PB001 Úvod do informačních technologií

Zálohování a bezpečnost

Doc. RNDr. Eva Hladká, Ph. D.

Fakulta Informatiky

podzim 2013

- Zálohování
  - Princip redundance
    - příroda
    - data: náklady $\times$ zajištění
  - Manuální zálohování
  - Zálohovací systémy s verzováním
  - RAID
  - Zálohování na MU
- Bezpečnost
  - Teoretické základy
  - Síťová bezpečnost
  - Bezpečnost $\times$ zveřejňování dat

Princip redundance

- Příroda
  - Párové orgány – např. ledviny
  - náklady $\times$ šance na přežití
- Lidé a dokumenty
  - originál a kopie
    - kvalita kopie
  - náklady na kopii – čas, energie, lidská práce
- Zajištění
  - dokumenty (data) zajištěna proti ztrátě
  - náklady na uchovávání kopií

Data v elektronické podobě

- Elektronická data:
  - multimediální povaha – text, zvuk, obraz, video. . . .
  - kopie ve stejné kvalitě – stejný datový objem, nelze rozlišit kopii a originál
  - kopie v nižší kvalitě
- Náklady na archivování
- Malá časová stabilita el. médií
- Elektrická energie

Manuální zálohování

- Zálohování bez podpory SW systémů
- Záloha – přesný obraz původního souboru, adresáře, systému souborů, ...
- Časový režim – důvody
- 1 – 7 – 28

Zálohování s verzováním

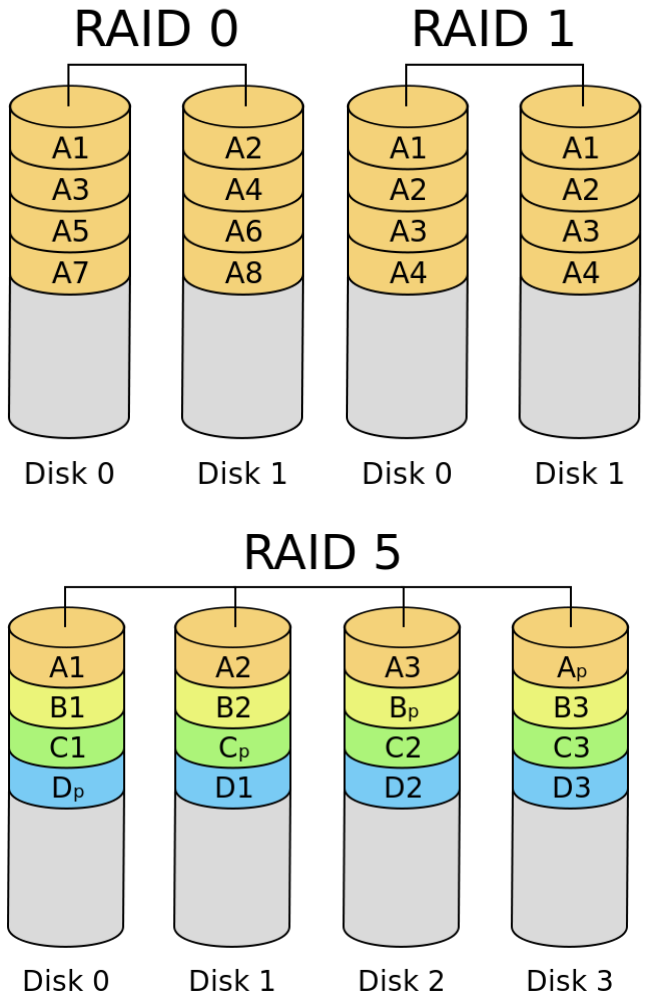
- Verze – práce několika jedinců nad jedním dokumentem
- Možnost se vrátit k předchozím podobám dokumentu
- CVS, SVN, GIT
- CVS – Concurrent Version System
  - repozitář obsahující 1 nebo více skupin souborů
  - víceuživatelská klient–server aplikace
  - příkazový řádek nebo graf. nadstavba (WinCVS)
- GIT
  - distribuovaný systém správy verzí
  - vytvořený původně pro vývoj jádra Linuxu

