7. Základy síťové bezpečnosti

PB156: Počítačové sítě

Eva Hladká

Fakulta informatiky Masarykovy univerzity

jaro 2010

Struktura přednášky

1. Úvod

2. Zabezpečená síťová komunikace
   - Symetrická kryptografie
   - Asymetrická kryptografie
   - Autentizace komunikujících stran
   - Zajištění důvěrnosti přenosu – šifrování
   - Zajištění integrity a nepopíratelnosti přenosu – digitální podpis

3. Protokoly pro zajištění zabezpečené komunikace v Internetu

4. Rekapitulace

Úvod

Bezpečnost v počítačových sítích – bezpečná komunikační síť by měla nabízet následující služby:

- **AAA**
  - *Authentication (Autentizace)*
  - *Authorization (Autorizace)*
  - *Accounting (Účtování)*
- \+ **zabezpečená komunikace**
  - *Důvěrnost (Confidentiality)*
  - *Integrita (Integrity)*
  - *Nepopíratelnost (Non-repudiation)*

Úvod

Autentizace

Authentication (Autentizace)

- **NE** autentikace, autentifikace, ...
- *ověření identity uživatele (původce zprávy)*
  - součástí je představení identity ověřovaného subjektu
  - zahrnuje prokázání identity jak vůči koncovému systému, tak vůči komunikujícímu partnerovi
- základní metody pro zjištění identity:
  - *podle toho, co uživatel zná* – správná dvojice uživatelské jméno a heslo/PIN
  - *podle toho, co uživatel má* – nějaký technický prostředek, který uživatel vlastní (USB dongle, smart card, privátní klíč, apod.)
  - *podle toho, co uživatel je* – uživatel má vlastnosti, které lze prověřit (otisk prstu, snímek oční zornice, apod.)
  - *podle toho, co uživatel umí* – umí správně odpovědět na náhodně vygenerovaný kontrolní dotaz

Úvod

Autorizace a Accounting (= účtování)

Autorizace

- *oprávnění použít určitou službu nebo zdroj*
  - následuje po autentizaci
- udělení oprávnění nebo odepření přístupu
  - na základě seznamů pro řízení přístupu – definice oprávnění pro vykonání určité operace či pro přístup k prostředkům počítače

Accounting (= účtování)

- *sledování využívání síťových služeb uživateli*
- informace mohou být využity pro správu, plánování, skutečné účtování nebo další účely

Úvod

Důvěrnost, Integrita a Nepopíratelnost

Důvěrnost (Confidentiality)

- *ochrana přenášených dat před neautorizovaným odhalením*
- pouze odesílatel a příjemce by měli rozumět obsahu přenášené zprávy
- zajištěno šifrováním zpráv

Integrita (Integrity)

- *ochrana přenášených dat před neautorizovanou modifikací*
- zajištění, že během přenosu nedošlo k modifikaci původním odesílatelem odeslané zprávy

Nepopíratelnost (Non-repudiation)

- *Nepopíratelnost odesílatele* a *Nepopíratelnost doručení* slouží k tomu, aby příjemce (odesílatel) mohl prokázat protistraně odeslání (přijetí) zprávy a tím zabránil pozdějšímu popření této akce protistranou

1 Úvod

2 Zabezpečená síťová komunikace
- Symetrická kryptografie
- Asymetrická kryptografie
- Autentizace komunikujících stran
- Zajištění důvěrnosti přenosu – šifrování
- Zajištění integrity a nepopíratelnosti přenosu – digitální podpis

