Internet a zdravotnická informatika

ZS 2007/2008

Zoltán Szabó
Tel.: (+420) 312 608 207
E-mail: szabo@fbmi.cvut.cz
č.dv.: 504, 5.p

Dnešní přednáška

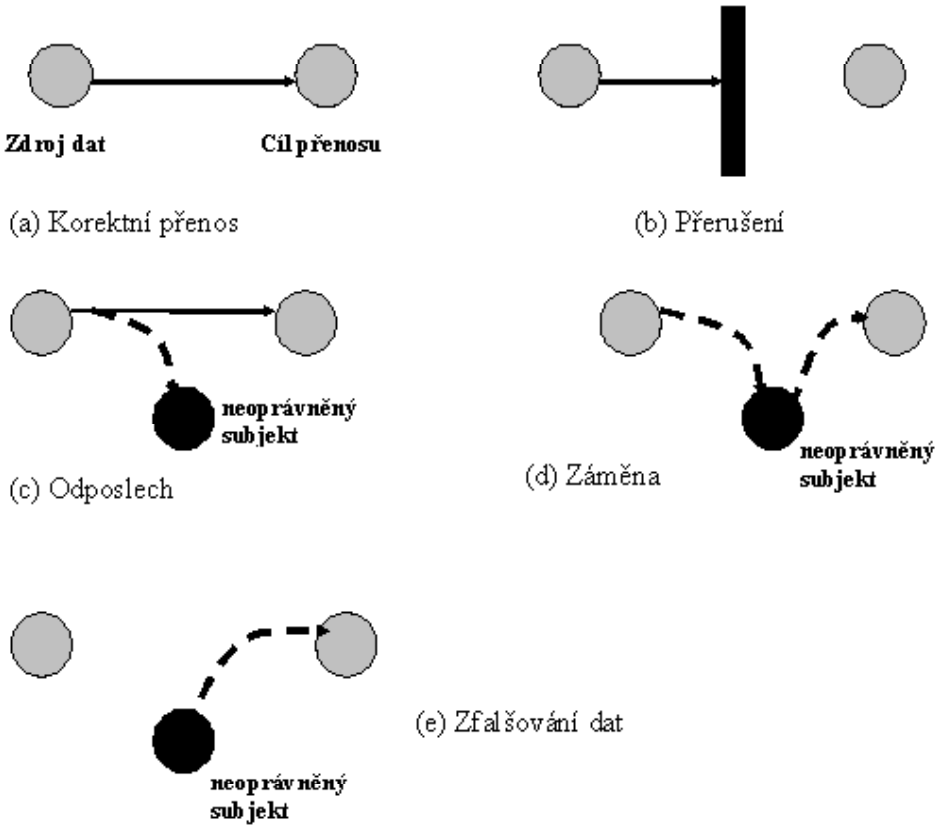
- Bezpečnost dat
- Virus, červ a trojský kůň
- Základní bezpečnostní koncepty – Šifrování
  - Symetrický šifrovací algoritmus
  - Asymetrický šifrovací algoritmus
- Výtah zprávy (hash)
- Řízené uživatelské přístupy

Bezpečnost dat

Výpočetní systém = HW + SW + data

Typy hrozeb

1. Přerušení
2. Odposlech
3. Pozměnění
4. Vytvoření falsifikátu



Virus, červ a trojský kůň

- Počítačový kód, který připojí sám sebe k programu nebo souboru a může se šířit mezi počítači. Při tomto šíření napadá počítače. Viry mohou poškodit váš software, hardware i soubory.

- Červ (podtřída viru) je stejně jako virus formován tak, aby kopíroval sám sebe z jednoho počítače do jiného, ale činí tak automaticky (velmi rychle se šíří).

- Trojský kůň je počítačový program, který se jeví jako užitečný, ale ve skutečnosti působí škody. Může být součástí softwaru, který stáhnete zdarma.

Počítačové viry

1. Neškodné
2. škodné.

1. viry, které napadají spustitelné soubory
2. viry, které napadají zaváděcí program OS.
3. makro viry, které napadají uživatelské programy.

