a sietí káblovej televízie.

Európska Únia - ENISA

- ***"Informačný systém"*** sa rozumie počítačová a elektronická komunikácia sietí, rovnako ako el. dáta uložené, spracované aleboopätovne získavané.

Európska Únia - ENISA

- ***"Bezpečnosť sietí a informácií"*** je definovaná ako schopnosť siete alebo informačného systému odolávať náhodným udalostiam alebo nezákonnému alebo zákernému konaniu, ktoré ohrozujú dostupnosť, autentickosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb, ktoré môžu byť ponúkané prostredníctvom týchto sietí a systémov.

Európska Únia – OCHRANA EURÓPY

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov z 30. marca 2009 o ochrane kritickej informačnej infraštruktúry - "Ochrana Európy pred rozsiahlymi cyber-útokmi a narušením: zvyšujeme pripravenosť, bezpečnosť a odolnosť "

Európska Únia – OCHRANA EURÓPY

- ***Pripravenosť a prevencia***

  Komisia vyzýva členské štáty, aby určili minimálnu úroveň schopností a služieb pre Computer Emergency Response Teams (CERT), s podporou agentúry ENISA. Okrem toho Komisia zaviedla európsku Public Private Partnership pre odolnosť na ciele bezpečnosti a odolnosti.

Európska Únia – OCHRANA EURÓPY

- ***Detekcia a reakcia***

  Vývoj a zavádzanie európskeho zdieľania informácií a varovania (EISAS), osloviť občanov a malé a stredné podniky.

Európska Únia – OCHRANA EURÓPY

- ***Zmierňovanie a obnova***

  Komisia vyzýva členské štáty, aby vypracovali národné pohotovostné plány, organizovale cvičenia simulujúce vo veľkom meradle cyber-incidenty a na posilnenie spolupráce medzi národnými a vládnymi skupinami CERT. Európska komisia bude finančne podporovať rozvoj cvičení, ktoré môžu predstavovať prevádzkovú platformu pre európsku účasť na medzinárodných cvičeniach.

Európska Únia – OCHRANA EURÓPY

- ***Medzinárodná spolupráca***

  Medzinárodná spolupráca sa predpokladá s ohľadom na stabilitu a odolnosť najmä internetu, definovanie priorít, zásady a usmernenia, najprv na európskej úrovni, a potom v celosvetovom meradle.

Európska Únia – OCHRANA EURÓPY

- ***Ustanovenie kritérií v európskej kritickej infraštruktúre v sektore IKT***

  Kritériá pre európskej kritickej infraštruktúry v sektore IKT bude aj naďalej stanovovať Európska Komisia.

Európska Únia – ZÁKON O SLEDOVANÍ ELEKRONICKEJ KOMUNIKÁCIE

- 14. 12. 2005 prijal Európsky parlament zákon o uchovávaní dát o telefónnych hovoroch, krátkych textových správach a dátových spojeniach (data retention directive)
- Cieľom zákona je pomoc národným bezpečnostným zložkám pri pátraní po páchateľoch závažných zločinov (organizovaný zločin, terorizmus)
- Prvý návrh sa objavil po teroristických útokoch v Madride 11. marca 2004

Európska Únia – ZÁKON O SLEDOVANÍ ELEKRONICKEJ KOMUNIKÁCIE

- Dáta je nutné uchovávať po dobu najmenej šiestich mesiacov a maximálne po dobu dvoch rokov.
- Náklady na vedenie agendy nesú jednotliví telekomunikační operátori.
- Prístup zainteresovaných zložiek je umožnený len pri "vyšetrovaní vážnych zločinov", namiesto pôvodne vágne definovanej "prevencii zločinu".

Európska Únia – ZÁKON O SLEDOVANÍ ELEKRONICKEJ KOMUNIKÁCIE

- Je v kompetencii legislatív jednotlivých členských krajín určiť, ktoré orgány a v akom kontexte majú mať k dátam prístup.
- Daný orgán nikdy nemá prístup k celej databáze operátora, iba k častiam relevantnom k vyšetrovanému prípadu.

