X36PKO
Bezpečnost v počítačových sítích

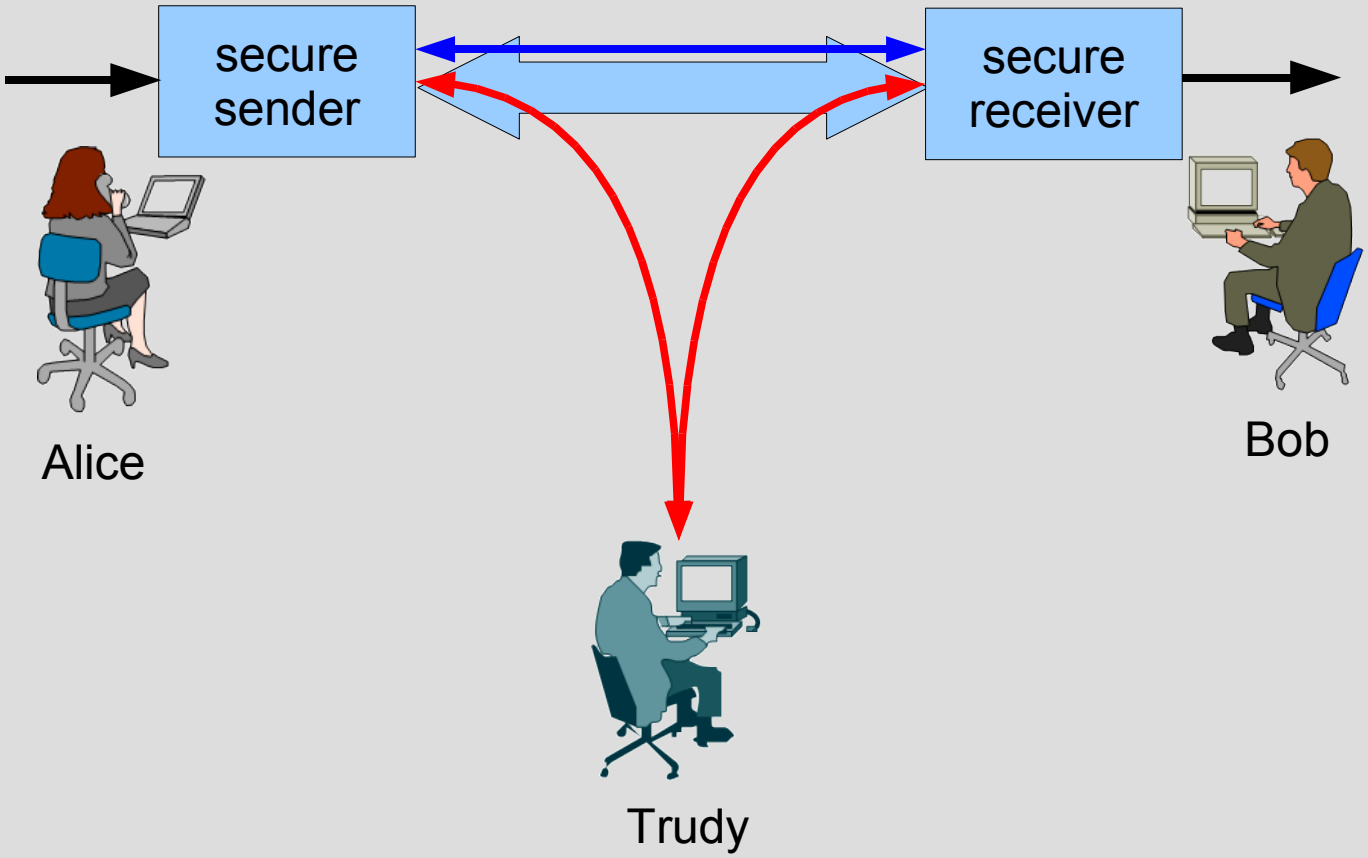
Osnova

- základní pojmy
- typy šifer
- autentizace
- integrita
- distribuce klíčů
- firewally
- typy útoků
- zabezpečení aplikací

Základní pojmy

- síťová bezpečnost
  - utajení přenášených dat
    - šifrování a dešifrování
  - autentizace
    - ověření totožnosti odesílatele a příjemce
  - integrita a nepopiratelnost
  - dostupnost a řízení přístupu
    - řízení přístupu ke zdrojům
    - zamezení zneužití zdrojů
    - znesnadnění DoS útoků
  - detekce útoků
  - reakce na útoky
    - Intruder Detection System

