

# Certifikační autorita



Rozdělení šifer  
Certifikáty a jejich použití  
Podání žádosti o certifikát  
Certifikační autority u nás



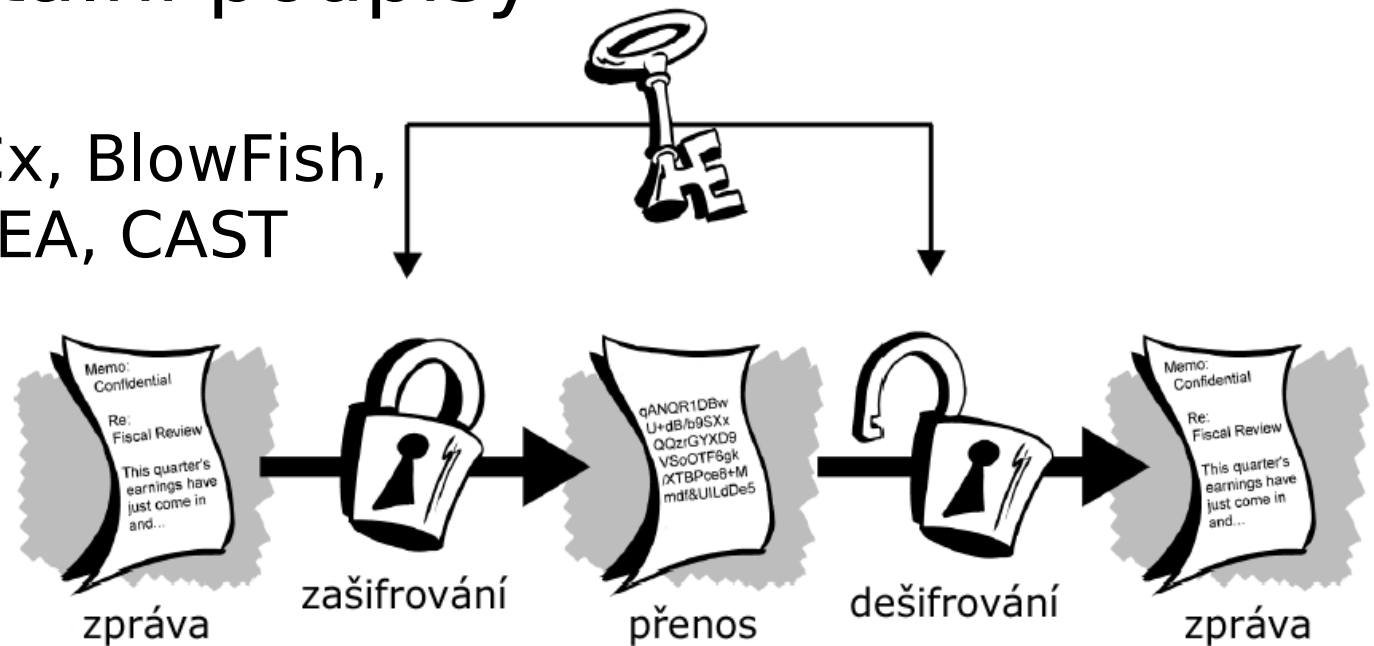
# Význam šifer

- umožnit zakódování a pozdější dekodování nějaké informace
- znemožnit komukoli, kdo má možnost nás odposlouchávat, možnost přečtení nebo dokonce změny naší informace
- základní rozdělení:
  - ♦ symetrické
  - ♦ asymetrické
  - ♦ hybridní (kombinované)
- možnost využití k elektronickému podpisu?

# Symetrické šifrování

- + rychlost
- problematická počáteční výměna klíčů
- počet klíčů roste s druhou mocninou komunikujících dvojic
- neřeší digitální podpisy