Slovenská republika

- *Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*

- *Vyhláška Národného bezpečnostného úradu č. 340/2004 Z. z.*

Slovenská republika – ZÁKON č. 215/2004 Z. z.

§65 Ústredný šifrový orgán

Ústredný šifrový orgán koordinuje a kontroluje činnosť ústredných orgánov štátnej správy na úseku šifrovej ochrany informácií. Je oprávnený požadovať od ústredných orgánov štátnej správy informácie potrebné na plnenie svojich úloh. Zamestnanci ústredného šifrového orgánu sú oprávnení v súvislosti s vykonávaním kontroly bezpečnosti systémov a prostriedkov šifrovej ochrany informácií vstupovať na pracoviská šifrových orgánov. Ak sa zistia závažné nedostatky na úseku šifrovej ochrany informácií, ústredný šifrový orgán môže zastaviť rozhodnutím prevádzku systému alebo prostriedku šifrovej ochrany informácií. Prevádzku systému alebo prostriedku šifrovej ochrany informácií možno obnoviť len s písomným súhlasom ústredného šifrového orgánu a po odstránení nedostatkov, ktoré viedli k zastaveniu prevádzky.

Slovenská republika – ZÁKON č. 215/2004 Z. z.

§ 66 Rezortný šifrový orgán

Na zabezpečenie šifrovej ochrany informácií v pôsobnosti ústredného orgánu štátnej správy si jeho vedúci s predchádzajúcim súhlasom ústredného šifrového orgánu môže zriadiť rezortný šifrový orgán ako osobitné pracovisko. Ten je priamo podriadený vedúcemu ústredného orgánu štátnej správy.

Slovenská republika – ZÁKON č. 215/2004 Z. z.

§ 68 Odborná spôsobilosť

Zamestnanec na úseku šifrovej ochrany informácií musí byť oprávnenou osobou na oboznamovanie sa s utajovanými skutočnosťami podľa tohto zákona a musí spĺňať podmienky odbornej spôsobilosti. Každý zamestnanec pri zahájení svojej pracovnej činnosti obdrží osvedčenie od vedúceho ústredného orgánu štátnej správy na prácu na určenom úseku šifrovej ochrany informácií. A taktiež pri ukončení pracovnej činnosti je mu toto osvedčenie odobrané.

Slovenská republika – ZÁKON č. 215/2004 Z. z.

§ 70 Pôsobnosť úradu, postavenie, povinnosti a oprávnenia príslušníkov úradu na úseku šifrovej ochrany informácií

Úrad na úseku šifrovej ochrany informácií plní funkciu ústredného šifrového orgánu Slovenskej republiky. Vypracúva koncepciu rozvoja a ustanovuje zásady šifrovej ochrany informácií. Certifikuje alebo overuje a uznáva zahraničné certifikáty a schvaľuje do prevádzky metódy, systémy a prostriedky. Taktiež vykonáva kontrolu bezpečnosti a vedie evidencie súvisiace so šifrovou ochranou informácií. Ďalej plní funkciu gestora vládneho i zahraničného spojenia a zabezpečovania prostriedkov šifrovej ochrany informácií. Tiež vykonáva znaleckú činnosť.

Slovenská republika – VYHLÁŠKA NBU č. 340/2004 Z. z.

§ 1 Predmet úpravy

a) certifikácia a schvaľovaní systémov a prostriedkov šifrovej ochrany informácií (ďalej len "prostriedok") do prevádzky, ich použití, nasadení, preprave, evidencii a používaní šifrových materiálov,

b) vedení evidencií zamestnancov na úseku šifrovej ochrany informácií a overovaní ich odbornej spôsobilosti,

c) zriaďovaní rezortného šifrového orgánu alebo jemu na roveň postaveného šifrového orgánu (ďalej len "rezortný šifrový orgán").

Slovenská republika – VYHLÁŠKA NBU č. 340/2004 Z. z.

