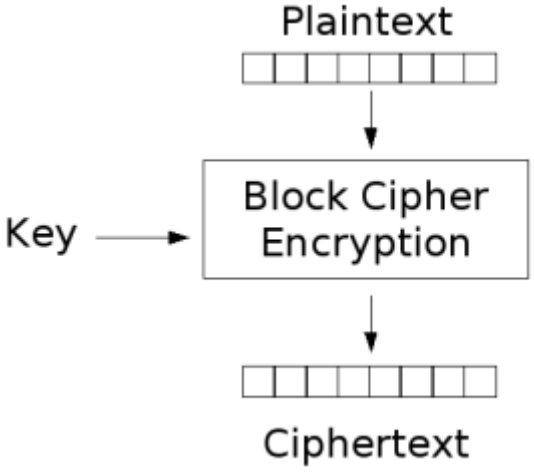
Šifrování

- Způsob jak ochránit data před nepovolanými
  - Ochránit je proti změně
  - Zamezit jejich přečtení nepovolanými
  - Podepsat data

- Šifra je
  - Kryptografický algoritmus, který transformuje vstupní data podle zadaného hesla

- Blok dat je nějaká posloupnost jedniček
  - Pro některé kryptografické operace se vyžaduje, aby byl blok roven násobku nějakého čísla
    - Dáno specifikací šifry
    - Blok o menší velikost se prostě doplní požadovaným počtem nějakého znaku
      - Např. nuly
        - padding

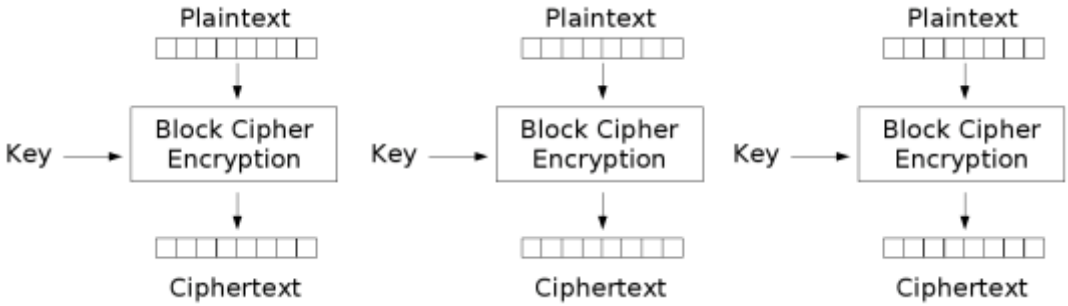
- Šifra
  - Bloková – šifruje se po blocích pevné délky



http://en.wikipedia.org/wiki/Block_cipher

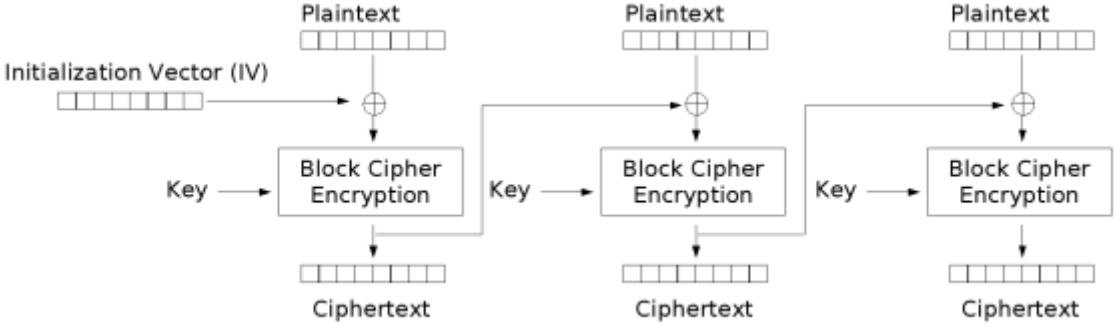
  - Proudová – šifruje se po jednotlivých znacích/bitech

- Režim kódové knihy
  - Electronic Code Book (ECB)
  - Šifruje se po blocích
    - => tj. identické bloky budou vypadat identické i po zašifrování, což už nějakým způsobem vypovídá o obsahu zašifrovaných dat



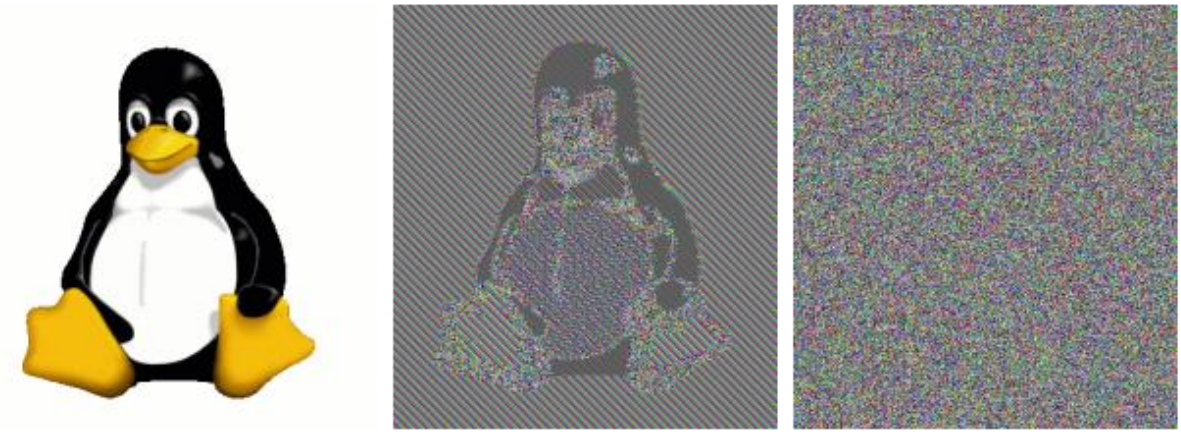
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

- Cipher Block Chaining (CBC)
  - Zřetězení šifrovaných bloků
  - Ještě existuje varianta PCBC
    - Propagating-CBC
  - Každý další blok je zašifrován i pomocí předcházejícího bloku
    - Takže identické nezašifrované bloky už nejsou identické po zašifrování
    - První blok vyžaduje inicializační vektor (IV)
      - Může být i veřejně známý, ale pokud se použije i více hesel, opět prozrazuje informaci o heslu



http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

- Dále ještě existují
  - Režimy se zpětnou vazbou
  - Režimy s čítačem
  - Oba dělají z blokové šifry proudovou
  - Mimo rozsah KIV/ZPS



Original *Encrypted using ECB mode* *Encrypted using other modes*

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

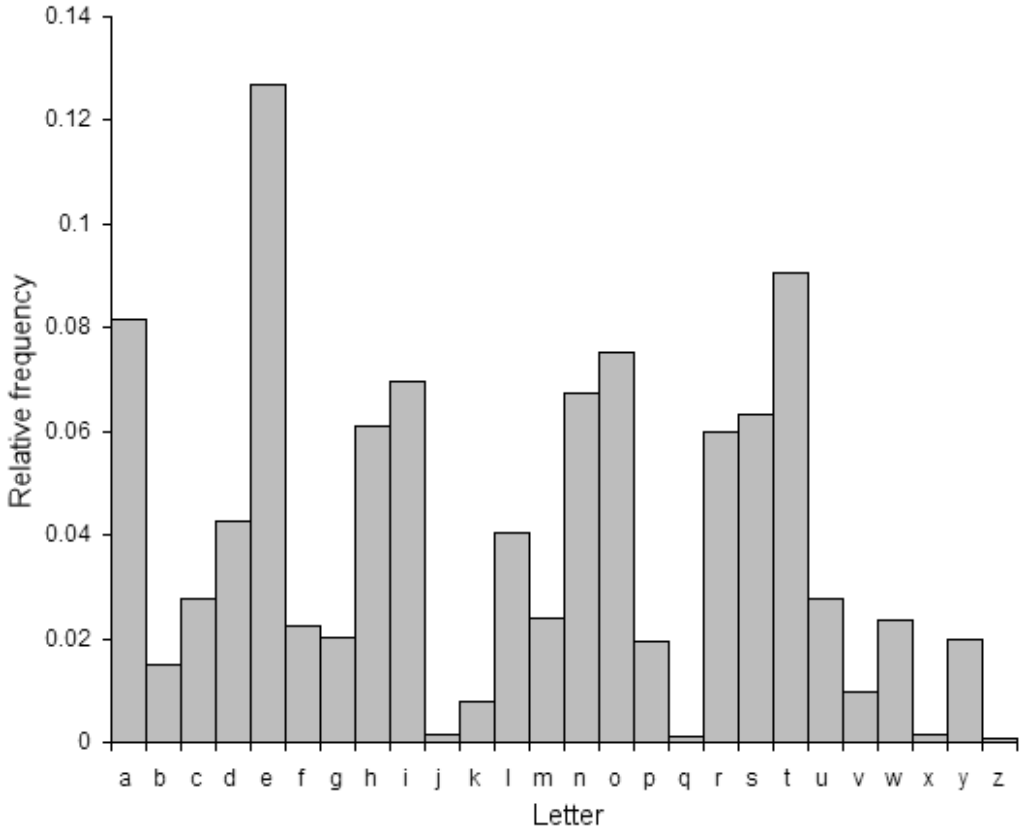
- Viz obrázek, jak ECB produkuje identické bloky i po zašifrování, obsah není „tak úplně“ utajen i po zašifrování oproti ostatním režimům