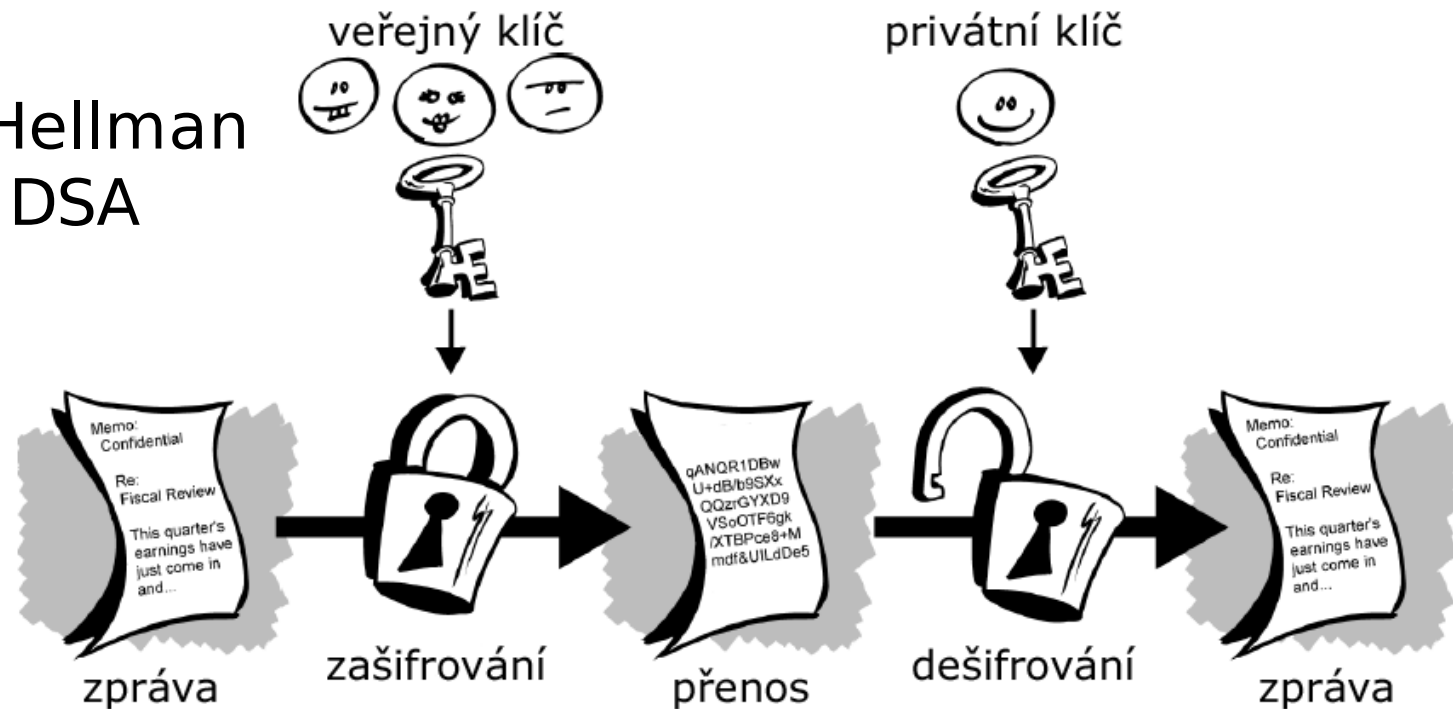
- např. AES, RCx, BlowFish, DES, 3DES, IDEA, CAST



# Asymetrické šifrování

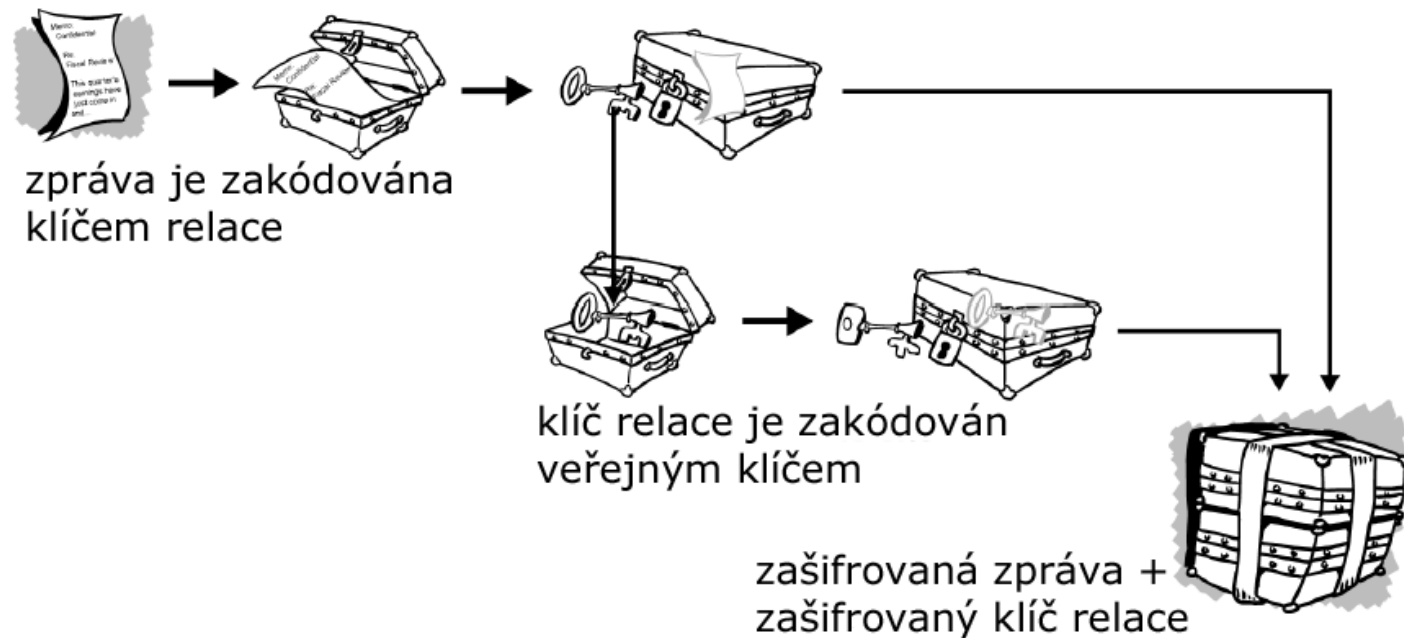
- + počet klíčů roste lineárně s počtem komunikujících dvojic
- + umožňuje digitální podpis
- rychlost (výpočetně náročné)

