PV157 – Autentizace a řízení přístupu

Zdeněk Říha

konz. hod v B415

Pondělí a úterý 13-14

Vašek Matyáš

konz. hod v B415

Úterý 8:30 – 9:30

Čtvrtek 15:00 – 16:00

Email: zriha / matyas @fi.muni.cz

Přednášky, slajdy a skripta

- Přednášky v D3 Út
  10:00 – 11:xx
- Doplňkové čtení, slajdy (před předn.) aj. v IS
  - *Skripta nakl. MU*

Hodnocení, spolupráce

- Polosemestrální písemka (asi 13. dubna)
- Závěrečná zkouška písemná
  - Otázky z většiny budou průběžně (v dávkách) zveřejňovány v ISu
- Možnost pokračování v práci formou bakalářské či diplomové práce
- Následné předměty pro zájemce o bezpečnost a aplikovanou kryptografii: PV181, PV204.

Hodnocení

A: 90 % (bodů) a více,

B: 80 % a více, ale méně než 90 %,

C: 70 % a více, ale méně než 80 %

D: 60 % a více, ale méně než 70 %

E: 50 % a více, ale méně než 60 %

F = neprospěl(a), za méně než 50 %.

- Kolokvium nebo zápočet alespoň 50 %.

Užitečné předchozí znalosti

- Informační bezpečnost – PV080, PV017
  - Není nutné, je užitečné
  - PV157 volně navazuje na PV080, resp. PV017
- Úvod do kryptografie
- Digitální podpis
- Internet a bezpečnost, ochrana soukromí

Témata kurzu – I

1. Úvod, pojmy
2. Autentizace dat/zpráv
3. Autentizace uživatelů tajnými informacemi
4. Autentizační protokoly
5. Autentizace mezi počítači
6. Autentizace uživatelů tokeny

Témata kurzu – II

7. Úvod do řízení přístupu
8. Řízení přístupu – trendy, víceúrovňové systémy (MLS), tyto a další modely
9. Úvod do biometrik
10. Biometrické autentizační metody
11. Problémy a využití biometrik
12. *Náhled na vybranou aplikaci – e-pasy, RFID*