Projevy virů

- **Blokování místa.** Vir musí být někde uložen, a to buď v paměti nebo na pevném disku (nebo na obou místech).
- **Zpomalení práce systému.** Vir pro svou "činnost" potřebuje část pracovních systémů počítače, které tak "krade" jiným programům.
- **Nestabilita systému.** Viry nejsou testované pro různé počítače a konfigurace hardware a software, a tak systém může často bez zjevné příčiny "zatuhnout".
- **Krádež dat.** Oblíbená kratochvíle především e-mailových virů, které čas od času odešlou elektronickou poštou náhodnému či předem určenému příjemci data z počítače.
- **Šifrování dat.** Některé viry se projevují tak, že zašifrují data na pevném disku, která berou jako "rukojmí" a za šifrovací klíč mohou požadovat finanční obnos na příslušné konto, nebo jen svoje nesmazání ze systému.
- **Zničení dat.** To je snad jedna z nejhorších věcí, která vás může potkat, pokud pravidelně nezálohujete data.

Kam kráčí počítačové viry?

- **Rychlost šíření**. Bude čím dál větší roli hrát Internet. Např. vir *I love you* během několika hodin zaútočit na milióny počítačů na celém světě.
- Viry budou k dispozici také pro čím dál **větší množství aplikací**.
- Větší **rozšíření pro "newindowsovské" OS**.
- **Počítačový terorismus** - Vzroste i počet virů "šitých na míru" s cílem poškodit konkurenci nebo nechat zašifrovat data na pevných discích a následně za jejich dekódování.
- Viry pro **mobilní telefony** a další podobná zařízení.