Ukázka příkazů verzovacího nástroje CVS

```
export CVSROOT=:gserver:lindir.ics.muni.cz:/cvs/collab
# ... export nastavení

cvs co eva-thesis
# ... vytvori lokalni kopii z CVSky (vytvori adrear eva-thesis)

cd eva-thesis

cvs update
#  ... zaktualizuje obsah aktualního adresáře, případně sloučí
       změny oproti repozitáři a vyhlásí, co nemohl sloučit,
       pokud je konflikt příliš zásadní (pak jsou označeny relevantní
       části souboru pomocí >>>> <<<<)

cvs ci
#  ... uloží aktuální verzi souborů do CVS

cd ..

cvs rel -d eva-thesis
  ... zkontroluje, jestli všechny změny byly commitnuty
```

RAID

- Ukládání na discích / diskových polích a redundance (zabránění ztráty dat)
- RAID – Redundant Array of Inexpensive/Independent Disks – vícenásobné diskové pole
  - metoda zabezpečení dat proti selhání pevného disku
  - ukládání dat na více nezávislých disků, uložená data zachována i při selhání některého z nich
  - úroveň zabezpečení se liší podle zvoleného typu RAID, které je označováno čísly
  - dojde-li k výpadku některého disku, je výkon pole nižší, avšak stále jsou všechna uložená data k dispozici



Zálohování na MU

- MU – centrální zálohovací systém spravovaný ÚVT MU
  - System NETWORKER od EMC (dříve Legato)
  - Uchovávají se data, jména souborů, poloha na disku
  - Časové značky $\Rightarrow$ lze se vrátit i ke starším verzím
  - Nevhodný pro archivaci databází (nutno zálohovat v jiném režimu)
  - Historie cca 2 měsíce
  - 2 servery + pásková knihovna
  - Brzy data z MU na datové úložiště CESNETu

Zálohování a IS

- Student má tyto možnosti zálohování dat v ISu (i po úspěšném absolvování)
  - *Můj web* – 500 MB
  - *Úschovna* – 5 GB POZOR expiruje !!!
  - *Dokumentový server* – pouze pro spec. typ souborů
  - *Kruhy* $\rightarrow$ v aplikaci Náš web
    - nápověda https://is.muni.cz/auth/help/komunikace/kruhy
    - kapacita úložného prostoru dle velikosti Kruhu

Bezpečnost – zpřístupňování dat

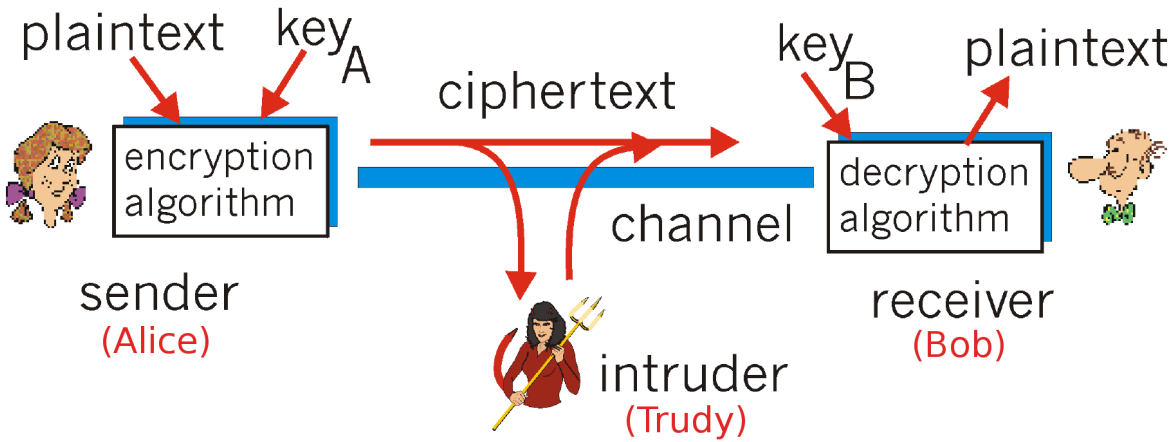
- Dva základní přístupy
  - Zveřejním vše – neexistují data, kterými by mě bylo možno vydírat, ale vše je o mě známo a nic nemohu skrýt
  - Nezveřejním nic, co nemusím
- Veřejný informační prostor
  - využití mnou zveřejněných dat v můj neprospěch
  - zneužití mnou zveřejněných dat
  - zneužití mé identity

