PV157 – Autentizace a řízení přístupu

Vašek Matyáš

konz. Po, St 12-13:00
B415

Zdeněk Říha
v současné době
mimo CZ
konzultace emailem

Email: matyas / zriha @fi.muni.cz

Průběh kurzu

- Přednášky v D2 Po 14:00 – 15:30
- Doplňkové čtení, slajdy (před předn.) aj. v IS
  - *Také materiály k procvičení znalostí*
- Polosemetrální písemka letos nebude
- Závěrečná zkouška písemná
- Možnost pokračování v práci formou bakalářské či diplomové práce

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. PV017/018
- Úvod do kryptografie
- Digitální podpis
- Internet a bezpečnost, ochrana soukromí
- Biometriky

Témata kurzu – I

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

Témata kurzu – II

7. Úvod do biometrik
8. Biometrické autentizační metody
9. Problémy a využití biometrik
10. Úvod do řízení přístupu
11. Řízení přístupu – trendy, víceúrovňové systémy (MLS), tyto a další modely
12. PKI, prostředky pro autentizaci

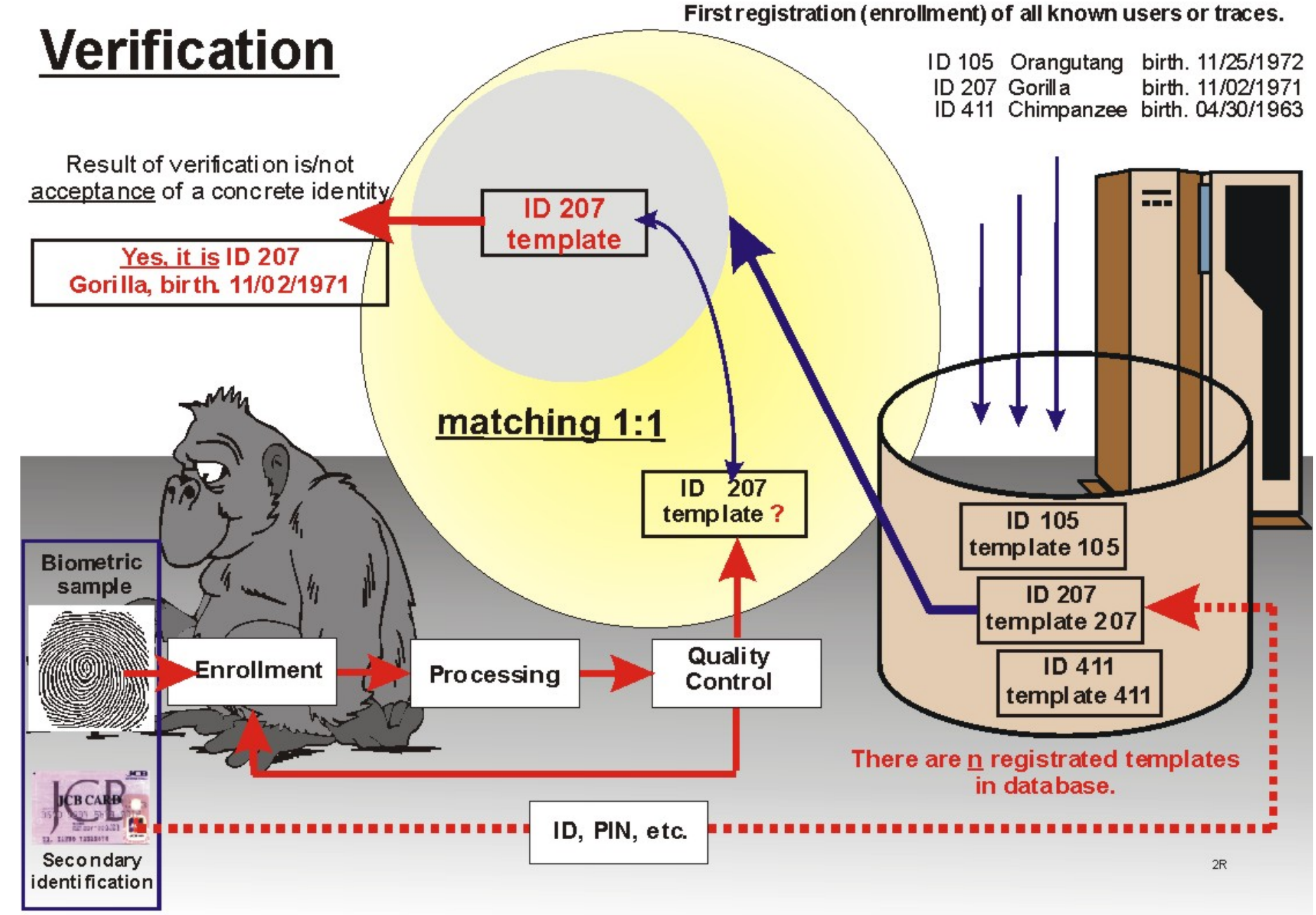
3 zásadní pojmy

- ***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.