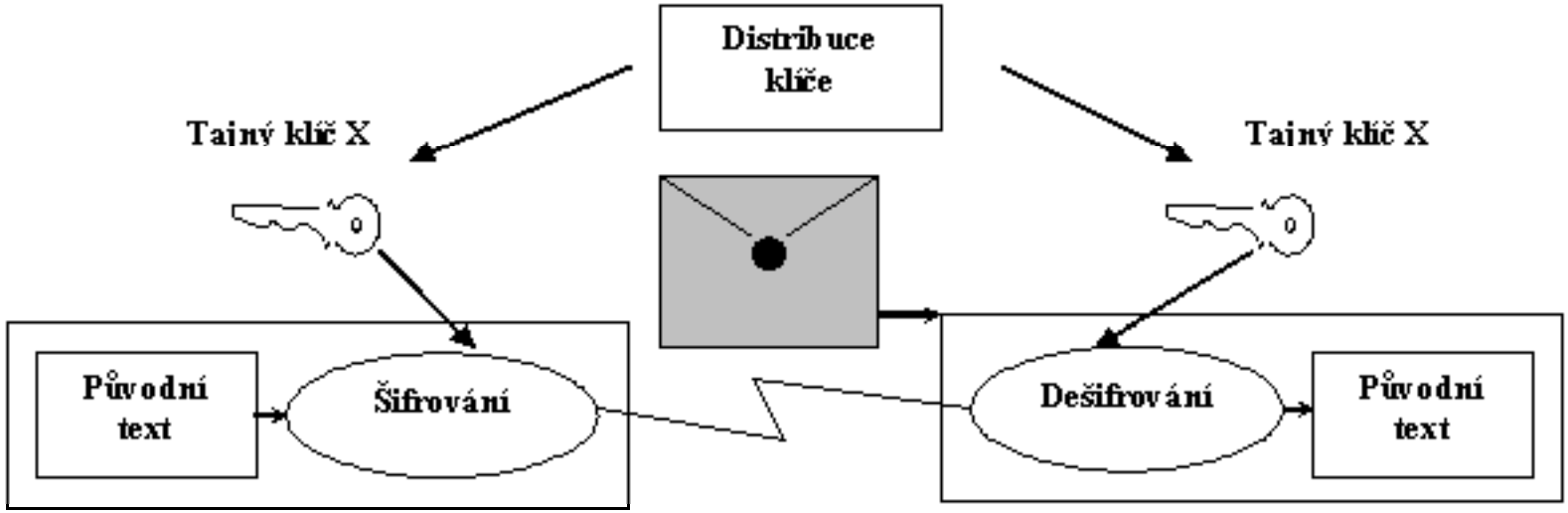
Zabezpečení

- Je třeba stanovit přiměřený způsob zabezpečení
- Zajistit
  - ***důvěrnosti dat*** - přístupná pouze pro autorizované subjekty.
  - ***autenticity dat*** (kdo je autorem dokumentu)
  - ***celistvosti (integrity) dat*** (příjemce s určitostí ví, že obsah podepsaného dokumentu nebyl pozměněn).
  - ***neodmítnutelné odpovědnosti*** (příjemce může prokázat, kdo je autorem dokumentu s daným obsahem)
  - ***dostupnosti dat*** - což znamená, že musí být pro oprávněné subjekty zajištěn přístup k dokumentu s daným obsahem

Šifrování

- *kryptologie* - věda o šifrování, zahrnuje dvě odvětví:
  - *kryptografii* - vědu o tvorbě šifer
  - *kryptoanalýzu* - vědu o luštění šifer
- *kryptosystém* - systém, ve kterém se provádí šifrování a dešifrování

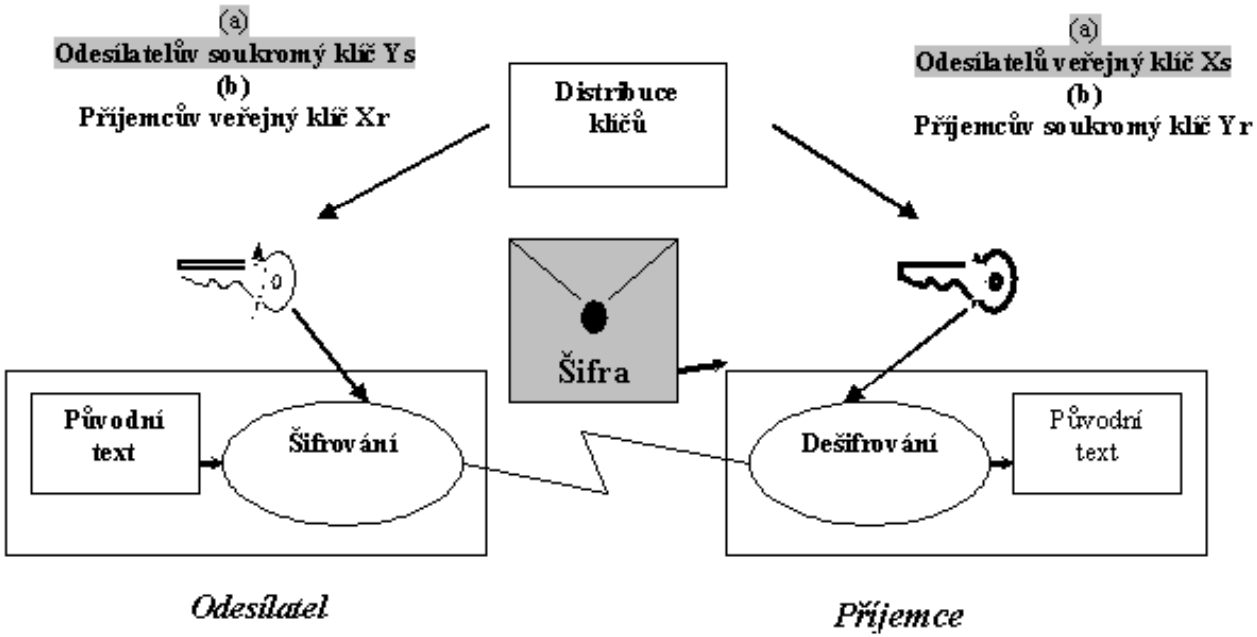
Symetrický šifrovací algoritmus



Mezi nejznámější standardy pro symetrické šifrování současnosti patří:

- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- RC2 a RC4 (Rivest Cipher).