- např. Diffie-Hellman (1975), RSA, DSA

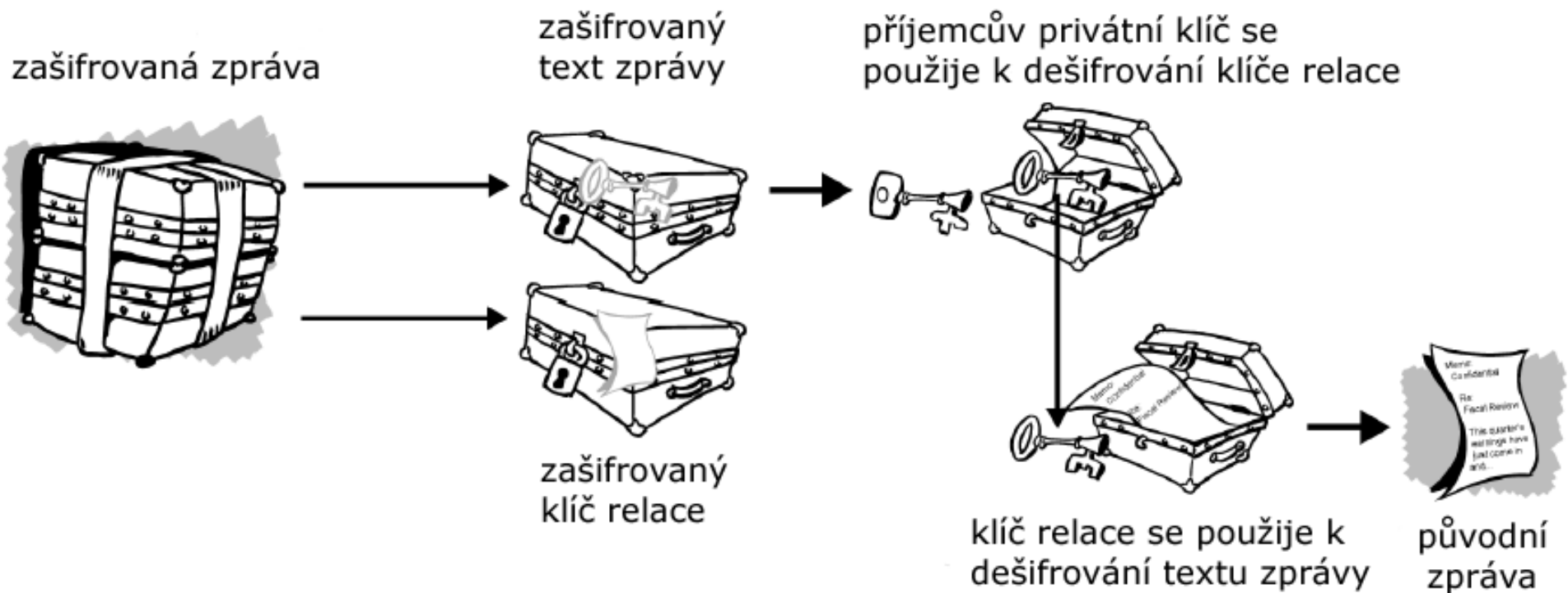


# Hybridní šifrování

- použití klíče relace (session key)
- spojuje výhody předchozích
  - ♦ lineární počet klíčů
  - ♦ přijatelná výpočetní náročnost
  - ♦ umožňuje digitální podpis