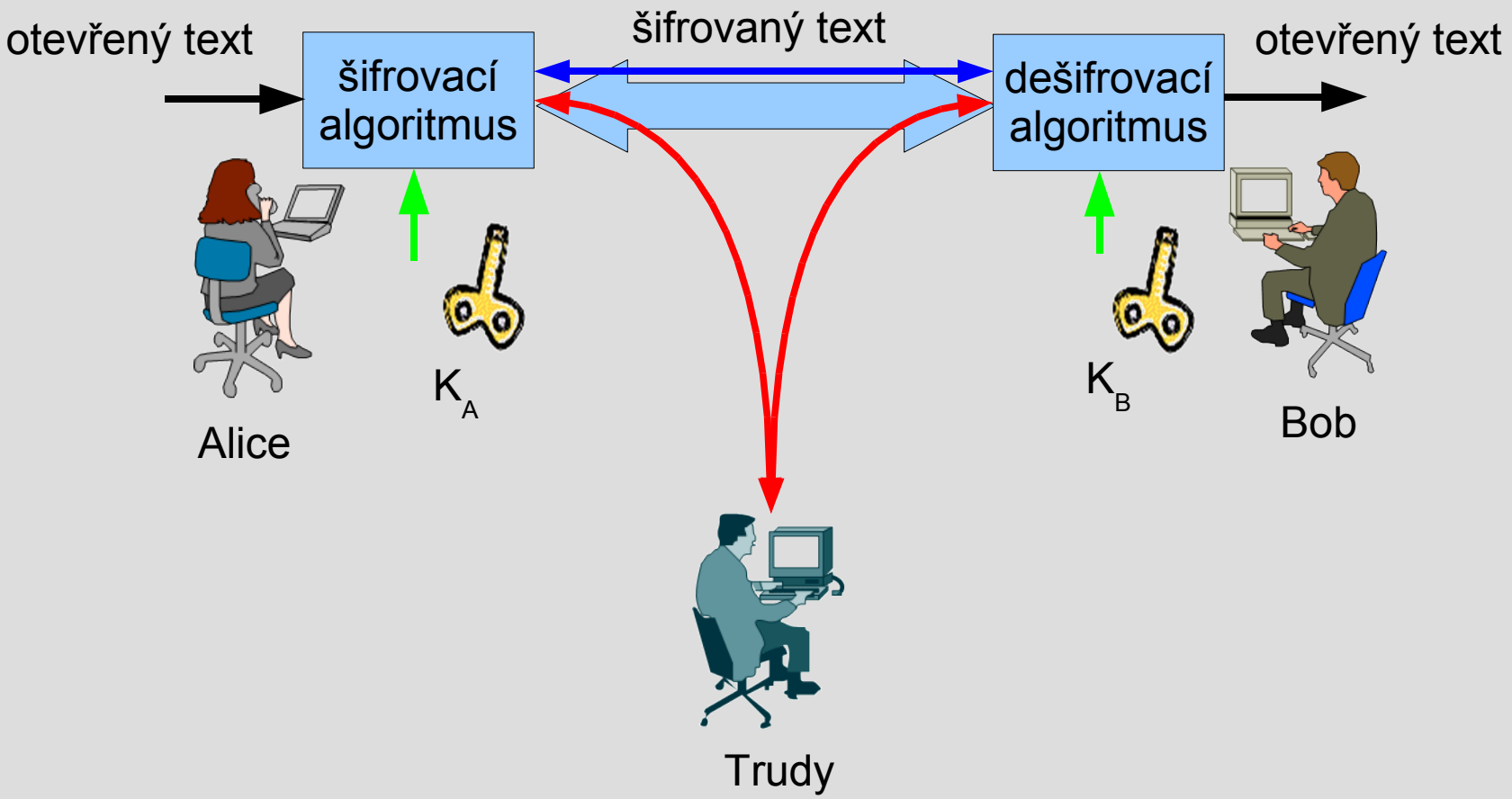
Komunikace



Principy kryptografie

- počátky v období Julia Caesara
- moderní techniky – cca 30 let
- šifrovací algoritmus umožňuje
  - odesílateli zašifrovat otevřený text na text šifrovaný
  - příjemci dešifrovat šifrovaný text na text otevřený
- klíč K_A K_B
  - sdílené tajemství využívané šifrovacím algoritmem
  - stejné klíče
    - symetrické šifrování
  - různé klíče
    - asymetrické šifrování, šifrování s veřejným klíčem
- m … otevřený text
- $c=K_A(m)$ … šifrovaný text
- $K_B(K_A(m))=m$ … otevřený (dešifrovaný) text

Principy kryptografie II



Symetrické šifry

- substituce, transpozice
- Caesarova šifra
  - substituce
    - `abcdefghijklmnop...`
    - `defghijklmnopqrs...`
    - klíč K=3 ahoj dkrm
    - 25 klíčů
- monoalfabetické šifry
  - náhrada jednoho písmena abecedy jiným písmenem
  - 26! klíčů (cca 10^{26})
  - statistický útok
- polyalfabetické šifry
  - náhrada jednoho písmena abecedy různými písmeny
  - více monoalfabetických šifer určených pozicí
    - `abcdefghijklmnop...`
    - `defghijklmnopqrs...`
    - `rstuvwxyzabcdefg...`
    - klíč K_1=3 K_2=16 vzor: C_1,C_2,C_2,C_1 ahoj dyfm