§2 Certifikácia prostriedkov

(1) Certifikáciou prostriedkov sa overuje a osvedčuje spôsobilosť prostriedku chrániť utajované skutočnosti v súlade s bezpečnostným štandardom pre systémy a prostriedky šifrovej ochrany informácií a s bezpečnostným štandardom na ochranu pred nežiaducim elektromagnetickým vyžarovaním.

(2) Úrad certifikuje prostriedky, o ktorých certifikáciu bol požiadaný rezortným šifrovým orgánom alebo právnickou osobou, ktorá spĺňa podmienky priemyselnej bezpečnosti podľa osobitného predpisu. 1)

. . .

Slovenská republika – VYHLÁŠKA NBU č. 340/2004 Z. z.

§4 Používanie a preprava prostriedkov

(1) Používať možno iba prostriedky certifikované a schválené do prevádzky. Prostriedky možno používať iba v súlade s návodom na obsluhu a pravidlami na ich používanie.

(2) Spôsob ničenia zariadení určených na šifrovú ochranu informácií a šifrových materiálov sa uvádza v pravidlách na používanie prostriedku.

(4) Za prenos utajovaných skutočností technickými prostriedkami 6) sa nepovažuje prenos vnútri chráneného priestoru.

(7) Zariadenia určené na šifrovú ochranu informácií a šifrové materiály určené do týchto zariadení sa prepravujú a ukladajú oddelene, ak to technické riešenie umožňuje.

Slovenská republika – VYHLÁŠKA NBU č. 340/2004 Z. z.

§ 6 Používanie šifrových materiálov

(1) Šifrové materiály ako súčasť prostriedku 8) sú heslá, kľúče, premenné parametre kryptografických algoritmov označené podľa druhu prostriedku a stupňa ochrany utajovaných skutočností. Šifrové materiály možno používať len v súlade s pravidlami na používanie prostriedku.

(2) Správu prostriedkov a výrobu šifrových materiálov vykonáva len úrad a rezortný šifrový orgán vo svojej pôsobnosti.

(3) Šifrové materiály, ktoré už boli použité, ktoré sú poškodené alebo podozrivé z neoprávnenej manipulácie, nemožno ďalej používať na šifrovú ochranu informácií. Na šifrovú ochranu informácií nemožno ďalej používať ani šifrové materiály po skončení doby ich platnosti.

. . .

Česká republika

- Vyhláška č. 485/2005 Z. z., o rozsahu prevádzkovaných a lokalizačných údajov, dobe ich uchovávania a forme a zpôsobe ich predávania orgánom oprávneným k ich využívániu
- Zákon č. 412/2005 Z. z., o ochrane utajovaných informacií a o bezpečnostnej zpôsobilosti, v znení neskorších predpisov
- Vyhláška Národného bezpečnostného úradu č. 76/1999 Z. z., o zaistení kryptografickej ochrany utajovaných skutočností, uskutočňovanie certifikácie kryptografických prostriedkov a náležitostí certifikátov

Česká republika – VYHLÁŠKA č. 485/2005 Z. z.

- Prevádzkovatelia verejných komunikačných sietí povinní uchovávať niekoľko mesiacov údaje o elektronickej komunikácii.

- Rozsah údajov je o niečo širší ako požaduje Európska Únia.

- Vyhláška ukladá uchovávať údaje po dobu šiestich mesiacov, s výnimkou niektorých údajov, ktorým stačí 3 mesiace.

Česká republika – VYHLÁŠKA č. 485/2005 Z. z.

- V prípade hlasových služieb je interpretácia pomerne priamočiara, zložitejšia situácia nastáva u dátových služieb.
- V architektúrach súčasných počítačových sietí nie je úplne jasná hranica medzi údajom potrebným pre identifikáciu spojenia a samotným obsahom.
- Podobný problém sa objavuje napríklad u niektorých technológií pre IP telefónov.

Česká republika – VYHLÁŠKA č. 485/2005 Z. z.