Asymetrický šifrovací algoritmus



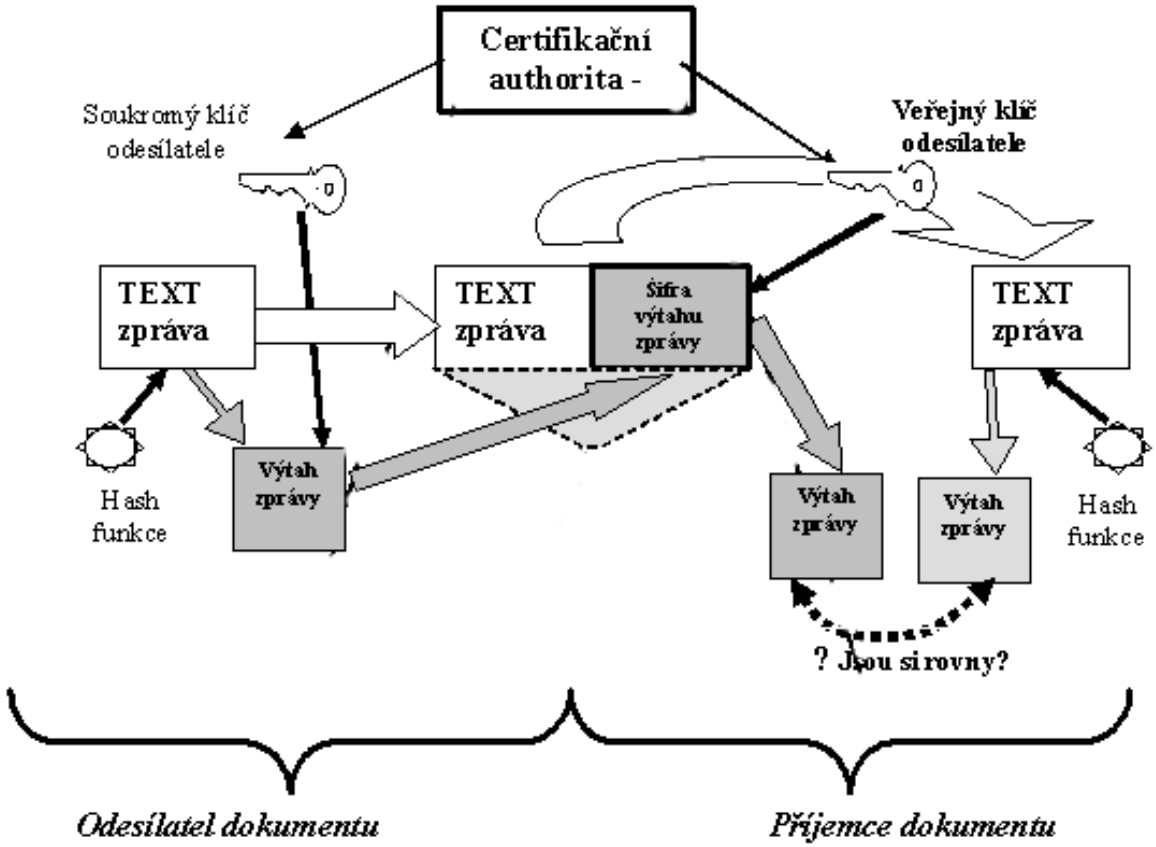
Přenášená data nemají chráněnu důvěrnost
avšak **u dat je zajištěna autenticita**

Mezi nejznámější standardy pro asymetrické šifrování patří:

- RSA (Rivest Shamir Adleman -- *jména tvůrců algoritmu*)
- DSS (Digital Signature Standard)
- EC (Eliptic Curve).