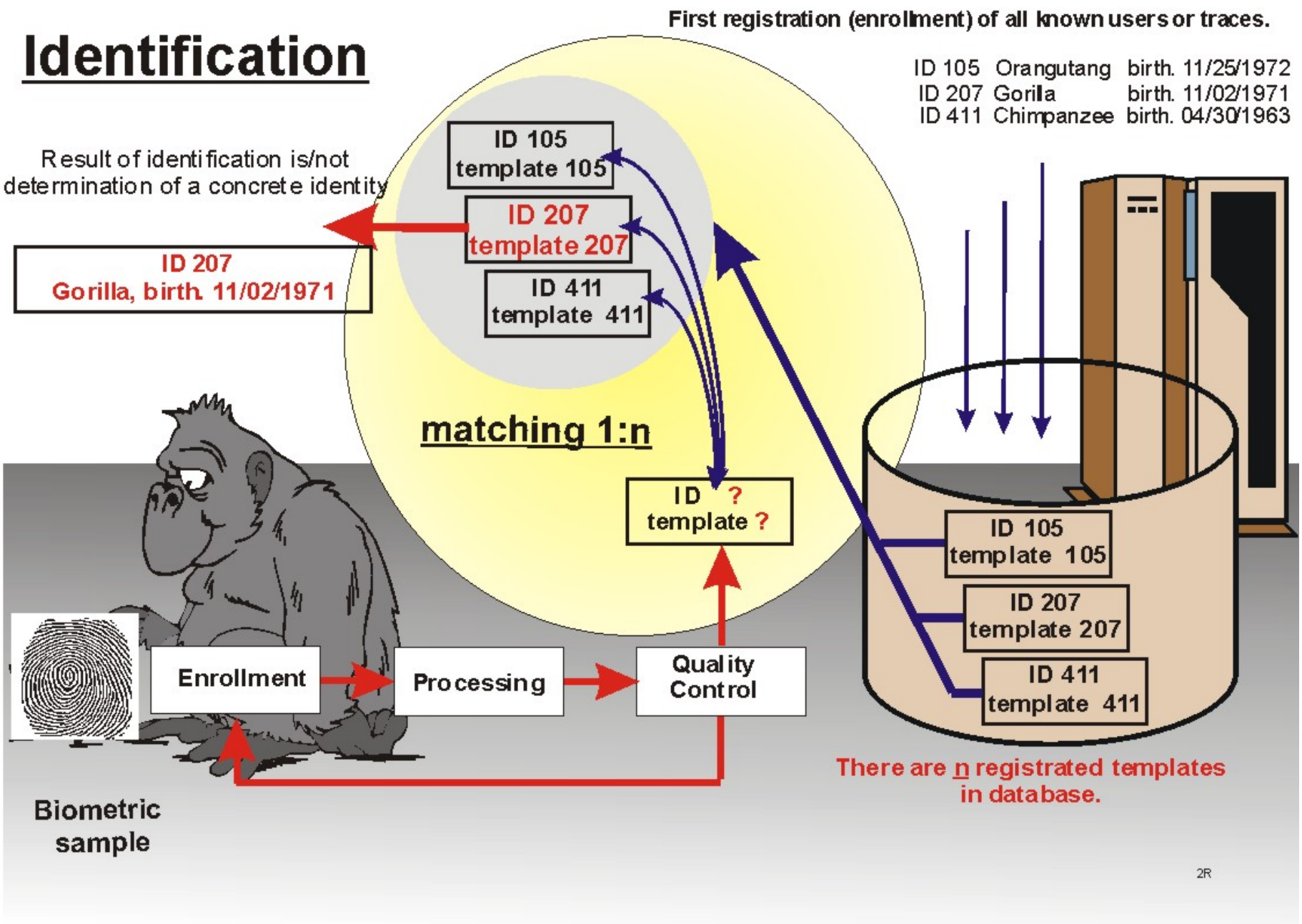
Autentizace a identifikace uživatele

- *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

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 orgánů
- 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

PKI

- Public-key infrastructure
  - Principy, použití
  - PKI není jen CA
  - PKI je prostředek, ne cíl
  - Výhody a nevýhody
- Na jednu z aplikací se podíváme v detailu na některé z posledních přednášek kurzu

Kryptologie

- Fyzická ochrana – cena!
- ***Kryptografie*** – ochrana významu (informační hodnotu) 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

