BUSLab

Brno University Security Laboratory

Praktická kryptografie, nástroje a ochrana soukromí

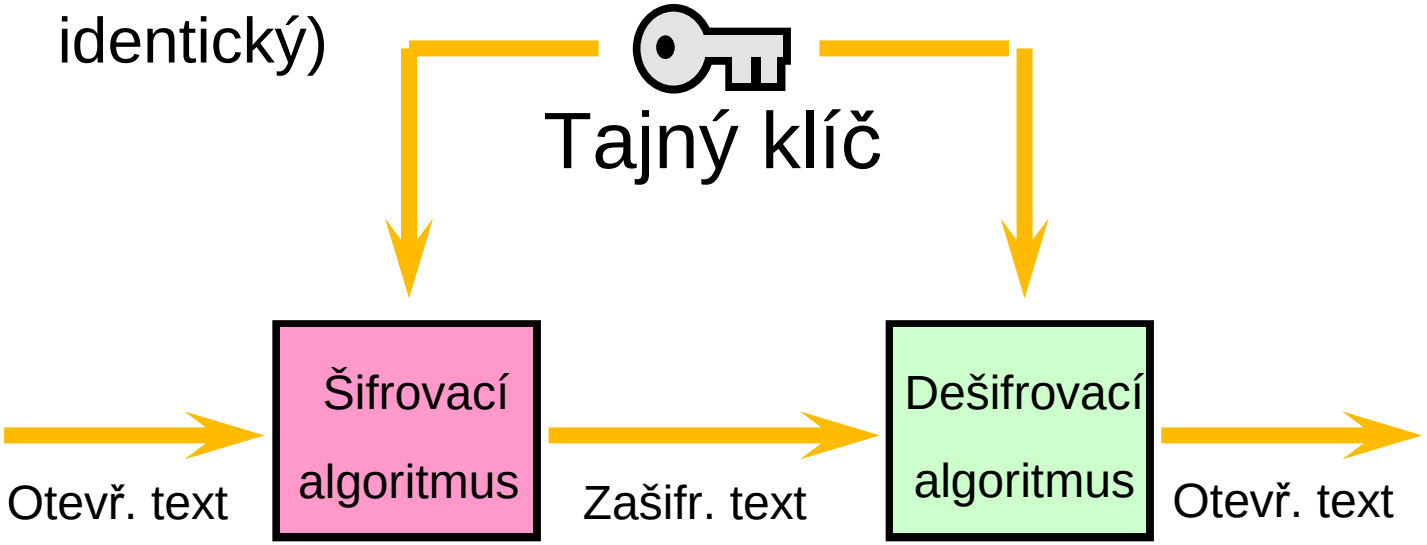
Petr Švenda <svenda@fi.muni.cz>
Fakulta informatiky, Masarykova univerzita, Brno
Laboratoř Bezpečnosti a aplikované kryptografie

Kde kryptografie pomáhá

1. Důvěrnost dat
2. Integrita dat
3. Autenticita dat (integrita a ověření původu)
4. Nepopiratelnost
5. Autentizace a autorizace uživatelů/strojů

Symetrická kryptografie

- Symetrická kryptografie
  - (správněji kryptografie se symetrickým klíčem)
  - stejným (tajným) klíčem se šifruje i dešifruje
  - (algoritmus šifrování a dešifrování nemusí být ale identický)

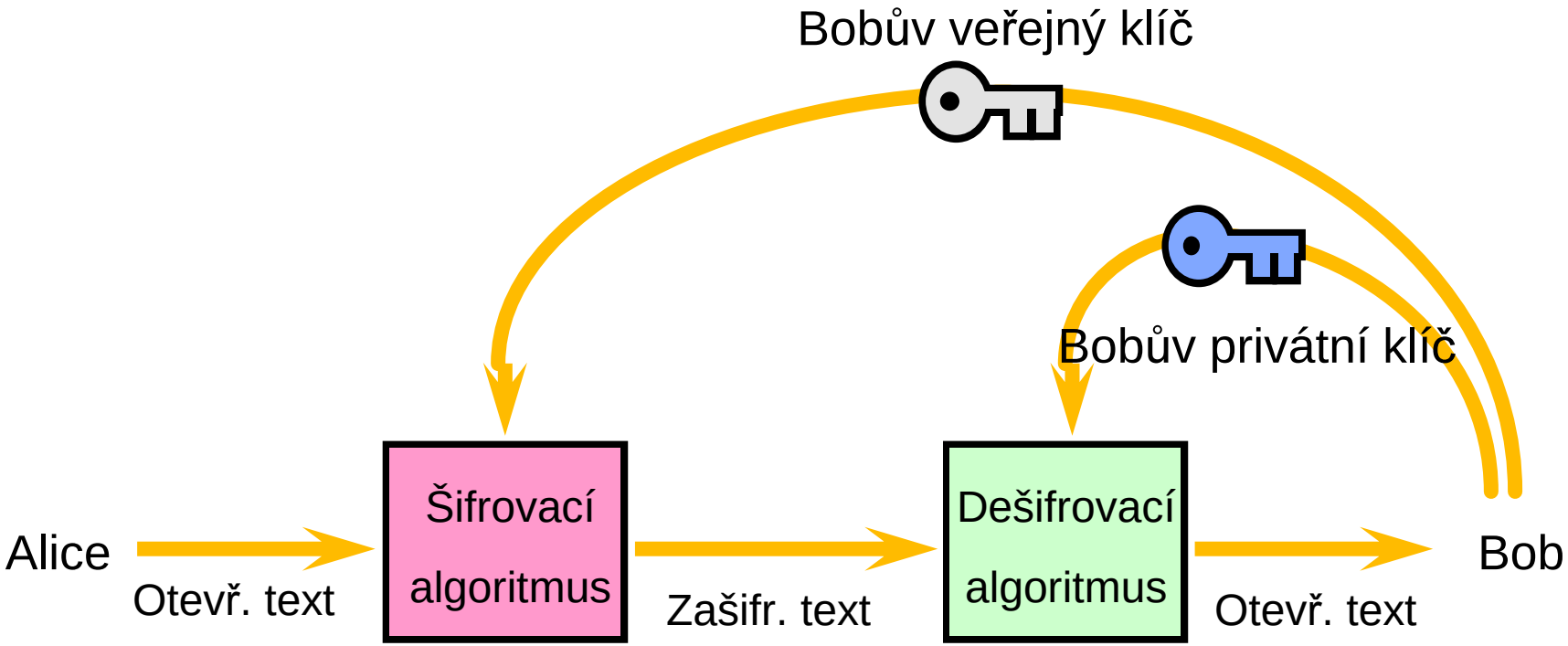


Převzato z: *Network and Internetwork Security* (Stallings)

Asymetrická kryptografie

- Asymetrická kryptografie
  - pracuje se se dvěma klíči (soukromým a veřejným)
  - veřejný klíč mají všichni, soukromý klíč jen jeden
- Co „transformujeme“ veřejným klíčem lze „odtransformovat“ jen privátním klíčem
  - šifrování pro konkrétního jedince
- Co „ transformujeme“ soukromým klíčem lze „odtransformovat“ veřejným klíčem
  - podepisování konkrétním jedincem

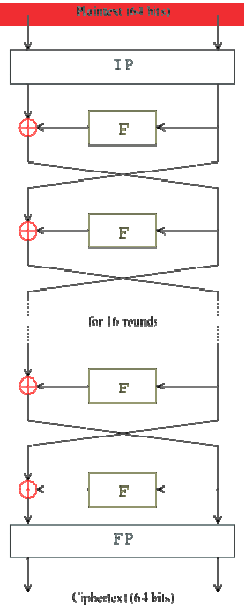
Schéma šifrování veřejným klíčem

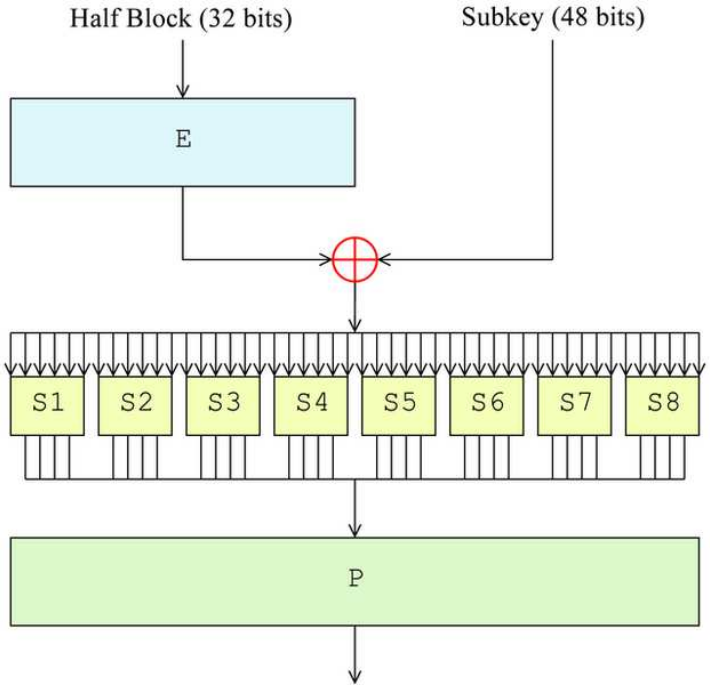


Převzato z: *Network and Internetwork Security* (Stallings)

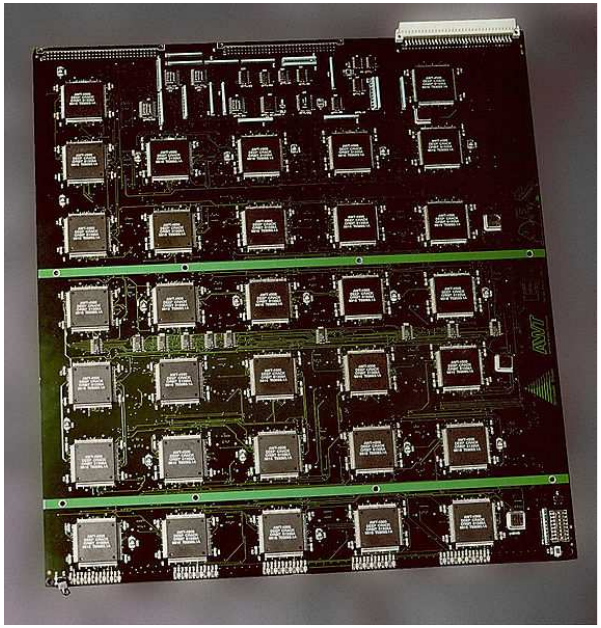
Symetrická kryptografie - DES

- DES (Data Encryption Standard)
  - IBM+NSA, 1977
  - 56bitový klíč (72,057,594,037,927,936 možností)
  - algoritmus veřejný, ale některé části bez zdůvodnění
- Základem je runda obsahující
  - přimíchání klíče (xor)
  - substituční část
  - permutační část
- Využívá tzv. Feistelova schéma
  - opakování základní rundy (16x)
- Stále široké využití
  - banky (3DES), starší systémy