- Substituce
  - Nahrazení jednoho znaku jiným
  - Např. Caesarova šifra nahrazuje znak znakem, který je o 3 znaky (modulo délkou abecedy) dál
    - Případně o jiný počet znaků a jiným směrem

A, B, Z → D, E, C

  - Dále k substituci pro zajímavost
    - mimo rozsah KIV/ZPS

- Konkrétně Caesarova šifra je velmi nenáročná na prolomení
- Pro každý jazyk existuje frekvenční charakteristika, jak často se vyskytuje konkrétní znak



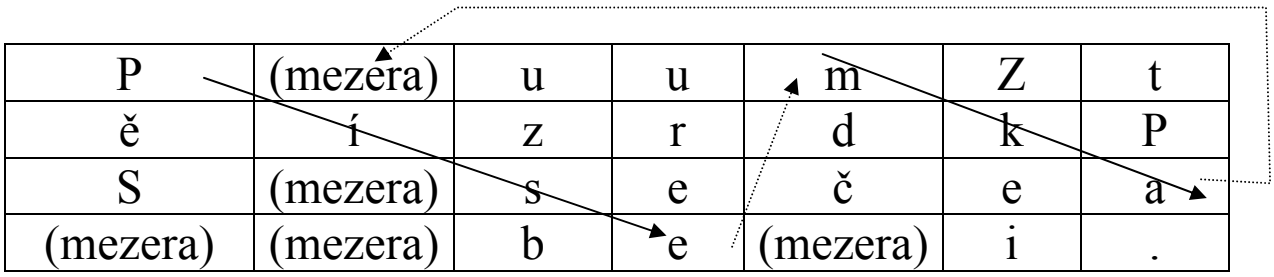
http://en.wikipedia.org/wiki/Caesar_cipher

- Lze udělat frekvenční charakteristiku zakódovaného textu a porovnat

- Možný útok hrubou silou
  - Porovnáním četností znaků se určí nejpravděpodobnější posun
  - Zkusí se rozšifrovat kus textu
  - V nově obdrženém textu se pokusíme najít známá slova
    - Známe-li typ souboru, např. X/HTML, víme přesně, co hledáme – <!DOCTYPE
  - Opakujeme, dokud nenajdeme použitý posun

- Substituce nemusí nahrazovat jeden znak jedním zakódovaným znakem, ale několika
- Někteří webmasteři, např. portálů s videem, používají kódování base64, aby v parametrech flash-playeru skryli cestu k video souboru
  - base64 končí jedním, nebo dvěma, znaky '='
    - víme-li, není problém „prolomit šifru“

- Transpozice
  - Znaky se nemění, ale přeuspořádávají se
  - Dále mimo rozsah KIV/ZPS
    - Až na sdělení zprávy v tabulce ;-)



P	(mezera)	u	u	m	Z	t
ě	í	z	r	d	k	P
S	(mezera)	s	e	č	e	a
(mezera)	(mezera)	b	e	(mezera)	i	.

  - Začátek je v levém horním rohu
  - Šikmo dolů po diagonále
  - Při dosažení okraje se přetočí na druhý okraj
    - Kromě druhého přetočení

  - Zašifrovaný text by byl

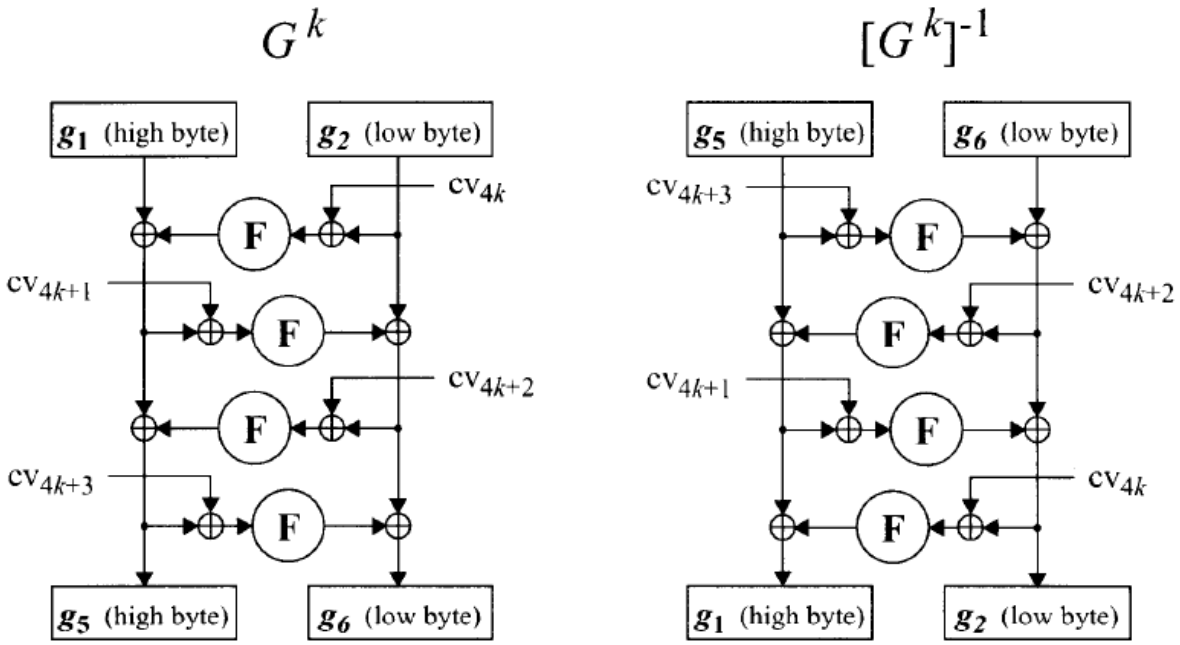
```
P uumZt
ěízrdkP
S sečea
  be i.
```

  - Útok by šlo opět realizovat s využitím frekvenční analýzy
  - Nicméně, druhé přetočení je nelineární vazba, která už to významně ztížila

- Útok – pokus o prolomení šifry
  - Hrubou silou – vyzkoušení všech možných kombinací hesel
  - Slovník – vyzkouší se hesla podle nějakého slovníku, kde jsou seřazena podle pravděpodobnosti úspěchu
  - Kryptoanalýza – bere do úvahy různé vlastnosti, nepostupuje naivně jako slovní a hrubá síla
    - Např. poslední případ ukazuje alespoň jeden artefakt – ZP a naproti S
    - Speciální stroje jako např. TWINKLE
      - Prolomení šifry je i otázka toho, kdo se snaží a jaké má k dispozici zdroje
      - Mimo rozsah KIV/ZPS
  - Protinávrhu se lze bránit vhodnou kombinací šifrovacích postupů
    - Existují i další, než které byly uvedeny

- Rotate over Carry
  - Mimo rozsah KIV/ZPS
  - rol, ror
    - instrukce x86, které provádějí rotaci bitů zvoleným směrem o zvolený počet bitů
    - ztěžuje to práci, ale ne moc
  - rcl, rcr
    - ty samé instrukce, ale rotace probíhá i přes carry flag registru r/eflags
    - velmi ztěžuje práci při prolomení
      - carry flag se nastavuje při přetečení rozsahu – tj. i při normální operacích
  - Šifry optimalizované na rychlost u daných procesorů se ukázaly jako relativně snadno prolomitelné

- Feistalovo schéma
  - Mimo rozsah KIV/ZPS
  - Je základem dalších šifer

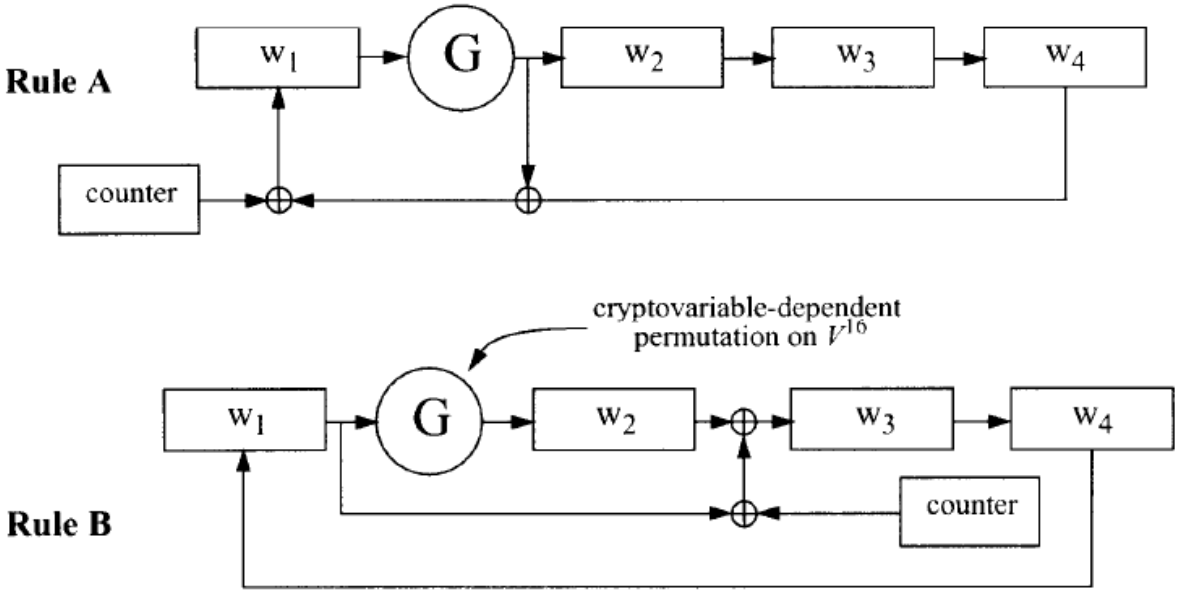


http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf

  - Blok šifrovaných dat se rozdělí na dva díly (high & low byte)
  - Jeden z nich se zašifruje jako blok v ECB
  - Pomocí XOR se přimíchá k druhému dílu
  - Několikrát se zopakuje