3 Protokoly pro zajištění zabezpečené komunikace v Internetu

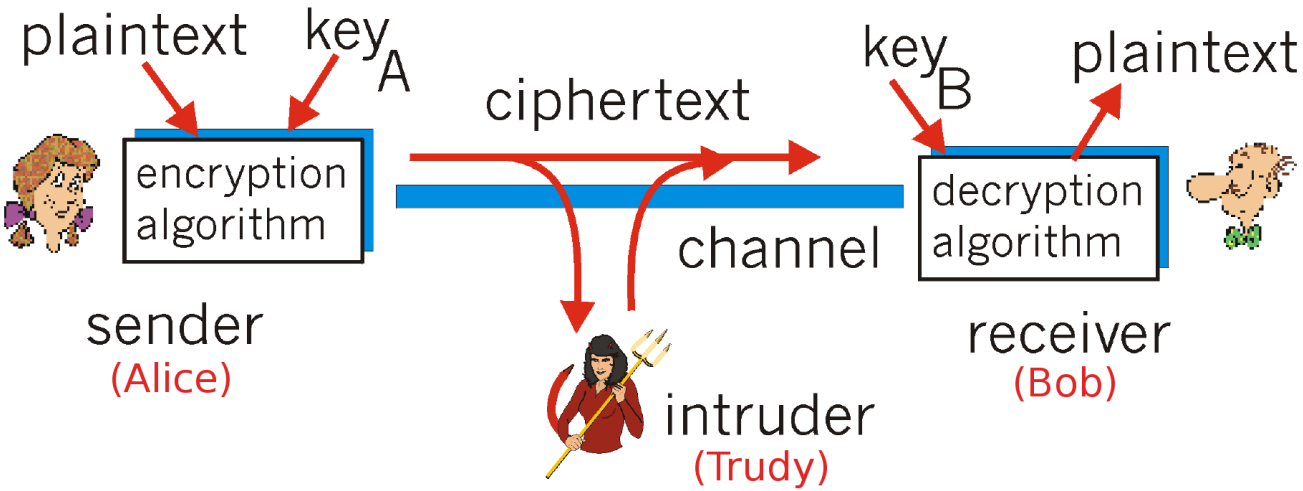
4 Rekapitulace

Zabezpečená síťová komunikace

- zabezpečená síťová komunikace = klasický problém *Kryptografie*

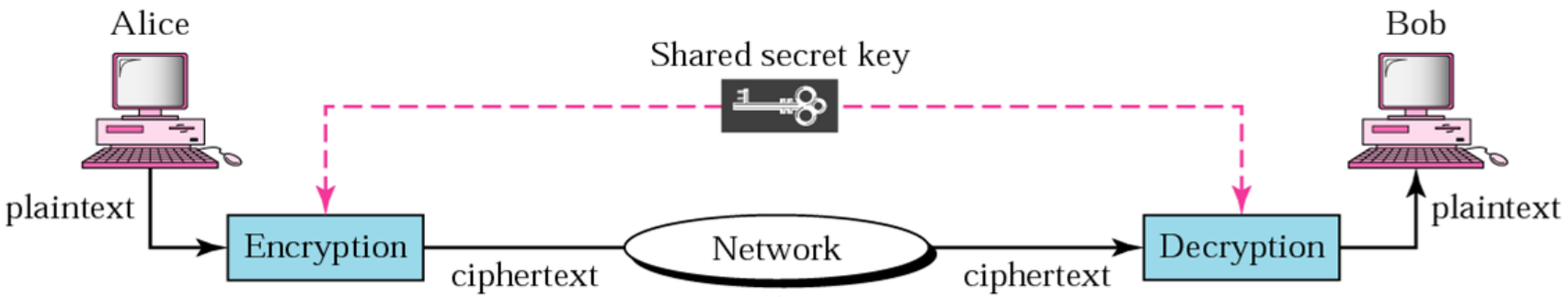
Kryptografie (Cryptography):

- 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, atp.

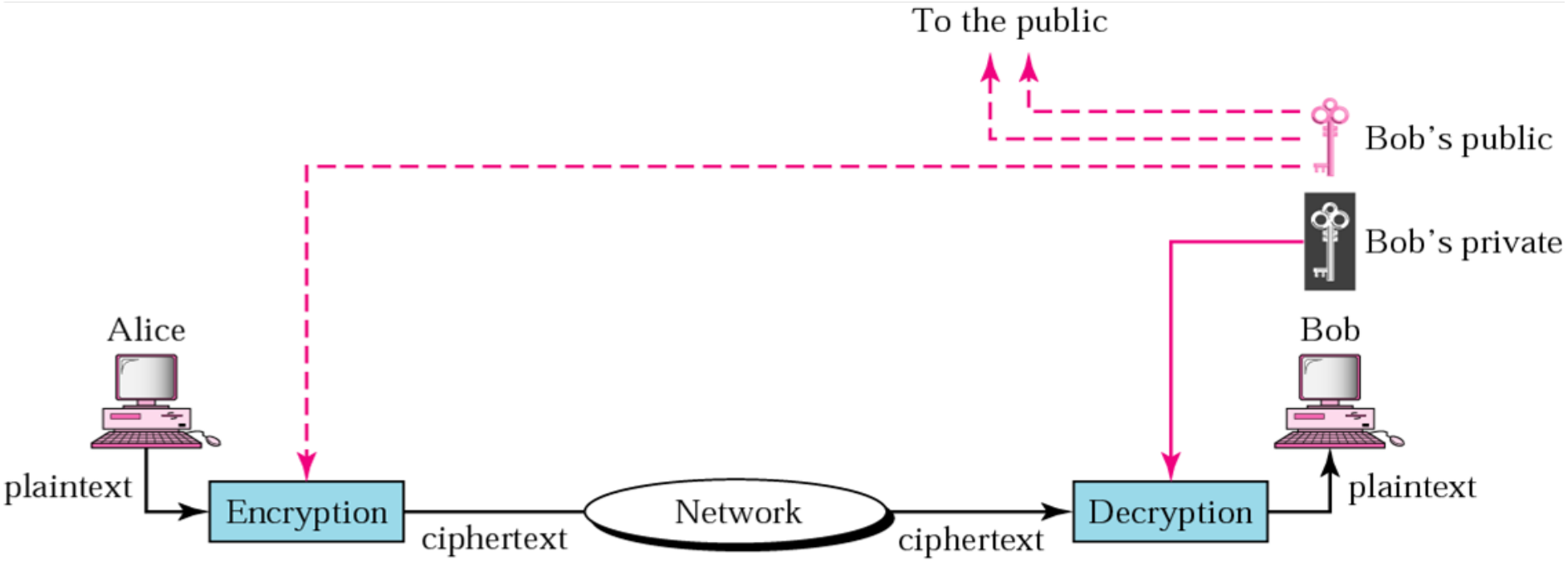


Asymetrická kryptografie

- 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, atp.

Asymetrická kryptografie

Ilustrace



Asymetrická kryptografie

Certifikát veřejného klíče

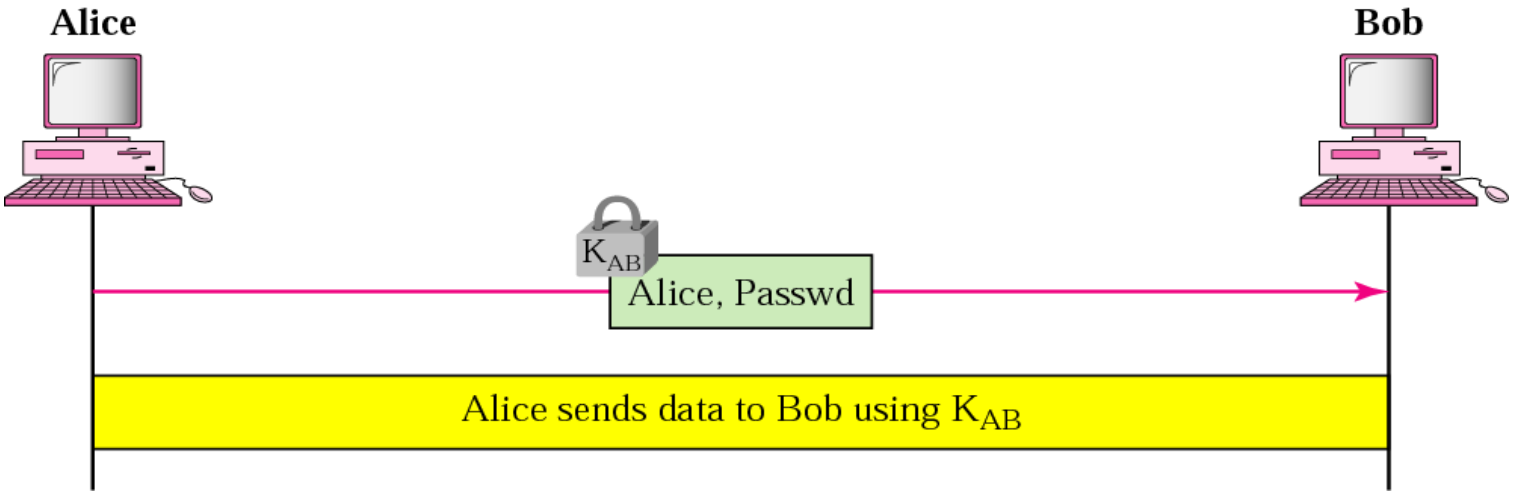
- *Certifikát* – informace, která váže identitu entity (uživatel, server, . . .) s jeho veřejným klíčem
- 4 základní informace obsažené v certifikátu:
  - *jméno vlastníka (držitele)*
  - **hodnota veřejného klíče**
  - *doba platnosti veřejného klíče*
  - *podpis vydavatele certifikátu*
- certifikáty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