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

Kryptografie – Kerckhoffův princip

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

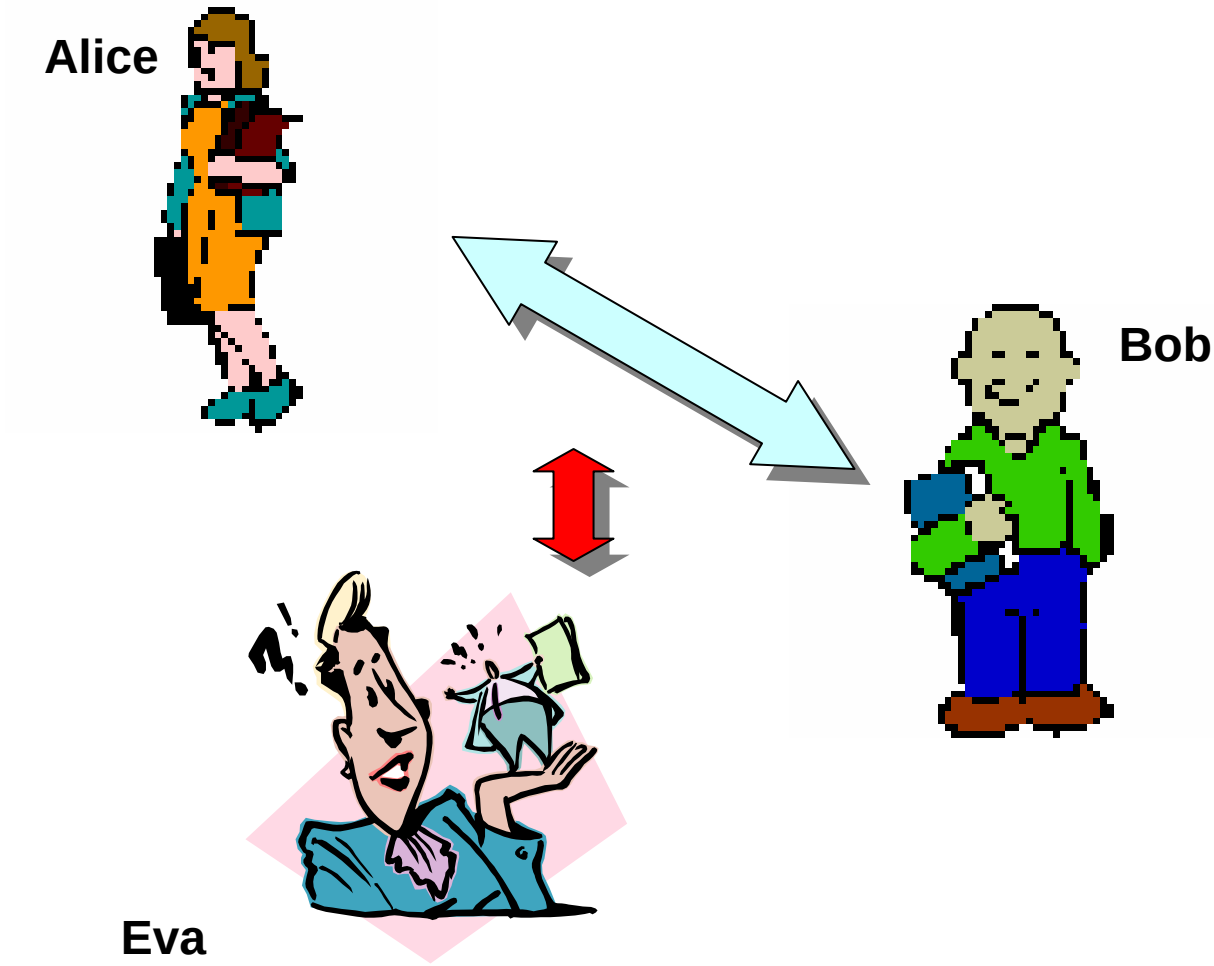
- Klíč – tajná informace – musí být chráněna před nepovolanými osobami

Co je hašování (hashování)