  - Od třetího kola jde o pseudonáhodnou permutaci
    - Tj. nelze ji odlišit od skutečně náhodné permutace vybrané s rovnoměrným rozdělením pravděpodobnosti
      - Ne s náklady, které jsou menší než útok hrubou silou
        - Tedy většinou :-)
  - Jednoduché dekódování – stačí obrátit pořadí operací

- Skipjack
  - Mimo rozsah KIV/ZPS
  - Pentagon, NSA



http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf

  - Používá registry s nelineární zpětnou vazbou
  - Produkuje různá schéma šifrování podle hesla/dat
  - Používá transformační tabulku k přeuspořádání znaků
    - Je pevně daná návrhem, ale dala by se generovat dynamicky podle hesla a dále snížit možnost prolomení

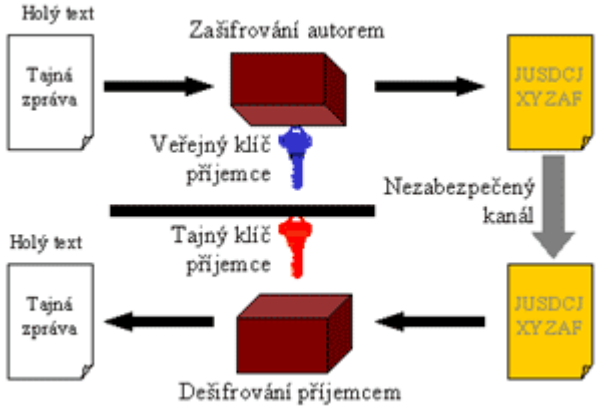
- Ghost
  - Mimo rozsah KIV/ZPS
  - KGB
  - Betonování
    - Šifrování jednoho bloku dat se několikrát opakuje
    - Data se pokaždé nějak změní
    - S narůstajícím počtem klesá získaná bezpečnost
    - Ghost „mnógo“ betonoval – čas. vs. bezpečnost

- AES
  - NSA
  - Advanced Encryption System
    - Šifra původně známá jako Rijndael
      - Ne však identická s Rijndael
        - podporuje více velikostí bloků data a hesel
  - 26. květen 2002 – stala se standardem NSA pro top-secret informace
  - Veřejně známý design
  - Současným standardem
    - Např. zabezpečené připojení k stag.zcu.cz
  - Symetrické šifrování
  - Pro zajímavost, mimo rozsah KIV/ZPS
    - Nepoužívá Feistalovo schéma, ale substitučně-permutační schéma
      - Jde o to, aby změna byť jednoho jediného bitu vyvolala změnu co nejvíce bitů v zašifrované podobě
    - Jediný úspěšný útok byl veden postraním kanálem
      - Tj. neprolomil šifru jako takovou, ale jenom systém, kde byla nasazena, díky jeho konfiguraci

Symetrické a asymetrické šifrování

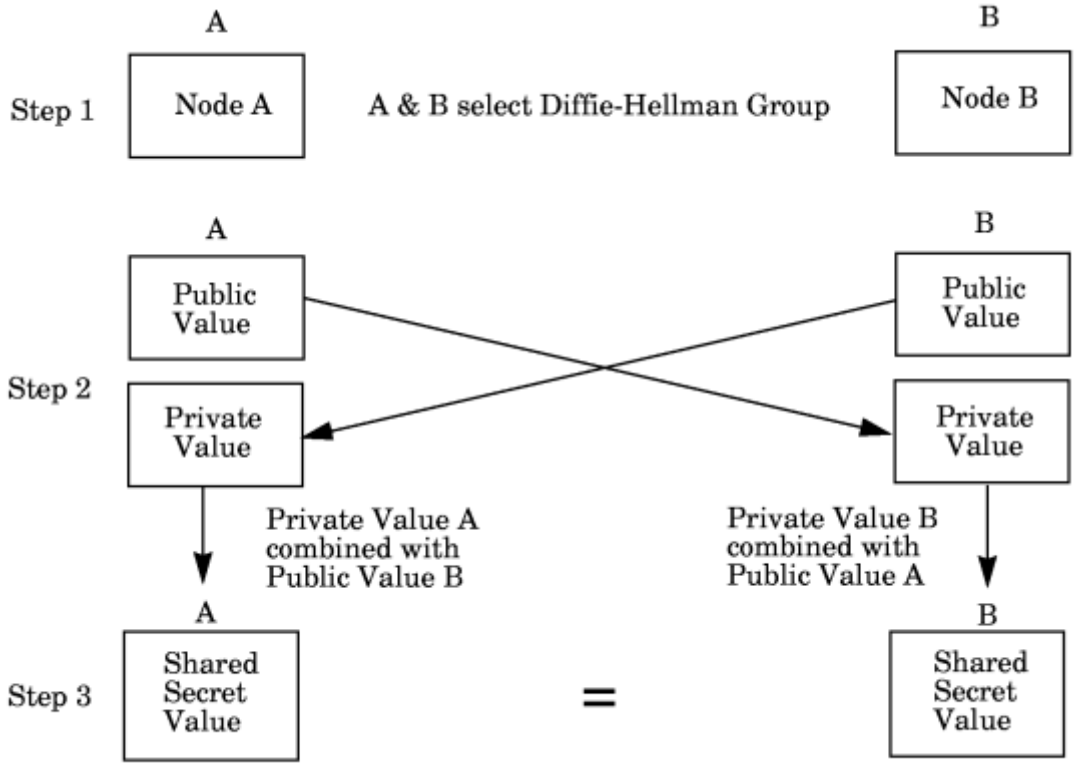
- Symetrické šifrování
  - Odesílající a příjemce musí znát ten samý klíč,
    - Který byl použit k zašifrování
    - A bude použit k jeho dešifrování
  - AES
    - DES, Skipjack, Ghost
  - Je jednodušší na implementaci, ale neřeší problém, jak bezpečně přenést sdílené heslo

- Asymetrické šifrování
  - Diffie-Hellman, RSA
  - Existují dva klíče
  - Veřejný klíč dostupný všem
  - Privátní klíč příjemce
    - Tvoří pár, oba klíče jsou vzájemně nějaký způsobem svázané
  - Odesílající zašifruje data veřejným klíčem
  - Příjemce dešifruje data svým privátním klíčem
    - A vo tom to je – o asymetrii



http://www.pgp.cz/this2print.php?l=cz&p=6&r=5

- Diffie-Hellman
  - Kryptografický protokol
  - Tvůrci Whitfield Diffie a Martin Hellman
    - Publikováno 1976
  - Umožňuje dvěma komunikujícím stranám si dohodnout tajné heslo po nezabezpečeném spojení, aniž by předtím byla potřeba nějaká akce
  - Poté, co je dohodnuto tajné heslo, je celá komunikace šifrována symetrickou šifrou
  - Používá se jako základ šifrovacích protokolů, které umožňují dohodnutí společného, utajeného hesla
  - Dále pro zajímavost
    - Mimo rozsah KIV/ZPS



http://docs.hp.com/en/J4255-90011/ch04s04.html

  - Bez zabezpečené autentizace je možnost napadení stylem Man in the Middle

- Trik je v tom, jaké vlastnosti budou mít vybraná čísla
- Využívá se problému diskrétního logaritmu
  - Není známa efektivní metoda, jak vypočítat obecný diskrétní logaritmus
    - $log_b\ g$ kde g náleží do cyklického prostoru G, jehož je b generátorem

  - Známé metody jsou v dostatečně krátkém čase úspěšné pouze tehdy, jsou-li počítaná čísla dostatečně malá
  - Od prvočísel od 300 číslic výše je výpočet mimo současné výpočetní možnosti

Hash (Message Digest)

- Hash funkce umožňuje vypočítat „otisk“ bloku dat
- Např. vytvoříme záložní 700 MB CD
- Hash funkcí vypočítáme jeho otisk – např. 4kB velký
- Kdykoliv je pak možné tou samou funkcí vypočítat otisk záložního CD a otisky porovnat, zda souhlasí
  - Pokud ne, víme, že alespoň jedno z CD je poškozené