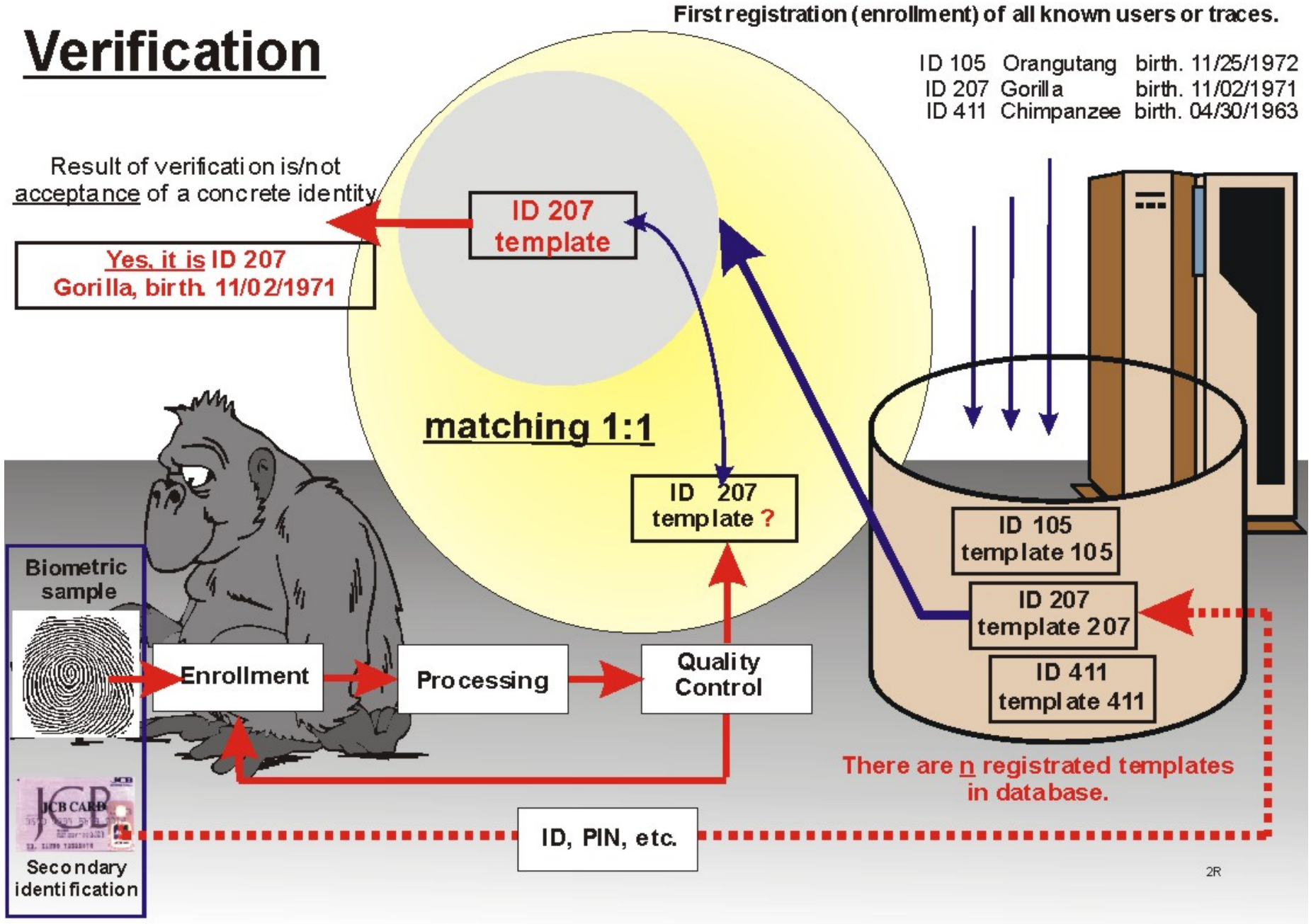
3 zásadní pojmy

- ***Autentizace*** – proces ověření (a tím i ustavení) identity (s požadovanou mírou záruky).
- ***Autorizace*** – udělení určitých práv a určení povolených aktivit.
- ***Identifikace*** – rozpoznání určité entity (systémem) v dané množině entit.

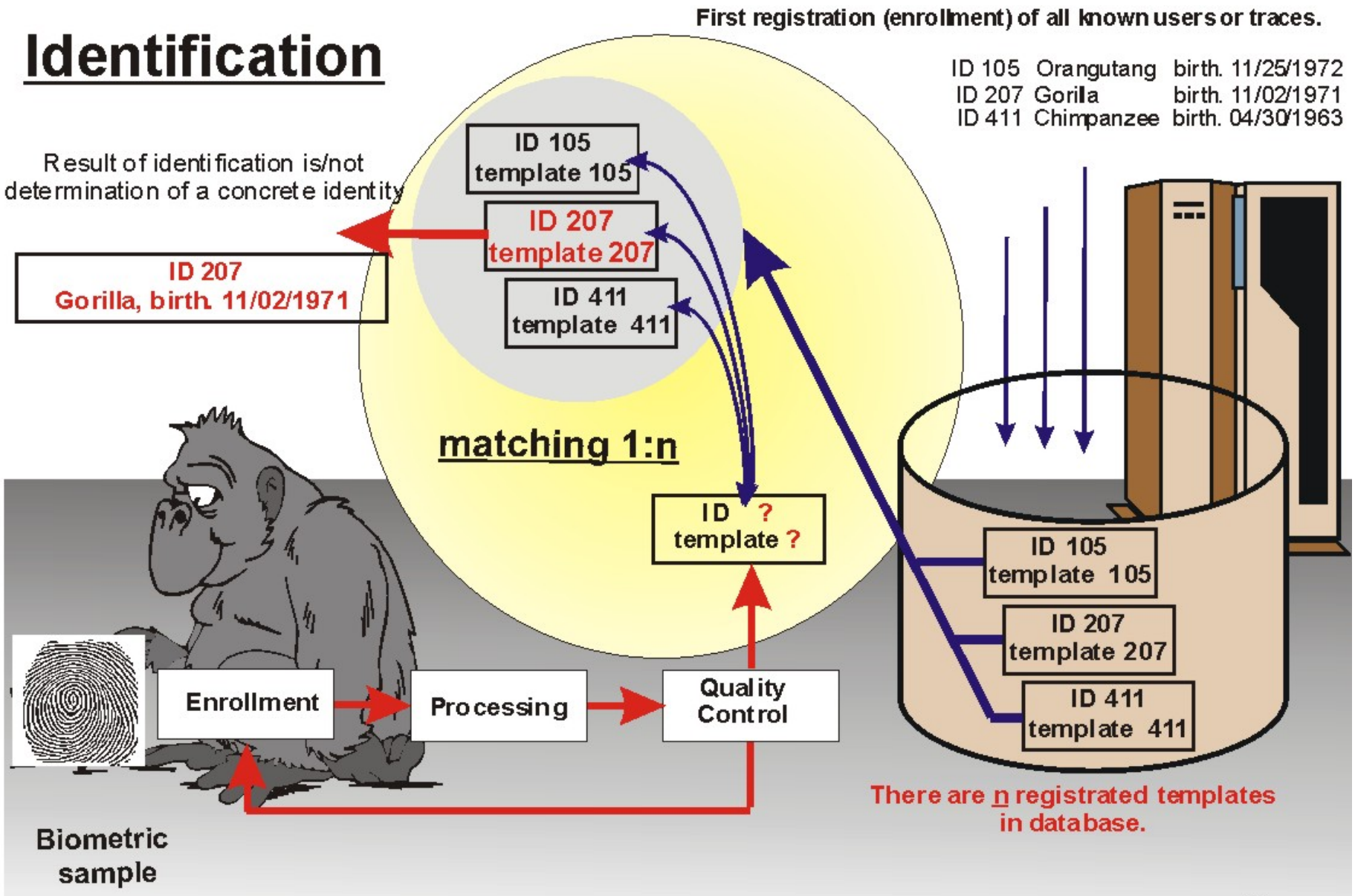
Autentizace a identifikace uživatele

- *Autentizace (verifikace)* – subjekt předkládá tvrzení o své identitě – 1:1
- *Identifikace* (*vyhledání*) – subjekt identitu nepředkládá. Systém prochází všechny (relevantní) záznamy v databázi, aby našel patřičnou shodu a identitu subjektu sám rozpoznal – 1:n
- Následující ilustrace od Romana Raka...