EFF DES cracker (1998)



- Krátký klíč DESu kritizován od počátku
  - vláda i firmy ale mají tendenci ignorovat
- Praktická demonstrace zranitelnosti
  - Electronic Frontiers Foundation (EFF)
  - hrubou silou zkouší všechny možnosti klíče
  - 4.5 dne/klíč
- Předpokládá se existence zařízení schopného hledat klíč v téměř „reálném čase“ (NSA)
- Délku klíče lze řešit pomocí tří DESů za sebou (3DES)
  - blok je zašifrován třikrát různými klíči
  - stále široce používané

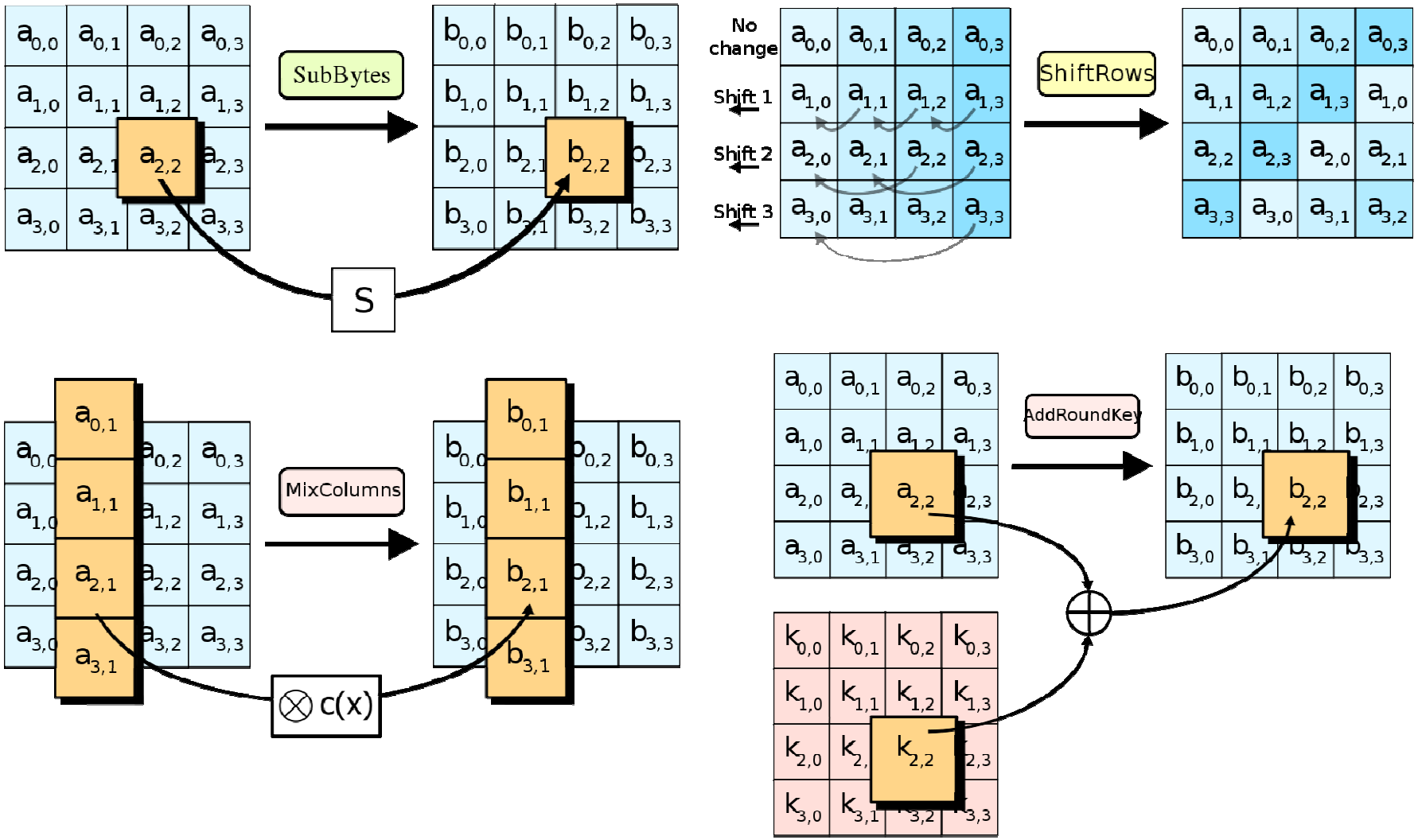
Čas potřebný pro prohledání prostoru možných klíčů (sym. krypt.)

Délka klíče (bit)	Počet možných klíčů	Čas potřebný při 10^6 dešifrování/µs
32	$2^{32} = 4.3 \times 10^9$	2.15 ms
56	$2^{56} = 7.2 \times 10^{16}$	10 hod
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} let
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} let

Symetrická kryptografie - AES

- AES (Advanced Encryption Standard)
  - tříkolová soutěž NIST, vybrán Rijndael (Belgie)
  - 128/196/256 bitů klíč, 16 bajtů blok
  - velice rychlý v SW i HW, zdůvodnění návrhu
- Základní runda je opakovaná 10x (14x pro delší klíče)
- Hrubou silou už nelze projít celý prostor klíčů
  - může ale existovat nedokonalost algoritmu, která prostor sníží
  - kryptoanalýza

Runda algoritmu AES

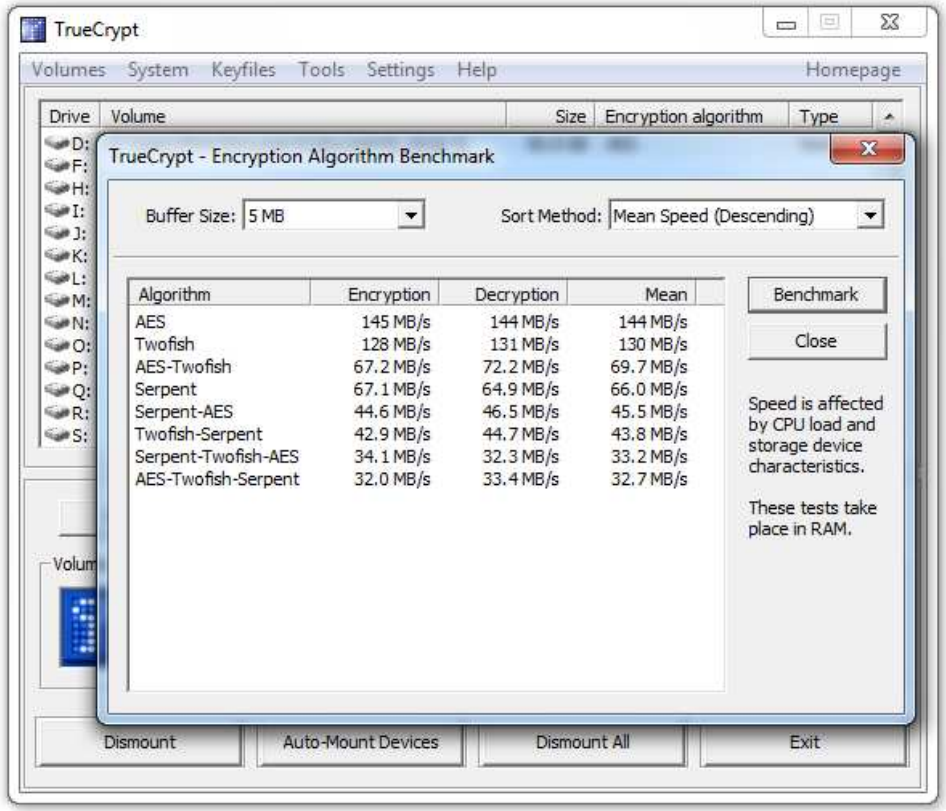


Šifrování dat na disku – TrueCrypt 6.3a

- Volně dostupný nástroj pro transparentní šifrování dat na disku *www.truecrypt.org*
  - data na disku jsou vždy šifrovaná
  - dešifrovaná data pouze v RAM paměti
- Hlavička disku obsahuje dlouhý klíč zašifrovaný heslem uživatele
  - lze použít dodatečné klíčové soubory nebo čipovou kartu
- Lze šifrovat systémový disk i přenosná média
  - nejčastěji ale šifrován soubor připojitelný jako virtuální disk
- Ideální pro použití na přenosných počítačích
  - ztráta počítače nevede k vyzrazení dat
  - dobrá ochrana proti zvědavým dětem/rodičům ☺

TrueCrypt – test rychlosti algoritmů

- Spuštění testu
  - *Tools->Benchmark*
- AES, Twofish, Serpent + jejich kombinace



Srovnání rychlosti algoritmů

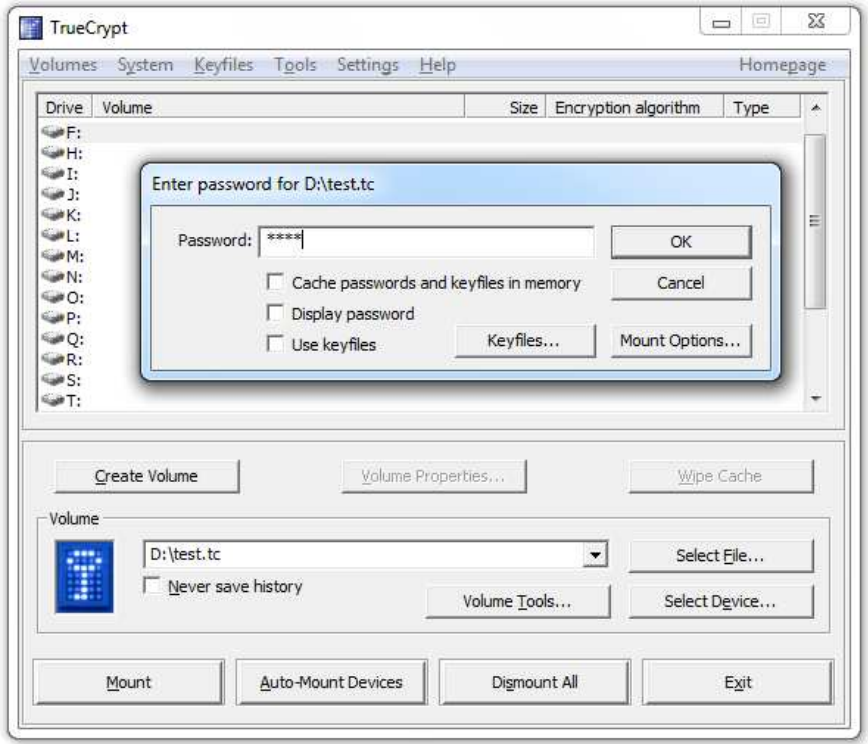
- http://www.cryptopp.com/benchmarks.html
- Intel Core 2 @ 1.83 GHz procesor