# Hybridní šifrování

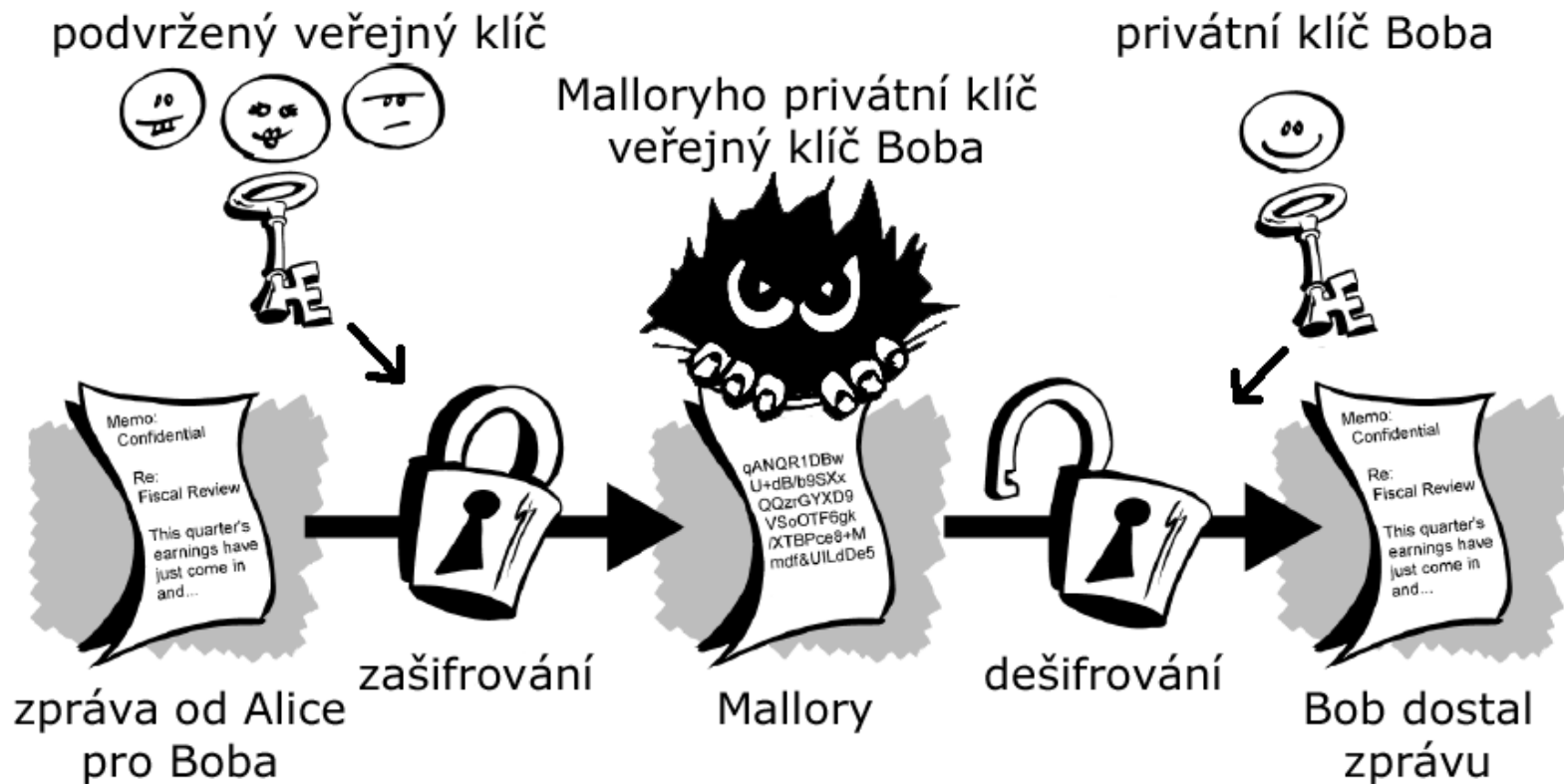


# Veřejný a privátní klíč

- veřejný klíč (public key)
- privátní klíč (private key)
- proč vlastně 2 klíče?
- osoby A a B (Alice a Bob)
- šifrování
  - ♦ A -> (public B) -> internet -> (private B) -> B
  - ♦ B -> (public A) -> internet -> (private A) -> A
- ověření identity a elektronický podpis
  - ♦ A -> (private A) -> internet -> (public A) -> B
  - ♦ Bob musí znát předem public A

# Man in the middle attack

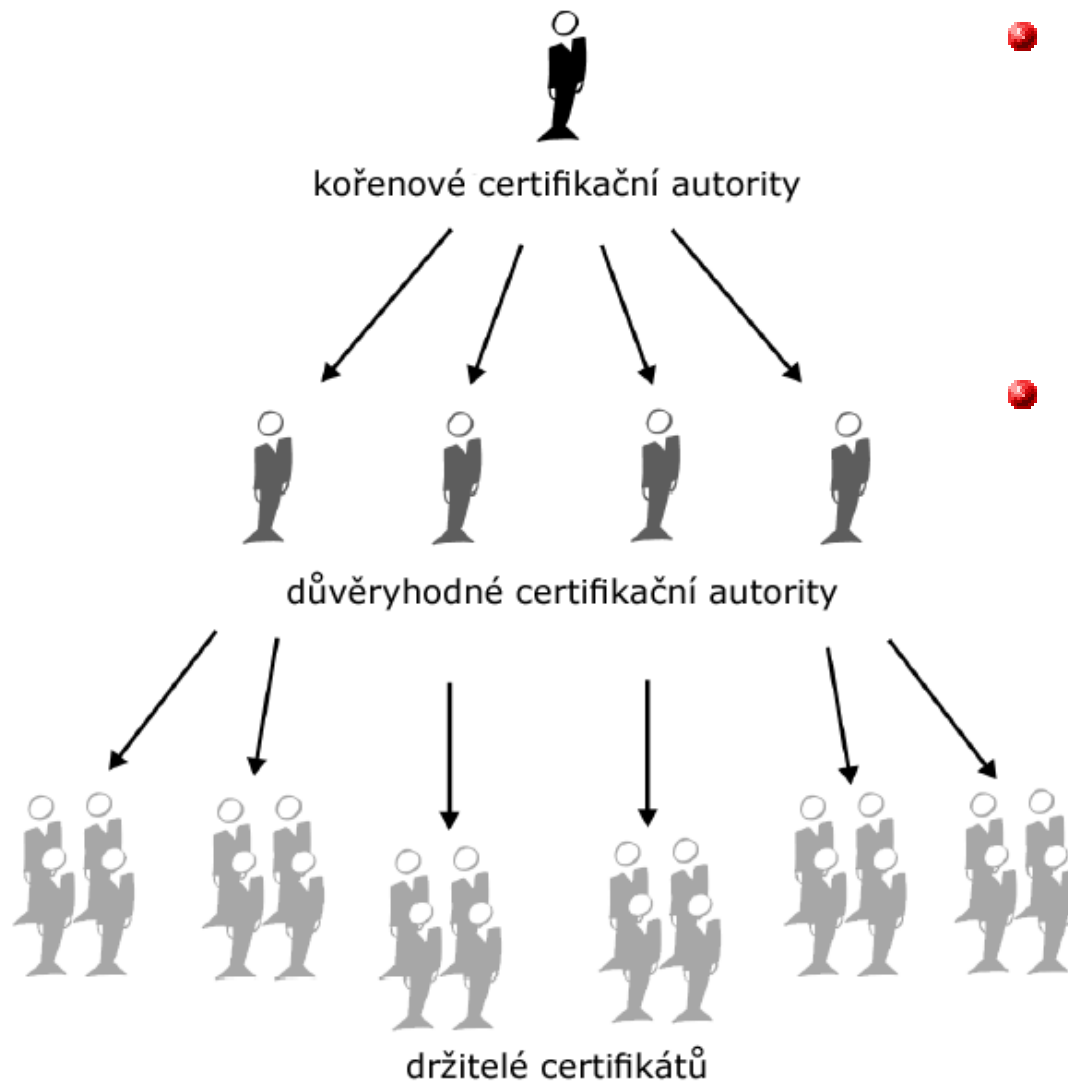
- Grand Chessmaster Problem
- Alice nezná Bobův veřejný klíč a Bob nezná veřejný klíč Alice