Verification



Identification



Autentizace dat/zpráv

- Problematika digitálního podpisu
  - Ochrana soukromého klíče
  - Veřejný klíč – certifikát, CA
- Hašování – hašovací funkce, jejich principy a typické použití
- Autentizační kódy (MAC) atd.
- Slabé mechanismy – CRC ap.
- Praktické nasazení autentizace dat/zpráv

PKI

- Public-key infrastructure
  - Principy, použití
  - PKI není jen CA
  - PKI je prostředek, ne cíl
  - Výhody a nevýhody

Autentizační protokoly

- Kryptografický protokol
- Cíle a metody kryptografických protokolů
- Autentizace jedné strany a oboustranná
- Spojení autentizace a jiných cílů kryptografických protokolů
- Standardy ISO/IEC – základní úroveň
- Protokoly vyšší úrovně (SSL, IPv6 ap.) a autentizace

Autentizace mezi počítači

- Netriviální problém – nelze použít biometriky a obvykle ani tokeny
- Autentizace podle síťových adres (MAC, IP adresy)
- Protokol výzva-odpověď – ověření znalosti tajné informace – kryptografie
- Např. protokoly ssh, SSL

Autentizace uživatelů tajnými informacemi

- „Něco, co uživatel zná“ (a ostatní ne ☺)
- Hesla
  - Druhy hesel a jejich použití
  - Správná práce s hesly
- PINy
- Výhody a nevýhody těchto autentizačních metod

Autentizace uživatelů tokeny

- Token – „něco, co uživatel má“ (a ostatní ne)
- Inteligentní token
  - Základní druhy
  - Jejich princip a použití
- Čipové karty – využití, parametry, bezpečnost
- Výhody a nevýhody těchto autentizačních metod

Úvod do biometrik

- „Něco, co uživatel je“ (a ostatní ne)
- Měřitelné biologické charakteristiky člověka-uživatele
- Fyzické – parametry částí těla
- Chování (behaviorální) – parametry činnosti
- Míra tolerance – prahová hodnota
- Nesprávné odmítnutí/přijetí

Biometrické autentizační metody

- Otisk prstu

- Vzor oční duhovky

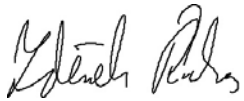
- Vzor oční sítnice

- Srovnání obličeje

- Geometrie ruky

- Verifikace hlasu

- Dynamika podpisu



- Dynamika psaní na klávesnici

Využití biometrik

- Problémy biometrik – bezpečnost
- Otázky praktického použití
  - Současná omezení a použitelnost
  - Vhodné použití
  - Nevhodné použití
- Vztah biometrik a kryptografie

Řízení přístupu I.

- Úvod do řízení přístupu
- Mechanismy pro systémy řízení přístupu
- Volitelné řízení přístupu – Discretionary Access Control (DAC)
- DAC systémy v praxi

Řízení přístupu II

- Povinné řízení přístupu – Mandatory Access Control (MAC)
- Víceúrovňové systémy – Multilevel Systems (MLS)
- Role-Based Access Control (RBAC) a další nové modely a trendy

Kryptologie

- Fyzická ochrana – cena!
- ***Kryptografie*** – ochrana významu (informační hodnoty) dat i „na dálku“
- ***Kryptoanalýza*** – zjišťování slabin kryptografických algoritmů a parametrů
- ***Kryptologie*** – kryptografie & kryptoanalýza
- ***Steganografie*** – utajení samotné existence dat
- ***Vodotisk (watermarking)*** – překryv se steganografií, metody vložení (ochranných) informací do dat

Kde kryptografie pomáhá

- Důvěrnost dat
- Integrita dat
- Autenticita dat (integrita a ověření původu)
- Nepopiratelnost
- Autentizace a autorizace uživatelů/strojů
  - Dostupnost
  - Prokazatelná zodpovědnost
  - Řízení přístupu

...

Tři dimenze kryptografie

- Druh a parametry klíčů
  - Symetrické = konvenční = sdílené
  - Asymetrické = veřejné & soukromé
  - Bez klíčů (hašovací funkce, RND)
- Způsob zpracování dat
  - Po blocích
  - V souvislém proudu
- Druhy použitých operací
  - Substituce
  - Permutace

Kryptografie – Kerckhoffsův princip

- Algoritmus – postup – je všem znám a všemi ověřitelný (jako bezpečný)