Algoritmus	rychlost
3DES	13 Mb/sec,
AES 128bit	139 Mb/sec,
RSA 1024bit (soukromý klíč)	0.7 Mb/sec
RSA 1024bit (veřejný klíč)	12.8 Mb/sec

asym. krypto 10-100x pomalejší

TrueCrypt – praktické cvičení

1. Instalace, spuštění
   - systémový ovladač (administrátorské práva)
2. Vytvoření nového virtuálního disku
   - *Tools->Volume Creation Wizard*
   - encrypted file container
   - standard TrueCrypt volume
   - umístění souboru s virt. diskem
   - šifrovací algoritmus
   - velikost disku
   - heslo pro přístup,sběr entropie
   - formátování
3. Připojení disku
   - výběr volného písmenka
   - soubor s virtuálním diskem
   - mount, zadání hesla



- Asymetrická kryptografie

Digitální podpis

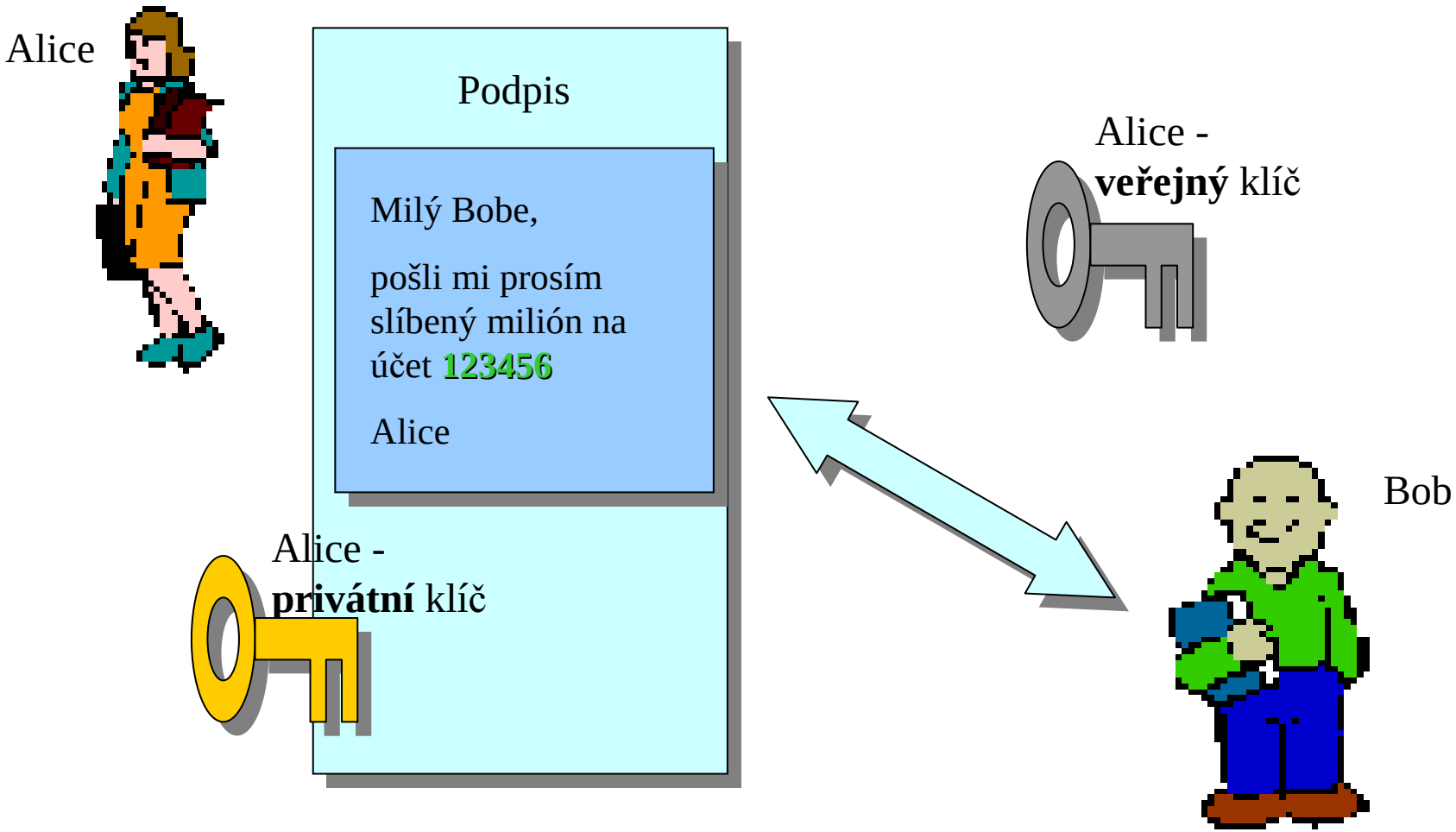
- Jedna ze stěžejních aplikačních oblastí kryptografie
- Využití asymetrické kryptografie k podpisu ale zjištěno až po letech znalosti principů šifrování
- Pouze majitel privátního klíče může vytvořit podpis
- Podpis mohou verifikovat všichni pomocí veřejného klíče

Digitální podpis bez certifikátu - naivně

1. Alice si vygeneruje dvojici veřejný-soukromý klíč
2. Alice zveřejní veřejný klíč
   - cokoli co lze ověřit tímto klíčem jsem podepsala
3. Bob si stáhne veřejný klíč
4. Bob může nyní může ověřit podpis od Alice

- Problém?

Digitální podpis – naivní řešení



Digitální podpis – problém?

Eva

Podpis

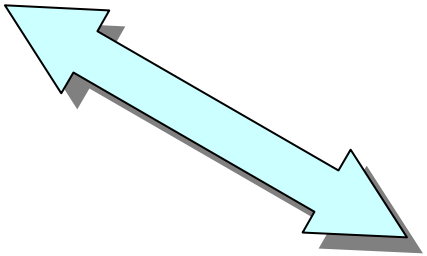
Milý Bobe,

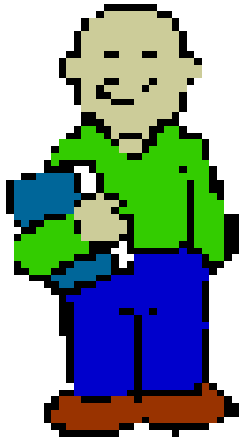
pošli mi prosím slíbený milión na účet **6666666**