# Interlock protokol

- ➔ Alice pošle Bobovi svůj veřejný klíč
- ➔ Bob pošle Alici svůj veřejný klíč
- ➔ Alice zašifruje zprávu veřejným klíčem Boba
- ➔ Alice pošle 1. polovinu zprávy Bobovi
- ➔ Bob zašifruje zprávu veřejným klíčem Alice
- ➔ Bob pošle Alici 1. polovinu
- ➔ Alice pošle Bobovi 2. polovinu
- ➔ Bob sestaví zprávu, dešifruje a pošle Alici 2. polovinu zprávy
- jaký je rozdíl oproti předchozímu?

# Certifikáty



- PGP
  - ♦ distribuovaná důvěra
- X.509
  - ♦ hierarchický princip autorizace
  - ♦ certifikační autorita

# Certifikační autorita

- vydává certifikáty určitých typů
- měla by být nezávislá a dostatečně důvěryhodná
- ověřuje pravdivost informací v žádostech o certifikát
- zneplatňování certifikátů
- vydávání následných certifikátů
- zveřejňování seznamu zneplatněných certifikátů

# Jak takový certifikát X.509 vypadá?

- verze X.509, veřejný klíč držitele certifikátu
- informace o držiteli certifikátu (owner)
  - ◆ Common Name
  - ◆ Email address
  - ◆ Organization, Organizational Unit
  - ◆ Country, State, Locality
- sériové číslo, platnost od/do
- informace o vystaviteli certifikátu (issuer)
- podpis vystavitele certifikátu
- možnosti využití certifikátu (extenze)

# Extenze certifikátu

- SSL client, SSL server
- email signing, email encryption
- CRL signing
- OCSP helper (OCSP=Online Certificate Status Protocol)
- `basicConstraints=CA:{TRUE,FALSE}`
- a další
  
- nepovinné:
  - ♦ `extendedKeyUsage=clientAuth,emailProtection`

# Privátní klíč

- především musí být bezpečně uložen (token, jakékoli přenosné medium, souborový systém s nastavením přístupových práv pro uživatele (ne FAT), bezpečné úložiště v systému, bezpečný počítač)
- chráněný heslem (3DES)
- privátní klíč (i chráněný heslem) nesmí nikdy získat nepovolaná osoba
- kompromitace privátního klíče