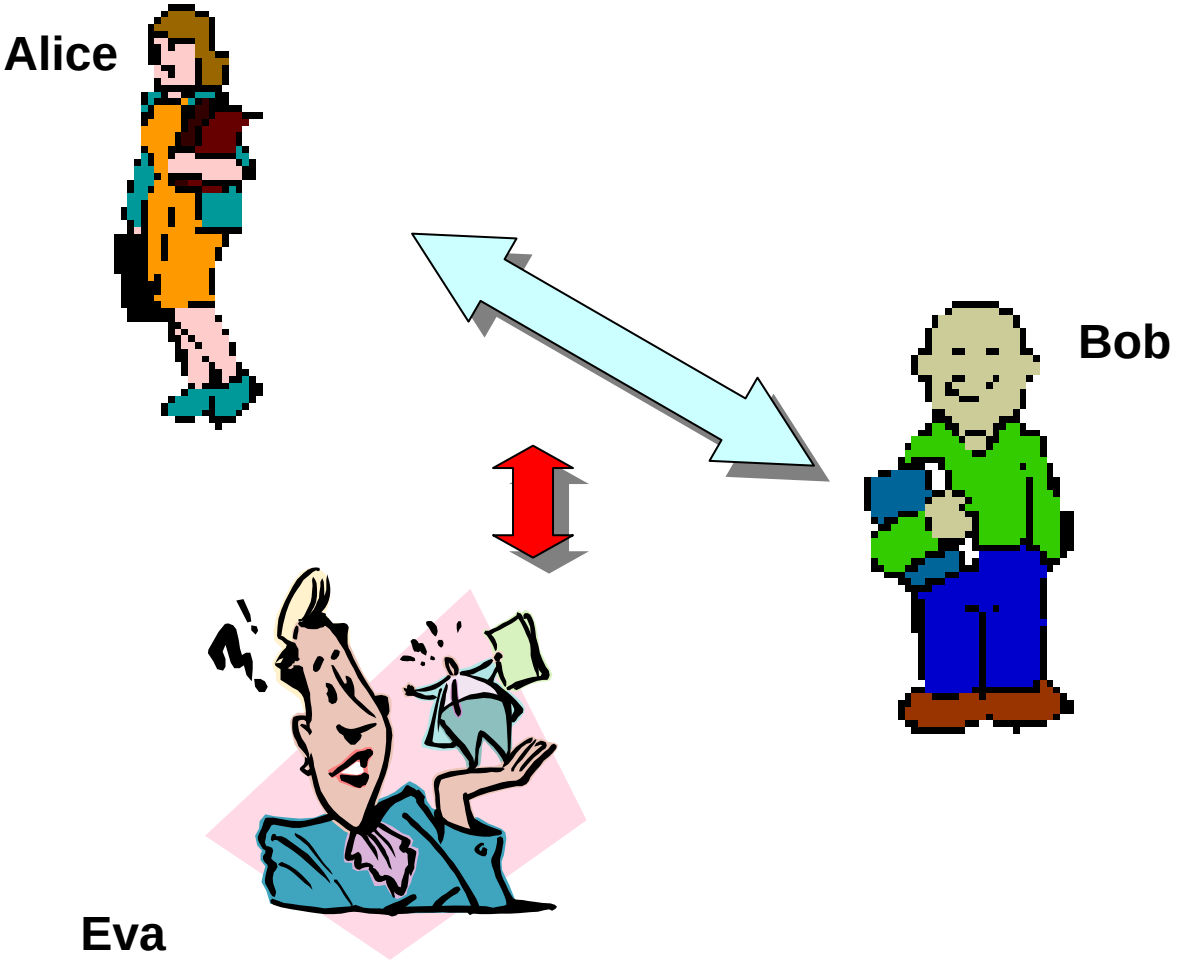
- Klíč – tajná informace – musí být chráněna před nepovolanými osobami

Co je hašování (hashování)

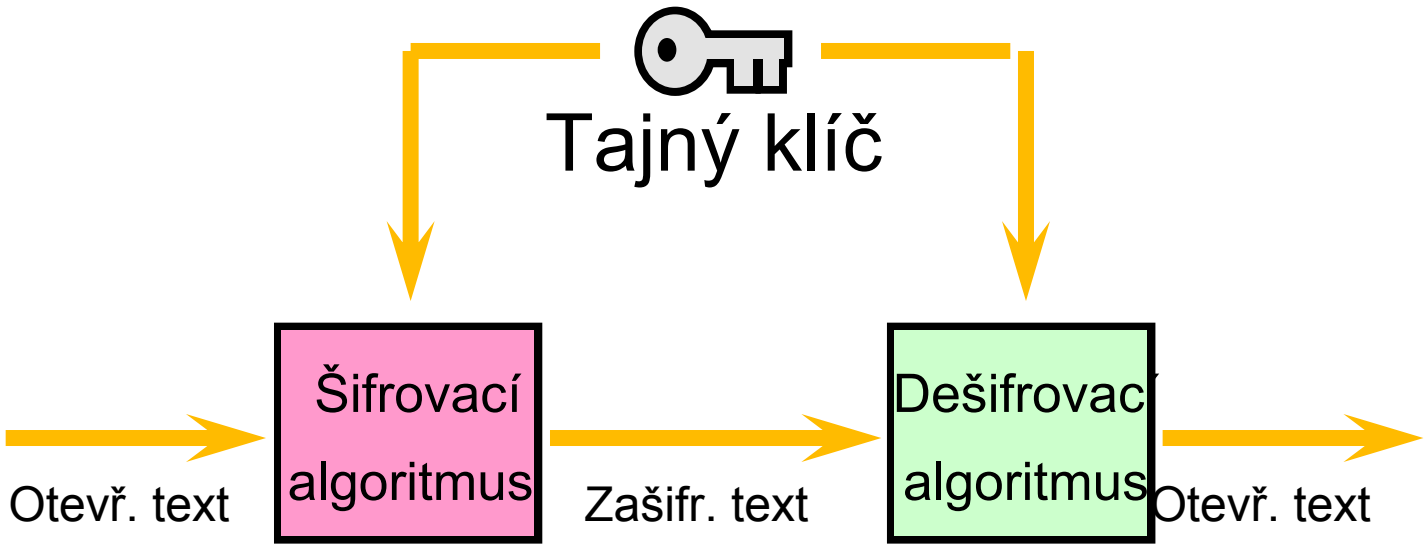
- “Otisk dat”
  - Malý a jedinečný reprezentant jakkoliv velkých dat
- 01:A0:7D:2B:76:52:67:05
- EC:43:6F:B3:68:CE:20:E7