- Prekážku kladie šifrovanie dátovej prevádzky na rôznych úrovniach, ktoré môže znemožňovať dekódovanie informácií.

Česká republika – ZÁKON č. 412/2005 Z. z.

- Upravuje zásady pre stanovenie informácií ako informácií utajovaných, podmienky pre prístup k nim a ďalšie požiadavky na ich ochranu, zásady pre stanovenie citlivých činností a podmienky pre ich výkon a s tým spojený výkon štátnej správy.

Česká republika – ZÁKON č. 412/2005 Z. z.

§5 spomína zaisťovanie ochrany utajovaných informácií od personálnej bezpečnosti, cez priemyslovú, administratívnu a fyzickú bezpečnosť až po kryptografickú ochranu, ktorú tvorí systém opatrení na ochranu utajovaných informácií použitím kryptografických metód a kryptografických materiálov pri spracovávaní, prenose alebo ukladaní utajovaných informácií.

Česká republika – ZÁKON č. 412/2005 Z. z.

- § 38 popisuje výkon kryptografickej ochrany. Chápe sa pod tým správa jej bezpečnosti, špeciálna obsluha kryptografických prostriedkov, alebo výroba kľúčového materiálu.

- Hlava X a nasledujúce paragrafy sa zaoberajú osvedčením osôb pre manipuláciu s utajovanými informáciami, ich povinnosťami rovnako ako povinnosťami daného úradu.

Česká republika – VYHLÁŠKA č. 76/1999 Z. z.

- Stanovuje predovšetkým spôsoby použitia, nasadzovania a evidenice kryptgrfických prostriedkov používaných k ochrane utajovaných skutočností.

Česká republika – VYHLÁŠKA č. 76/1999 Z. z.

§2 Pre účely tejto vyhlášky sa rozumie

a) **"*informácia*"** znalosť, ktorú je možné akoukoľvek formou poskytovať,

b) **"*utajovaná informácia*"** informácia, ktorá je klasifikovaná stupňom utajenia,

c) **"*kryptografia*"** vedná disciplína, ktorá rozvíja a aplikuje matematické a fyzikálne princípy pre tvorbu metód a prostriedkov k ochrane informácií za účelom ich skrytia pred nepovolanou osobou, zaistenie ich autenticity, zabránenia ich modifikácie, odmietnutie alebo neoprávnené použitie, (ďalej len „ochrana informácií")

d) . . .

Česká republika – VYHLÁŠKA č. 76/1999 Z. z.

- §4 tejto vyhlášky podrobne objasňuje kľúčové materialy.

- Predovšetkým akým stupňom utajenia sa material klasifikuje, a že spôsob manipulácie, distrubúcie a ničenia sa riadia určitými štandardami.

Česká republika – VYHLÁŠKA č. 76/1999 Z. z.

§4 kľúčové materiály

(2) Nezabezpečené kľúčové materiály, materiály bez technickej alebo kryptografickej ochrany sa klasifikujú stupňom utajenia, ktorý je zhodný so stupňom utajenia utajovanej skutočnosti, k ochrane ktorej sú kľúčové materiály určené , alebo stupeňom utajenia vyšším.

(3) Zabezpečené kľúčové materiály, materiály s technickou alebo kryptografickou ochranou sa klasifikujú stupňom utajenia, ktorý je zhodný so stupňom utajenia utajovanej skutočnosti, k ochrane ktorej sú kľúčové materiály určené, alebo stupňom utajenia nižším.

Česká republika – VYHLÁŠKA č. 76/1999 Z. z.

- Vyhláška ďalej pojednáva o opatrení proti kriminalite.
- Zaoberá sa aj definíciou požiadavkou na pracovníkov kryptografickej ochrany ako aj certifikáciou kryptografických prostriedkov.