- ACL (Acces Control List), připojen ke každému souboru
- Základní ACL (UNIX like)
  - `r` – read, čtení
  - `w` – write, zápis
  - `x` – spuštění (sestup do podaresáře)
- Definována pro trojici (svět, skupina, vlastník)

- Zabezpečení = klasický problém *Kryptografie*

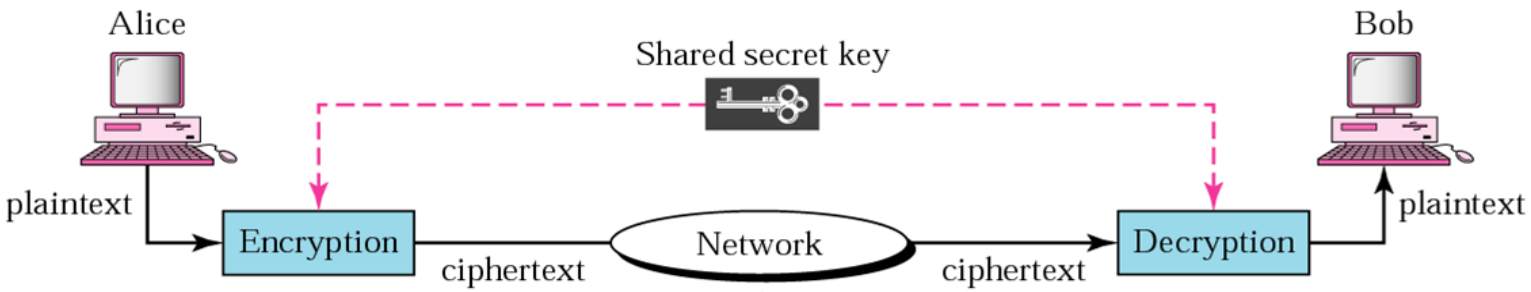
Kryptografie (Cryptography):

- Nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí (= *klíčem*)
- Základní mechanismy kryptografie:
  - kryptografie s využitím symetrických klíčů (*symetrická kryptografie*)
  - kryptografie s využitím asymetrických klíčů (*asymetrická kryptografie*)



Symetrická kryptografie

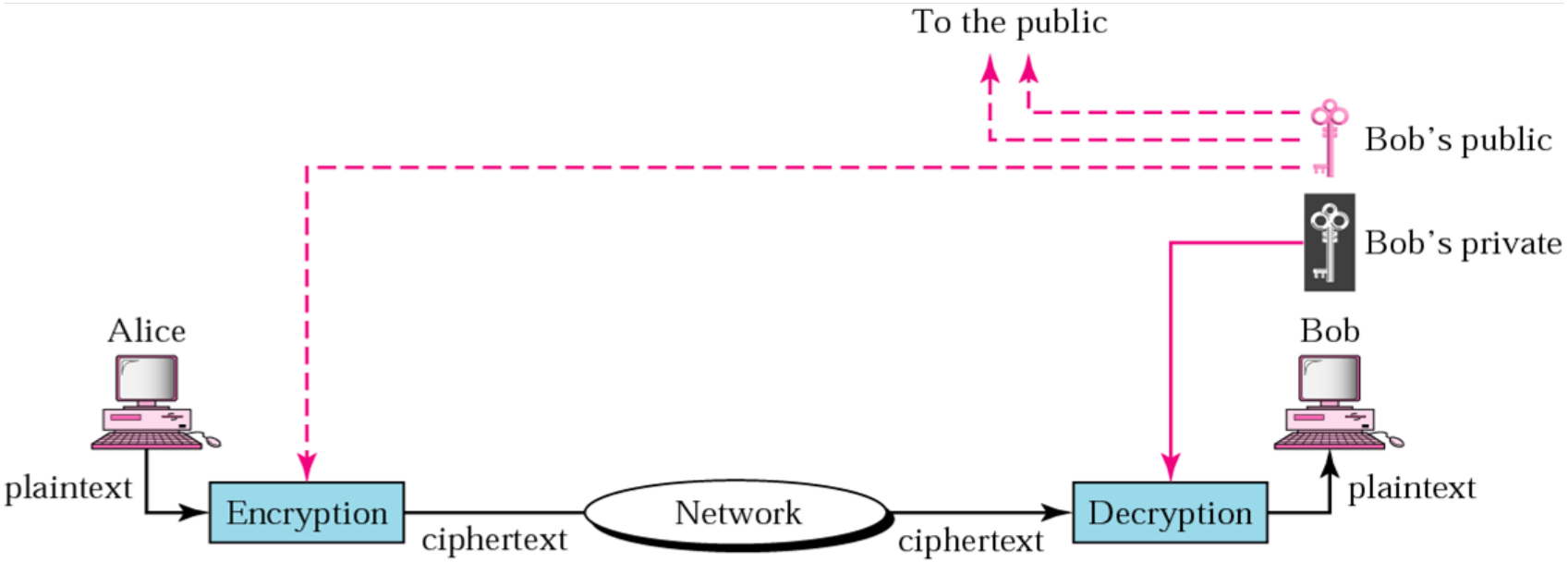
- K šifrování i dešifrování využit jediný klíč
- Výhody:
  - nízká výpočetní náročnost
  - vhodné pro šifrování dlouhých zpráv
- Nevýhody:
  - nutnost sdílení tajného klíče
- Např. DES, 3DES, IDEA, apod.