- Hašovací funkce
  - jednosměrnost, bezkoliznost
  - SHA-256 a verze vyšší
  - SHA-1 (160 bit), MD5 (128 bit)

Obvyklá označení činitelů

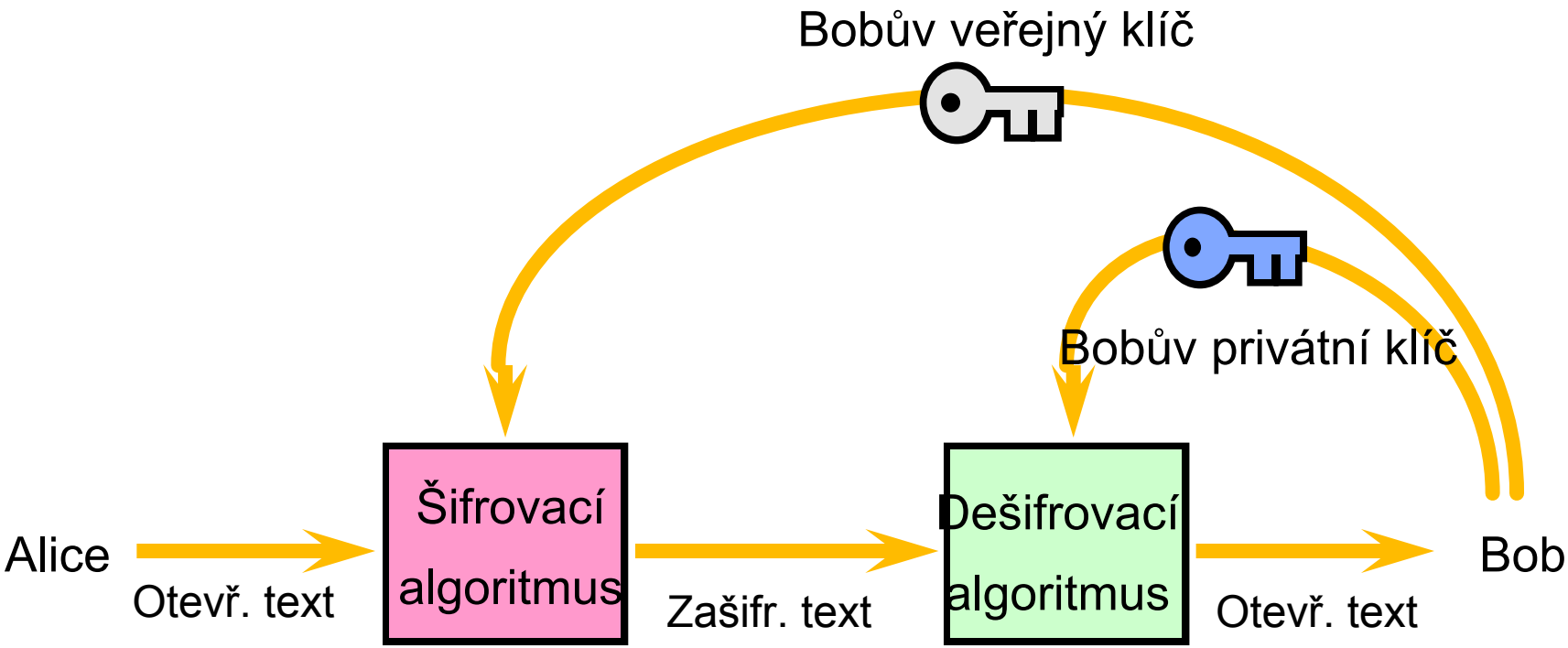


Zjednodušený model konvenčního šifrování



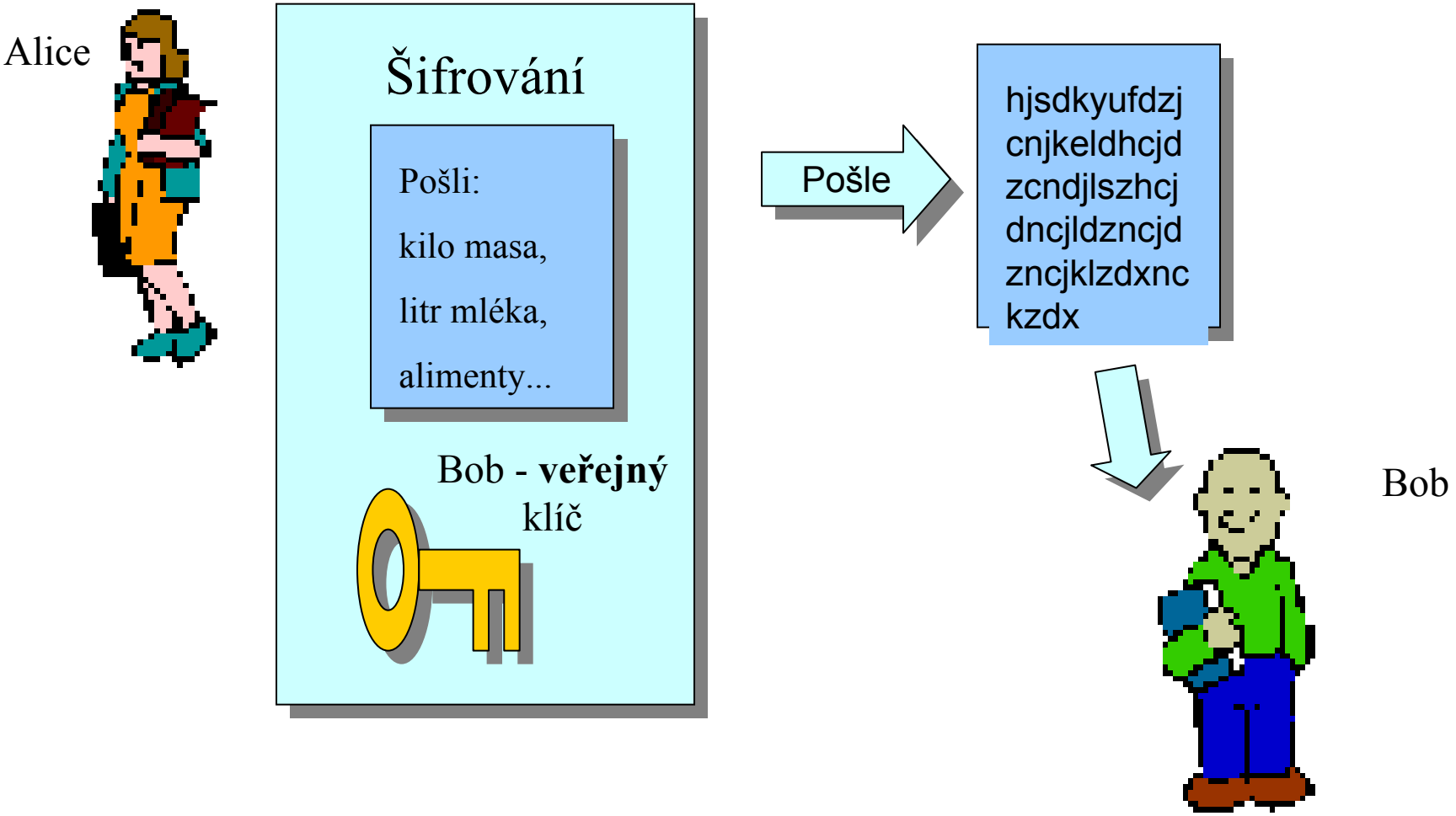
Převzato z: *Network and Internetwork Security* (Stallings)