Alice

Eva - **privátní** klíč

Eva - **veřejný** klíč





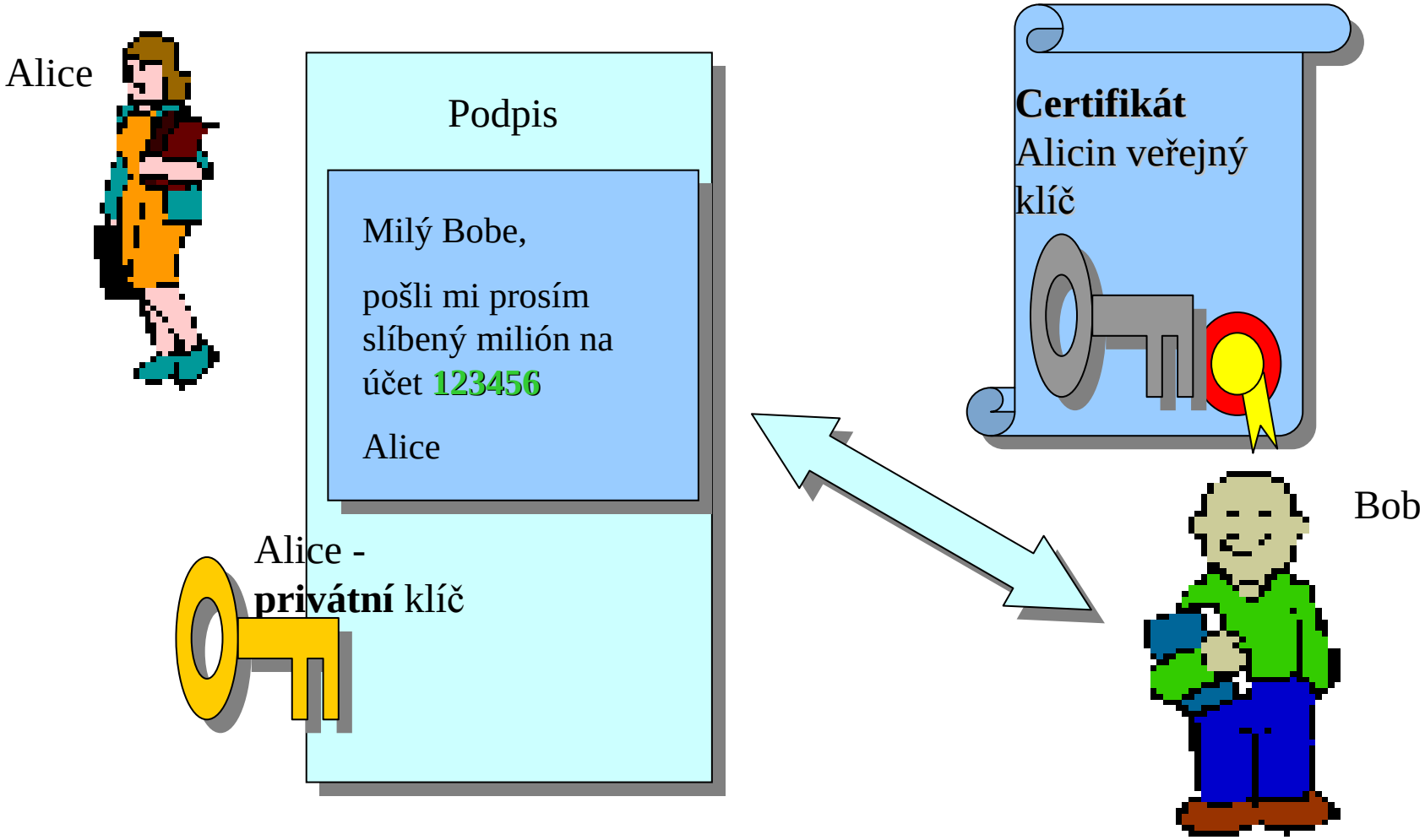
Bob

Digitální podpis bez certifikátu - lépe

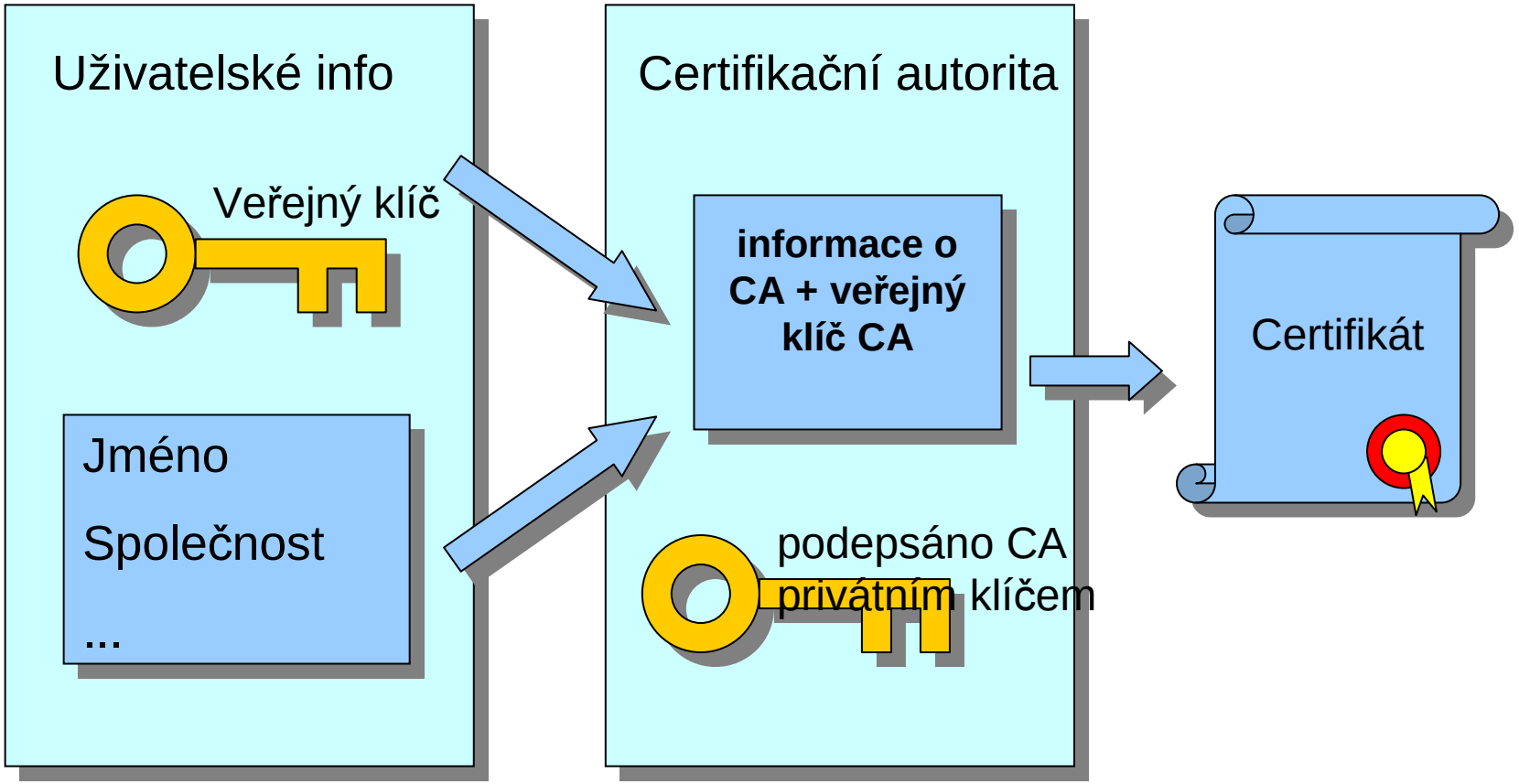
1. Alice si vygeneruje dvojici veřejný-soukromý klíč
2. Alice předá osobně veřejný klíč Bobovi
   - cokoli co lze ověřit tímto klíčem jsem podepsala já
3. Bob může nyní může ověřit podpis od Alice
4. Eva už nemůže podstrčit svůj klíč
   - Bob již veřejný klíč od Alice má

- Problém: co když Alice nemůže dát klíč osobně?
  - neznají se (znáte pana Seznama a pana Googla?)
  - geografická vzdálenost...

Certifikát veřejného klíče

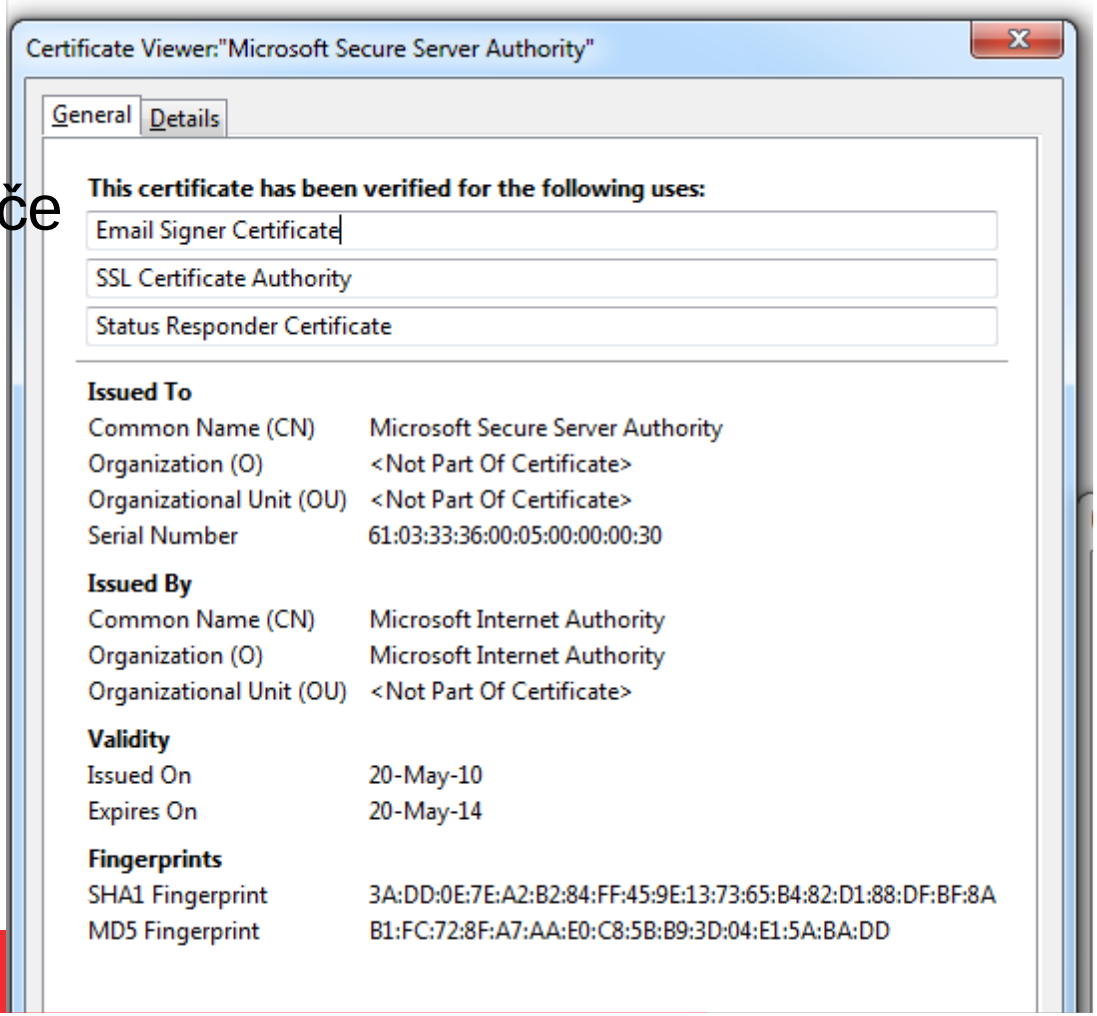


Co je certifikát?