# It's all about trust

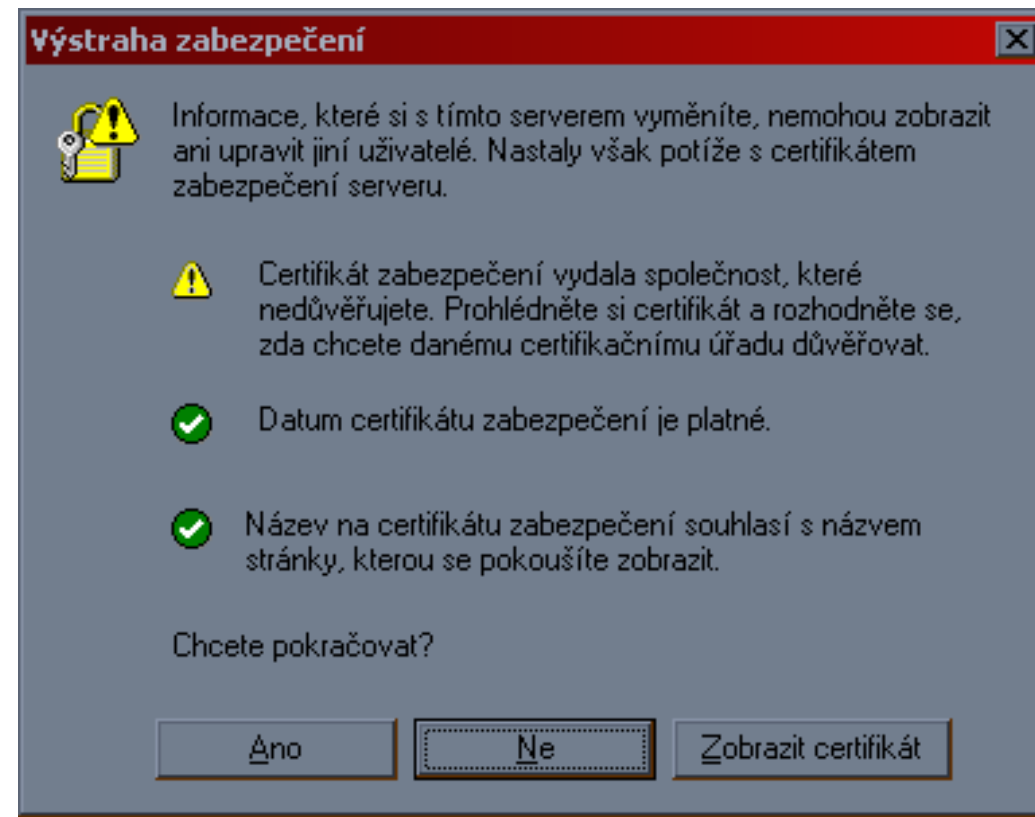
- proč věřit informacím uvedeným v certifikátu?
- certifikát podepíše certifikační autorita
- věříme certifikační autoritě?
  - ◆ pokud ano, věříme zároveň i všem certifikátům touto autoritou podepsaným
  - ◆ nutno zjistit, jakým způsobem daná certifikační autorita prověřuje pravdivost údajů uvedených v certifikátu
- <http://www.caczechia.cz/ca/poslatmail.asp>

# It's all about trust

- ➔ Alice a Bob spolu nikdy nekomunikovali a neznají veřejný klíč druhé strany
- ➔ Alice naváže kontakt s Bobem
- ➔ předají si navzájem certifikáty a zjistí, zda se jedná o důvěryhodný (trusted) certifikát
- ➔ Alice má podepsaný certifikát od CA, které Bob důvěřuje
- ➔ Bob má podepsaný certifikát od CA, které Alice důvěřuje
- ➔ oba mají jistotu, že komunikují s druhou stranou

# Do you trust?

- posoudíme důvěryhodnost certifikátu dle známých certifikátů v systému
- předinstalované certifikační autority
- můžeme se rozhodnout věřit neznámému certifikátu, případně ho i nainstalovat do systému



# Žádáme o certifikát

- vybereme si certifikační autoritu
  - ♦ důvěryhodnost dané autority
  - ♦ způsob podání žádosti o certifikát
  - ♦ nabízené služby a typy poskytovaných certifikátů, cena
- vlastní žádost
  - ♦ vyplníme údaje o sobě
  - ♦ vygenerujeme pár veřejný a privátní klíč
  - ♦ veřejný klíč přiložíme k žádosti
  - ♦ předáme žádost certifikační autoritě (CSR=Certificate Signing Request)
- CA ověří oprávněnost žádosti
  - ♦ vyzvedneme si podepsaný certifikát

# Jak vytvořit žádost

- binárka OpenSSL
- CryptoAPI v MS Internet Exploreru či v Mozille (bezpečná úložiště)
- aplikace napsaná pro tento účel s využitím OpenSSL knihoven
- speciální k tomu určená zařízení
  
- požadavky
  - ♦ otevřený kód nebo důvěryhodný program
  - ♦ při vytváření žádosti nesmí dojít ke kompromitaci privátního klíče

# OpenSSL

- v systému většinou v /etc/ssl/ nebo /usr/lib/ssl/
- struktura adresáře
  - ♦ *certs/*
  - ♦ *crl/*
  - ♦ *newcerts/*
  - ♦ *private/*
  - ♦ cacert.pem
  - ♦ crl.pem
  - ♦ index.txt
  - ♦ serial
  - ♦ openssl.cnf