Zjednodušený model šifrování veřejným klíčem

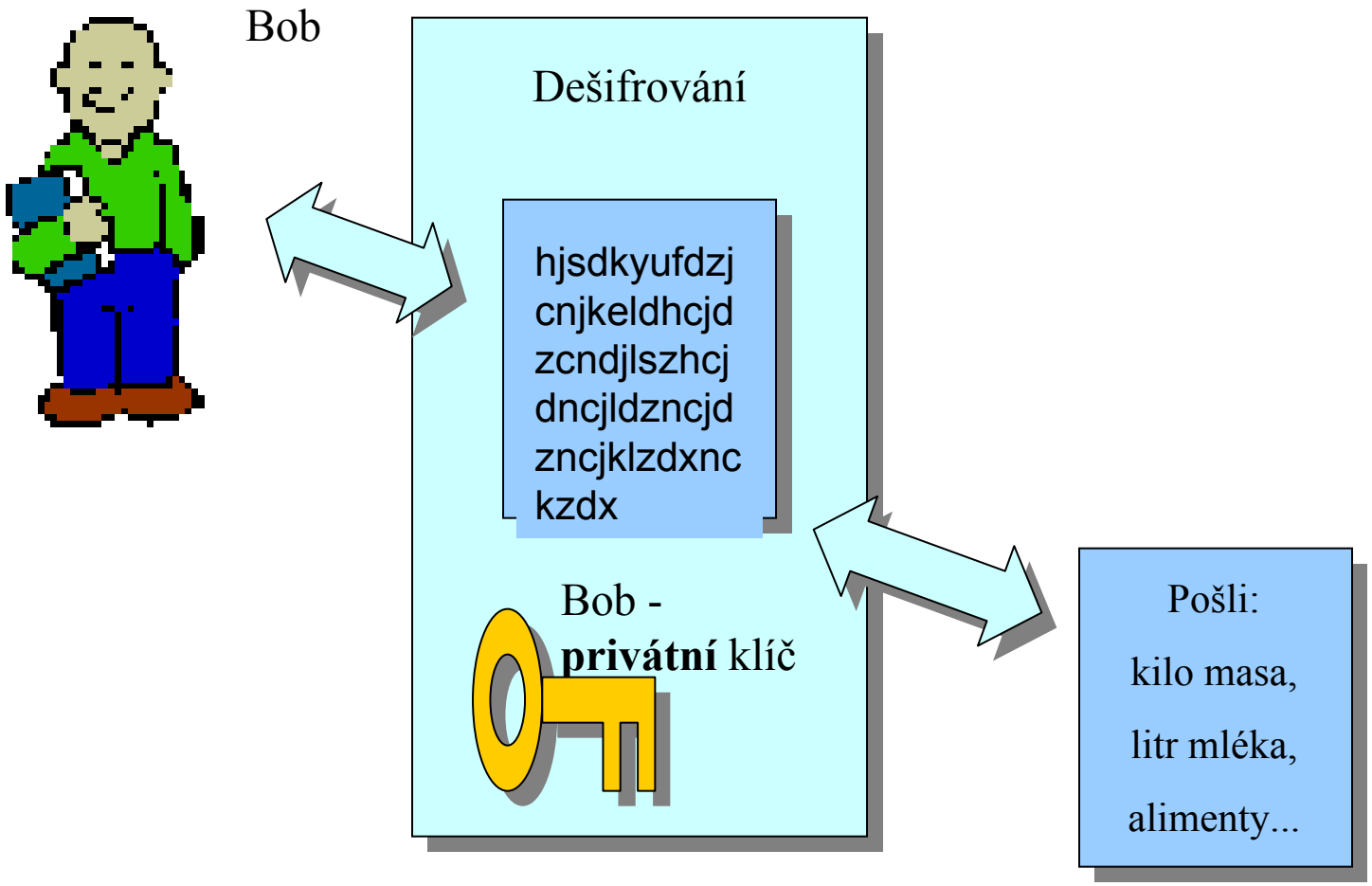


Převzato z: *Network and Internetwork Security* (Stallings)

Šifrování veřejným klíčem

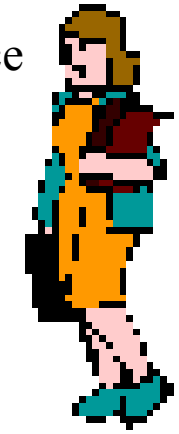


Dešifrování zprávy od Alice



Co je digitální podpis?