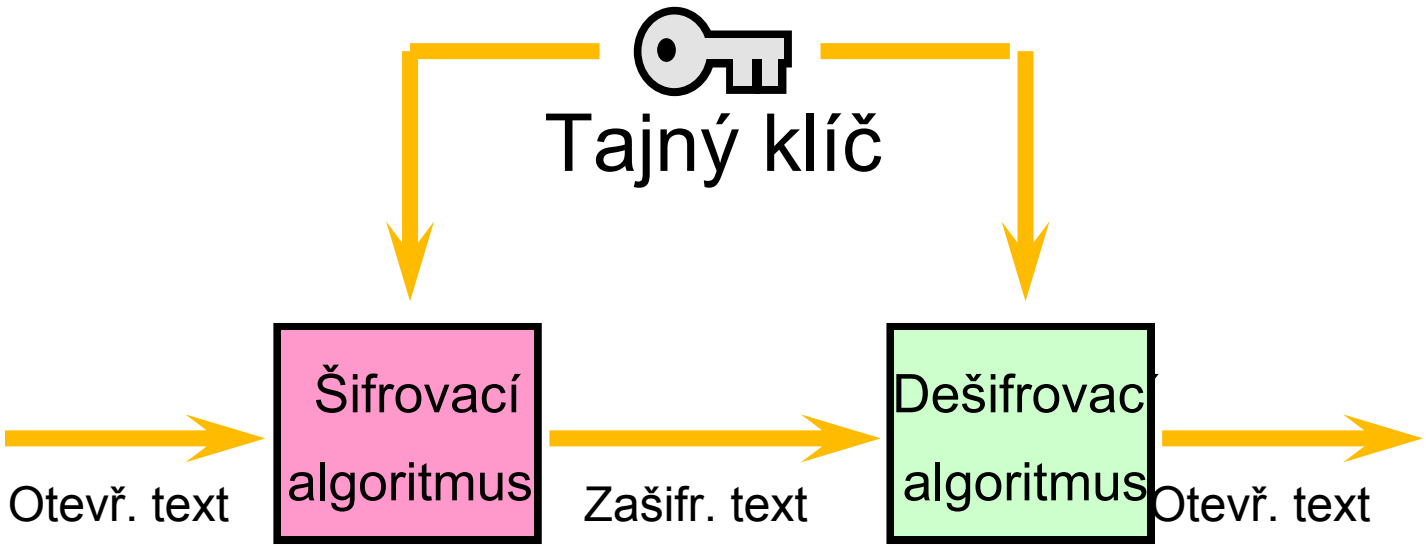
- “Otisk dat”
  - Malý a jedinečný reprezentant jakkoliv velkých dat
- 01:A0:7D:2B:76:52:67:05
- EC:43:6F:B3:68:CE:20:E7