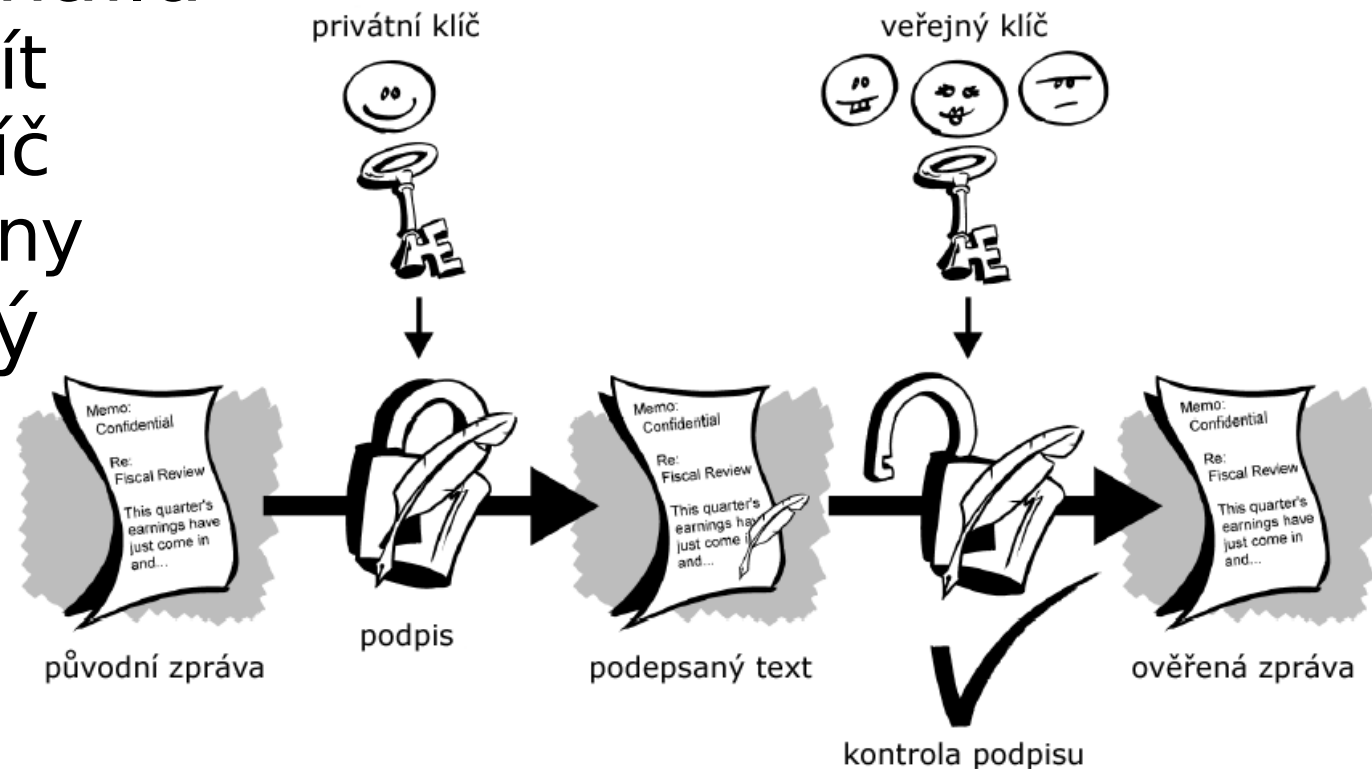
Why buy an  
**SSL**  
toolkit as a  
black-box when  
you can get an  
**open**  
one for  
**free** ?

# Používáme OpenSSL

- vytvoření žádosti  
openssl req -config openssl.cnf -new -out cert.req  
-keyout cert.key [-nodes]
- vytvoření vlastní CA  
openssl req -new -x509 -keyout private/cakey.pem  
-out certs/cacert.pem -days 365  
chmod 600 private/cakey.pem
- podepsání certifikátu pomocí CA  
openssl ca -config openssl.cnf -out cert.crt -infiles  
cert.req
- přidat/odebrat/změnit heslo privátního klíče  
openssl rsa -in cert.pem -out new.pem [-des3]