- Z otisku nelze vypočítat data, ze kterých byl vypočítán
- Používá se např. k uložení hesel
  - Uživatel zadá heslo, z něj se vypočítá otisk a ten se teprve porovná, zda bylo zadáno správné heslo
  - Něco o heslu je nutné uložit, takže i kdyby někdo zcizil databázi jmen a hesel, z otisků hesla nezjistí
- MD5, SHA, Whirlpool-T (standard k AES) – algoritmy
- Ač různá, příliš velká vstupní data mohou vést ke stejnému otisku – např. CD (700 MB) a MD5 (16B)

Elektronický podpis

- Chceme-li zaručit autentičnost veřejně čitelné zprávy
  - E-mailu, dokumentu ve Wordu, spustitelného programu…

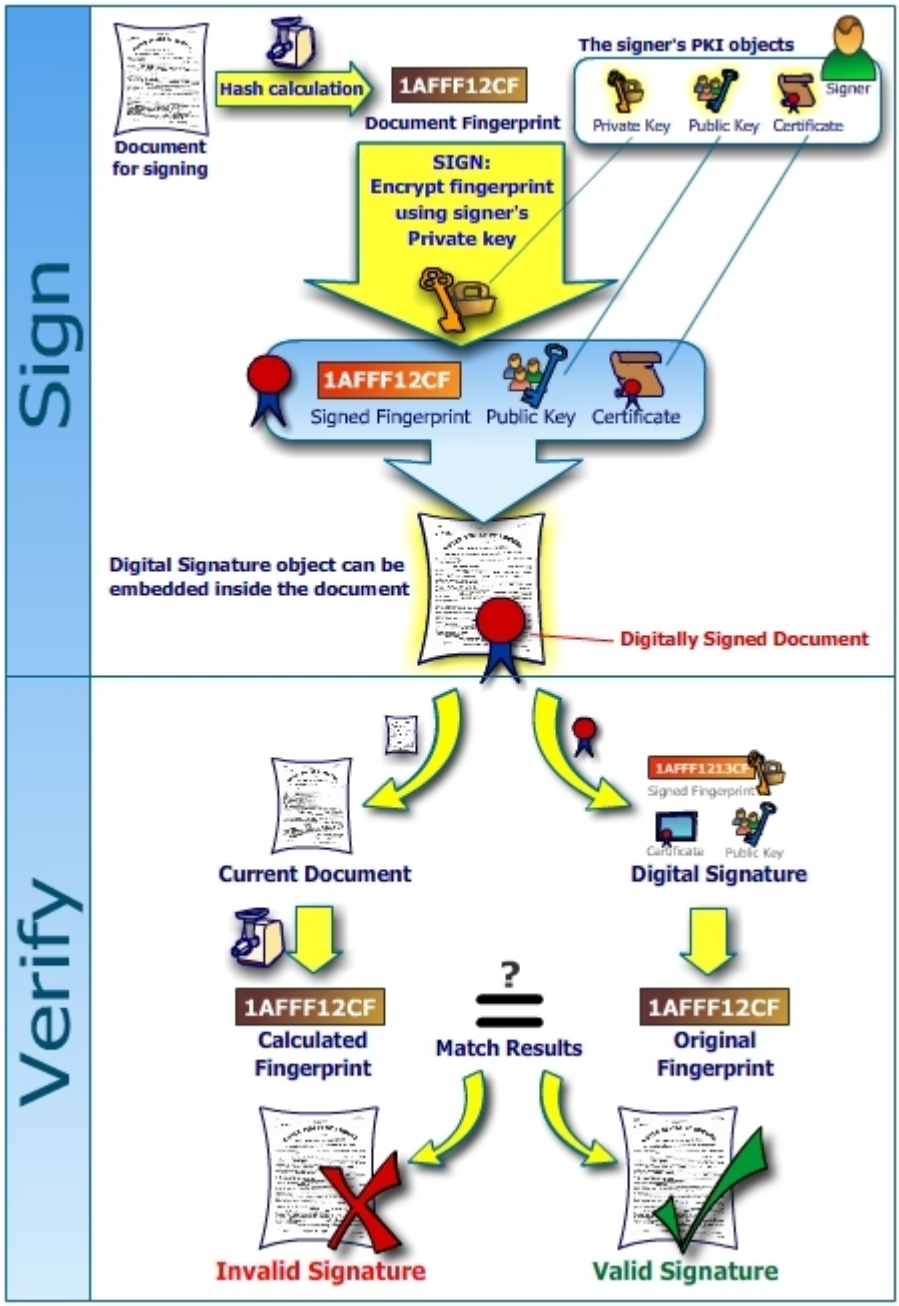
- Vypočítáme její otisk hash-funkcí
  - Pokud by ji však někdo modifikoval, může si vypočítat otisk upravené verze a podvrhnout ho místo našeho otisku

  - Privátním klíčem zašifrujeme vypočítaný otisk a přiložíme ho ke zprávě

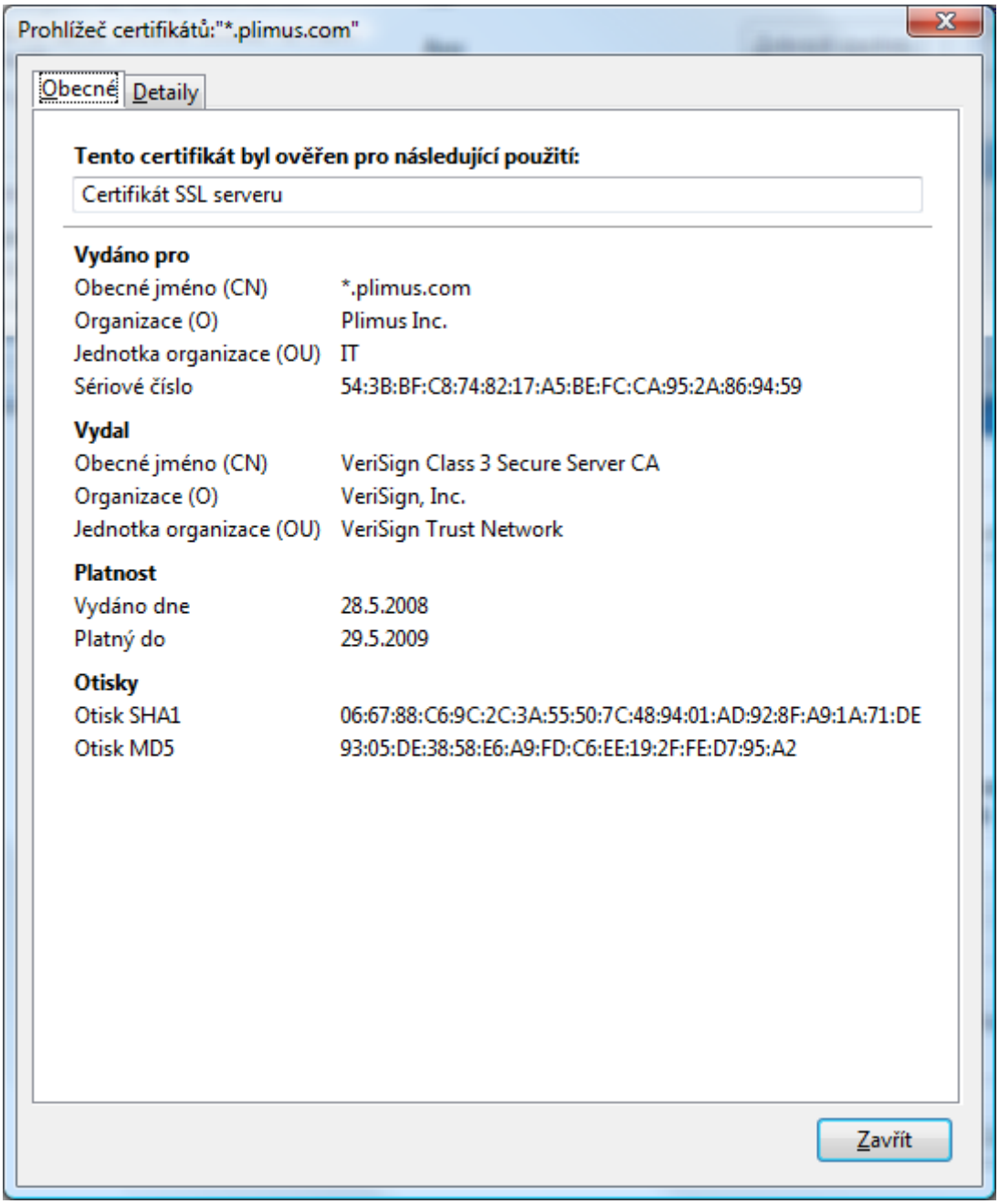
  - K ověření zprávy je ještě třeba přidat certifikát toho, kdo ji podepsal
  - Certifikát obsahuje
    - Popis (podepsané) osoby – viz LDAP
    - Platnost certifikátu
    - Veřejný klíč, kterým je možné dešifrovat zašifrovaný otisk zprávy
      - Tj. otisk nelze podvrhnout bez znalosti privátního klíče