Symetrické šifry II

- transpozice

3	4	1	5	2
A	H	O	J	A
L	I	C	E	Z
D	R	A	V	I
T	E	B	O	B

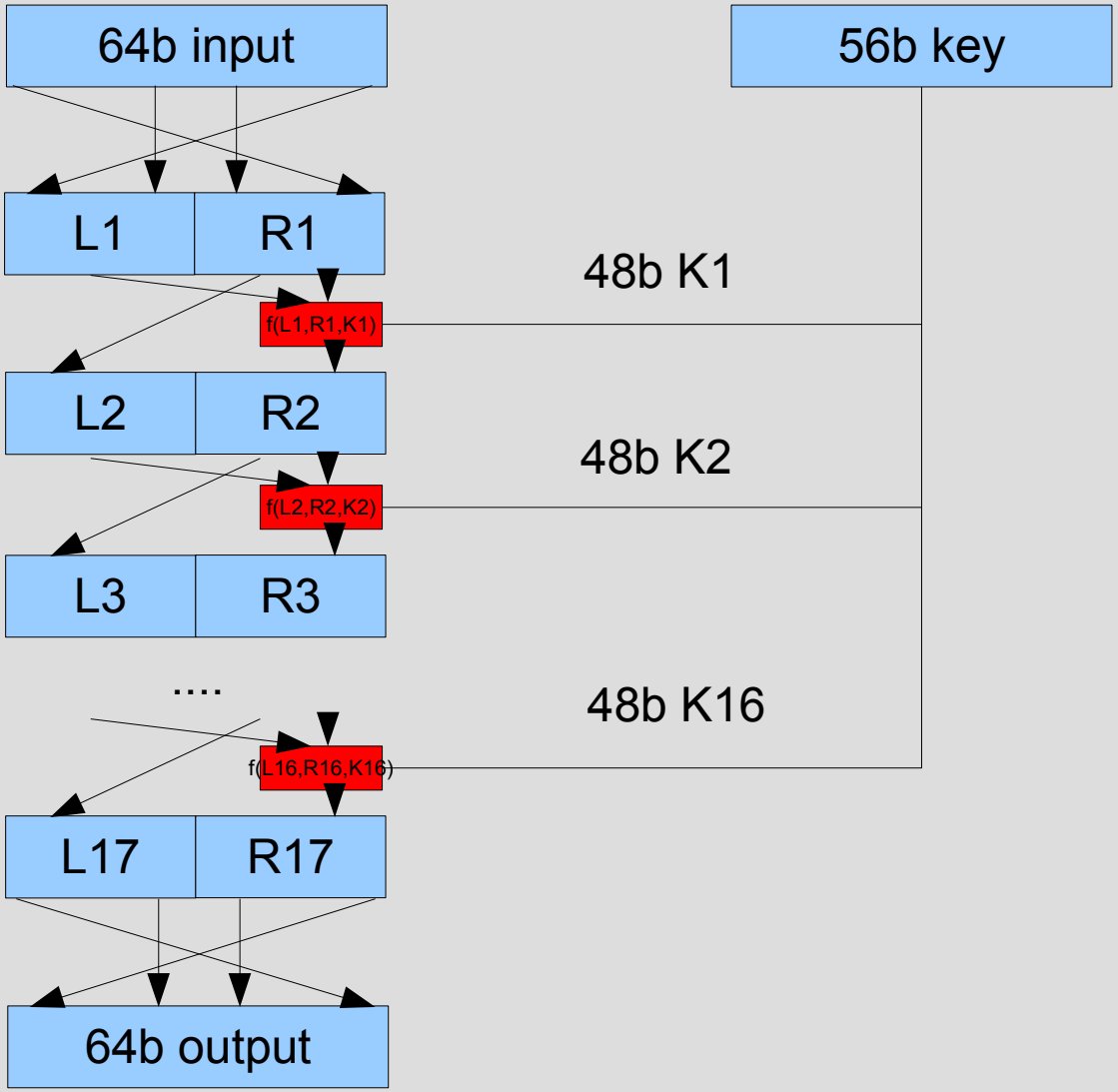
AHOJALICEZDRAVITEBOB

OAAHJCZLIEAIDRVBTEBO

Data Encryption Standard

- DES, publikován 1977
- 56b symetrický klíč (+8b parita)
- původní návrh 112b klíč, IBM Lucifer
- několikrát obnovený standard
- v současnosti slabá šifra
  - 1997 … 4 měsíce
  - 2/1998 … 41 dní
  - 7/1998 … 56 hodin
  - 1/1999 … 22h 15m
  - prodloužení klíče
  - Triple DES
  - 2001 přijat standard AES (Advanced Encryption Standard)
    - 128b bloky; 128, 192, 256b klíče

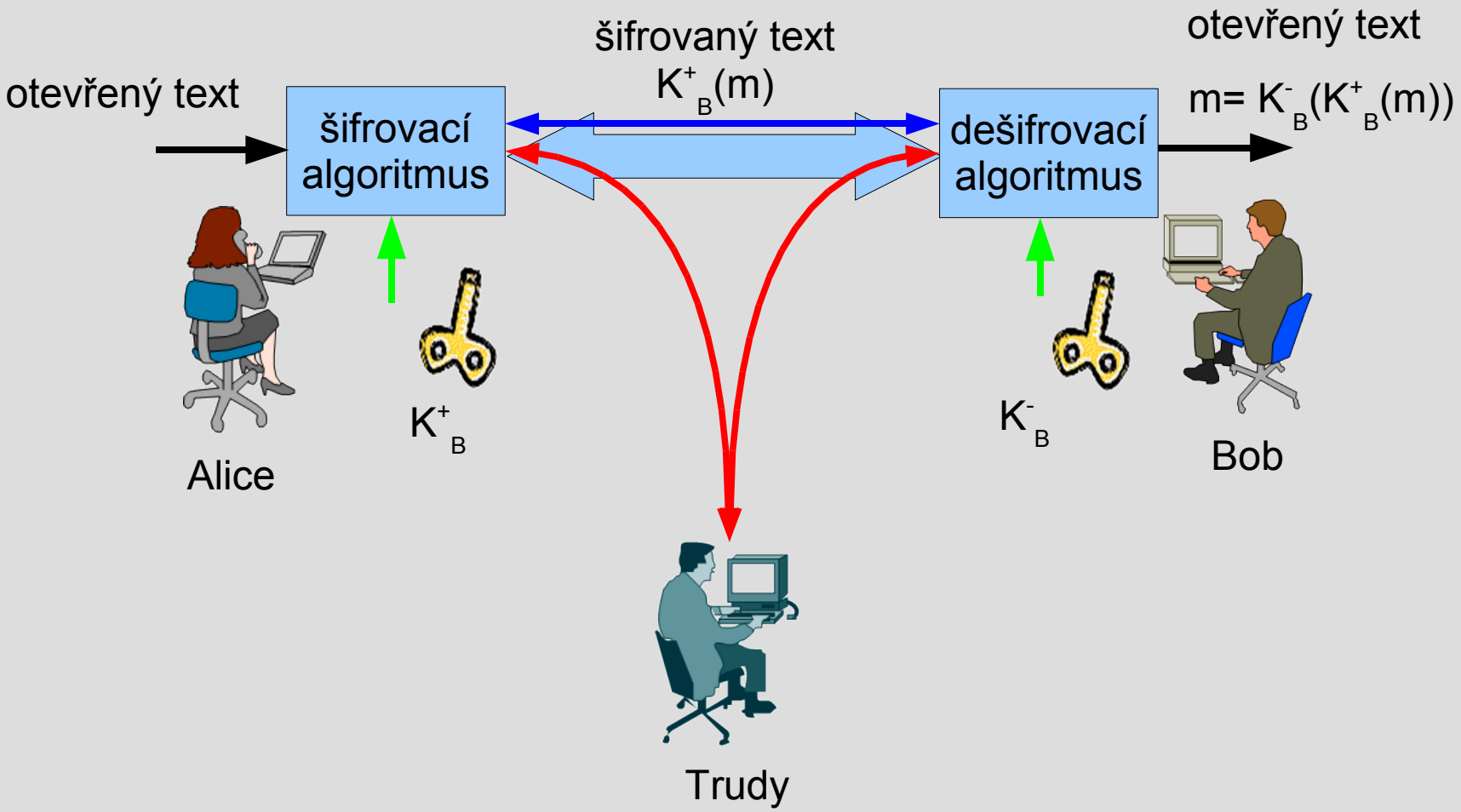
DES


64b input
56b key
L1
R1
48b K1
f(L1,R1,K1)
L2
R2
48b K2
f(L2,R2,K2)
L3
R3
....
48b K16
f(L16,R16,K16)
L17
R17
64b output

Asymetrické šifry

- řešení problému předání sdíleného klíče
- množství klíčů při komunikaci různých subjektů
- privátní klíč K^-_B
  - k dispozici pouze Bobovi
- veřejný klíč K^+_B
  - veřejně k dispozici
  - je složité je vzájemně odvodit
- $c_1 = K^+_B(m)$, nebo $c_2 = K^-_B(m)$
- $K^-_B(K^+_B(m)) = K^+_B(K^-_B(m)) = m$