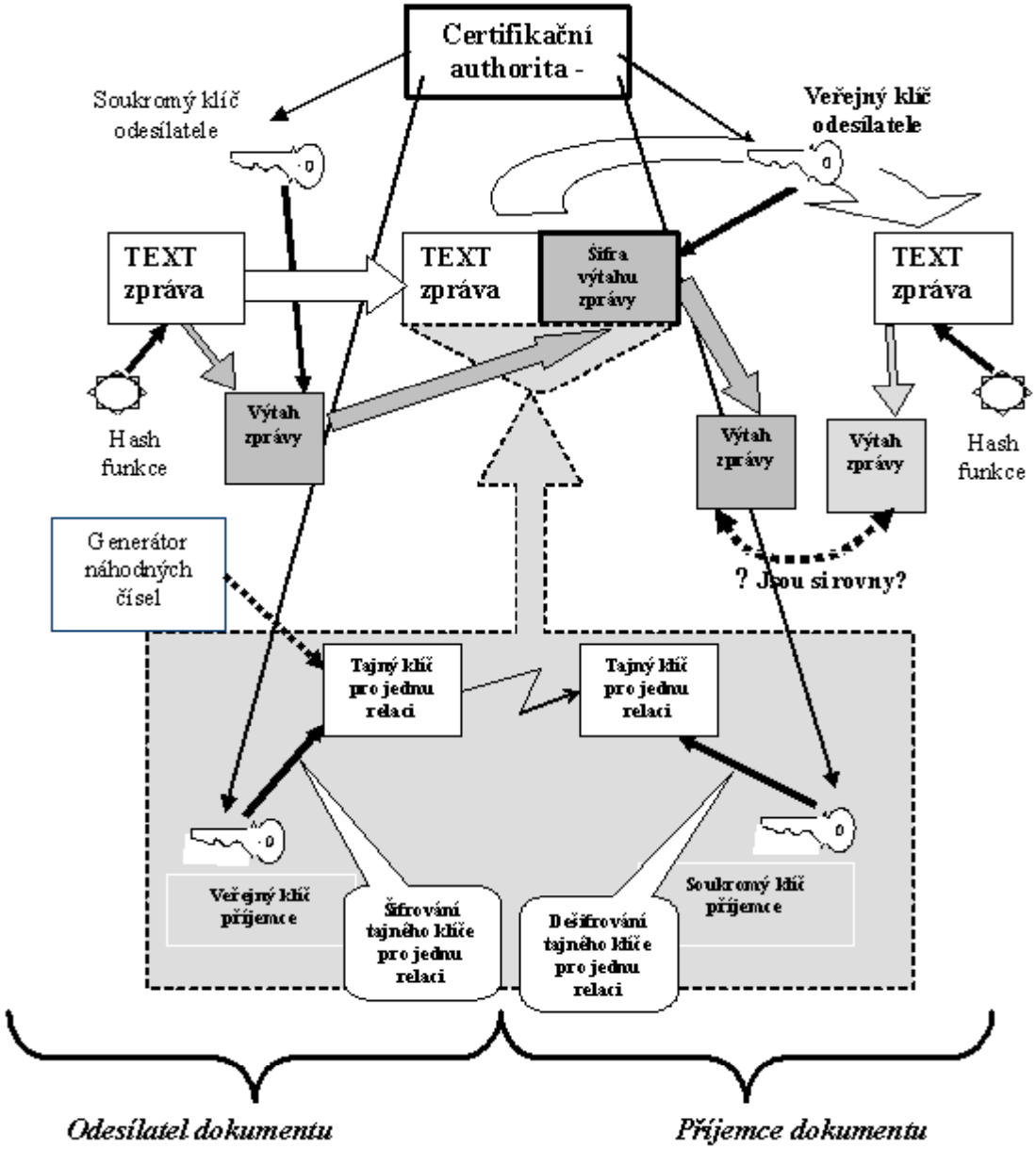
Výtah zprávy (hash)

Hash funkce je technika ověřující pravost zprávy, tzn. její **autenticitu** a **celistvost**.



Dodatečné šifrování dokumentu

- Odesílatel dokumentu vlastní svůj soukromý klíč a má k disposici veřejný klíč příjemce dokumentu.
- Příjemce dokumentu vlastní svůj soukromý klíč a má k disposici veřejný klíč odesílatele dokumentu.



Řízené uživatelské přístupy

autentizace v sítích

Smart Card

iKey

Díky za pozornost

Následující přednáška
22.11.2007