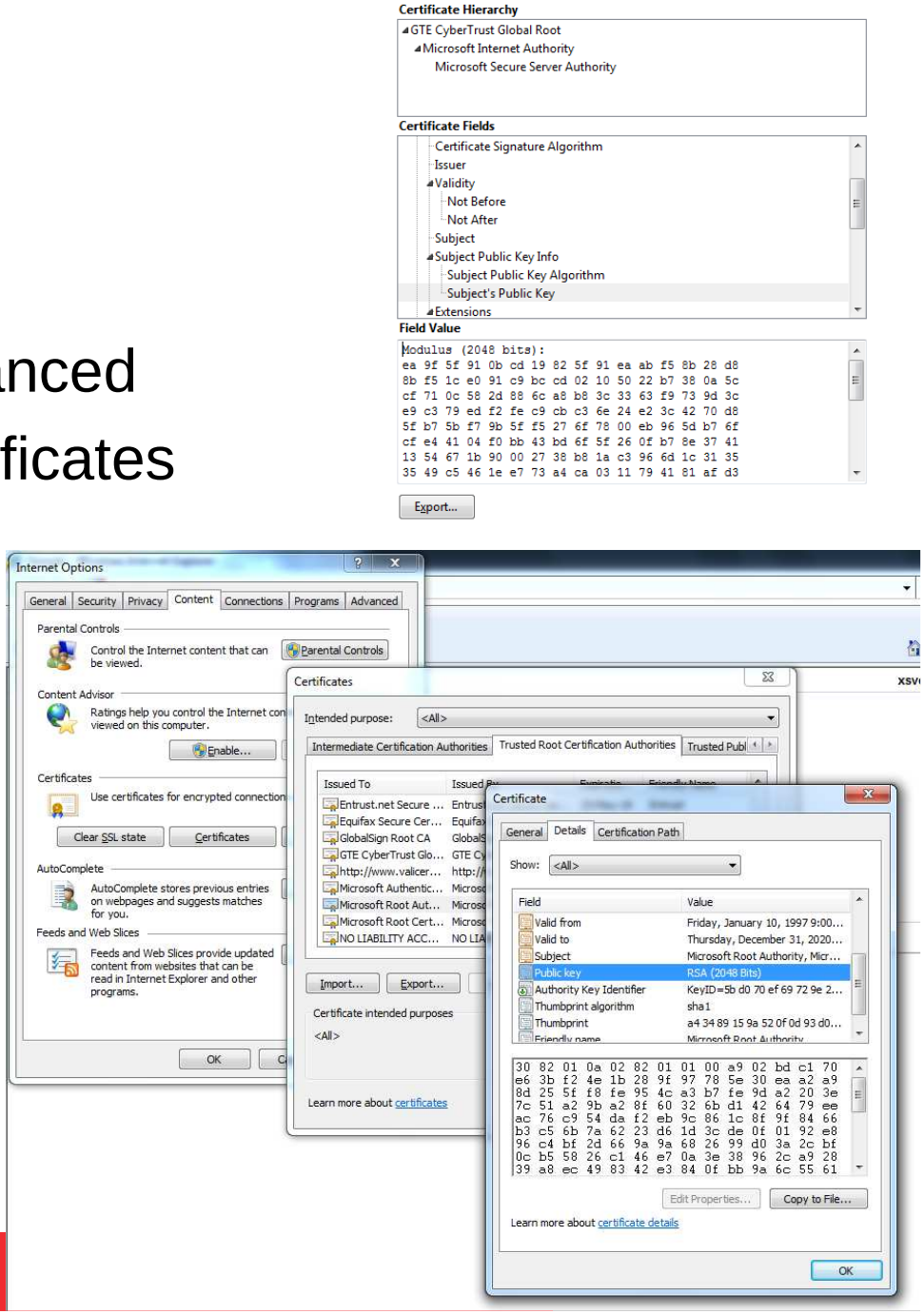
Co je certifikát?

- Balík dat podepsaný certifikační autoritou
  - veřejný klíč
  - majitel certifikátu
  - povolené použití klíče
  - rozsah platnosti
  - použité algoritmy
  - další info...
  - podpis autority

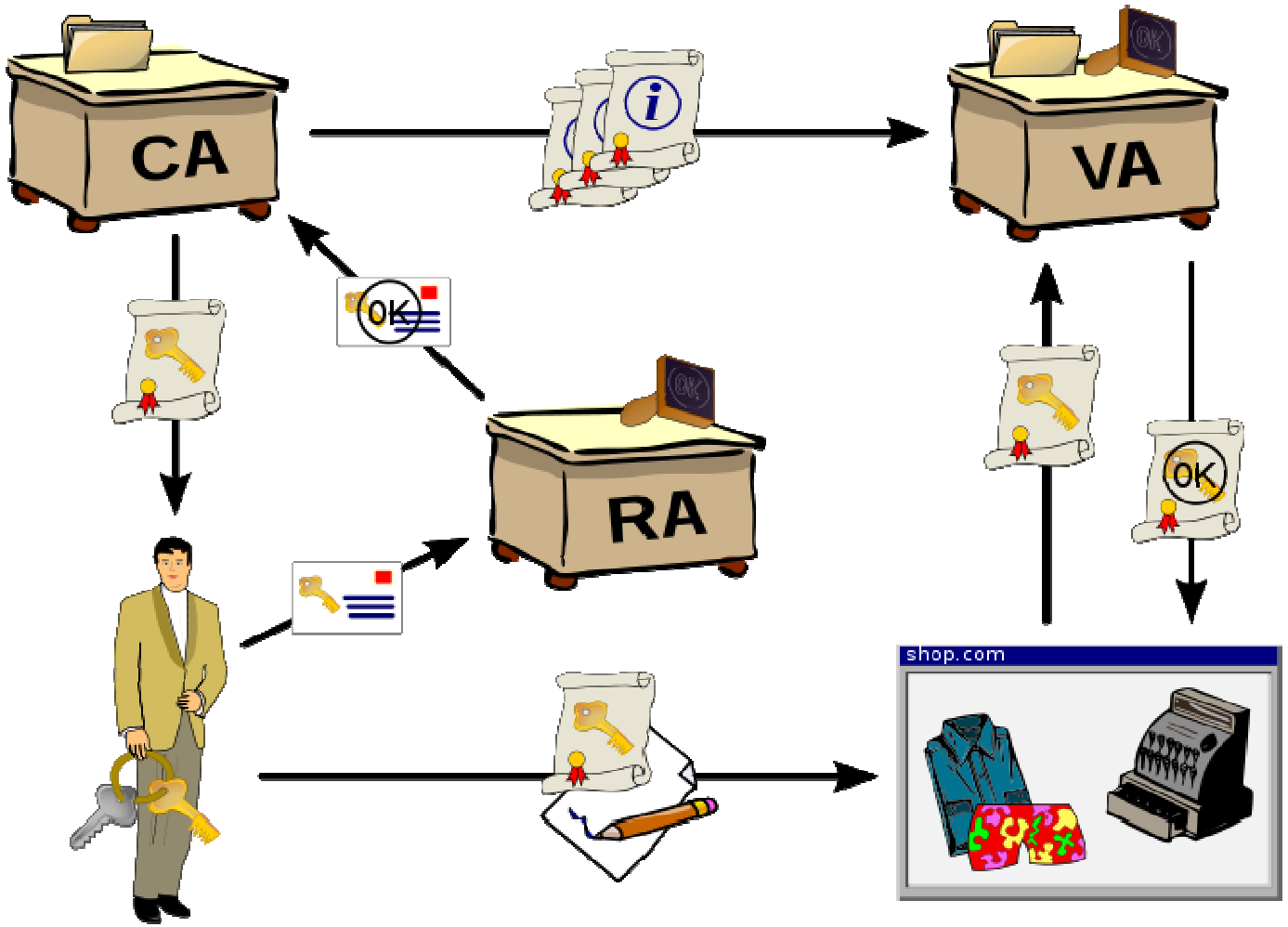


Detaily certifikátu

- Firefox
  - Tools→Options → Advanced
  - Encryption → View certificates
- Internet Explorer
  - Tools→Internet Options
  - Content →Certificates



Digitální podpis s certifikátem (PKI)

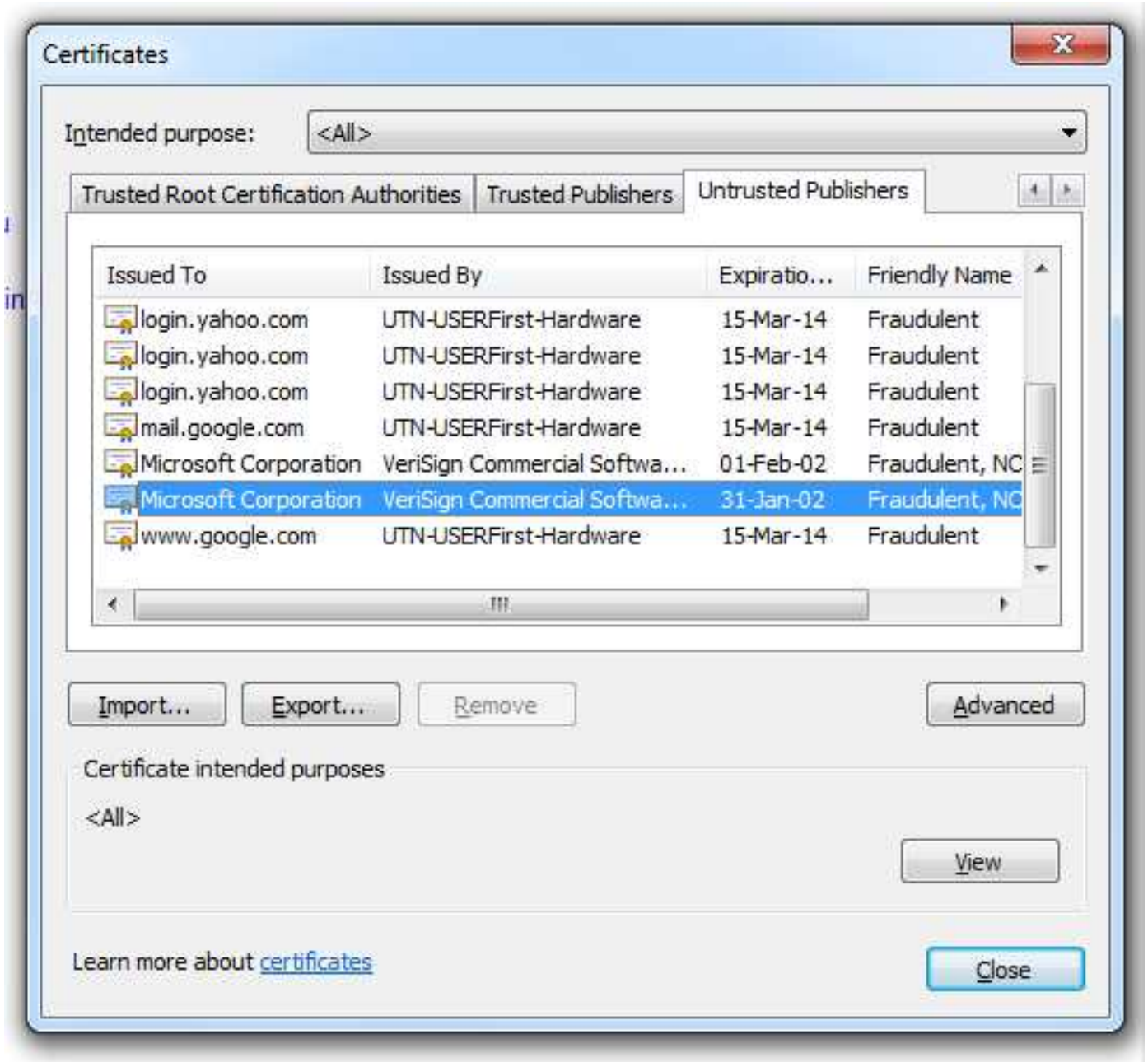


Kdo může dělat certifikační autoritu?