Asymetrické šifry



RSA

- Ron Rivest, Adi Shamir, Leonard Adleman
- výběr (vytváření) klíčů
  - dvě prvočísla p,q (cca 1024b, 768b)
  - n=pq; z=(p-1)(q-1)
  - e (e<n, nesoudělné se z)
  - d (e*d mod z = 1)
  - $K^{+}_{B}=(e,n)$; $K^{-}_{B}=(d,n)$
- algoritmus pro šifrování a dešifrování
  - šifrování – $c=m^{e} \bmod n$
  - dešifrování – $m=c^{d} \bmod n$

RSA - příklad

- p=11; q=13
- n=143; z=120
- e=17 (<143, nesoudělné s 120)
- d=113 ((17*101-1)/120=16)
- K^{+}_{B}=(17,143)
- K^{-}_{B}=(113,143)

a	97	15
h	104	91
o	111	89
j	106	6

šifrování: $c=m^e \bmod n$

97	595826043858805133328118345676553 7	15
104	19479004955562800041143429584912384	91
111	589509270858085346126218637373274 71	89
106	269277278576681147178794658054799 36	6

dešifrování: $m=c^d \bmod n$

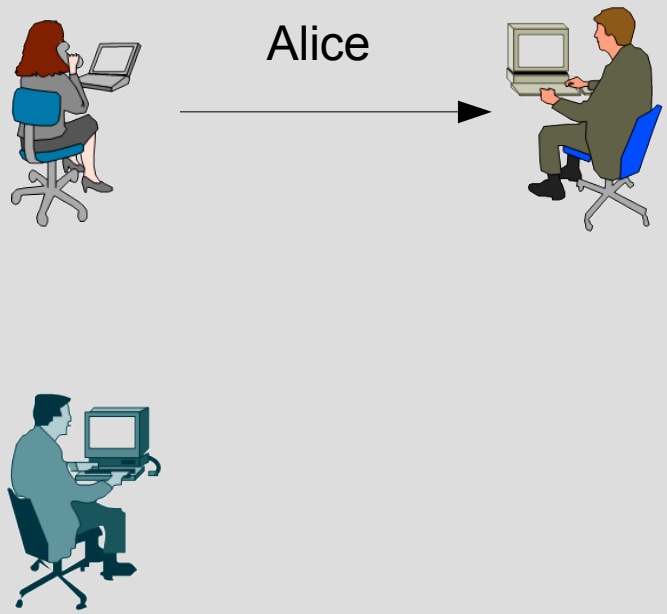
15	791247358705416214517752899423106174377801090035019044884638799937022110750082473725059686777555389980420841311570256948471069335937 5	97
91	235330020306433888581424803782979895833988112645915012928091461931015209041921281141423188605893790789892256195891639038011777159440723864868389202730650215311698134079596531469164024580497081700375937796851962658130610971	104
89	191016441793429911630773179406452709402780400799032837444588056890676559267013049668174260902615223818891648923942096113701669348884003354792465908971705006954477349019311421807664716425565050232487056163153099201332973 69	111
6	85327946364887330588327404896766871028714747651061582206006487174194445606226701225820 16	106

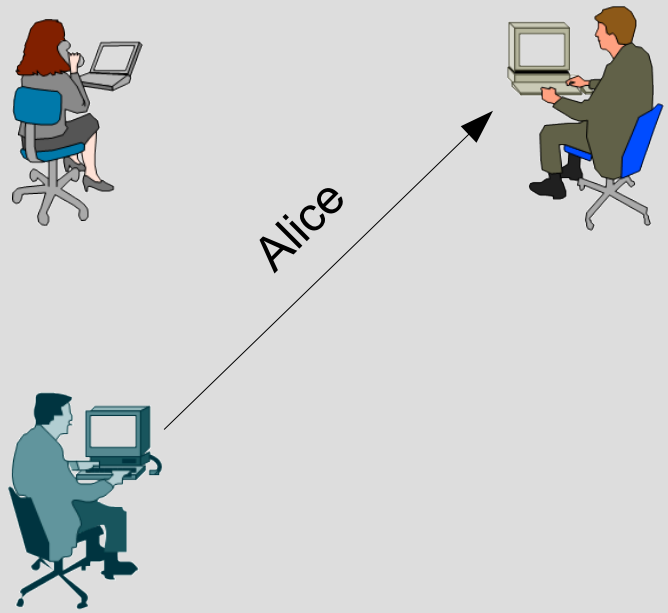
Autentizace

- poskytnutí informace o identitě jednoho subjektu subjektu druhému
- provádí se před použitím dalších protokolů
- často se provádí oboustranně

Autentizační protokoly 1.0

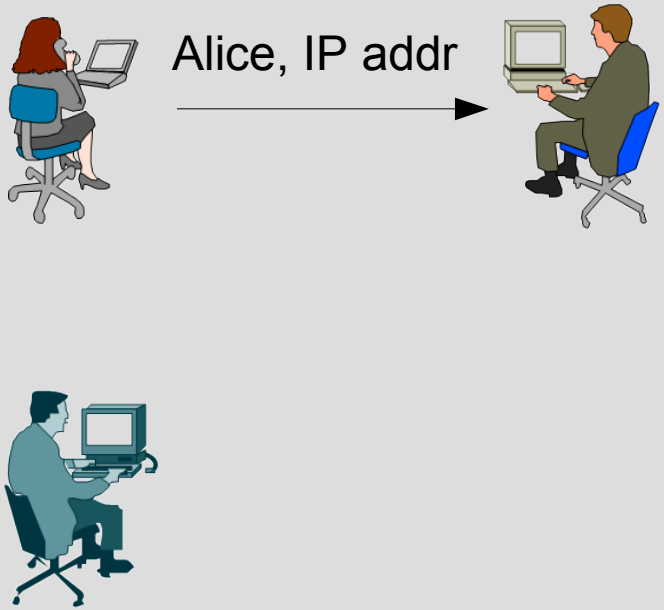
- Alice se pouze představí
- velmi nedostatečný