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

Obvyklá označení činitelů

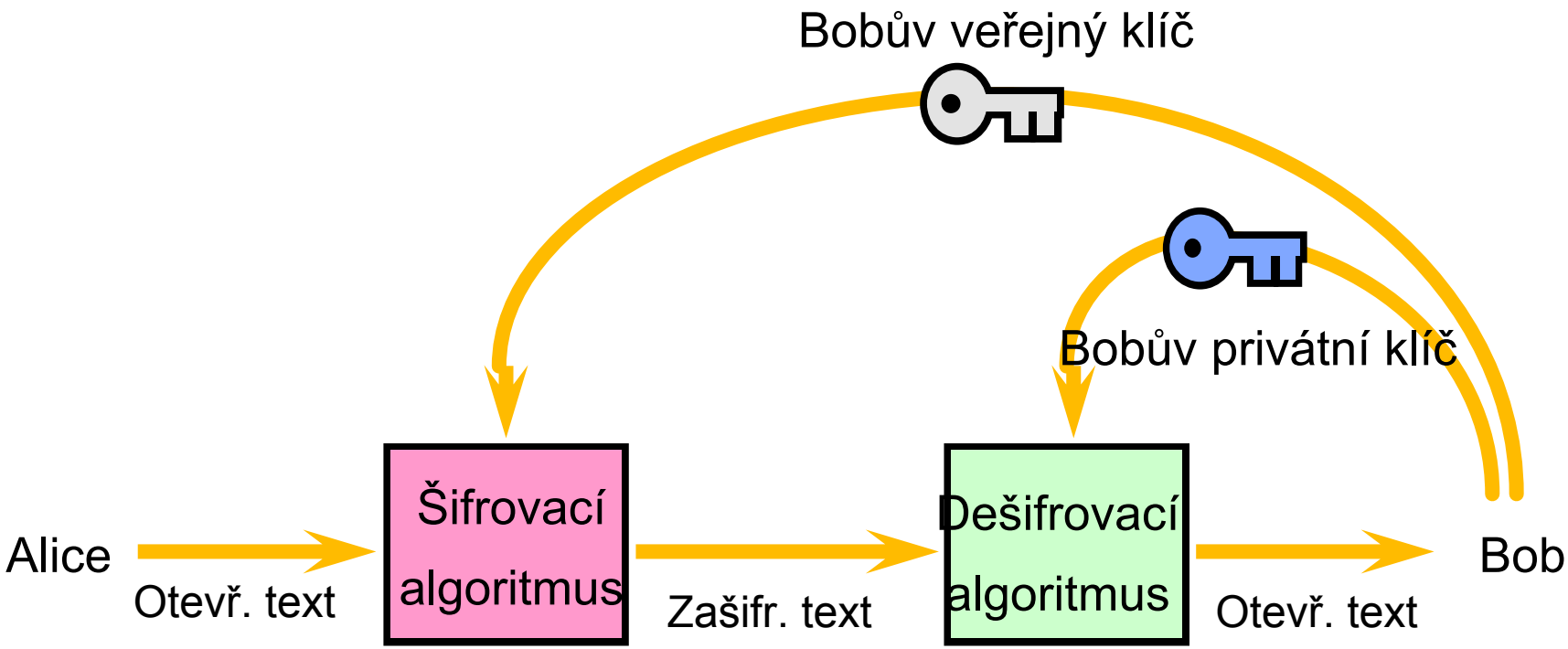


Zjednodušený model konvenčního šifrování



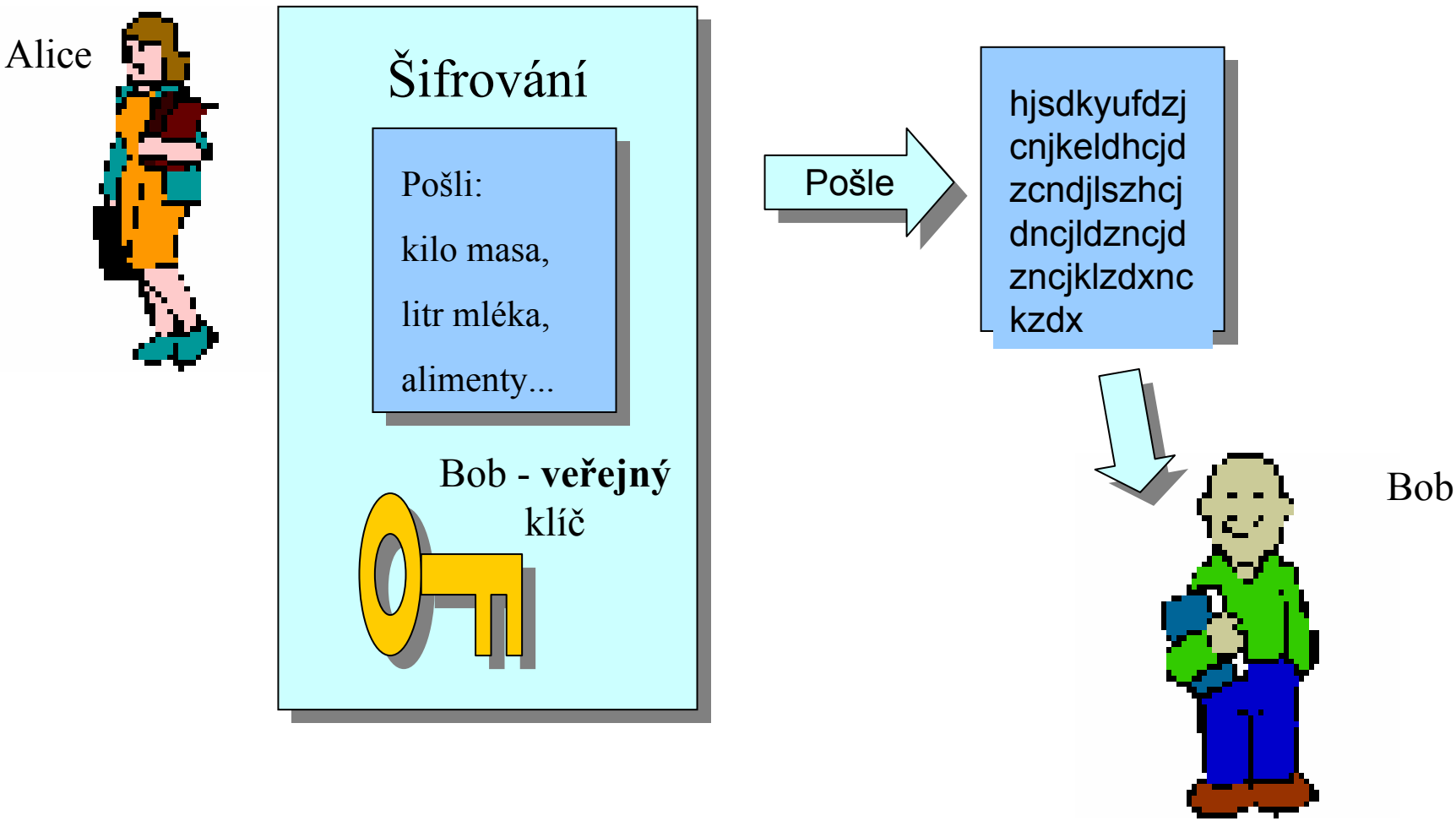
Převzato z: *Network and Internetwork Security* (Stallings)