Autentizace komunikujících stran

Autentizace heslem

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)

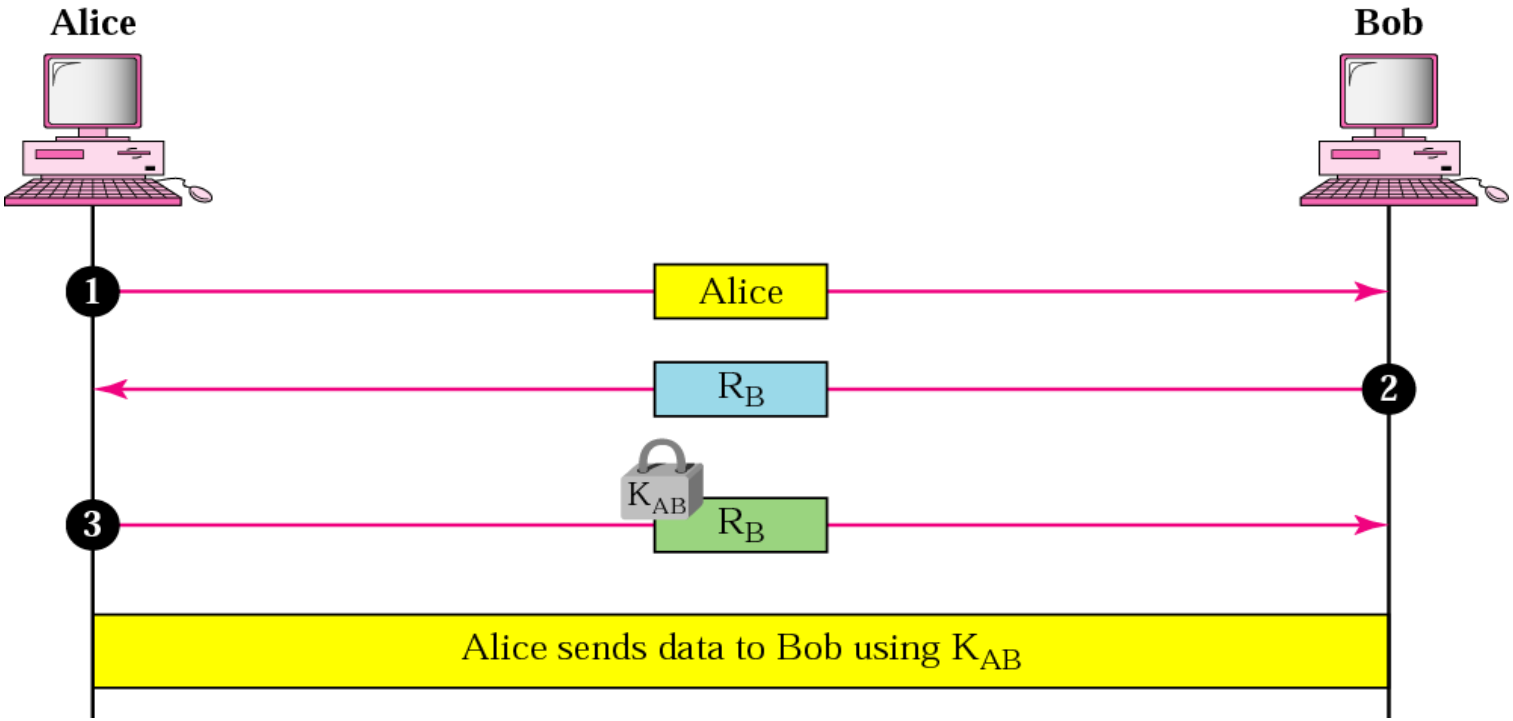


Autentizace komunikujících stran

Autentizace s využitím náhodných čísel

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

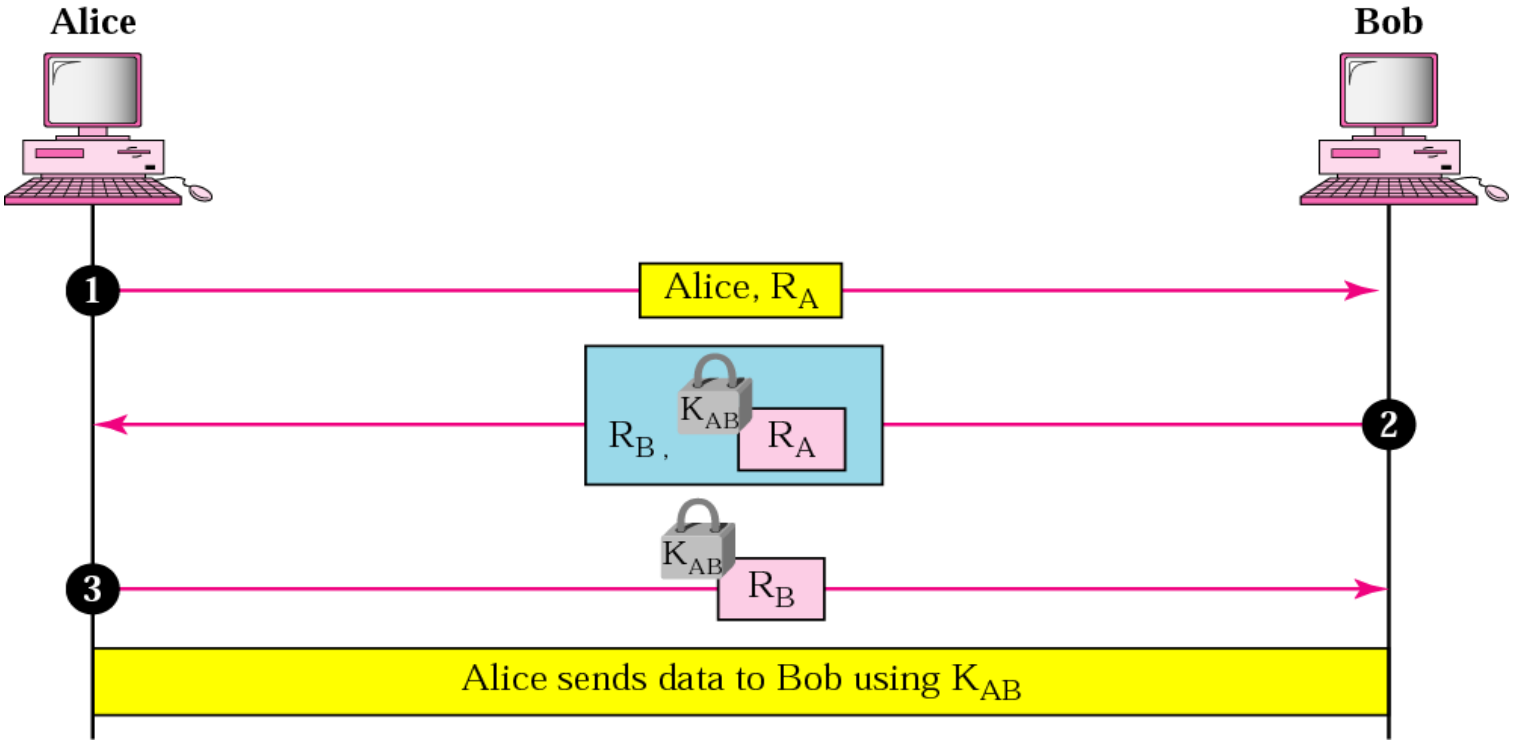


Autentizace komunikujících stran

Vzájemná autentizace s využitím náhodných čísel

Vzájemná autentizace s využitím náhodných čísel:

- stejný princip jako předchozí, autentizace je však obousměrná



Autentizace komunikujících stran