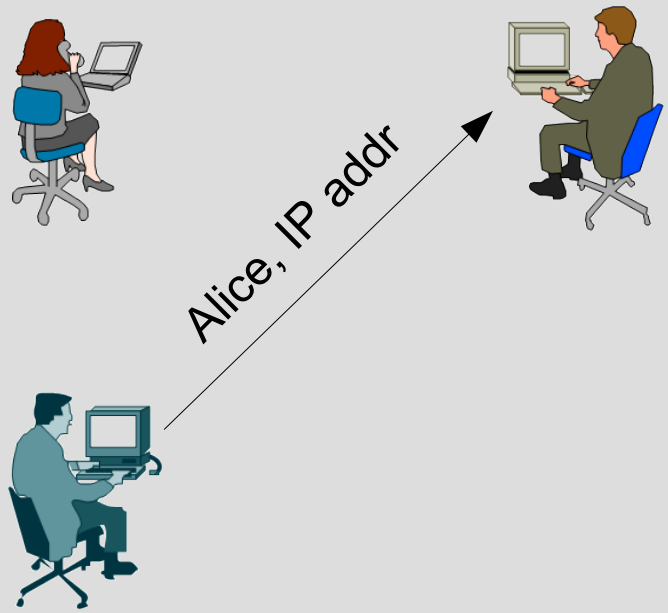




Autentizační protokoly 2.0

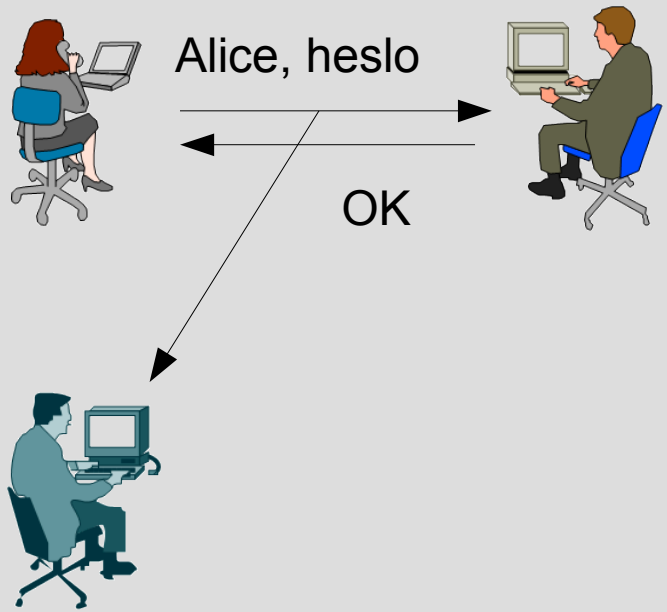
- Alice se představí a použije velmi známou IP adresu (rlogin)
- možnost podvržení adresy

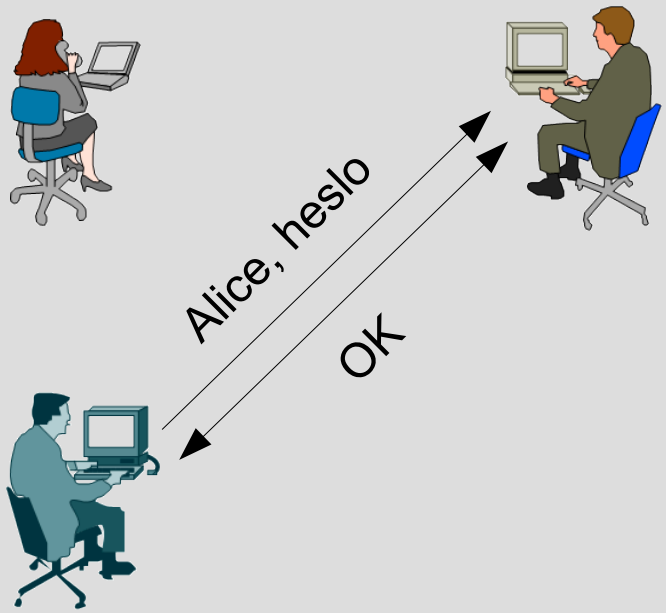




Autentizační protokoly 3.0, 3.1

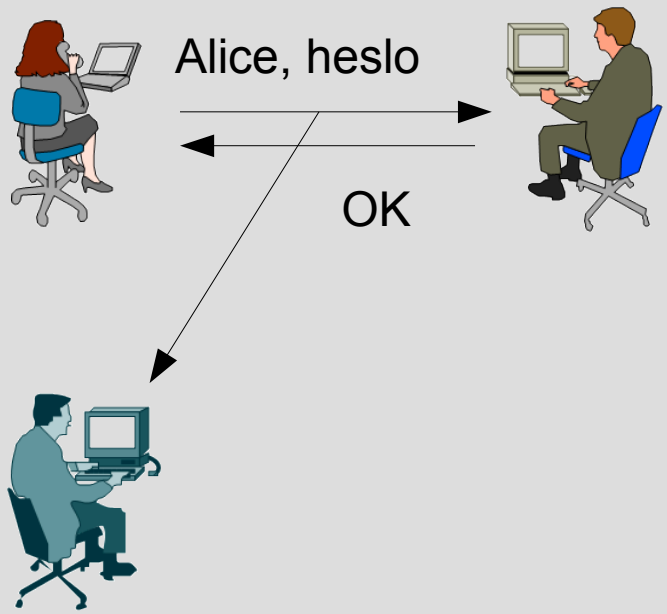
- Alice použije heslo (telnet, ftp)
- možnost odposlechnutí hesla, zašifrování hesla je nedostatečné