Alice



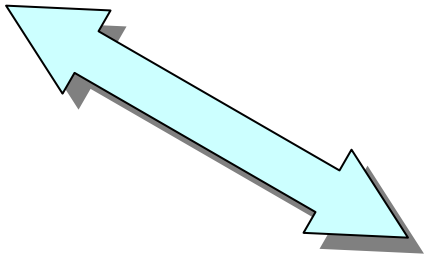
Podpis

Milý Bobe,

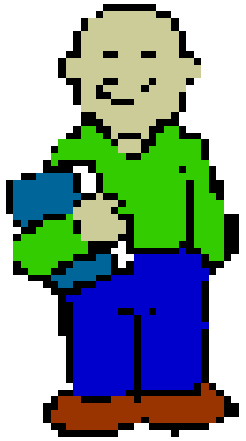
o ty alimenty skutečně žádám já - Alice

Alice - **privátní** klíč

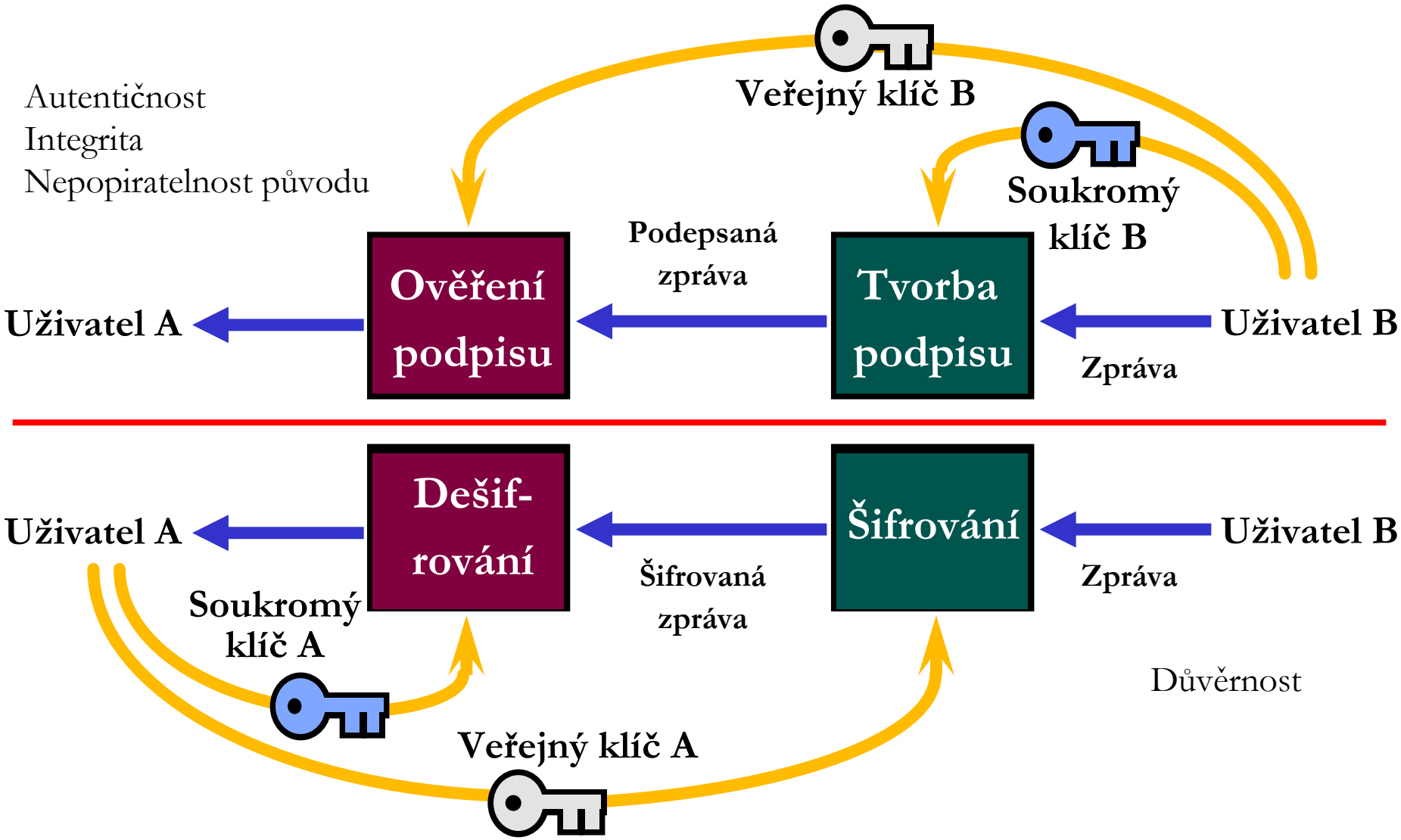
Certifikát - Alicin veřejný klíč



Bob



Asymetrická kryptografie (pokr.)



Certifikát

- **certifikát** – veřejný klíč uživatele podepsaný soukromým klíčem důvěryhodné třetí strany
- certifikát spojuje jméno držitele páru soukromého a veřejného klíče s tímto veřejným klíčem a potvrzuje tak identitu osoby
- poskytuje záruku že identita spojená s vlastníkem daného veřejného klíče není podvržená
- případně také představuje doklad o tom, že totožnost držitele veřejného klíče byla ověřena

Obsah certifikátu

- označení typu (běžný, kvalifikovaný…)
- identifikace vydavatele a podepisující osoby (pseudonym)
- unikátní číslo v rámci vydavatele
- počátek a konec platnosti
- volitelně: doplňkové atributy (lze i definovat vlastní pole)
- volitelně: omezení použití
- podpis vydavatele

Standard X.509

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signature            BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
     version         [0]  Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,       -- notBefore, notAfter
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,  -- algID, bits
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
     extensions      [3]  Extensions OPTIONAL
        -- sequence of: extnID, crit, value }
```

PKI

- pomocná infrastruktura pro správu veřejných klíčů
- PKI je založena na prvcích:
  - bezpečnostní politika (BP) – definuje pravidla pro provoz celé infrastruktury PKI
  - procedury – definice postupů pro generování, distribuci a používání klíčů
  - produkty – HW/SW komponenty pro generování, skladování a používání klíčů
  - autority – prosazují plnění BP s pomocí procedur a produktů

Komponenty PKI

- **certifikační autorita (CA)** – poskytovatel certifikační služby, vydavatel certifikátu
- **registrační autorita (RA)** – registruje žadatele o vydání certifikátu a prověřuje jejich identitu
- **adresářová služba** – prostředek pro uchovávání a distribuci platných klíčů a seznam zneplatněných certifikátů (CRL)