Zjednodušený model šifrování veřejným klíčem

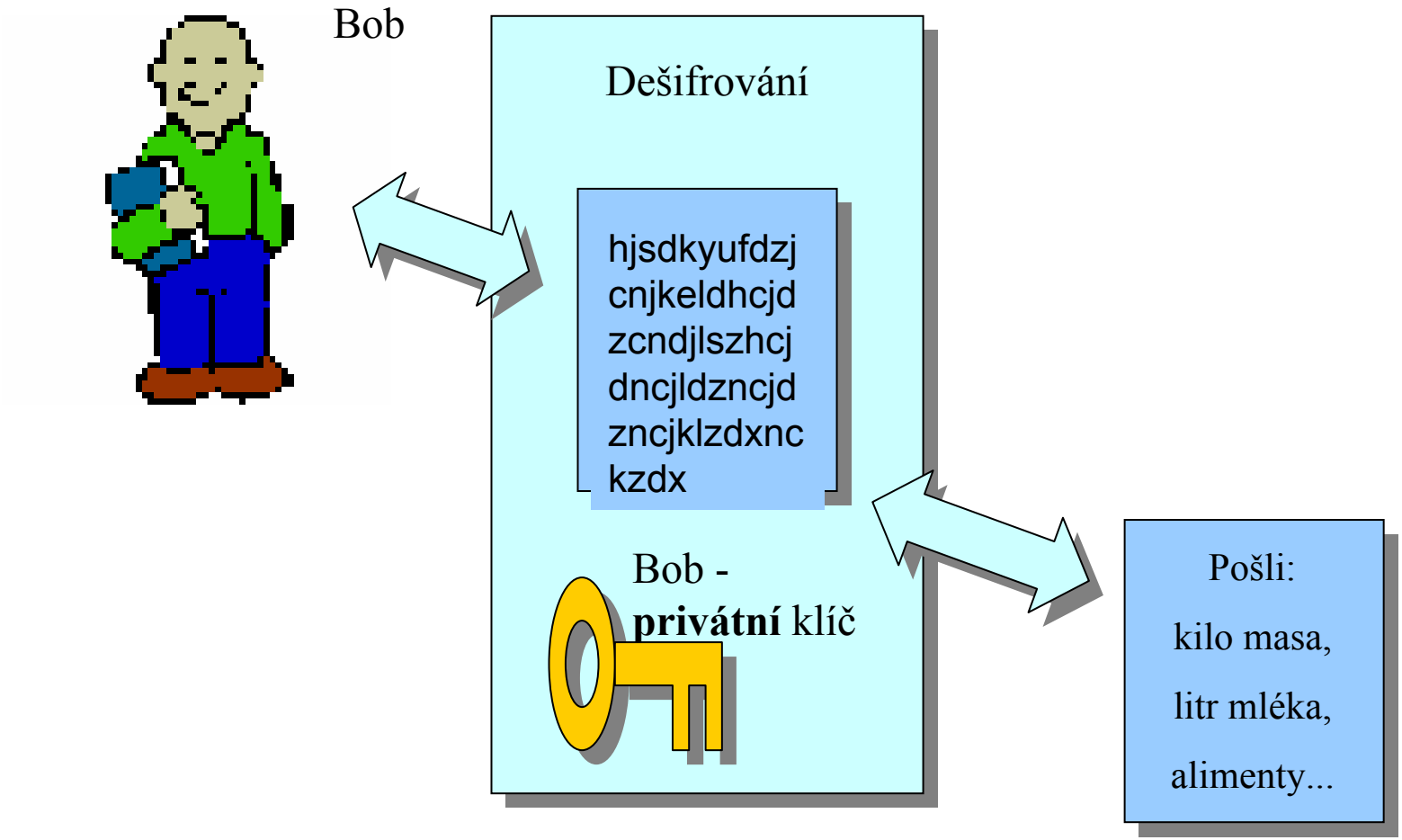


Převzato z: *Network and Internetwork Security* (Stallings)