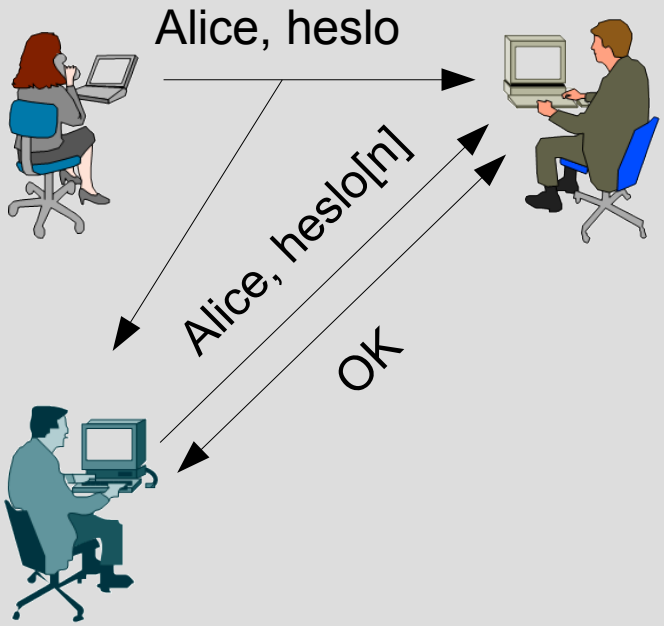




Autentizační protokoly 4.0

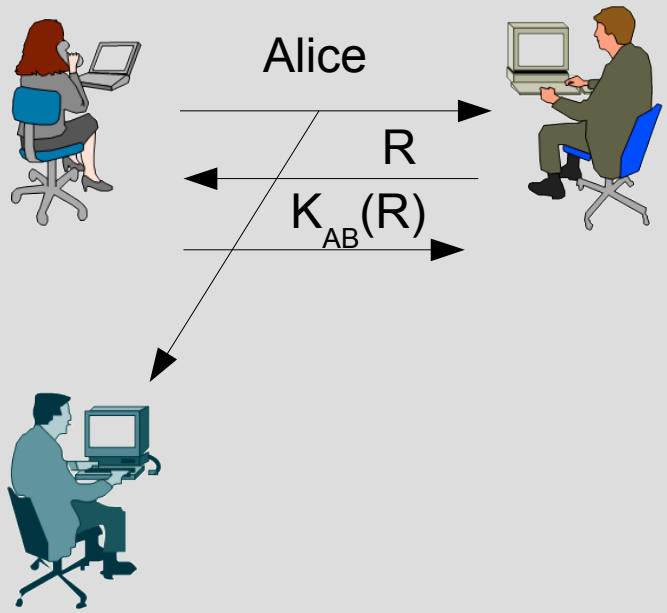
- Alice použije pokaždé jiné heslo (S/KEY)
- problém generování hesel, race útok

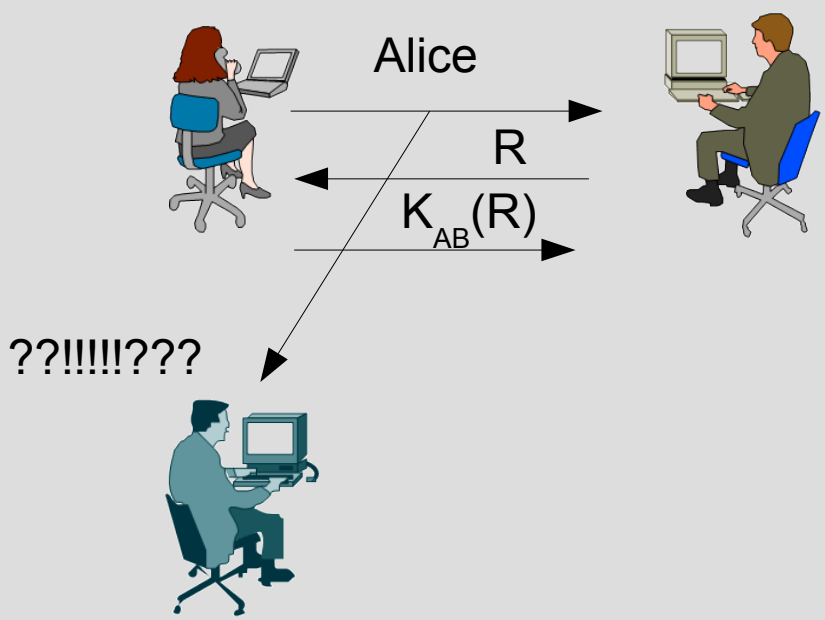




Autentizační protokol 4.1

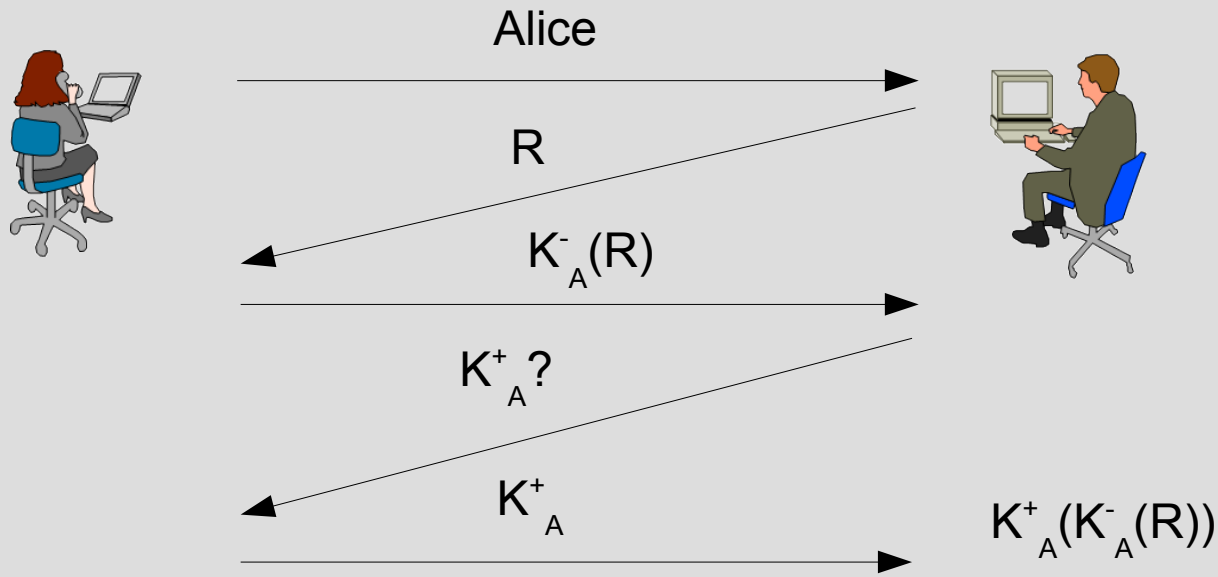
- Alice použije heslo pro zašifrování výzvy
- bezpečné, problém s předáním klíčů