Medzinárodný prieskum šifrovacej politiky – VÝZAM KRYPTOGRAFIE

- Vďaka používaniu kryptografie, môže byť komunikácia a informácie uložené a prenášané počítačmi veľmi efektívne chránené proti odpočúvaniu.
- Moderné šifrovacie technológie - matematické procesy používajúce vzorce (alebo algoritmy) - boli tradične nasadzované najmä na zachovanie dôvernosti vojenských a diplomatických komunikácií.

Medzinárodný prieskum šifrovacej politiky – VÝZAM KRYPTOGRAFIE

- S príchodom počítačovej revolúcie, a s nedávnymi inováciami vo sfére kryptografie, sa stihol vytvoriť a vyvinúť pre kryptografické produkty nový trh.
- Neustále tiež rastú nároky pre uchovávanie a výmenu osobných údajov či dôverných lekárskych a finančných dát.
- Vládne nariadenia o bezpečnosti kryptografických techník teda môžu ohrozovať osobné súkromie

Medzinárodný prieskum šifrovacej politiky – VÝZAM KRYPTOGRAFIE

- Vo svojom uznesení "o podpore slobody používania kryptografie," členovia Global Internet Liberty kampane (GILC) poznamenali, že *"používanie kryptografie sa dotýka ľudských práv a otázky osobnej slobody,"* a že *"Ochrana osobných údajov komunikácie je výslovne chránená článkom 12 Všeobecnej deklarácie ľudských práv OSN, článkom 17 Medzinárodného paktu o občianskych a politických právach, a vnútroštátneho práva OSN "*.

Medzinárodný prieskum šifrovacej politiky – ŠIFROVANIE A ĽUDSKÉ PRÁVA

- US Department of State, v ich správe z roku 2006 o dodržiavaní ľudských práv v jednotlivých krajinách, hlásilo rozsiahle protizákonné alebo nekontrolované používanie odposluchov vládnymi i súkromnej skupiny vo viac ako 90 krajinách.
- V niektorých krajinách, ako je Honduras a Paraguaj, boli štátom vlastnené telekomunikačné spoločnosti aktívnymi účastníkmi v pomoci bezpečnostnej službe.

Medzinárodný prieskum šifrovacej politiky – ŠIFROVANIE A ĽUDSKÉ PRÁVA

- Francúzsky národný kontrolný úrad pre zachovanie bezpečnosti napríklad odhaduje, že sa v ich krajine každoročne vykoná vyše 100 tisíc takýchto zásahov.
- Mimovládne organizácie vo Veľkej Británii poukázali na početné prípady odhalenia ilegálneho odpočúvania sociálnych aktivistov, odborov a organizácií pre občiansku slobodu .

Medzinárodný prieskum šifrovacej politiky – ŠIFROVANIE A ĽUDSKÉ PRÁVA

- Mnohé skupiny pre ľudské práva v súčasnej dobe používajú šifrovanie aby chránili svoje dokumenty a komunikačné kanály pred externými zásahmi zo strany vlády.
- Medzi spomínané vlády patria vlády Guatemaly, Etiópie, Haiti, Mexika, Juhoafrickej republiky, Hong Kongu a Turecka.

Medzinárodný prieskum šifrovacej politiky – ŠIFROVANIE A ĽUDSKÉ PRÁVA - GILC

- Global Internet Liberty Kampaň bola založená v júni 1996 ako celosvetová organizácia pre ochranu občianskych slobôd a ľudských práv na internete.
- Medzi zásady prijaté GILC na svojom ustanovujúcom stretnutí bolo presvedčenie, že používatelia internetu by mali mať právo "šifrovať svoju komunikáciu a informácie bez obmedzení."
- V septembri 1996, GILC vydalo "Uznesenie na podporu slobody používať kryptografiu" na medzinárodnej konferencii sponzorovanej GILC v Paríži.

Medzinárodný prieskum šifrovacej politiky – PRIESKUM

- Bol vykonaný za účelom poskytnutia komplexného prehľadu kryptografickej politiky prakticky všetkých krajín i autonómnych oblastí sveta.

- Pri prieskume boli odoslané listy na veľvyslanectvá, misie OSN, ministerstvá a informačné kancelárie v zhruba 230 krajinách a územiach.