Certifikační autorita (CA)

- registrace uživatelů certifikátů
- vydávání certifikátů k veřejným klíčům
- odvolávání platnosti certifikátů
- vytváření a zveřejňování seznamu certifikátů
- vytváření a zveřejňování zneplatnělých certifikátů CRL (Certificate Revocation List)
- správa klíčů po dobu jejich platnosti (životního cyklu)
- dodatkové služby – např. poskytování časových razítek (time-stamping)

Registrační autorita (RA)

- nepovinná složka
- vytváří vazbu mezi klientem a CA v souladu s popisem postupů při poskytování certifikačních služeb
- přijímá žádosti o certifikace
- ověřuje pravdivost uvedených údajů
- předává certifikát CA k podpisu
- podepsaný certifikát předá klientovi

Adresářová služba

- obvykle minimálně 2 adresáře:
  - privátní – zálohování platných klíčů a pro archivování klíčů, kterým uplynula doba platnosti (provozovanou pod bezpečnostní ochranou zajišťovanou CA)
  - veřejný – uchovávání a distribuce certifikátů a CRL, sklad certifikačních informací
- požadavky:
  - rozšiřitelné schéma
  - replikovatelnost
  - vysoký vyhledávací výkon

Proces vystavení certifikátu

- **generování klíčových dat** – pomocí dostupného SW vybavení uživatelem, případně u poskytovatele certifikačních služeb (PCS)
- **příprava identifikačních údajů** – doložení dokladů
- **předání klíčových dat a identifikačních údajů PCS/RA** – žadatel předá PCS data spolu s doklady o jejich pravosti
- **ověření informací** – PCS si ověří, že lze vydat certifikát
- **tvorba certifikátu** – CA vytvoří potřebná data, ta podepíše
- **předání certifikátu** – certifikát je předán žadateli a zveřejněn

Hierarchické struktury CA

- **problém** – vzájemné ověření certifikátů, které jsou vydány různými CA
- **cíl** – vytvoření jediné struktury CA s kořenovou CA
- **řešení** – vzájemné propojení CA
  - kořenová hierarchie CA – primární CA pro vydávání certifikátů podřízeným CA
  - křížové ověření CA (tzv. mesh PKI architektura) – na úrovní kořenových CA nebo primárních CA
  - ověření CA přes brány – při nekompatibilních implementacích CA

Otázky?

Vítány!!!

Příští přednáška 2. 3. 2010 v 10:00

zriha@fi.muni.cz
matyas@fi.muni.cz