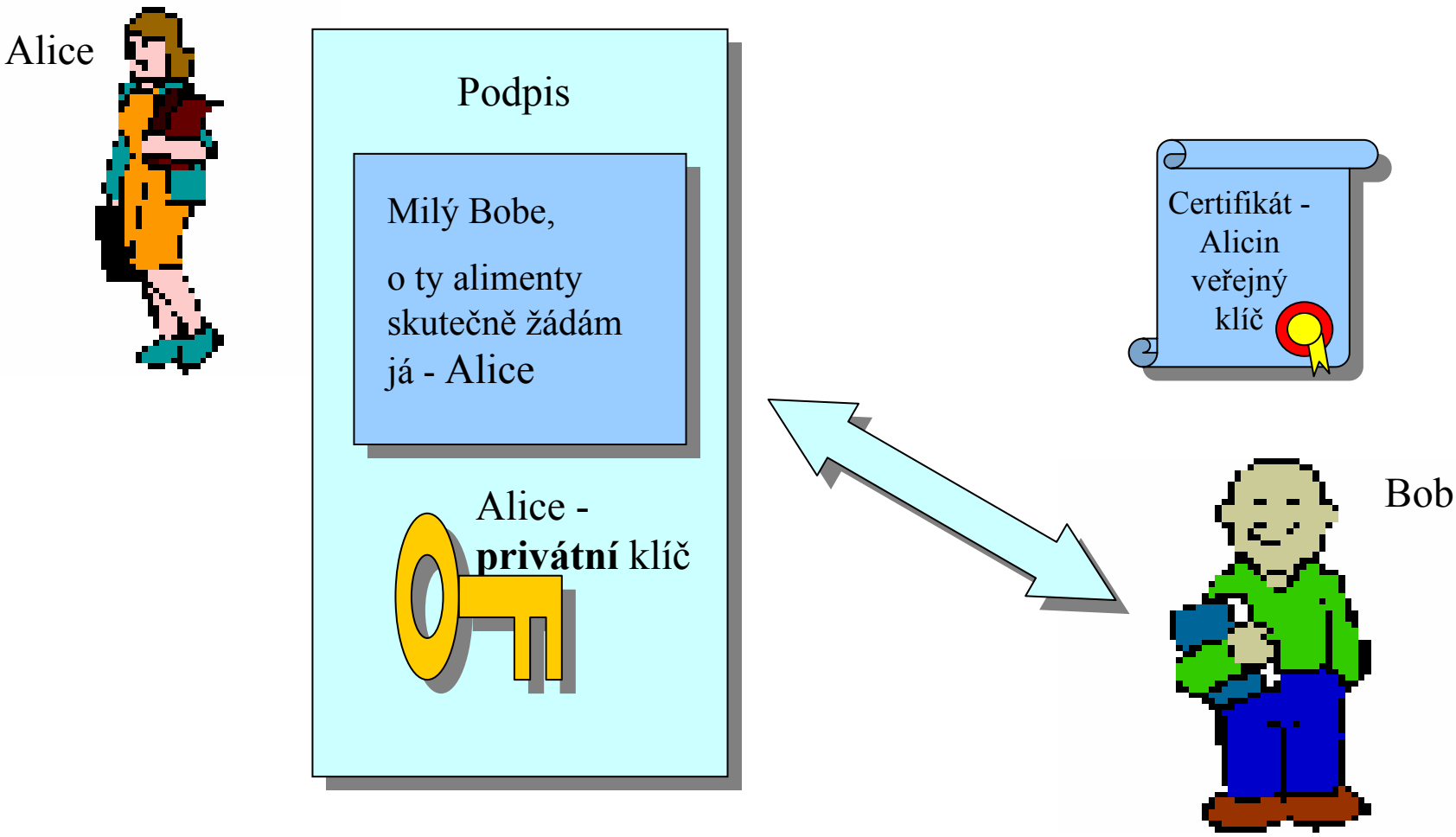
Šifrování veřejným klíčem



Dešifrování zprávy od Alice



Co je digitální podpis?



Autentizace dat a zpráv

Základní pojmy

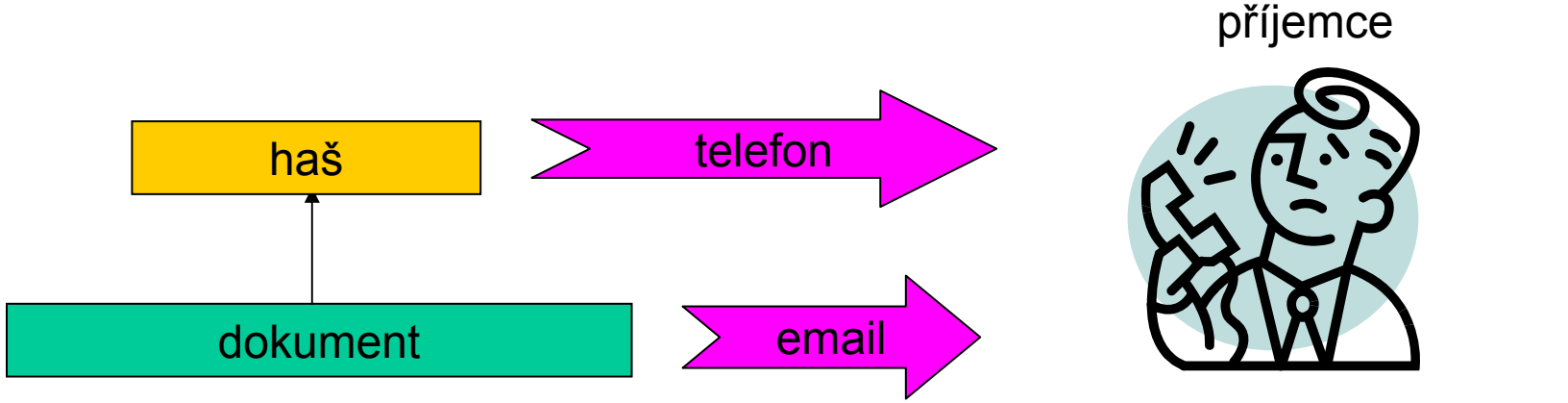
- **Integrita** dat – data nebyla neautorizovaně změněna (vložení dat, smazání dat, přeskupení dat…) od doby vytvoření, přenosu…
- **Autentizace původu** dat – potvrzujeme, že data pocházejí od určitého subjektu.