Asymetrická kryptografie

- Též *Kryptografie veřejným klíčem*
- K šifrování je použit jiný klíč než pro dešifrování
  - oba klíče se dohromady nazývají *pár klíčů (keypair)*
  - šifruje se pomocí *veřejného klíče (public key)*, dešifruje pomocí *soukromého klíče (private key)*
    - zpráva zašifrovaná veřejným klíčem lze dešifrovat **pouze** příslušejícím soukromým klíčem
- Výhody:
  - není potřeba nikam posílat šifrovací klíč $\Rightarrow$ snížení rizika jeho vyzrazení/odposlechnutí
  - veřejný klíč je možno dát všem
- Nevýhody:
  - rychlost $\Rightarrow$ asymetrické šifry jsou vhodné pro krátké zprávy
- Např. RSA, DSA, apod.

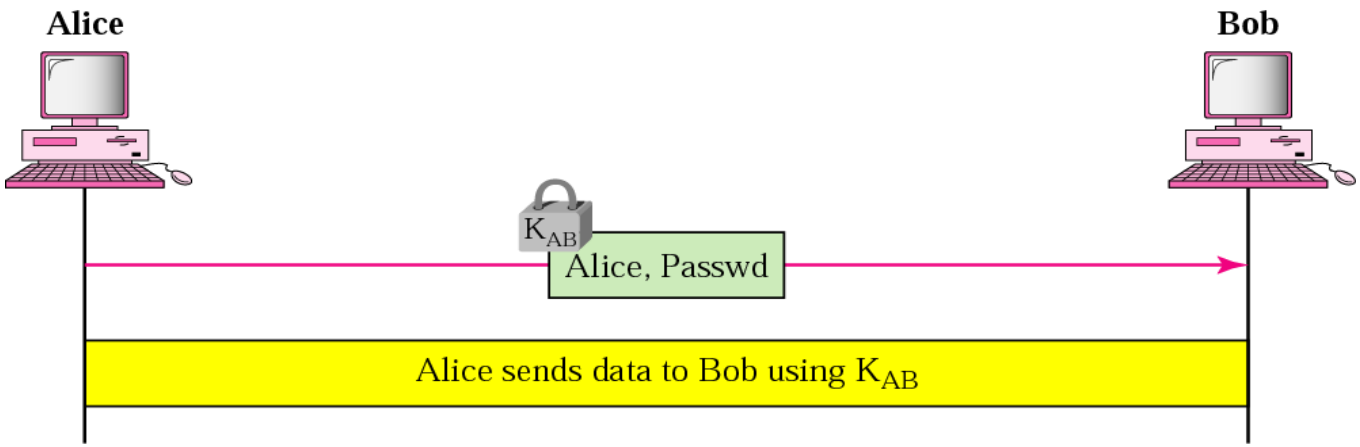
Asymetrická kryptografie
Ilustrace



- *Certifikát* – informace, která váže identitu entity (uživatel, server, . . .) s jeho veřejným klíčem
- 4 základní informace obsažené v certifikátu:
  - *jméno vlastníka (držitele)*
  - **hodnota veřejného klíče**
  - *doba platnosti veřejného klíče*
  - *podpis vydavatele certifikátu*
- Certifikáty vydávají tzv. *Certifikační autority*
  - organizace, kterým se důvěřuje
  - vydané certifikáty mohou být dostupné na veřejném serveru
    - kdokoli může o jeho kopii požádat