- V zásadě kdokoli ☺
- Problém je v důvěře
  - Bob musí věřit autoritě, že Alici dobře zkontrolovala
  - Bob musí věřit autoritě, že neudělala v procesu chybu
  - Bob musí věřit, že autorita nebyla ovládaná útočníkem

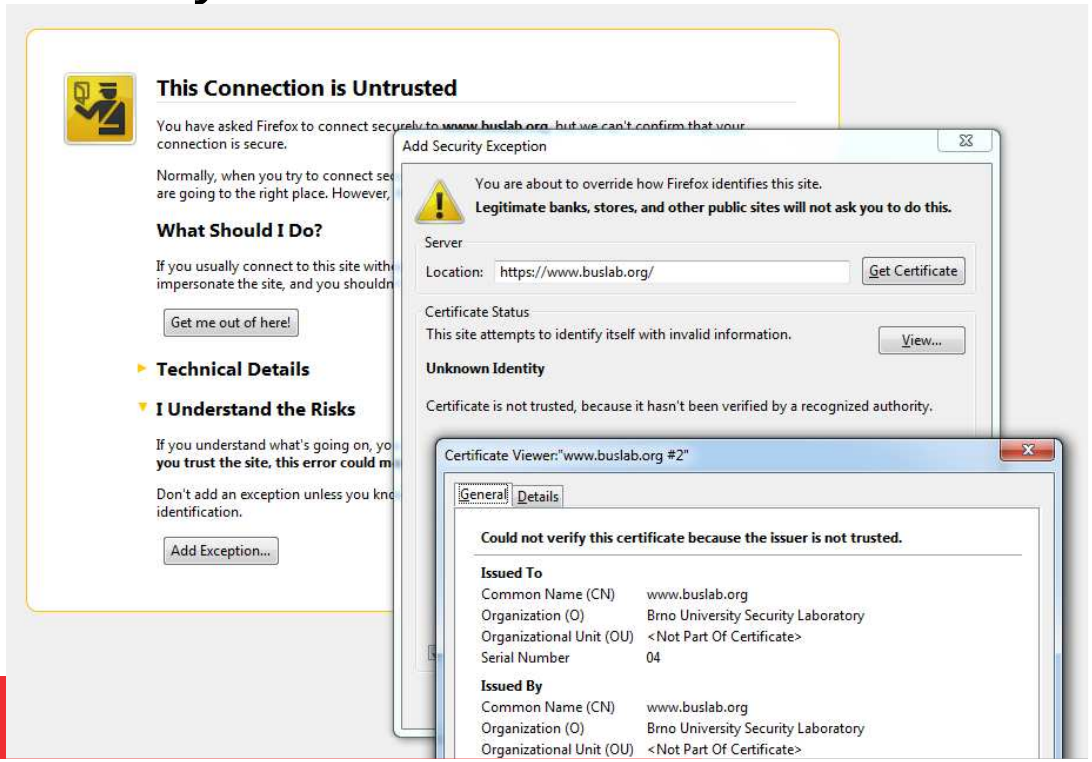
Problémy s certifikáty I.

- Certifikát musí někdo důvěryhodný vystavit
  - např. placená autorita (I.CA, Verisign, Comodo...)
- Jak moc je důvěryhodná?
  - 15. března 2011 kompromitována autorita Comodo
- Vydány falešné certifikáty pro tyto domény
  - *mail.google.com*
  - *login.yahoo.com*
  - *login.skype.com*
  - *login.live.com*
  - ...
- Útočník se nyní může vydávat za tyto servery
  - klíče revokovány, ale...


Certificates
Intended purpose:
<All>
Trusted Root Certification Authorities
Trusted Publishers
Untrusted Publishers
Issued To
Issued By
Expiratio...
Friendly Name
login.yahoo.com
UTN-USERFirst-Hardware
15-Mar-14
Fraudulent
login.yahoo.com
UTN-USERFirst-Hardware
15-Mar-14
Fraudulent
login.yahoo.com
UTN-USERFirst-Hardware
15-Mar-14
Fraudulent
mail.google.com
UTN-USERFirst-Hardware
15-Mar-14
Fraudulent
Microsoft Corporation
VeriSign Commercial Softwa...
01-Feb-02
Fraudulent, NC
Microsoft Corporation
VeriSign Commercial Softwa...
31-Jan-02
Fraudulent, NC
www.google.com
UTN-USERFirst-Hardware
15-Mar-14
Fraudulent
Import...
Export...
Remove
Advanced
Certificate intended purposes
<All>
View
Learn more about certificates
Close

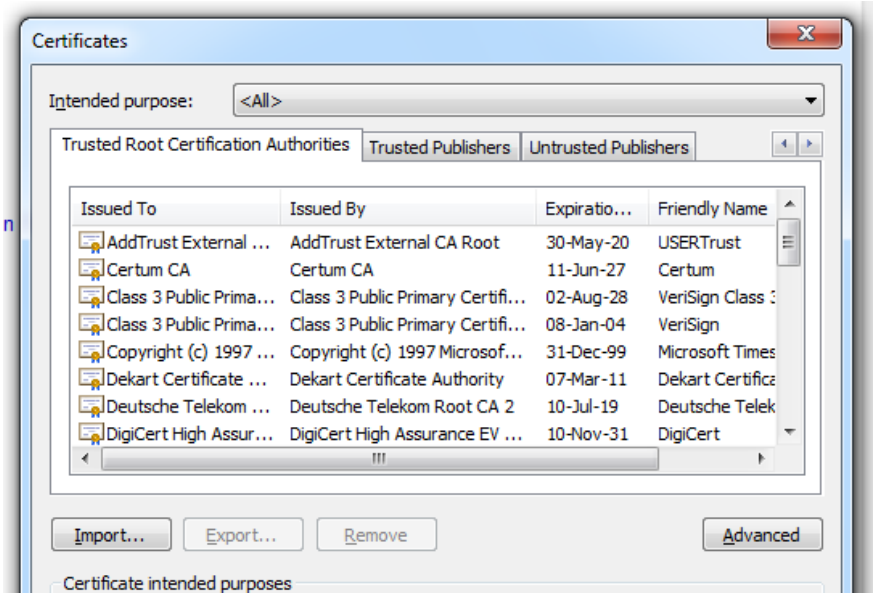
Problémy s certifikáty II.

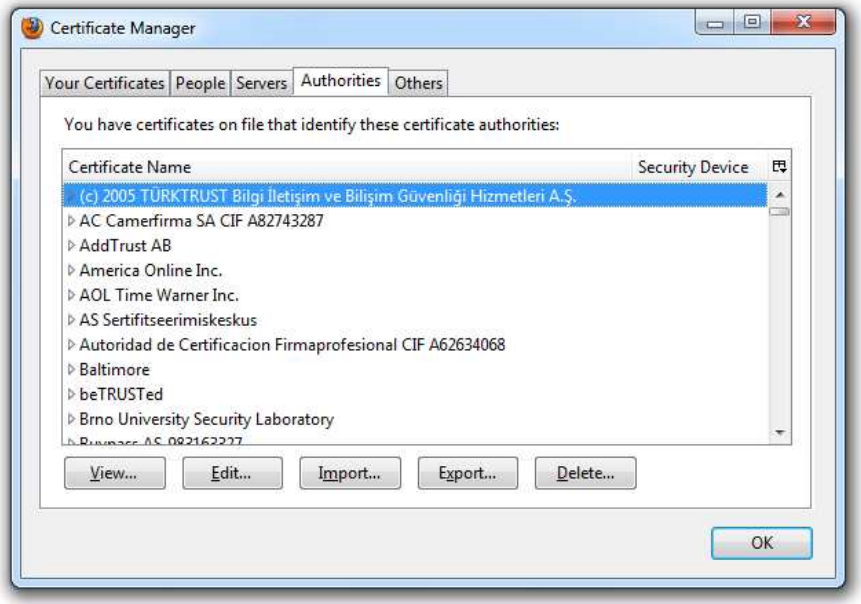
- Jakým řekneme, že autoritě věříme?
  - zkuste jít na https://buslab.org
- Velké množství stránek není certifikováno
  - uživatel odklikne bez rozmyslu



Problémy s certifikáty III.

- Kterým autoritám vlastně věříme?
- Předinstalované certifikáty v OS/prohlížeči
  - v současné době desítky autorit
  - některé přímo kontrolovány různými vládami...





Šifrování a podepisování data komunikace

- Cílem je buď utajit obsah zprávy nebo zajistit autentičnost původu dat (nebo obojí)
- Pretty Good Privacy www.pgp.com
  - nyní komerční produkt, některé části stále volné
    - PGP Desktop Trial Software
  - generování vlastního páru klíčů, správa uživatelů, šifrování, podepisování mailů, podepisování software...
- GnuPG - volná verze, kompatibilní s PGP www.gnupg.org
- Lze integrovat do poštovního klienta
  - Thunderbird + Enigmail + GPG (***enigmail**.mozdev.org*)
  - MS Outlook + PGP Mail

PGP/GPG – symetrické šifrování

1. Stažení GnuPG 1.4.10 (www.gnupg.org)
2. Zašifrování souboru symetrickou šifrou (např. AES)
   - gpg.exe --cipher-algo AES -c test.txt
   - zadání šifrovacího hesla/klíče
   - vznikne soubor test.txt.gpg
3. Dešifrování souboru symetrickou šifrou
   - gpg.exe --cipher-algo AES -d test.txt.gpg
   - zadání šifrovacího hesla/klíče

Soubor test.txt.gpg je při opakovaném šifrování stejným klíčem různý – proč?

PGP – praktické cvičení (vlastní klíč)

1. Vygenerovat pár vlastních klíčů
   - File → New PGP Key
   - volitelně Advanced Key Settings a délka klíče
   - zadání hesla, které bude chránit privátní klíč na disku
2. Export veřejného klíče do souboru
   - Klíč → Export → soubor.asc
   - (lze včetně privátního klíče, typicky NEděláme)
3. Zobrazení/publikace souboru veřejného klíče
   - soubor.asc (BASE64, notepad)
   - http://pgp.mit.edu/ → Submit a key

PGP – praktické cvičení (cizí klíč)

1. Stažení cizího klíče
   - http://pgp.mit.edu/, Petr Svenda, 0x89CEB31C
2. Import klíče
   - File → Import → soubor.asc
3. Kontrola fingerprintu
   - osobně, vizitka, telefon
   - A890 0285 D837 AEBB B522 771E 86E8 F87A 89CE B31C
   - poté Import
4. Nastavení důvěry
   - Key properties → Trust → Trusted
5. Podpis (certifikace) cizího klíče
   - Klíč → Keys → Sign...