  - Příjemce podepsané zprávy
    - Veřejným klíčem získaným z certifikátu dešifruje přiložený (zašifrovaný) otisk
    - Pokud nelze, zpráva se označí jako podvrh

    - Vypočítá otisk zprávy a porovná ho s dešifrovaným otiskem
    - Pokud nesouhlasí, zpráva se označí jako podvrh



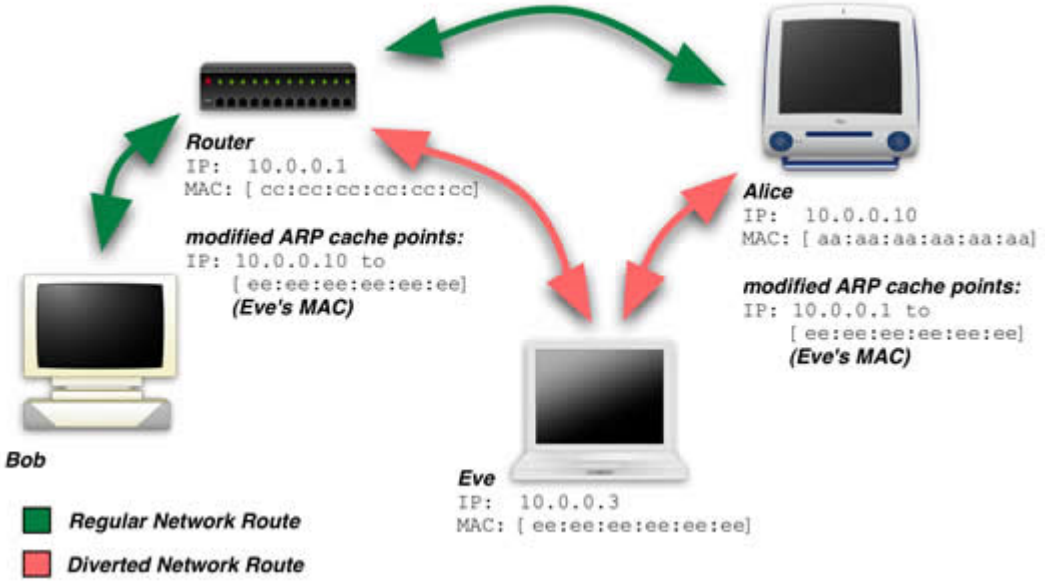
http://en.wikipedia.org/wiki/Electronic_signatures


Prohlížeč certifikátů:"*.plimus.com"
Obecné
Detaily
Tento certifikát byl ověřen pro následující použití:
Certifikát SSL serveru
Vydáno pro
Obecné jméno (CN) *.plimus.com
Organizace (O) Plimus Inc.
Jednotka organizace (OU) IT
Sériové číslo 54:3B:BF:C8:74:82:17:A5:BE:FC:CA:95:2A:86:94:59
Vydal
Obecné jméno (CN) VeriSign Class 3 Secure Server CA
Organizace (O) VeriSign, Inc.
Jednotka organizace (OU) VeriSign Trust Network
Platnost
Vydáno dne 28.5.2008
Platný do 29.5.2009
Otisky
Otisk SHA1 06:67:88:C6:9C:2C:3A:55:50:7C:48:94:01:AD:92:8F:A9:1A:71:DE
Otisk MD5 93:05:DE:38:58:E6:A9:FD:C6:EE:19:2F:FE:D7:95:A2
Zavřít

Bezpečnost

- Proč se v protokolech šifruje?
  - Vyměňujeme si informace s cílovým uzlem a nikomu po cestě po nich nic není
  - „Ti špatní“ by se mohli nabourat do naší komunikace a svévolně měnit posílané zprávy, aby dosáhli nějakých nekalých záměrů
  - „Ti špatní“ by mohli odposlouchávat naši konverzaci a zjištěné informace později zneužít
    - Např. číslo kreditní karty

- Nutnost autentizace
  - Existuje možnost útoku Man in the Middle



http://www.acm.org/crossroads/xrds11-1/wifi.html

  - Mezi dvěma komunikujícími uzly je někdo, kdo odposlouchává jejich komunikaci
    - Případně ji přesměruje, aby šla přes něj a on ji mohl měnit – to platí i pro Diffie-Hellman
  - Je třeba autentizace uzlů – prokázání se něčím, co Man in the Middle nezná a nemůže podvrhnout

- Autentizace
  - Znalost – např. heslo
  - Poznávací znak – např. id karta
  - Něco změřitelného – např. otisk prstu

  - Jednoduchá autentizace spočívá v dodání jména a hesla
    - Ke všem možnostem existuje možnost napadení
      - Sociální inženýrství, krádež, a …

  - Přísné metody vyžadují výměnu několika informací

Černá postava vyklepala na vrata složitou řadu zvukových značek. Otevřela se uzoučká špehýrka a tou vyhlédlo oko plné podezření.

„Významná sova houká jen v noci," zašeptal návštěvník a pokoušel se setřást z černé kápě dešťovou vodu.

„A přesto mnoho prošedlých vládců navrací se k mužům bez pána;" prohlásil hlas za zamřížovanou špehýrkou.

„Třikrát hurá dceři sestry staré panny," pokračovala promočená postava.

„Katovi připadají všichni žadatelé stejně vysocí."

„Což není pravdou, že zárodek růže ukrývá se v každém trnu?"

„Dobrá matka uvaří fazolovou polévku i toulavému chlapci," odtušil hlas za branou.

Rozhostilo se ticho přerušované jen zvukem padajícího deště. Pak příchozí zmateně zašeptal: „Cože?"

„Dobrá matka uvaří fazolovou polévku i toulavému chlapci."

Zavládla znovu dlouhá odmlka. Nakonec promáčená postava řekla: „Jsi si jistý, že věž postavená na špatných základech se nechvěje i při mávnutí křídel motýlích?"

„Houby. Je to fazolová polívka. Je mi líto." V rozpačitém tichu neodbytně šuměl déšť.

„A co takhle velryba v kleci?" nadhodil najednou promoklý návštěvník, který se pokoušel ukrýt před deštěm pod tím malým převisem, který poskytovala stříška nad branou.

„A co s ní má být?"

„Ta neměla by znát volné hlubiny mořské, když už to tedy chceš vědět."

„Aha! Velryba v kleci! Ty hledáš Osvícené bratrstvo ebenové noci! O tři domy dál!"

„A vy jste tedy vlastně kdo?"

„My jsme Zářící a prastaré bratrstvo Ee."

„Já měl dojem, že vy se scházíte v Přeslazené ulici?" ozval se promočený muž po chvilce.

„No jo, původně. Jenže víš, jak to chodí. Každý úterek si ty místnosti najímal spolek figurálních řezbářů. Pořád se to nějak pletlo dohromady."

„Aha. No tak v každém případě díky."

„Potěšení na mý straně." Špehýrka se zaskřípěním zapadla.

Postava v černém na ni chvilku znechuceně zírala a pak se šplouchánim vykročila dál ulicí. O tři domy dál byl skutečně neméně pochmurný portál. Stavitel se ani příliš nenamáhal zakrýt, že jeden návrh se dá zhodnotit dvakrát.

Terry Pratchett, „Stráže! Stráže!"

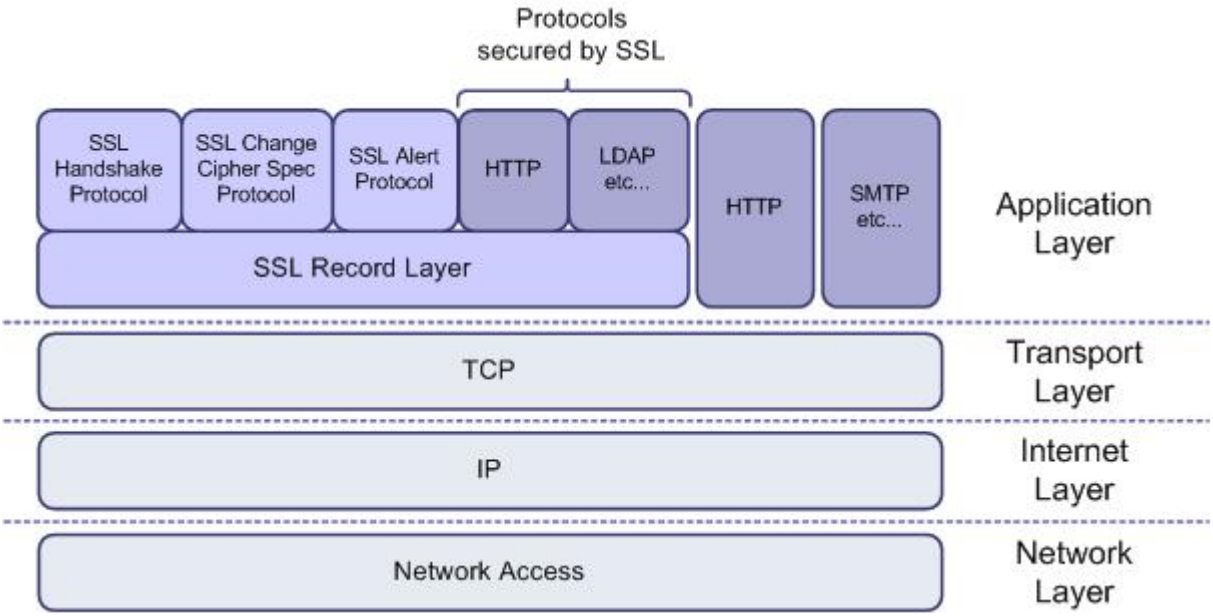
- Šifrované protokoly
  - Doposud uvedené protokoly jako např. HTTP a SMTP se nemění, pouze se zašifrují jejich zprávy dalším protokolem, který je na nižší úrovni