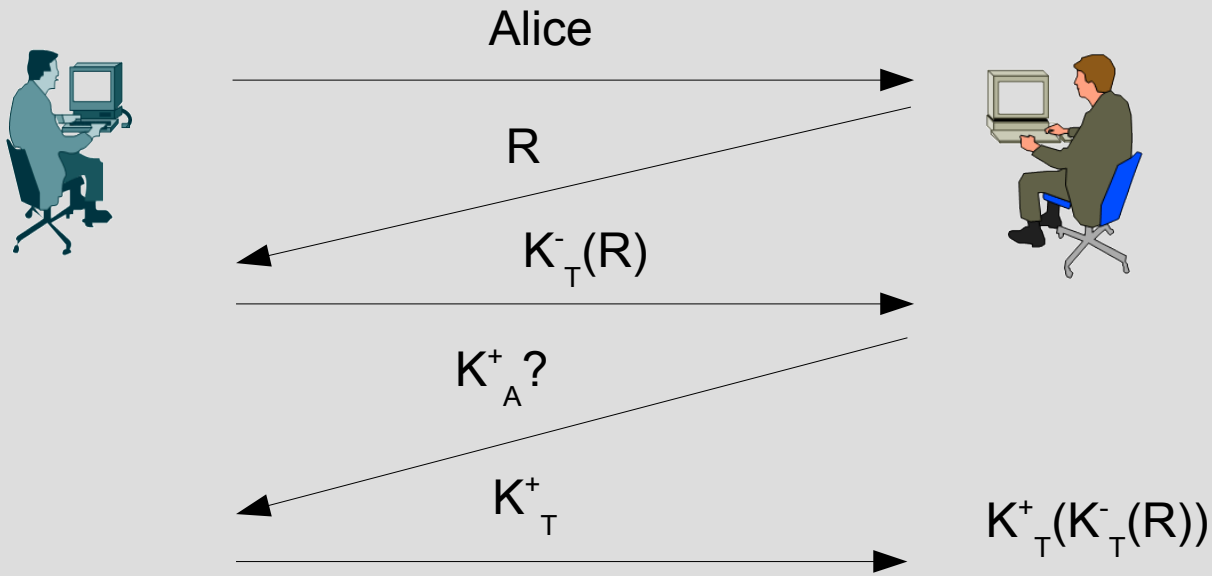
Autentizační protokoly 5.0

- využití asymetrické šifry



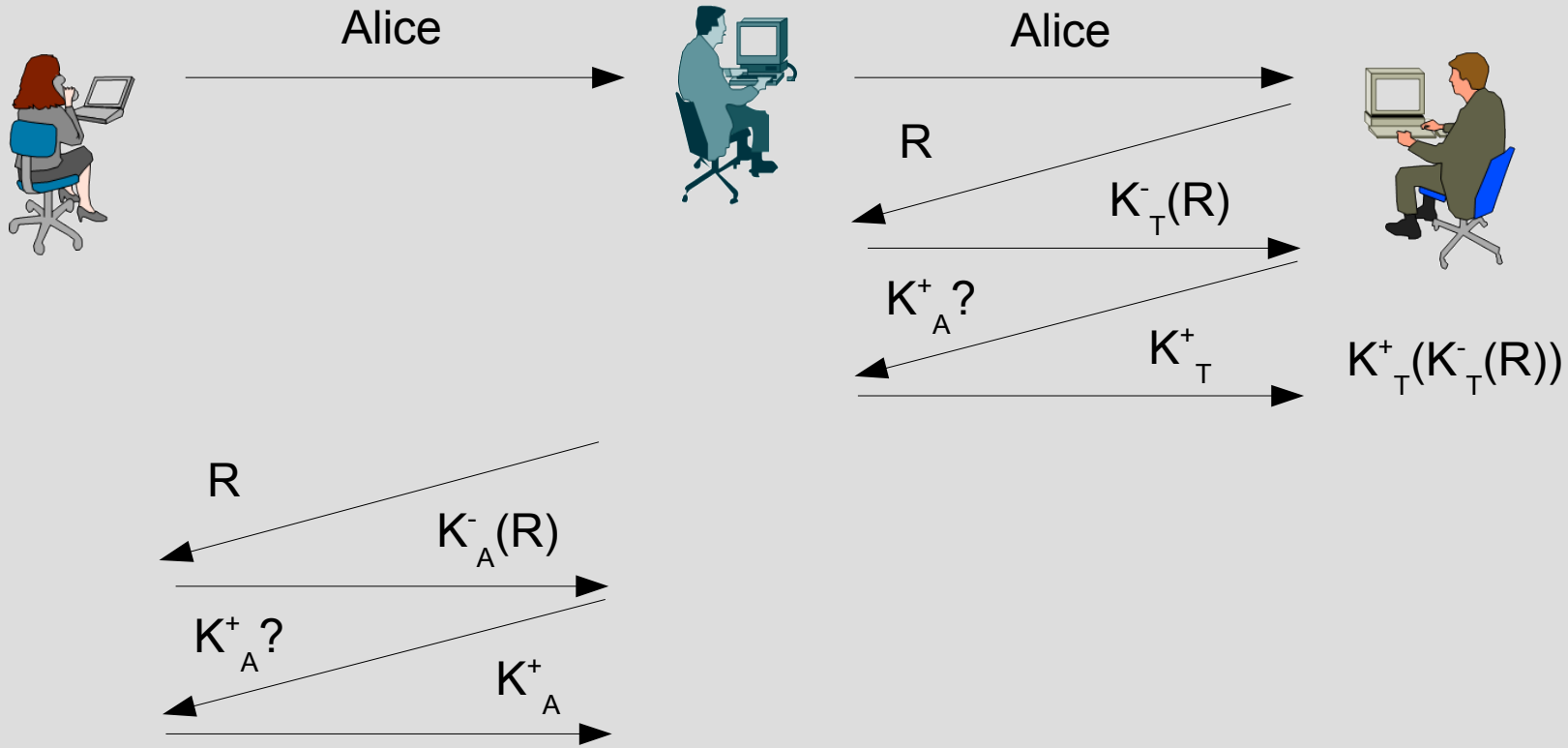
Autentizační protokoly 5.0

- chyba při získání veřejného klíče
- možnost zjistit, že Alice nekomunikovala



Autentizační protokoly 5.0

- chyba při získání veřejného klíče
- nemožnost zjistit, že Alice nekomunikovala



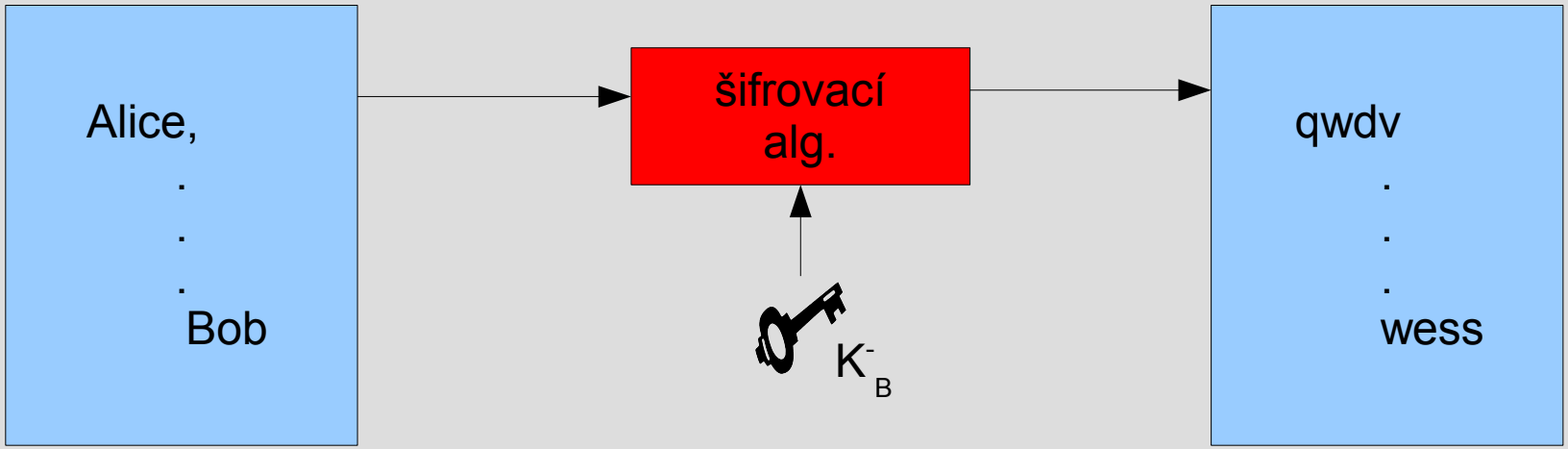
Autentizační protokoly 5.0

- nutnost bezpečného předání veřejného klíče