Vzájemná autentizace s využitím náhodných čísel – asymetrická kryptografie

Vzájemná autentizace s využitím náhodných čísel (asymetrická kryptografie):

1. `Alice` $\rightarrow$ `Bob:` $r_A \;||\; sig_A(Bob, r_A) \;||\; Cert_{VK_A}$
2. `Bob` $\rightarrow$ `Alice:` $r_B \;||\; sig_B(Alice, r_A, r_B) \;||\; Cert_{VK_B}$
3. `Alice` $\rightarrow$ `Bob:` $sig_A(Bob, r_B)$

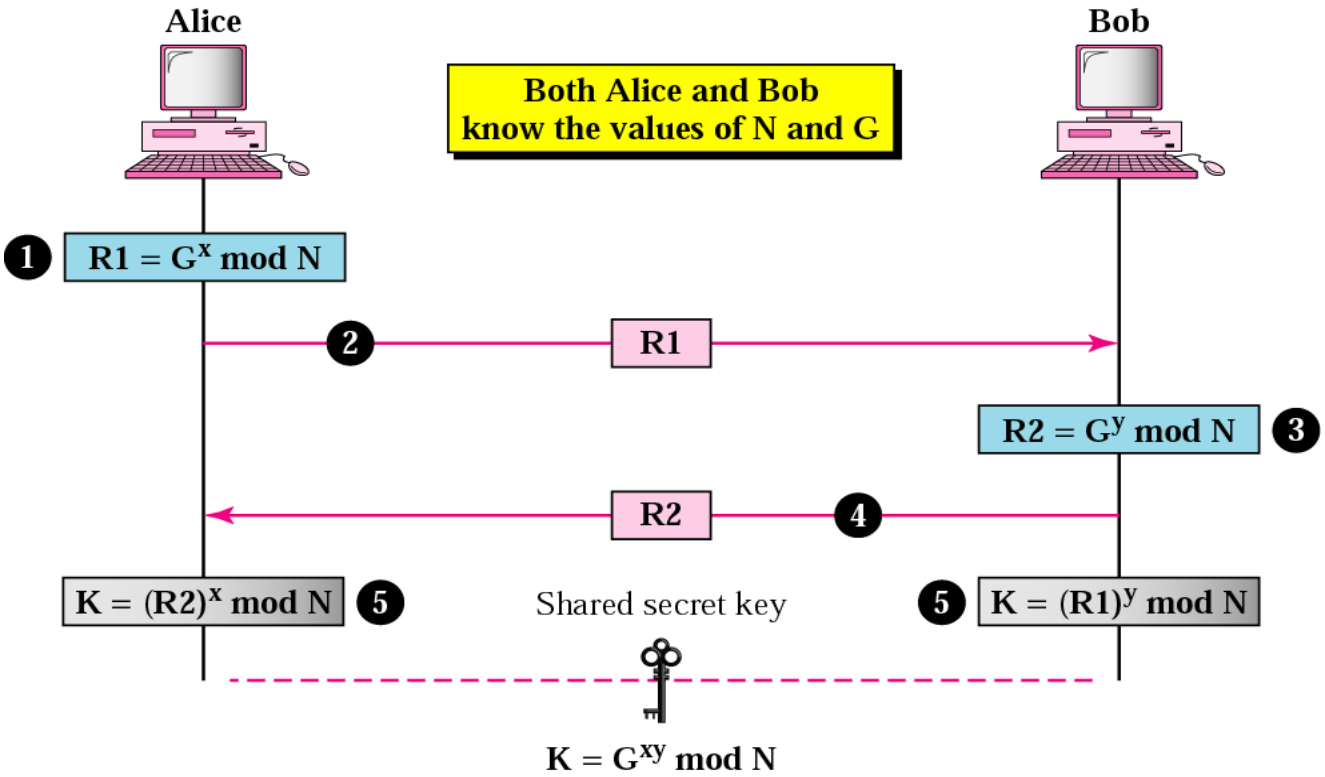
- r_X ... náhodná čísla

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 důvěrnosti přenosu – šifrování

Diffie-Hellman algoritmus



Ilustrace algoritmu Diffie-Hellman.