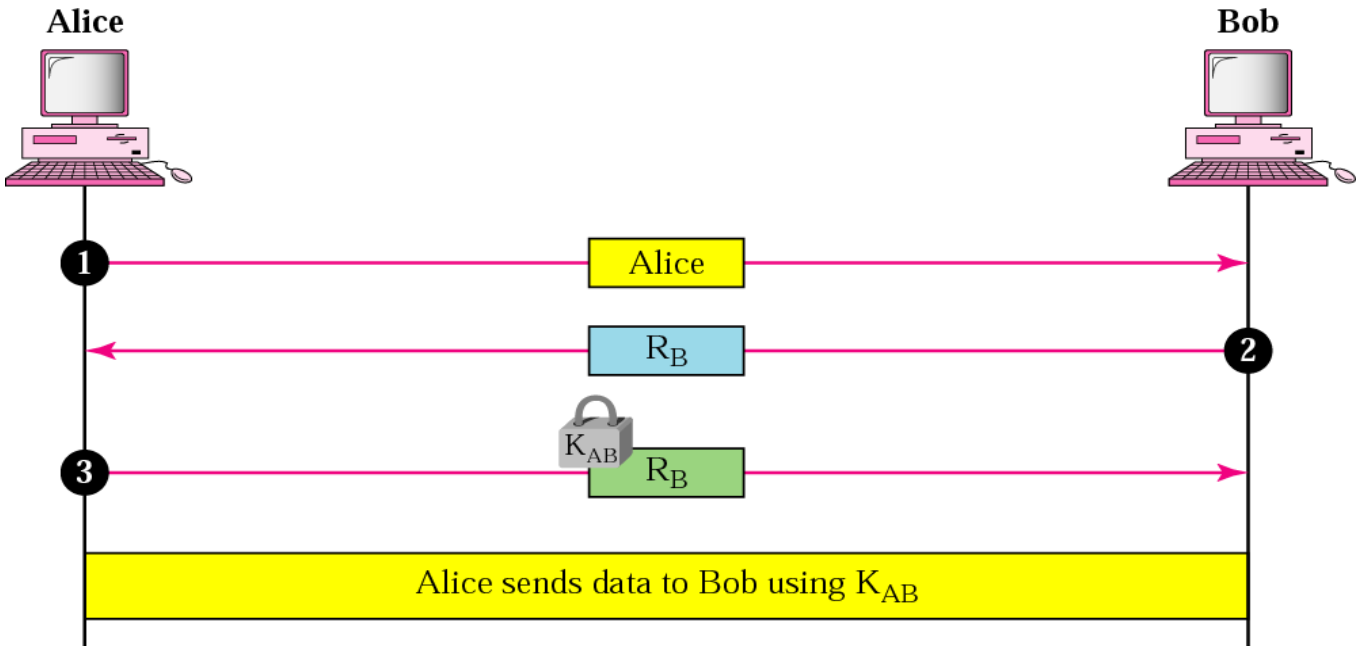
Autentizace heslem:

- Alice se autentizuje Bobovi zasláním hesla
- Heslo je šifrováno sdíleným symetrickým klíčem
- – negarantuje „čerstvost“ hesla
  - heslo mohlo být uloženo a nyní se jedná o pokus o opakovanou autentizaci (možný útok)