  - SSL, TSL
    - Secure Socket Layer – vyvinuto Netscape
    - Transport Security Layer – SSL převzatý a přejmenovaný IETF
      - Internet Engineering Task Force
    - Šifrování dat na prezentační vrstvě ISO/OSI
      - Tj. mezi TCP a protokolem jako např. HTTP, či SMTP
    - HTTPS
      - HTTP over SSL

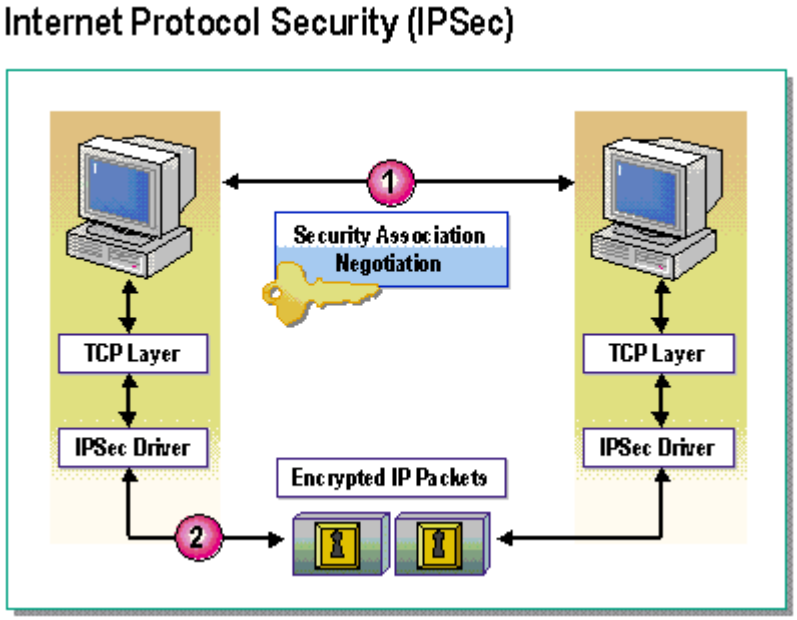
  - IPsec
    - Internet Protocol Security
    - Množina protokolů pro bezpečnou komunikaci po Internetu

    - Používají se na síťové (3) vrstvě ISO/OSI, kde je i IP
      - Mohou tak pohodlně zabezpečit protokoly vyšších vrstev
      - Tj. aplikace nemusí zajímat IPsec a přesto je možné komunikaci zabezpečit
      - SSL, TSL, SSH používají 4-7 vrstvu

  - SSH
    - Secure SHell
    - Nástupce Telnetu –zabezpečený kanál
    - Operuje na aplikační vrstvě TCP/IP modelu



http://www.securityfocus.com/infocus/1818



http://technet.microsoft.com/en-us/library/bb742596.aspx

- Mimo rozsah KIV/ZPS
  - SSL a TSL si mohou programátoři implementovat bez ohledu na OS
  - Pro IPsec musí existovat podpora v jádře OS
  - IPsec je systémově lepší, ale SSL/TSL se snáze dodá zákazníkovi – nemusí si pořizovat nový OS

Ověřovací server

- Kerberos, Single Sign On
  - Kerberos se používá v ZČU Orion
- Existuje centrální databáze uživatelů a jejich hesel
  - Databáze nemusí být nutně uložena jenom na jednom počítači – distribuované databáze
    - Mimo rozsah KIV/ZPS

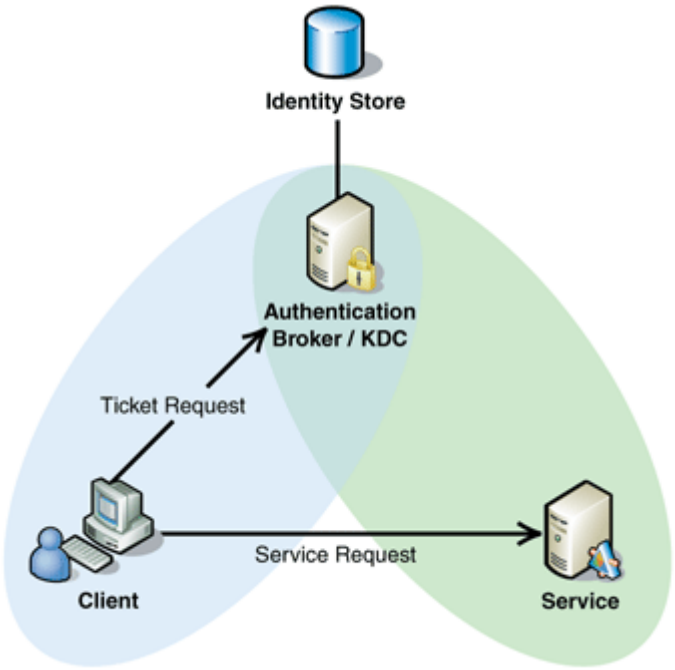
- Uživatel se přihlásí a ověřovací server mu poskytne tzv. token
  - Token je časově omezen
  - Token je identifikace uživatele ověřovacímu serveru

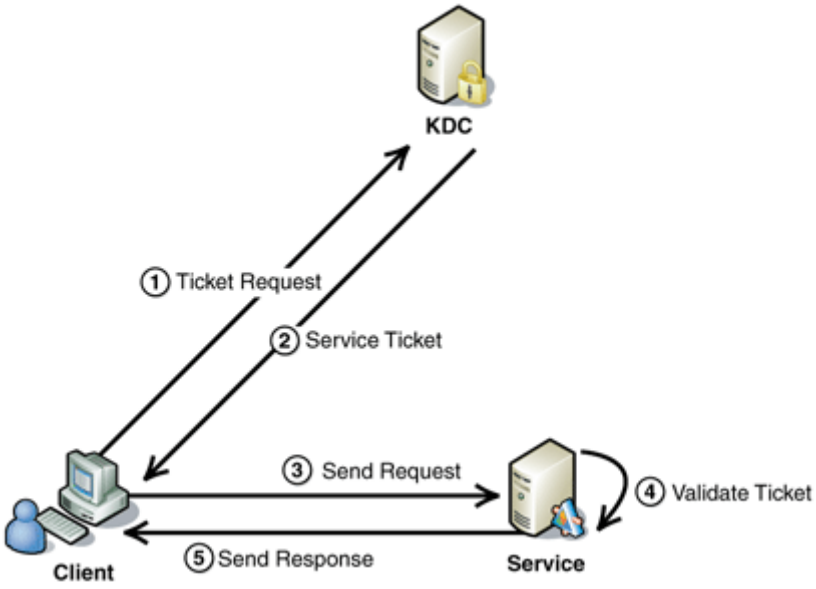
- V okamžiku, kdy se uživatel přihlašuje ke „spřáteleným“ serverům, místo jména a hesla se prokáže tokenem
- Spřátelený server přes token získá od ověřovacího serveru údaje o uživateli

- Uživatel se nemusí pořád někam přihlašovat
- Systém serverů má jednotnou reprezentaci uživatelů
  - Snazší údržba a správa
    - Když tomu ovšem správce rozumí:-)

- Je to však jeden klíč ke všemu
  - Co když ho získají „ti špatní“?