- čísla G, N jsou prvočísla, která mohou být sítí šířena volně
- využitý princip:
  - $(G^x \bmod N)^y \bmod N = (G^y \bmod N)^x \bmod N = G^{xy} \bmod N$

Zajištění integrity a nepopíratelnosti přenosu – digitální podpis

Digitální podpis:

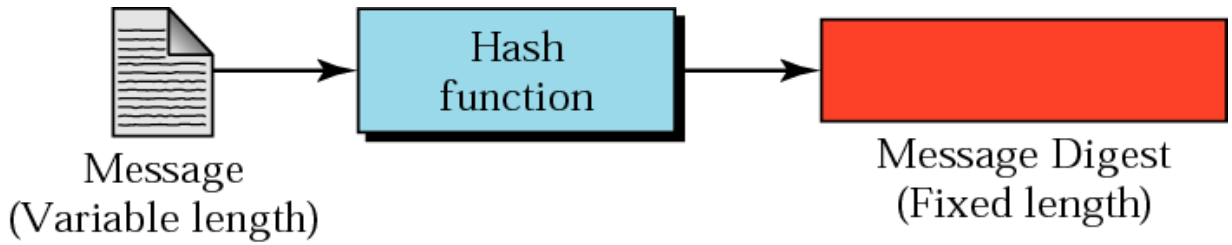
- mimo integrity a nepopíratelnosti zajišťuje i autentizaci komunikujících stran
- obrácený mechanismus asymetrické kryptografie
  - zpráva podepisována (= šifrována) soukromým klíčem odesílatele, ověřována (= dešifrována) veřejným klíčem odesílatele
- 2 základní mechanismy:
  - podpis celého dokumentu
  - *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

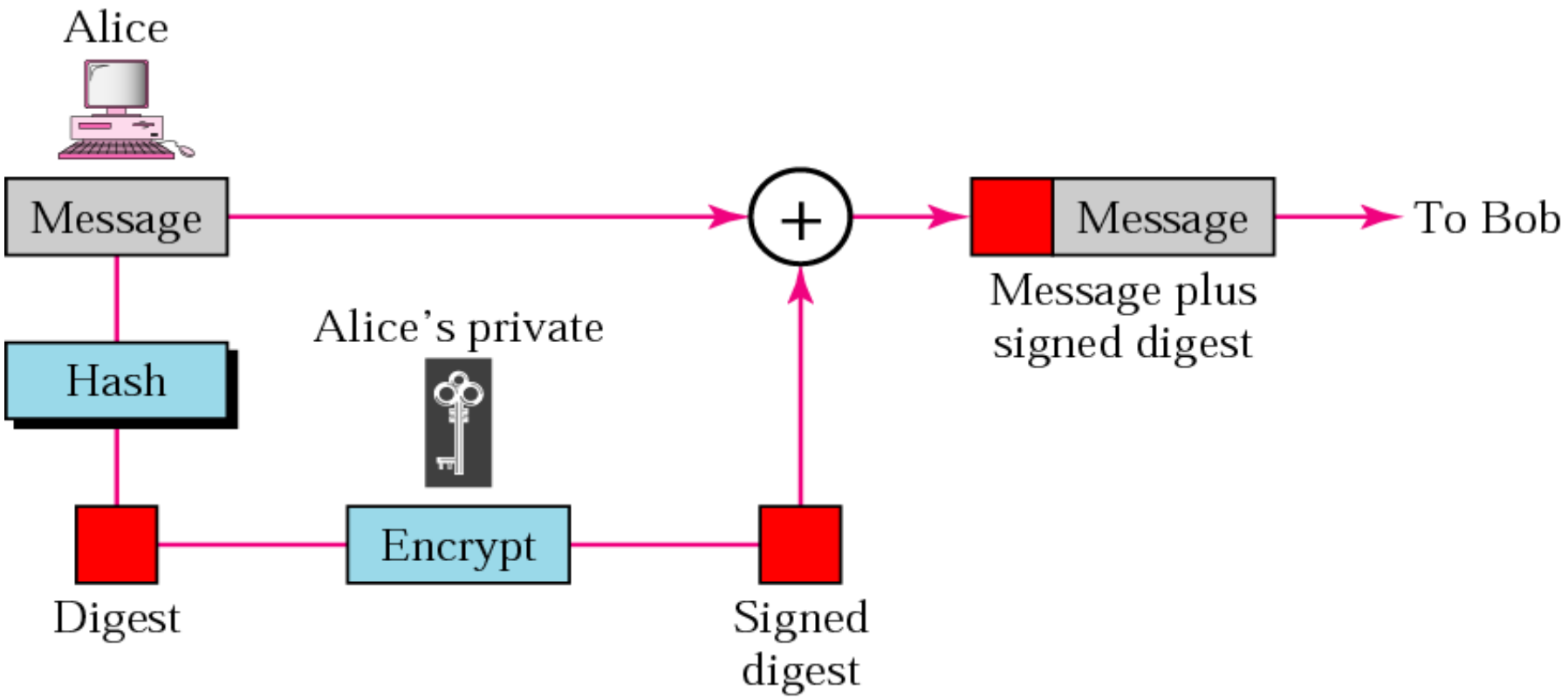
Hashovací funkce:

- 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

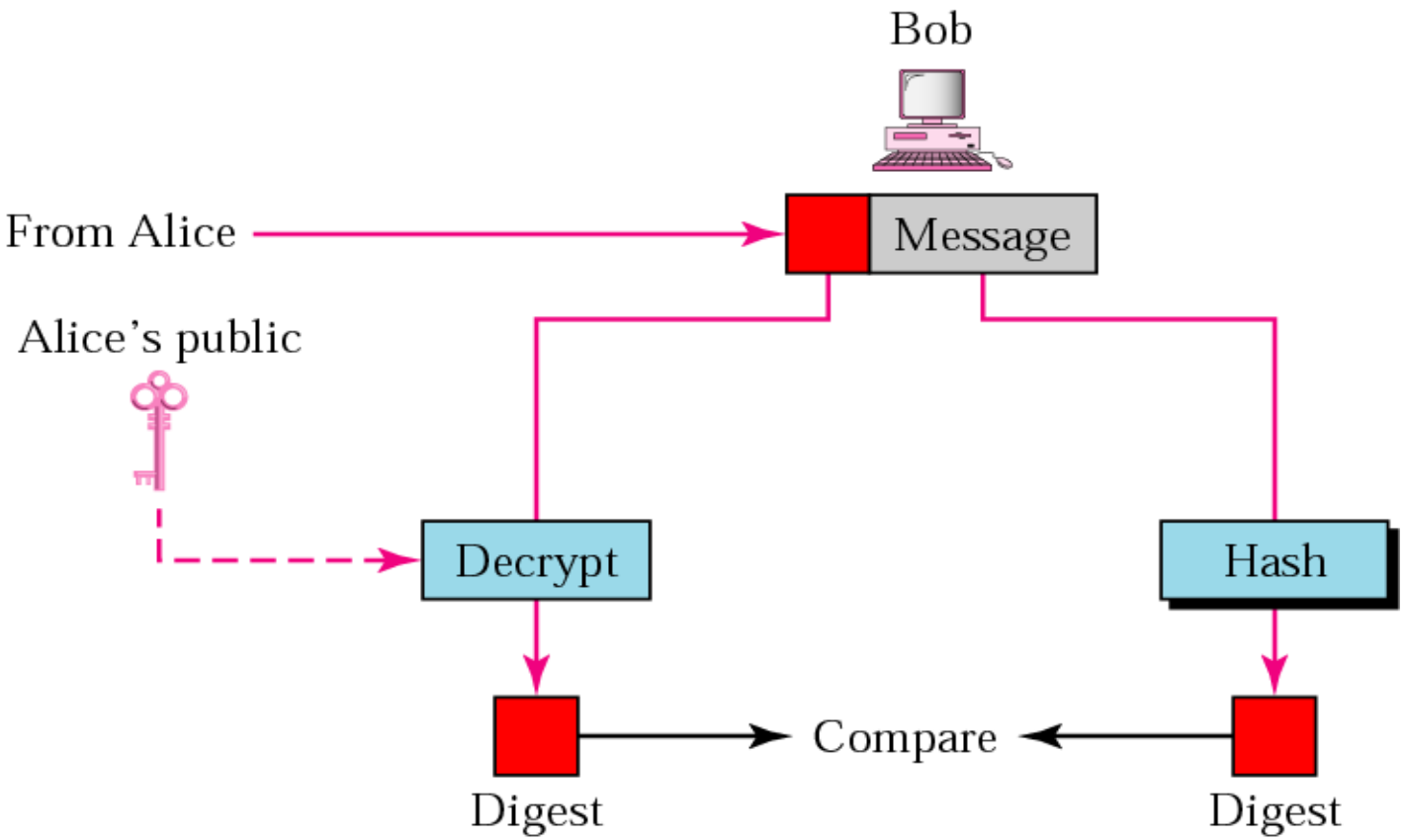
Strana odesílatele



Obrázek: Mechanismus podepisování odesílané zprávy (strana odesílatele).

Zajištění integrity a nepopíratelnosti přenosu – digitální podpis

Strana příjemce



Obrázek: Mechanismus ověřování přijaté zprávy (strana příjemce).

Protokoly pro zajištění zabezpečené komunikace v Internetu

- všechny představené bezpečnostní koncepty lze realizovat na:
  - *aplikační vrstvě*
  - *transportní vrstvě*
  - *síťové vrstvě*

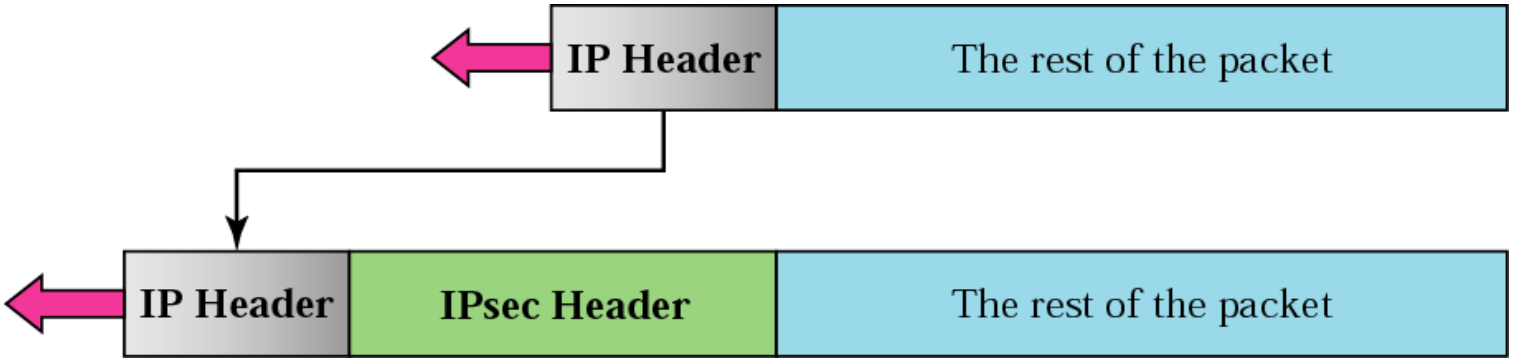
Zabezpečená komunikace na síťové vrstvě – IPSec

IP Security (IPSec)

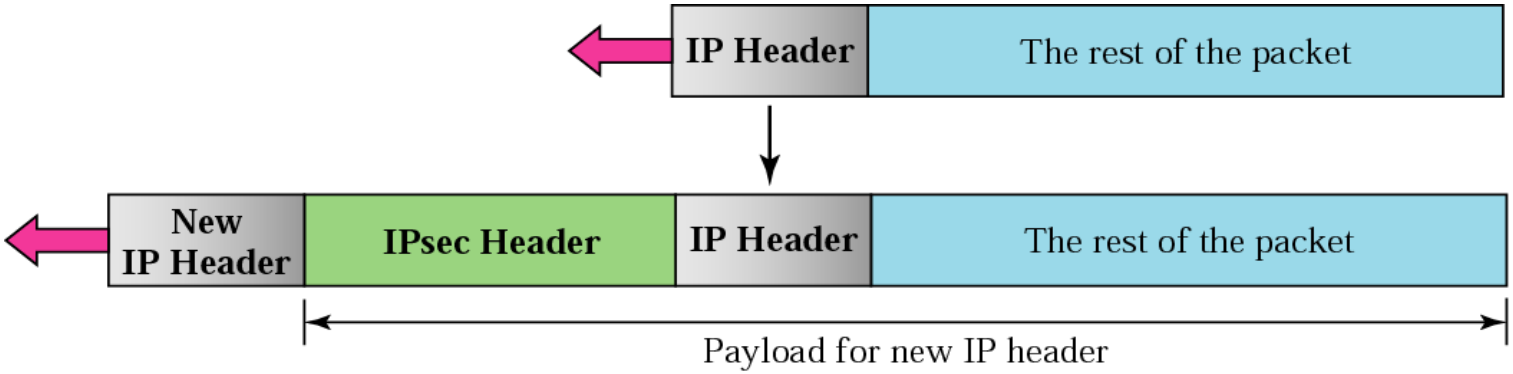
- kolekce protokolů pro zajištění zabezpečené komunikace na síťové vrstvě
  - protokol *Authentication Header (AH)* – určen pro zajištění autentizace odesílatele a integrity zprávy (NE důvěrnosti přenosu)
  - protokol *Encapsulating Security Payload (ESP)* – určen pro zajištění autentizace odesílatele, integrity zprávy i důvěrnosti přenosu
  - možno využít libovolný z nich či jejich kombinaci
- operuje ve 2 módech:
  - *Transportní mód* – IPSec hlavička je vkládána mezi IP hlavičku a tělo zprávy
  - *Tunelovací mód* – IPSec hlavička je vkládána před původní IP hlavičku; následně je generována nová IP hlavička
- výhody: zabezpečení všech datových toků mezi dvěma komunikujícími uzly, není potřeba upravovat aplikace
- nevýhody: žádné automatizované prostředky pro správu kryptografických klíčů