- Listy sa zameriavali na výskum štyroch hlavných oblastiach týkajúcich sa politiky kryptografie:

Medzinárodný prieskum šifrovacej politiky – PRIESKUM

- vládnu kontrolu nad voľným používaním kryptografie vo svojich krajinách;
- vládnu kontrolu nad importom počítačových programov alebo zariadení, ktoré umožňujú šifrovanie;
- vládnu kontrolu nad exportom počítačových programov alebo zariadení, ktoré umožňujú kryptografiu a ktoré sú vyvinuté v tuzemsku;
- identifikáciu agentúr alebo vládnych oddelení zodpovedných za politiku používania, dovozu alebo vývozu kryptografických technológií.

Medzinárodný prieskum šifrovacej politiky – VÝSLEDKY PRIESKUMU

- ***Wassenaarské usporiadanie (WA)*** - režim kontroly exportu konvenčných zbraní, tovarov a technológií dvojakého použitia, ktoré je duchovným následníkom bývalého COCOM-u, zameraného najmä proti štátom bývalého socialistického bloku v období studenej vojny
- ***WA*** však nie je jediným kontrolným režimom pripomienkujúcim používanie kryptografie, k tým ešte patrí Austrálska skupina, Skupina jadrových dodávateľov, Zanggerov výbor a Režim kontroly raketových technológií (MTCR)

Medzinárodný prieskum šifrovacej politiky – VÝSLEDKY PRIESKUMU

- Wassenaarske usporiadanie klasifikuje vývoz kryptografie ako tovaru dvojakého použitia

- Avšak, akýkoľvek softvér obsahujúci kryptografiu môže byť predmetom podliehajúcim kontrole ako tovar dvojitého použitia

Medzinárodný prieskum šifrovacej politiky – **VÝSLEDKY PRIESKUMU**

- V 1996 pristúpilo 31 krjín k ***WA*:** medzi nimi aj **Česká republika** a **Slovenská republika**

- Od 2009 ***WA*** zoskupuje 40 krajín: Argentína, Austrália, Rakúsko, Belgicko, Bulharsko, Chorvátsko, **Česká republika**, Dánsko, Fínsko, Francúzsko, Kanada, Nemecko, Grécko, Maďarsko, Írsko, Taliansko, Japonsko, Luxembursko, Holandsko, Nový Zéland, Nórsko, Poľsko, Portugalsko, Kórejská republika, Rumunsko, Ruská federácia, **Slovenská republika**, Španielsko, Estónsko, Lotyšsko, Litva, Malta, Slovinsko, Južná Afrika, Ukrajina, Švédsko, Švajčiarsko, Turecko, Veľká Británia a USA

Medzinárodný prieskum šifrovacej politiky – VÝSLEDKY PRIESKUMU

- **"Zelené„** - krajina buď vyjadrila podporu usmernenia OECD o kryptografii, ktoré vo všeobecnosti podporuje neobmedzené právne kryptografie, alebo nemá kontrolu kryptografie.
- **"Žlté"** - krajina buď navrhla nové kontrolné prvky pre kryptografiu , vrátane kontroly domáceho použitia, alebo preukázala ochotu k zmene klasifikácie kryptografického softvéru ako tovaru dvojitého použitia v súlade s WA.
- **"Červené"** - krajina, ktorá zaviedla rozsiahle kontroly kryptografie, vrátane domáceho použitia.

Medzinárodný prieskum šifrovacej politiky – VÝSLEDKY PRIESKUMU

- Čína => ***Červené***
- Česká republika => ***Zelené*** / ***Žlté***
- Európska únia => ***Zelené*** / ***Žlté***
- Nemecko => ***Zelené***
- India => ***Žlté*** / ***Červené***
- Japonsko => ***Žlté***
- Rusko => ***Červené***
- Slovenská republika => ***Zelené*** / ***Žlté***
- USA => ***Žlté*** / ***Červené***

Ďakujem za pozornosť !