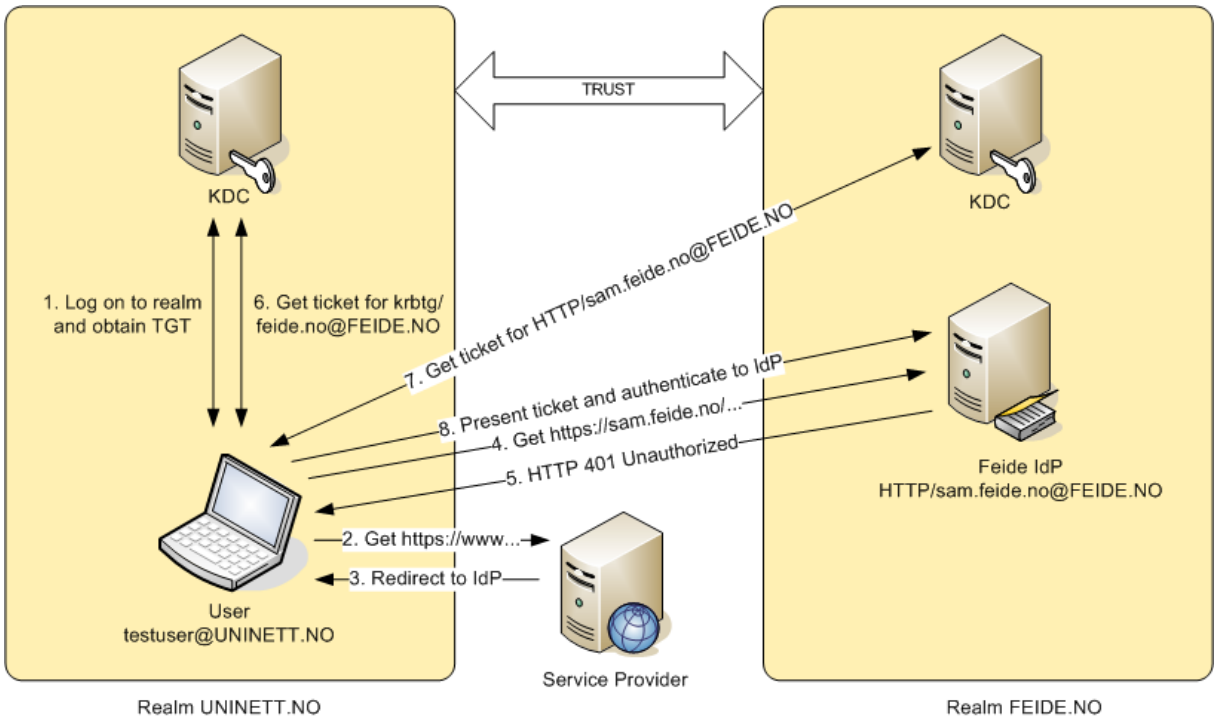
- Kerberos obecně





http://msdn.microsoft.com/en-us/library/aa480562.aspx

- Kerberos přes dvě domény
  - Pro zajímavost
  - Mimo rozsah KIV/ZPS



http://rnd.feide.no/content/feide-and-ssh-secure-shell

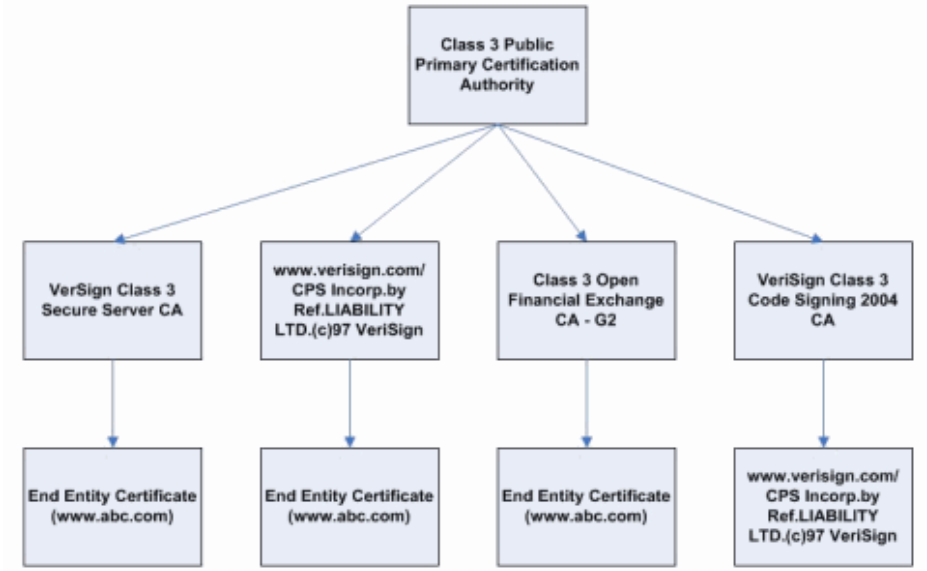
Certifikát

- Popis držitele
- Podpis vydavatele
- Platnost
- Účel vydání
- Veřejný klíč - viz elektronický podpis

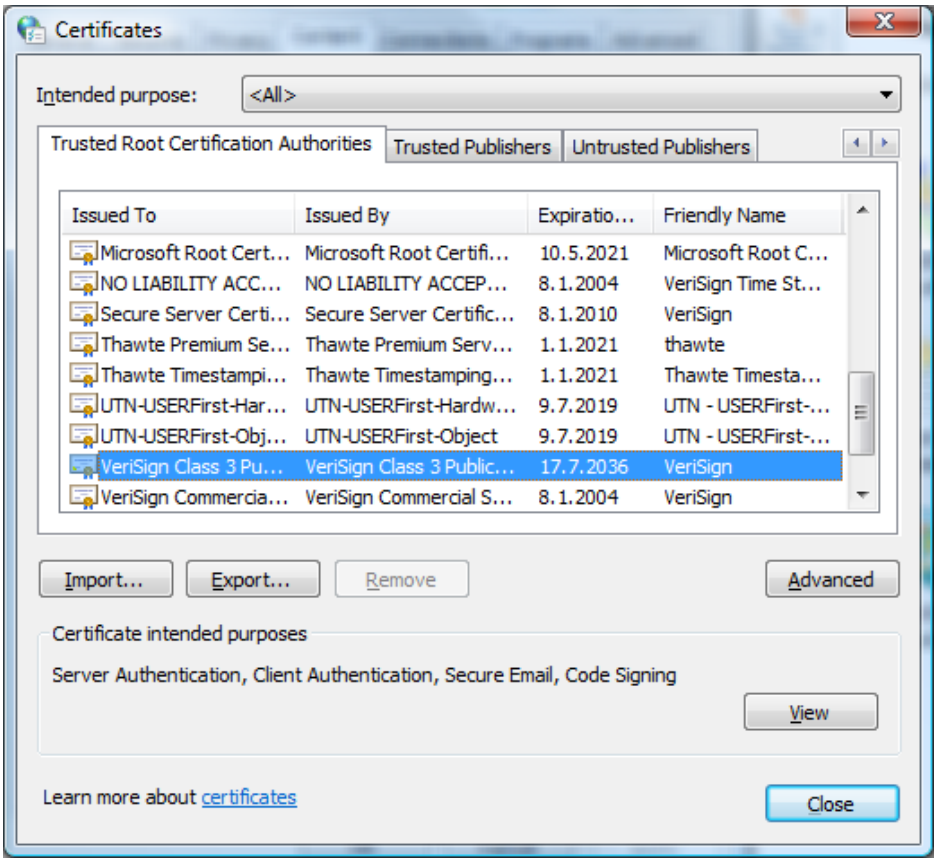
- Certifikát je považován za důvěryhodný
  - Jsou-li jeho hodnoty OK
  - A je-li považován za důvěryhodný i jeho vydavatel

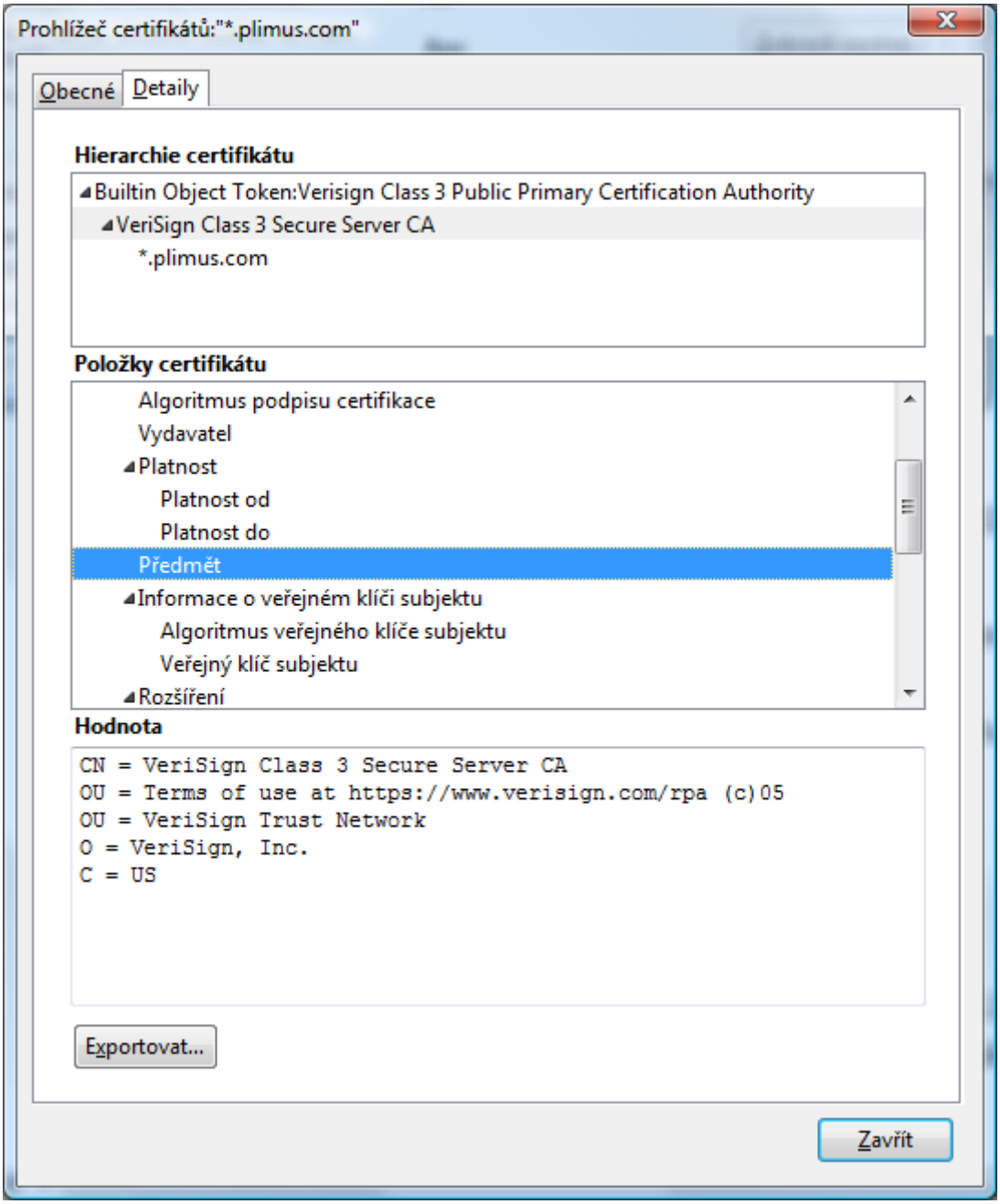
- Buď certifikát za důvěryhodný označí přímo uživatel
  - Případ ZČU, která si je vydává sama