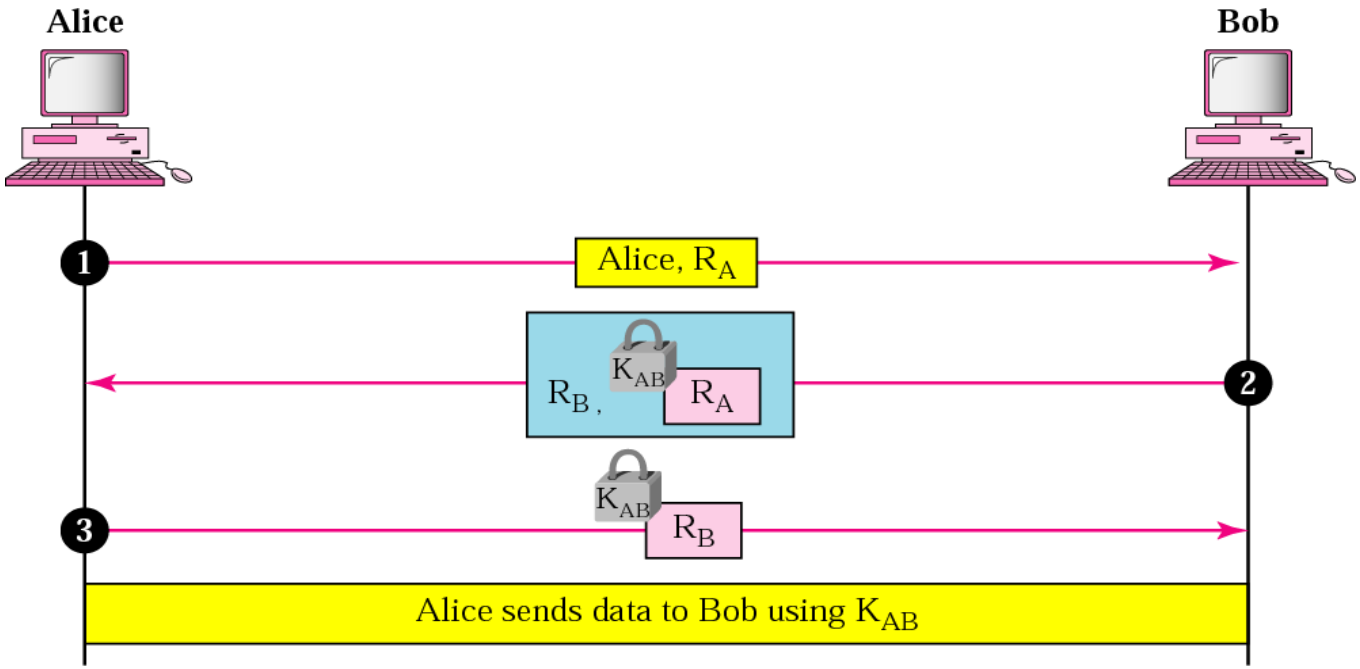
Autentizace s využitím náhodných čísel:

- Alice si od Boba vyžádá zaslání náhodného čísla (tzv. *keksík*)
- Alice toto náhodné číslo zašifruje symetrickým klíčem
- \+ řeší problém „čerstvosti“ hesla



Vzájemná autentizace s využitím náhodných čísel:

- Stejný princip jako předchozí, autentizace je však obousměrná



Zajištění důvěrnosti přenosu – šifrování

- Přenášená data šifrována nejčastěji s využitím *symetrické kryptografie*
- Pro získání sdíleného tajemství (před začátkem přenosu) lze využít:
  - např. *algoritmus Diffie-Hellman*
  - *asymetrickou kryptografii* – zvolený symetrický klíč je šifrován veřejným klíčem protistrany

Zajištění integrity a nepopíratelnosti přenosu – digitální podpis

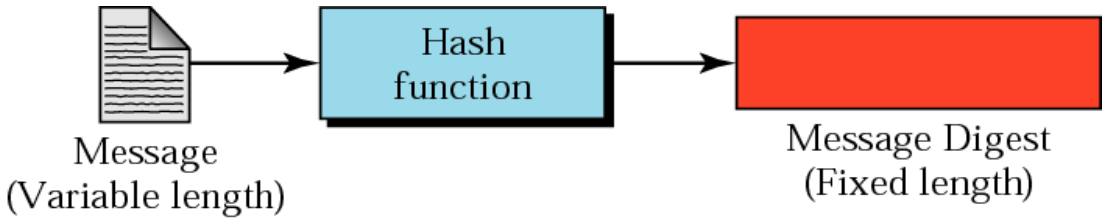
Digitální podpis:

- Mimo integrity a nepopíratelnosti zajišťuje i autentizaci komunikujících stran
- Obrácený mechanismus asymetrické kryptografie
  - zpráva podepisována (= šifrována) soukromým klíčem odesílatele, ověřována (= dešifrována) veřejným klíčem odesílatele
- 2 základní mechanismy:
  - podpis celého dokumentu
  - *podpis otisku dokumentu* (tzv. *message digest*, *hash*)
    - nejčastěji využívané
    - ze zprávy vypočten *otisk (hash)*, který je pak podepsán (= šifrován soukromým klíčem odesílatele) a odeslán spolu s původním (**nijak nešifrovaným**) dokumentem
    - řeší problém podpisu dlouhých zpráv, pro které jsou asymetrické šifry nevhodné – otisk je vždy *pevné (malé) délky*

Zajištění integrity a nepopíratelnosti přenosu – digitální podpis

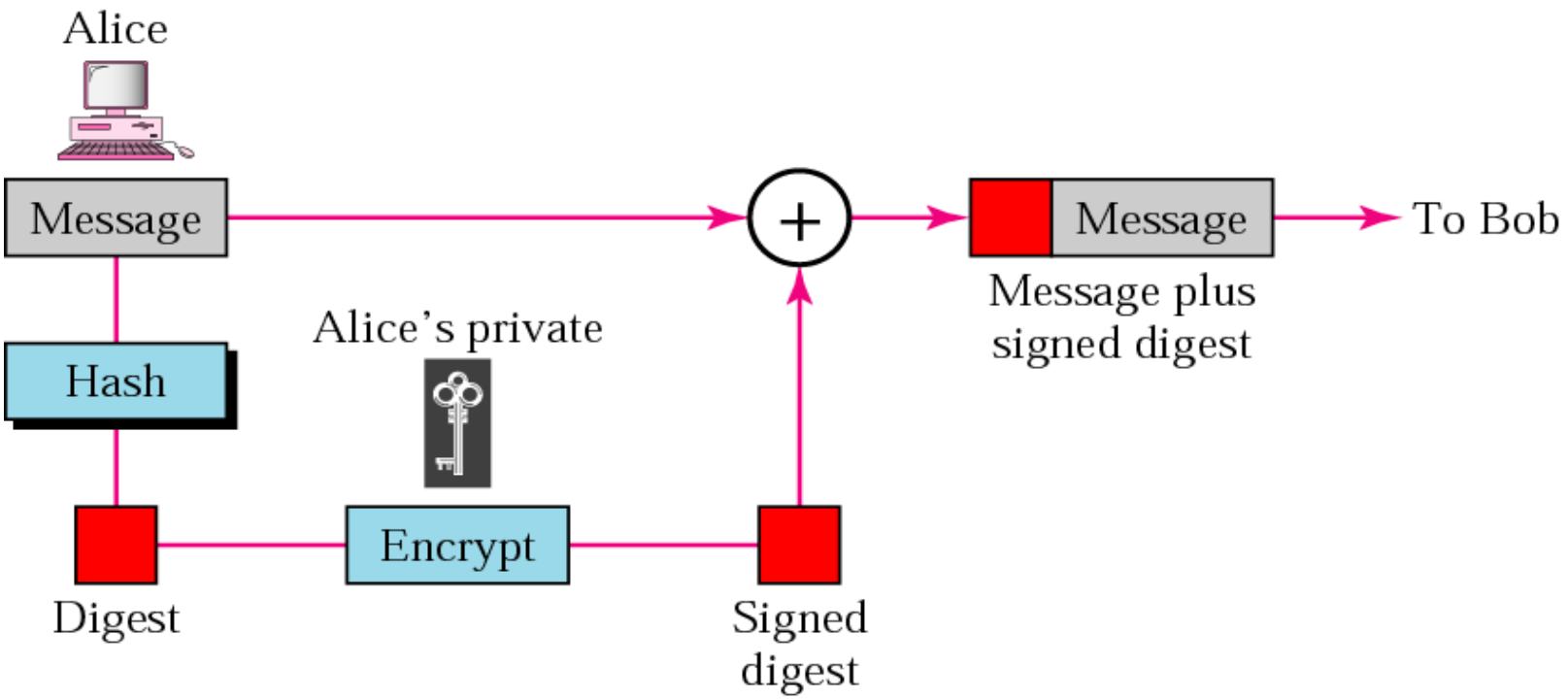
Hashovací funkce

- Musí poskytovat dvě základní vlastnosti:
  - *jednosměrnost* – jakmile je z dokumentu vytvořen otisk, **nelze** (žádným způsobem) z otisku získat původní dokument
  - *one-to-one* – je velmi malá pravděpodobnost, že dvě různé zprávy budou mít stejný otisk
- Pro jakkoli dlouhý dokument má vždy pevnou délku
- Např. MD5 (již prolomena), SHA-256 (nyní aktuální)