Zabezpečená komunikace na síťové vrstvě – IPSec

Transportní vs. Tunelovací mód



Obrázek: Transportní mód.

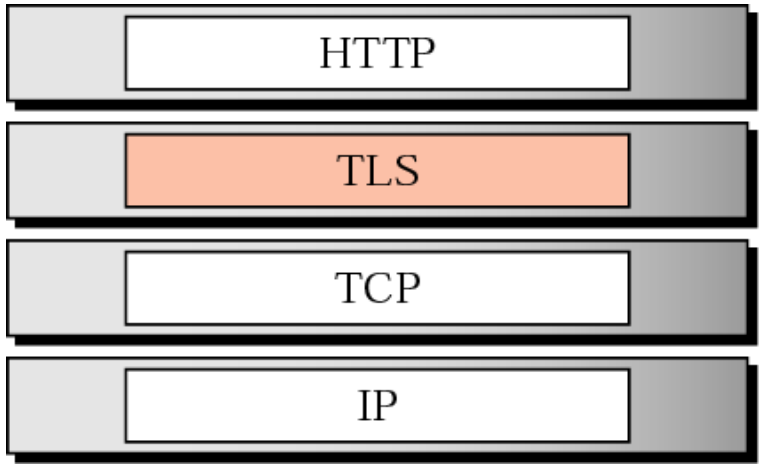


Obrázek: Tunelovací mód.

Zabezpečená komunikace na transportní vrstvě – SSL/TLS

Secure Sockets Layer (SSL) / Transport Layer Security (TLS)

- protokoly pro zajištění zabezpečené komunikace na transportní vrstvě
  - (SSL je předchůdcem TLS)
  - SSL 3.0 $\approx$ TLS 1.0
- protokoly aplikační vrstvy je nutno pro jejich využití upravit
  - HTTP $\rightarrow$ HTTPS (HTTP Secure)
  - FTP $\rightarrow$ FTPS (FTP Secure)
  - atd.
- nevýhody: nutnost úpravy aplikací