- Nebo je jeho vydavatel kořenovou autoritou, popř. ho software zná – má nainstalovány příslušné certifikáty
- Anebo se postupně prohledají vydavatelé certifikátu až po nejbližší známou a důvěryhodnou certifikační autoritu (vydavatele)
    - Certifikát lze zneplatnit – vydavatelem označen KO

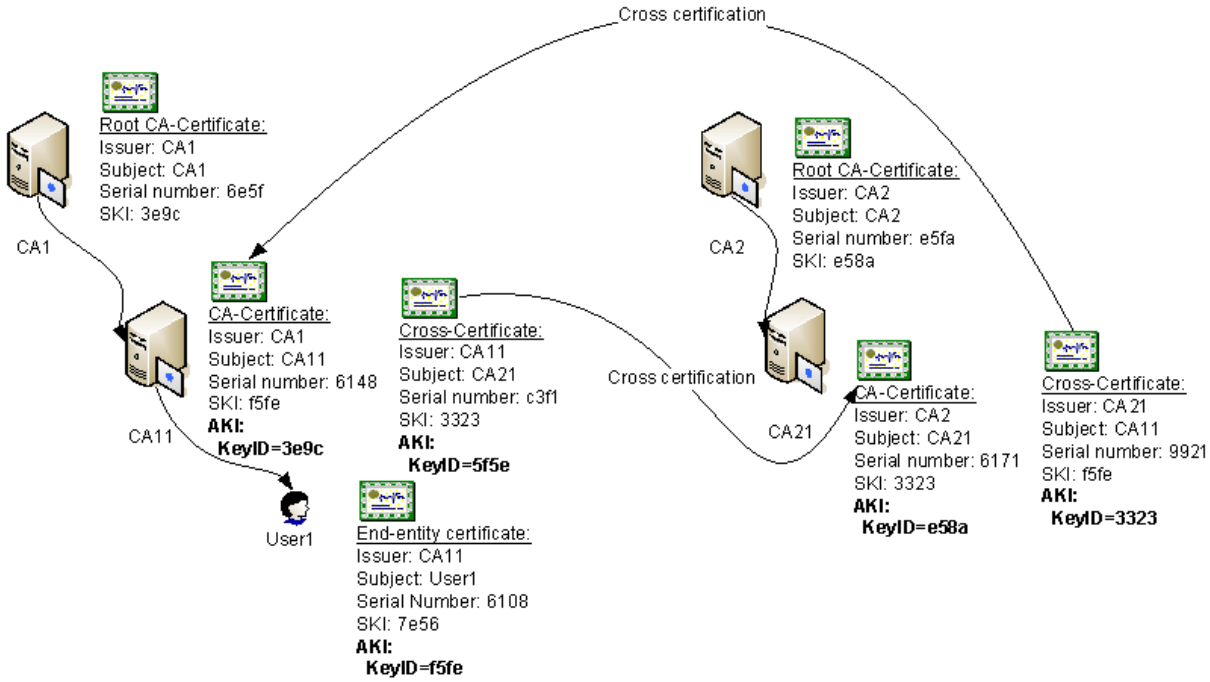


https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AD4&actp=LIST




Prohlížeč certifikátů:"*.plimus.com"
Obecné
Detaily
Hierarchie certifikátu
Builtin Object Token:Verisign Class 3 Public Primary Certification Authority
VeriSign Class 3 Secure Server CA
*.plimus.com
Položky certifikátu
Algoritmus podpisu certifikace
Vydavatel
Platnost
Platnost od
Platnost do
Předmět
Informace o veřejném klíči subjektu
Algoritmus veřejného klíče subjektu
Veřejný klíč subjektu
Rozšíření
Hodnota
CN = VeriSign Class 3 Secure Server CA
OU = Terms of use at https://www.verisign.com/rpa (c)05
OU = VeriSign Trust Network
O = VeriSign, Inc.
C = US
Exportovat...
Zavřít

- Pro zajímavost
  - Mimo rozsah KIV/ZPS
  - Existuje i možnost vzájemné certifikace
    - Cross-Certification



http://technet.microsoft.com/en-us/library/bb457027.aspx

Heslo

- Nemělo by se jednat o názvy věcí, osob, zvířat z blízkého okolí, nebo jinak známých – slovníkový útok
- Stejně tak data narození a jiná čísla, která se dají předpokládat – útok na základě profilu napadaného
- Triky jako slovo pozpátku nejsou pro hackera problémem

- K prolomení hrubou silou se vyzkouší možné kombinace
  - Čím více znaků, tím více celkových kombinací
  - Čím více typů znaků, tím opět více celkových kombinací
    - Písmena, číslice, zvláštní znaky
- Nejlépe si ho jenom pamatovat a měnit v náhodných, dostatečně krátkých intervalech
- Místo hesla lze použít i privátní klíč – např. v SSH, 4kB

Steganografie

- Pro zajímavost, mimo rozsah KIV/ZPS

- Šifrování je metoda utajení, která neskrývá svůj záměr
- Steganografie je metoda utajení záměru utajit

- PNG
  - Grafický formát
  - Na rozdíl od JPG používá neztrátovou kompresi
    - Tj. body obrazu (pixely) jsou identické před zakódováním obrazu i po jeho dekódování
      - Pixel = Picture Element

- Obdélníky obrázku vpravo jsou následky ztrátové komprese JPG – změnily se hodnoty pixelů

- Jeden pixel je při zobrazování reprezentován čtveřicí ARGB
  - A – Alpha, průhlednost pixelu
  - R, G, B – červená, zelená a modrá, barevné složky pixelu jejichž smícháním dojde k vytvoření požadované barvy
  - Každá složka z ARGB má 8 bitů, tj. dohromady 32

- PNG umožňuje uložit pixely ve formátu ARGB
- Pokud si z každé složky vezmeme nejméně významný bit, lidské oko rozdíl oproti originálu nepozná

- Máme k dispozici mobil s 3,4 MiPix foťákem
- Tj. 3,4x1024x1024 obrazových bodů
  - Krát 4 (počet bitů, které máme v každém pixelu)
    - Děleno 8 je počet bytů, které takto můžeme ukrýt do obrázku

- Tj. 1, 7 MiB, kterou můžeme odeslat
- Pokud by nám stačil text v Western Character Set
  - 1,7*8/7 = 2 037 233 znaků k odeslání
    - Kolik je to např. Shakespearových her?
    - Např. 2. přednáška o IP má 25 446 znaků včetně mezer
- Zdánlivý nepoměr velikostí je dán kompresí obrazu a tím, že 3,4 MiPix je počet bodů obrazu, ne velikost souboru

- Utajovaný text lze samozřejmě ještě před vložením do obrazu zašifrovat
- Při vkládání do obrazu se dále ještě může použít transpozice – ne jenom po sloupcích/řádcích
  - A využít nějaké nelineární závislosti
- Změněný obraz bude hůře komprimovatelný -> odhalení

Eliptické křivky

- Pro zajímavost, mimo rozsah KIV/ZPS
- Elliptic Curve Cryptography (ECC)

- Stejně jako Diffie-Hellman, jde o třídu matematických problémů, které jsou extrémně těžké k vyřešení, není-li známo, jak byly vytvořeny
  - Lze je ovšem řešit hrubou silou, je-li objem dat dostatečně malý

- Privátním klíčem je tajemství, jak byl problém vytvořen
- Veřejným klíčem je pak problém sám

- Např. vezmeme dvě pročísla (privátní klíč) a vynásobíme je (veřejný klíč)
  - Jednoduchá operace, ale jak zpětně vypočítat, která dvě prvočísla se vynásobila?
  - S čísly nad 1024 bitů (doporučeno pro RSA) jsou výpočetní nároky příliš vysoké
    - Dokud nedojde k dalšímu pokroku např. ve výpočtu faktorizace celých čísel

- Diskrétní logaritmus je problém $a^b = c$

- Eliptická křivka je problém $y^2 = x^3 + ax + b$

- K dosažení stejné míry bezpečnosti eliptickým křivkám stačí kratší heslo než předešlým metodám