Metody autentizace dat a zpráv

- Bez použití kryptografie
  - CRC (Cyclic Redundancy Check).
- S použitím kryptografie
  - Sdílený tajný symetrický klíč.
  - Získání haše autentizovaným kanálem.
  - Haš s tajným klíčem / MAC (Message Auth. Code) – dříve označováno jako digitální pečeť.
  - Digitální podpis.

Hašování a autentizace dat

- Využití jiného komunikačního kanálu
  - Data pošleme standardním nezabezpečeným kanálem (např. elektronickou poštou).
  - Spočítáme haš dat a tento haš sdělíme příjemci jiným kanálem (např. telefonicky, na vizitce předané při osobním setkání).
  - Příjemce spočítá haš získaných dat a porovná haše.



Elektronický podpis

- Zákon o elektronickém podpisu č. 227/2000 Sb. (změněn zákony č. 226/2002, 517/2002 a 440/2004 Sb.).
- *„Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“*
- Elektronickým podpisem tak může být i pouhé jméno napsané na klávesnici.

Není podpis jako podpis

- Elektronický podpis
  - téměř cokoliv
- Zaručený elektronický podpis
  - v podstatě digitální podpis
- Zaručený elektronický podpis založený na kvalifikovaném certifikátu
  - digitální podpis, certifikát veřejného klíče vydán kvalifikovanou CA (splnila podmínky zákona a oznamovací povinnost)
- Zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb
  - také nazýván jako „uznávaný podpis“
  - digitální podpis, certifikát veřejného klíče vydán akreditovanou CA (splnila podmínky zákona a získala akreditaci)
  - jen tento podpis je uznáván v komunikaci se státní správou a samosprávou
  - v ČR dnes tři akreditované CA (I.CA, PostSignum, také eIdentity)

Zaručený elektronický podpis

- Je jednoznačně spojen s podepisující osobou (jen fyzická osoba!);
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě;
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou;
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Elektronická značka

- Jednoznačně spojena s označující osobou (i právnickou osobou nebo i org. složkou státu) a umožňuje její identifikaci prostřednictvím kvalifikovaného systémového certifikátu;
- byly vytvořeny a připojeny k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou;
- jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Elektronický podpis vs. značka

- Elektronický podpis
  - podepisující osoba je fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby;
  - pro ověření podpisu je vydáván certifikát (veřejného klíče).
- Elektronická značka
  - označující osobou fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou;
  - pro ověření podpisu je vydáván systémový certifikát (veřejného klíče).

Elektronický podpis vs. značka

- Technologicky jde o totéž
  - Jen úroveň ochrany soukromého klíče je jiná.
- Podle vyhlášky č. 366/2001 Sb. se jedná o klasické algoritmy digitálního podpisu
  - (asymetrický kryptografický algoritmus, hašovací funkce):
  - RSA, SHA1
  - RSA, RIPEMD160
  - DSA, SHA1
  - ECDSA-F_p, SHA1
  - ECDSA-$F2^m$, SHA1
  - RSA, MD5

Elektronický podpis vs. značka

- Rozdíl je pouze procedurální
  - „Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se **podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila**.“ (§3 odst. 1)
    „Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.“ (§3 odst. 2)
  - „Použití elektronické značky založené na kvalifikovaném systémovém certifikátu a vytvořené pomocí prostředku pro vytváření elektronických značek umožňuje ověřit, že datovou zprávu označila touto elektronickou značkou označující osoba.“ (§3a odst. 1)
    „Pokud označující osoba označila datovou zprávu, má se za to, že tak učinila **automatizovaně bez přímého ověření obsahu datové zprávy** a vyjádřila tím svou vůli. “ (§3a odst. 2)

Otázky?

Vítány!!!

Příští přednáška 27. 2. 2006 14:00

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