Zajištění integrity a nepopíratelnosti přenosu – digitální podpis

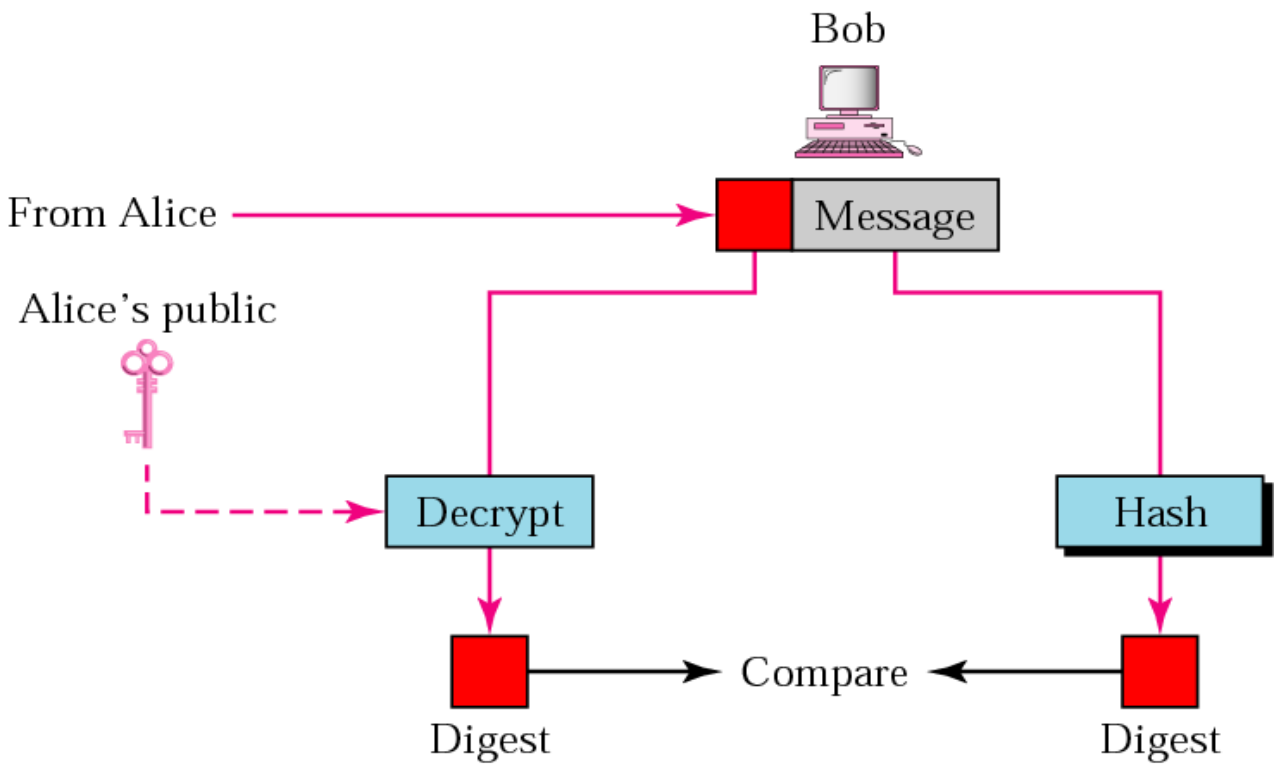
Strana odesílatele



Obrázek: Mechanismus podepisování odesílané zprávy (strana odesílatele).

Zajištění integrity a nepopíratelnosti přenosu – digitální podpis

Strana příjemce



Obrázek: Mechanismus ověřování přijaté zprávy (strana příjemce).