PGP – Šifrování a podpis souboru

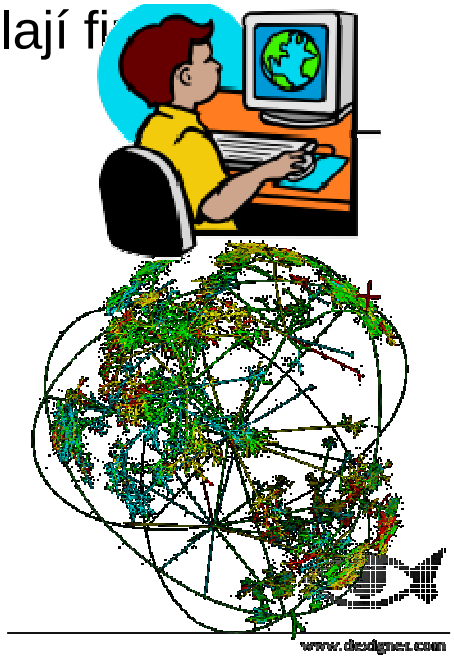
1. PGP Zip → New PGP Zip
2. Přidat soubory určené k šifrování
3. Volba Recipient Keys (šifrujeme pro někoho)
   - výběr adresáta: Petr Svenda petr@svenda.com
4. Výběr podepisovacího klíče (podepisujeme my)
   - Finish (zadání hesla k našemu soukromému klíči)
5. Vzniká nový soubor s příponou *.pgp
   - podepsaný námi (nikdo jiný nemohl vytvořit)
   - šifrovaný pro Petra Svendu (nikdo jiný nemůže číst)
6. Dvojklikem na zašifrovaný soubor se ověří podpis a dešifruje

Digitální podpis - shrnutí

- Nezajišťuje důvěrnost (tam použijeme šifrování)
- Nejznámější algoritmy – RSA, DSA
- Asymetrické algoritmy jsou relativně pomalé
  - cca 10-100x pomalejší než symetrické
- Proto se podepisuje haš – „otisk dat“
- Fáze postupu:
  - Vytvoření a registrace klíčů (certifikát)
  - Vlastní podepsání
    - Dokument → haš → podpis
  - Ověření podpisu

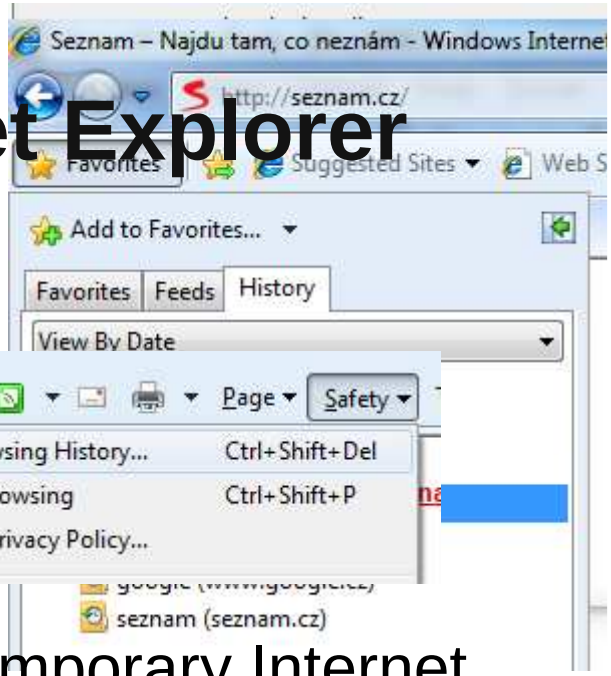
Anonymní brouzdání

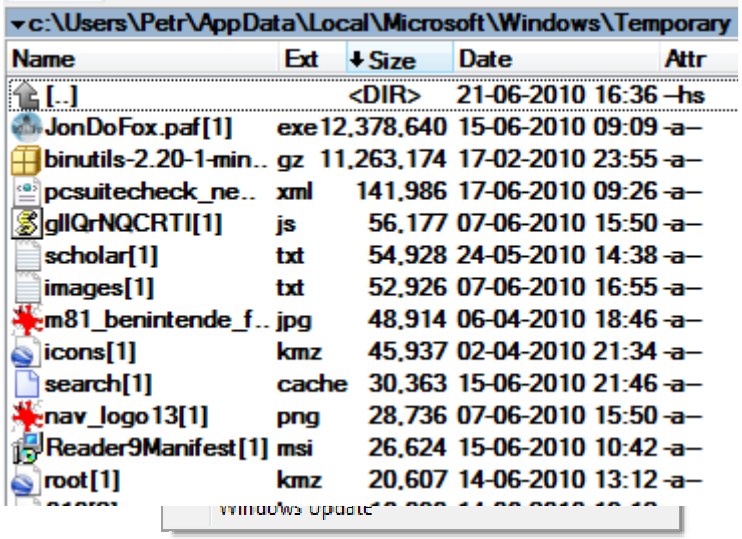
- Význam ochrany soukromí
  - ochrana před represivními režimy (cenzura)
  - ochrana vlastních údajů před cílenou reklamou (dělají fi
  - ochrana před profilováním (dělají i naše vlády)
  - základní občanské právo
- Kde vůbec zanecháváme stopy o brouzdání?
  - vlastní počítač
  - připojení v lokální síti
  - připojení k internetovému poskytovateli (ISP)
  - směrovače v Internetu
  - cílový server



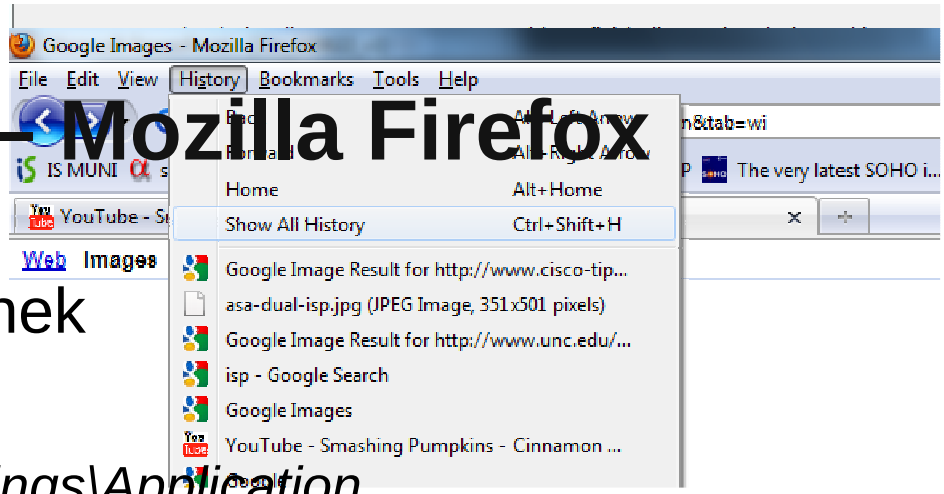
Soukromé brouzdání – Internet Explorer

1. Historie navštívených stránek
   - prozrazuje velmi mnoho
   - lze vymazat
2. Obsah cache prohlížeče
   - *uživatelský_profil*\Local Settings\Temporary Internet
   - soubory včetně přípony – obrázky, fotky, dokumenty…
3. Safety->InPrivate browsing
   - není uchována historie, cache,
   - ale pořád dost informací
     - viz. http://www.getip.com/

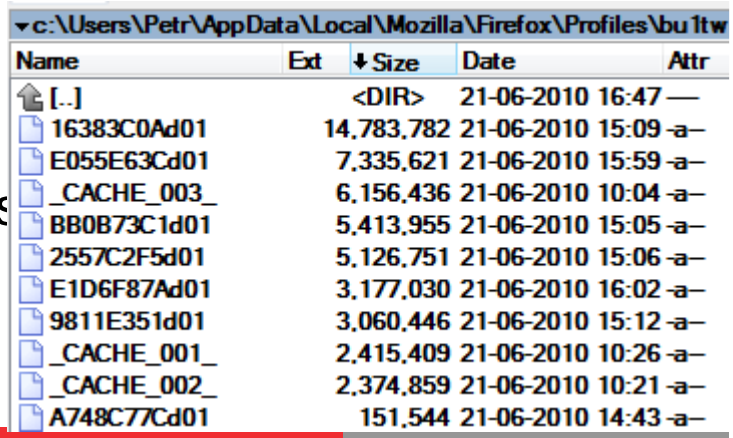




Soukromé brouzdání – Mozilla Firefox



1. Historie navštívených stránek
2. Obsah cache prohlížeče
   - *uživatelský_profil\Local Settings\Application data*\Mozilla\Firefox\Profiles*jmeno_profilu*.default\Cache\
   - soubory přejmenovány, bez přípony
   - původní obsah ale obsažen (údaj v hlavičce)
   - např. přejmenovat vše na *.jpg a zobrazit
     - cmd.exe copy * *.jpg
3. Tools->Start private browsing
   - bez historie, bez cache... (jako IE)
   - problém s informacemi na serveru zůs
   - ip-check.info



IP Address Information	
IP Address:	147.251.42.10
Hostname:	minotaur.fi.muni.cz
Obfuscated IP Address:	2482711050
IP Reverse:	minotaur.fi.muni.cz
Remote Port:	2675