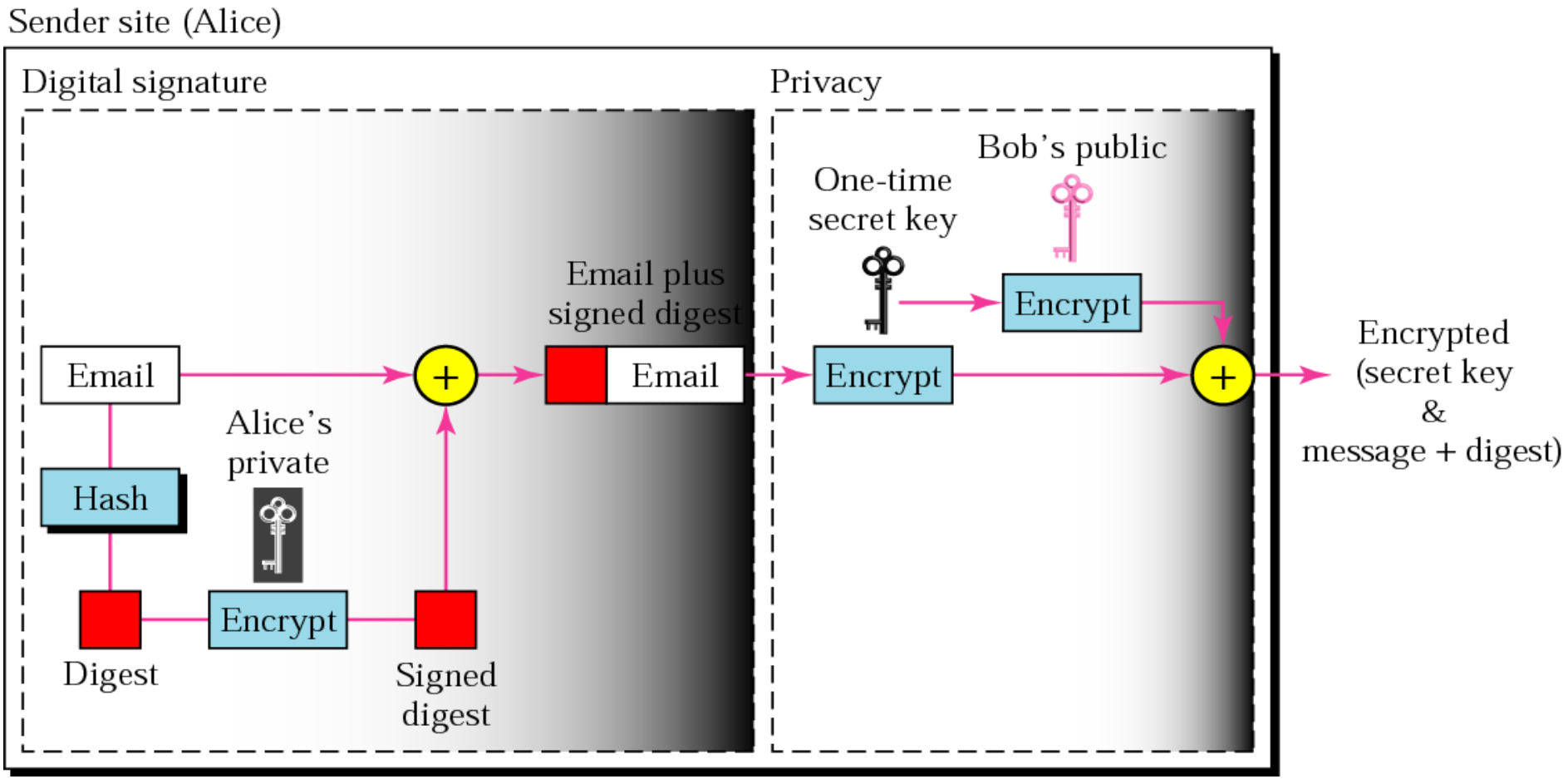


Zabezpečená komunikace na aplikační vrstvě

- zabezpečení komunikace na základě vlastních mechanismů síťových aplikací
- např. *Pretty Good Privacy (PGP)*
  - navrženo Philem Zimmermannem (1996)
  - mechanismus pro zasílání bezpečné elektronické pošty
  - postihuje všechny základní bezpečnostní aspekty: důvěrnost přenosu, integritu zpráv, autentizaci odesílatele a nepopíratelnost

Zabezpečená komunikace na aplikační vrstvě – PGP

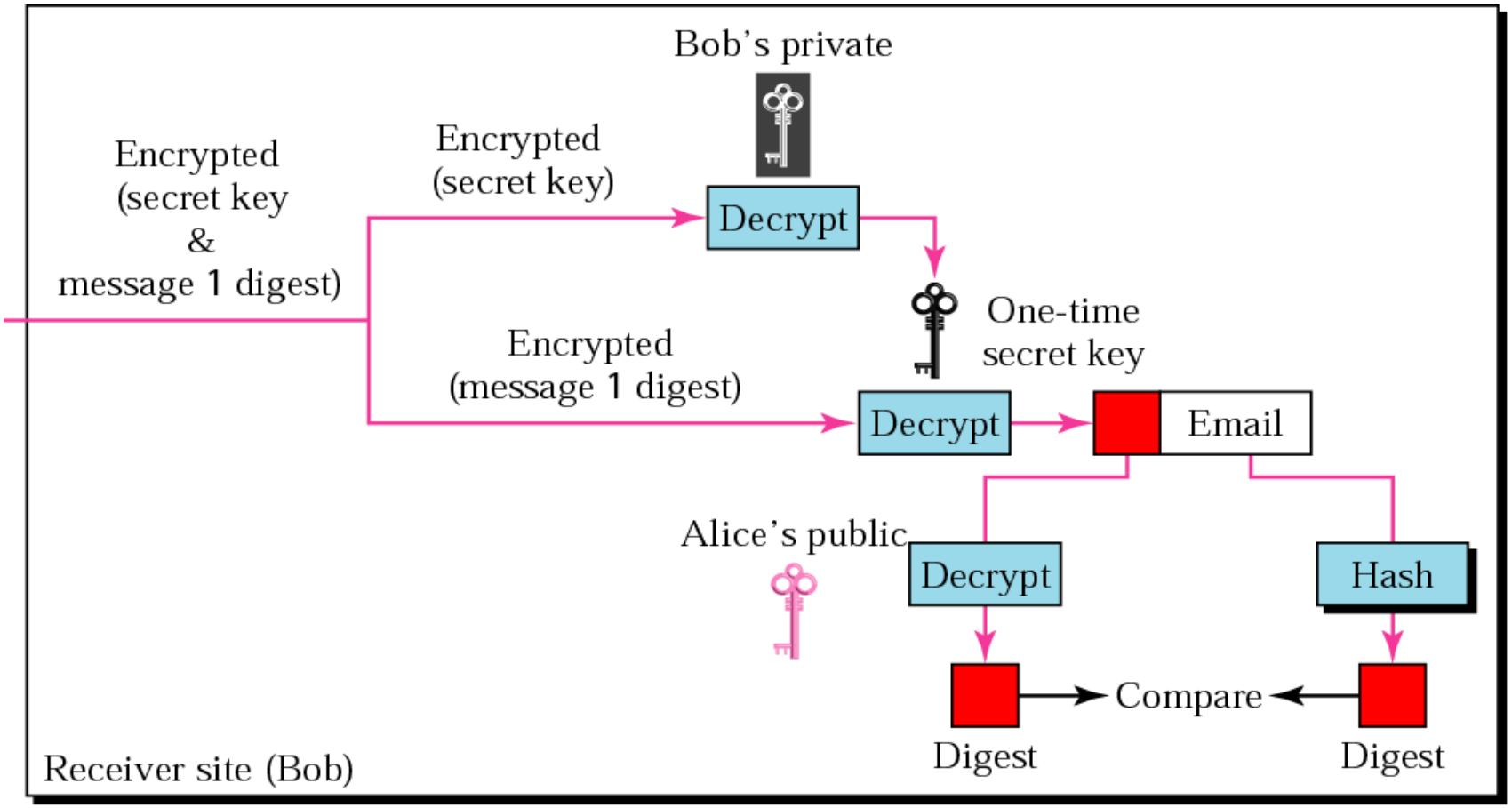
Strana odesílatele



Obrázek: Mechanismus podepisování a šifrování odesílané zprávy (strana odesílatele).

Zabezpečená komunikace na aplikační vrstvě – PGP

Strana příjemce



Obrázek: Mechanismus dešifrování a ověřování přijaté zprávy (strana příjemce).

Rekapitulace – Základy síťové bezpečnosti

- mechanismy pro zajištění AAA + mechanismy pro zajištění zabezpečené komunikace
- vlastnosti bezpečné komunikační sítě:
  - Důvěrnost (Confidentiality)
  - Integrita (Integrity)
  - Nepopíratelnost (Non-repudiation)
- symetrická (sdílený klíč) a asymetrická (dvojice klíčů – soukromý, veřejný) kryptografie
- mechanismy zabezpečené komunikace možno zajistit na různých vrstvách (aplikační, transportní, síťová)
- *další informace:*
  - PV017: Bezpečnost informačních technologií (doc. Staudek)
  - PV079: Aplikovaná kryptografie (doc. Matyáš)
  - PV080: Ochrana dat a informačního soukromí (doc. Matyáš)
  - PV157: Autentizace a řízení přístupu (doc. Matyáš)
  - PV159: Počítačové sítě a jejich aplikace I. (prof. Matyska, doc. Hladká)
  - atd.