# Využití certifikátu

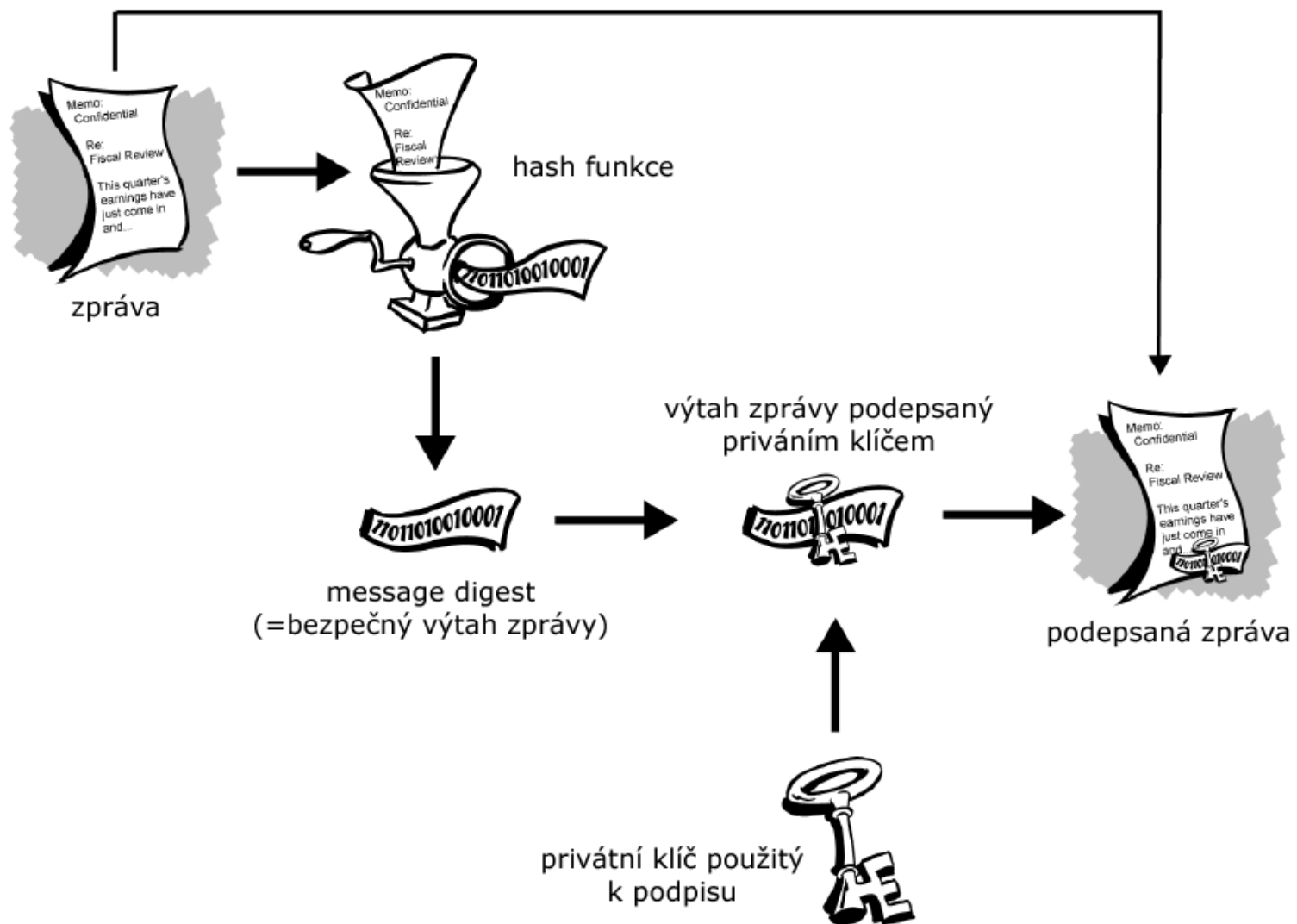
- ověření serveru
  - ◆ https, pop3s, imaps, smtps, ftps, ...
- ověření klienta
- šifrování emailu
  - ◆ musíme mít
  - ◆ veřejný klíč druhé strany
- elektronický podpis



# Elektronický podpis

- asymetrická šifra přes celý dokument příliš náročná
- vytvoříme otisk dokumentu (zhuštění zprávy do malého objemu pomocí matematické funkce)
- výsledná hash se zašifruje privátním klíčem
- druhá strana oddělí hash od dokumentu a také ji spočítá, dešifruje zaslanoú hash veřejným klíčem a výsledky porovná
- autentičnost zprávy
- autentičnost autora

# Elektronický podpis podruhé



# Hash funkce

- bezpečný výtah zpravy = message digest
- hash - číslo s konstantní délkou za stanovených podmínek
- jednoduchost výpočtu
- jednocestnost funkce (irreversibility)
- malá změna na vstupu způsobí velkou změnu na výstupu
- vymyslet zprávu, aby měla konkrétní hash musí být obtížné
- např. MDx (Message Digest 2,4,5), SHA (Secure Hash Algorithm), RIPE-MD

# Formáty certifikátu

- informace obsažené v certifikátu jsou popsány pomocí jazyka ASN.1 (popisuje obecné datové struktury)
  - PEM, DER, PKCS#12
  - PEM
    - ◆ -----BEGIN CERTIFICATE-----
    - ◆ DER -> Base64
    - ◆ -----END CERTIFICATE-----
  - možnost konverze mezi formáty
    - ◆ převod PEM do PKCS#12 pomocí OpenSSL
      - včetně privátního klíče pro import do IE a Mozilly
- ```
openssl pkcs12 -export -in cert.pem -inkey cert.key -out cert.p12
```

# Generování CRL

- CRL (Certificate Revocation List) - seznam zneplatněných certifikátů
- důvody ukončení platnosti certifikátu:
  - ♦ změna údajů uvedených v certifikátu
  - ♦ kompromitace privátního klíče
- certifikační autorita by měla poskytovat co možná nejaktuálnější CRL
- CRL by měl být dostupný dvěma na sobě nezávislými způsoby

# Certifikační authority u nás

- První certifikační autorita
  - ◆ jediná státem akreditovaná certifikační autorita u nás
  - ◆ certifikáty použitelné při komunikaci s úřady
- CA Czechia
- CA TrustPort
- CA Globe Internet
- CA kpnQwest
- CESNET CA
- PostSignum (Česká pošta)

Q&A

**Děkuji Vám za pozornost**