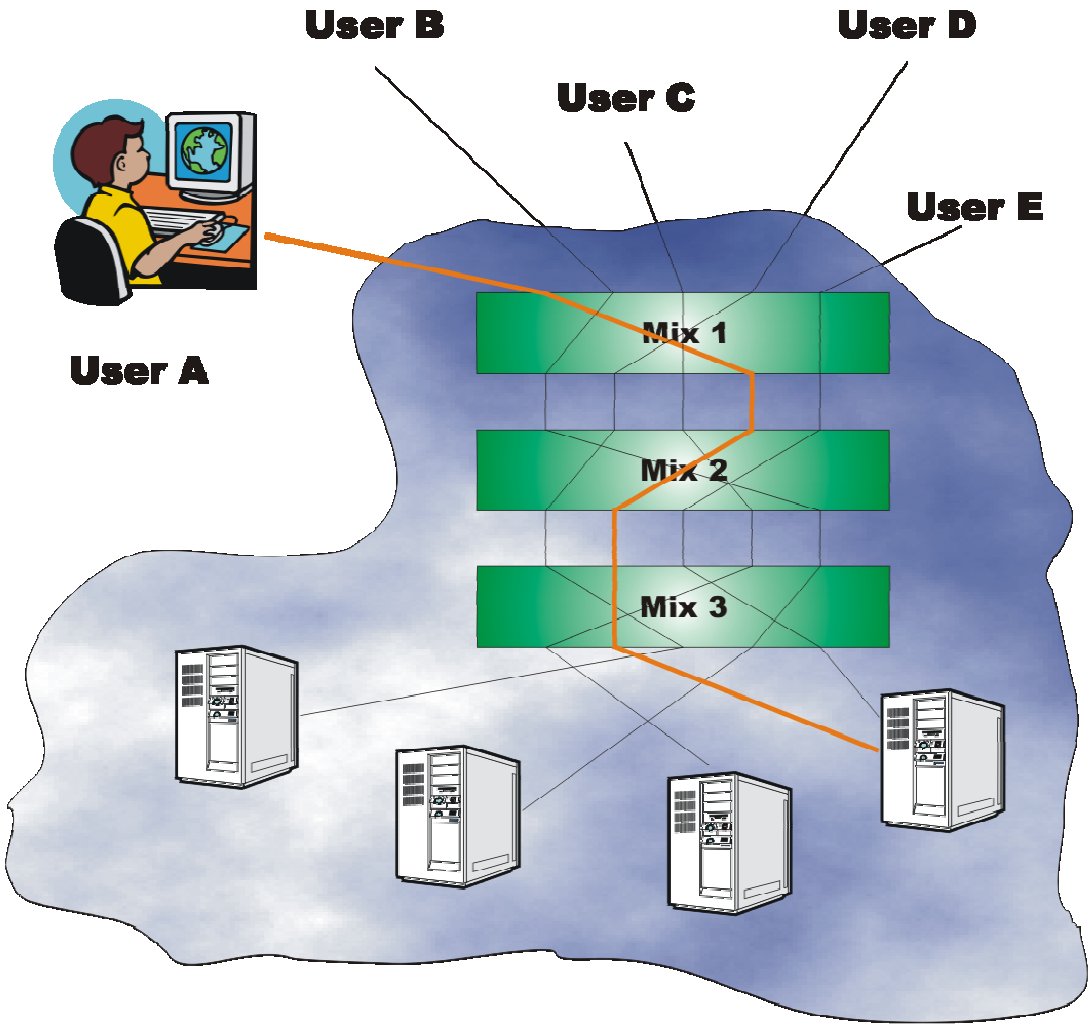
Logo Design for an Affordable $149!
» 5 Unique Logo Design Concepts to Choose from
» 5 Logo Designers will work on the Project
» Unlimited Revisions till you are 100% Satisfied
» No Cliparts Used
Find Out More
RISK FREE 100% MONEY BACK GUARANTEE

IP Location Information	
Country:	Czech republic (CZ)
State or Province:	78
City or Town:	Brno
Latitude:	49.2
Longitude:	16.6333
Internet Service Provider:	Masaryk university

Linux Hosting from The Planet - Great Hosting At A Great Price	
Features:	Super fast network with 100% uptime guarantee
Support:	Secure data centers with 24/7 support
Get Started Today	Chat With A Linux Hosting Expert!

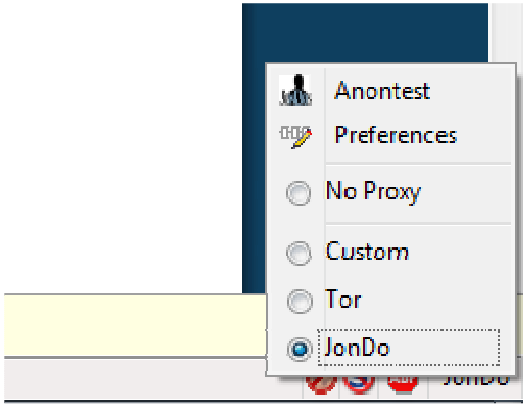
System Information	
Operating System Platform:	Microsoft Windows
Browser Version:	Firefox
Cookies Enabled:	yes
Java Enabled:	yes
CPU class/type:	OS/CPU Windows NT 6.1
Screen Width:	1680
Screen Height:	1050
Screen Color Depth:	24
Window Width:	1680 (100.0% of 1680)
Window Height:	857 (81.6% of 1050)
Language(s) Accepted:	en-us,en;q=0.5

JAP (http://www.jondos.de)



JonDo – praktické cviče

1. Instalace
   - JonDo (proxy), JonDoFox (
2. Spuštění JonDo proxy
   - připojení k volným ka
3. Spuštění JonDoFoxu
   - standardní Firefox, proxy na JonDo
   - vypnutý JavaScript, reklamy…
4. Test anonymity
   - http://www.getip.com/
   - vypnutí/zapnutí proxy



IP Address Information	
IP Address:	212.227.103.74
Hostname:	p15202001.pureserver.info
Obfuscated IP Address:	3571672906
IP Reverse:	p15202001.pureserver.info
Remote Port:	58330

IP Location Information	
Country:	Germany (DE)
State or Province:	01
City or Town:	Karlsruhe
Latitude:	49.0047
Longitude:	8.3858
Internet Service Provider:	Schlund + partner ag

Proxy Information	
Proxy IP Address:	212.227.103.74
Proxy HostName:	p15202001.pureserver.info
Proxy Name:	1.1 p15202001.pureserver.info:3128 (squid/2.7.STABLE5)
Proxy Info:	HTTP_VIA=1.1 p15202001.pureserver.info:3128 (squid/2.7.STABLE5)
Proxy Type:	Anonymous

System Information	
Operating System Platform:	Unknown
Browser Version:	Firefox
Cookies Enabled:	not available, or not enabled...
Java Enabled:	not available, or not enabled...
CPU class/type:	not available, or not enabled...
Screen Width:	not available, or not enabled...
Screen Height:	not available, or not enabled...
Screen Color Depth:	not available, or not enabled...
Window Width:	not available, or not enabled...
Window Height:	not available, or not enabled...
Language(s) Accepted:	en

Možnosti profilování uživatelů – proč

- Uživatelé si neuvědomují množství informací o nich dostupných
- Uživatelé většinou předpokládají nedostupnost privátních informací sdělených jen "přátelům"
- Praktické vyzkoušení si možnosti profilovat třetí osobu vede k lepšímu uvědomění si problému a přiměřenějšímu publikování/chování na Internetu

Možnosti profilování uživatelů - základ

- Postupně budujeme a upřesňujeme profil osoby
  - pozor na duplicity ve jménech

1. Základní hledání na google.com
   - vytvoříme si základní profil uživatele
   - poznačíme si možné nejasnosti
2. Veřejně dostupné fotky na images.google.com
   - obličej? fotky z akcí?
3. Základní údaje v informacích Skype, ICQ...
   - lidé neradi uvádí chybné informace
   - datum narození...

Profilování – dobrovolné informace

4. Domácí stránka, vlastní blog...
   - lidé mají tendenci dát světu najevo, jak jsou „dobří“
   - většinou se nedozvíme „špatné věci“
5. Starší verze stránek na archive.org
   - postupem času zmoudří a odeberou některé informace (odebrané dokumenty, starší fotky...)
   - Wayback machine – archiv stránek a dokumentů webu
6. Blogy kamarádů a známých
   - nejvíce pikantních informací o vás napíšou přátelé
   - navíc jsou to často informace, které původní osoba považuje za neveřejné

Profilování – sociální síť

- Dříve složitější hledání v předchozích zdrojích
  - např. seznamy absolventů školy → spolužáci

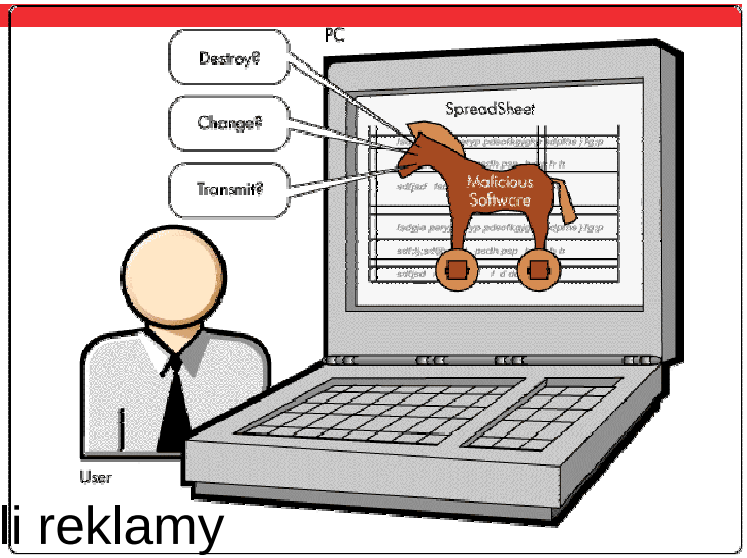
7. Facebook – zlatá studnice ☺
   - fotky, zájmy, vzdělání,
   - síť známých typicky zobrazena, i když nejsme přátelé
8. Náhodně vymyšlená osoba s návrhem přátelství
   - spousta lidí má ráda hodně přátel
9. Falešný profil reálné osoby návrhem přátelství
   - spolužák ze základky, který ještě není v přátelích
   - pomůže nějaká fotka (případně špatně čitelná)

Shrnutí

- Symetrická vs. asymetrická kryptografie
  - asymetrická kryptografie není řešením všech problémů
- Šifrování disku – TrueCrypt
  - virtuální disk v souboru
- PGP/GPG
  - symetrické i asymetrické šifrování
- Soukromé data v prohlížeči – IE, Firefox
  - historie, cache
- Opravdu anonymní brouzdání – JonDo
  - server neví, kdo s ním komunikuje
- Ochrana soukromí je reálný problém

Otázky

Škodlivý software



- Virus, červ, trojský kůň, …
- Adware
  - cílem je stahovat a zobrazovat uživateli reklamy
  - sledování reklam je často alternativa, jak platit za používání programu
  - ne vždy úplně škodlivý
  - RealPlayer, Kazaa…
- Spyware
  - program, jenž shromažďuje data o uživateli
    - hesla, historii brouzdání po internetu…
  - keyloggers
  - tracking cookies

SpyBot S&D – praktické cvičení

1. Instalace, spuštění
   - http://www.safer-netw
2. Stažení aktualizací
   - Search for updates
3. Hledání problémů
   - Check for problems
   - *(běží delší dobu)*
   - pouštět cca 1x týdně

4. Odstranění nalezených problémů
   - Fix selected problems
   - tracking cookies, malware…