- osobní předání
- obecné zveřejnění
- důvěryhodný prostředník
  - certifikační autorita
  - digitální podpis

- asymetrická šifra je výpočetně složitější (xor x ^)
  - předání dočasného klíče pro symetrickou šifru

Integrita, digitální podpis

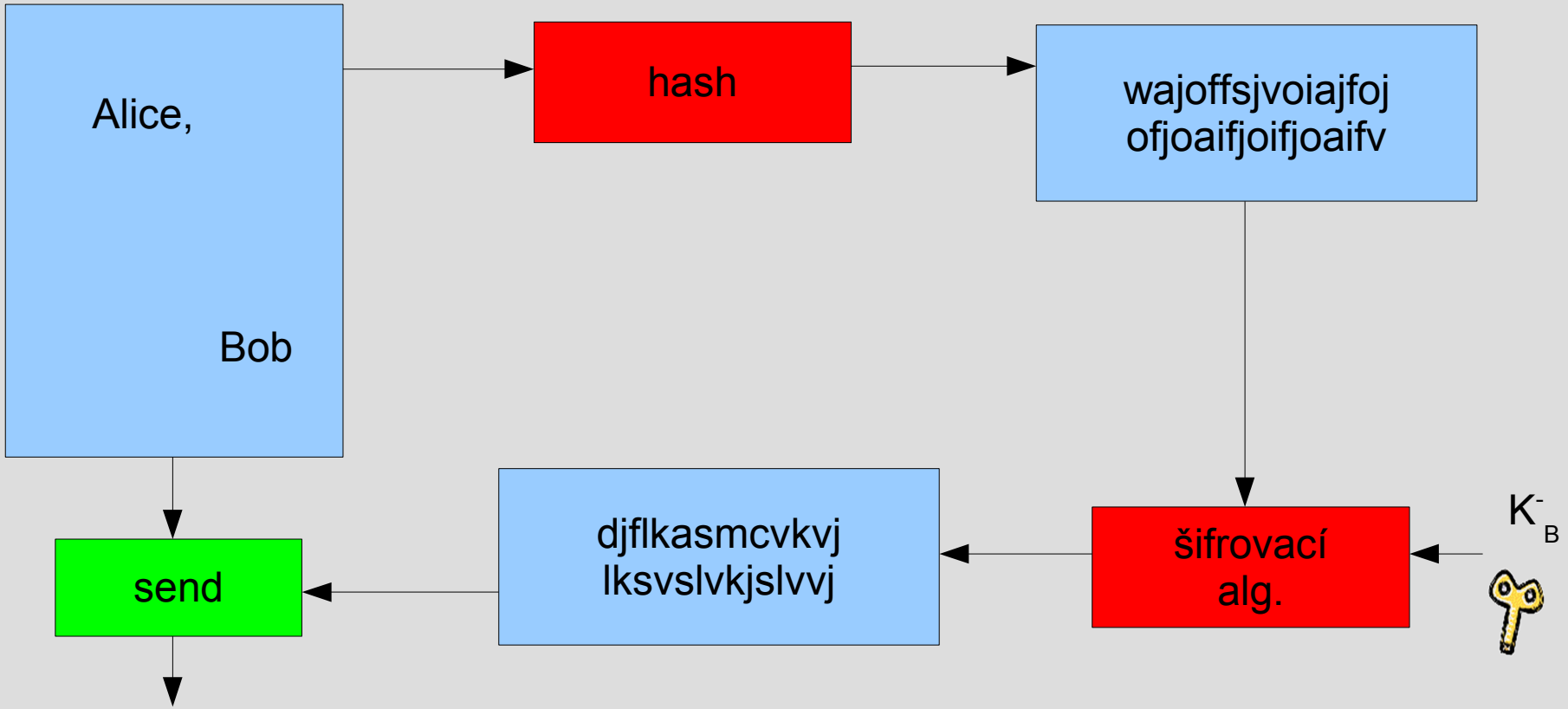
- integrita
  - zaručení, že dokument nebyl změněn
- nepopiratelnost
  - podpis zodpovědného subjektu
- doručenka
- využití asymetrického šifrování
  - podpis soukromým klíčem
  - ověření veřejným klíčem



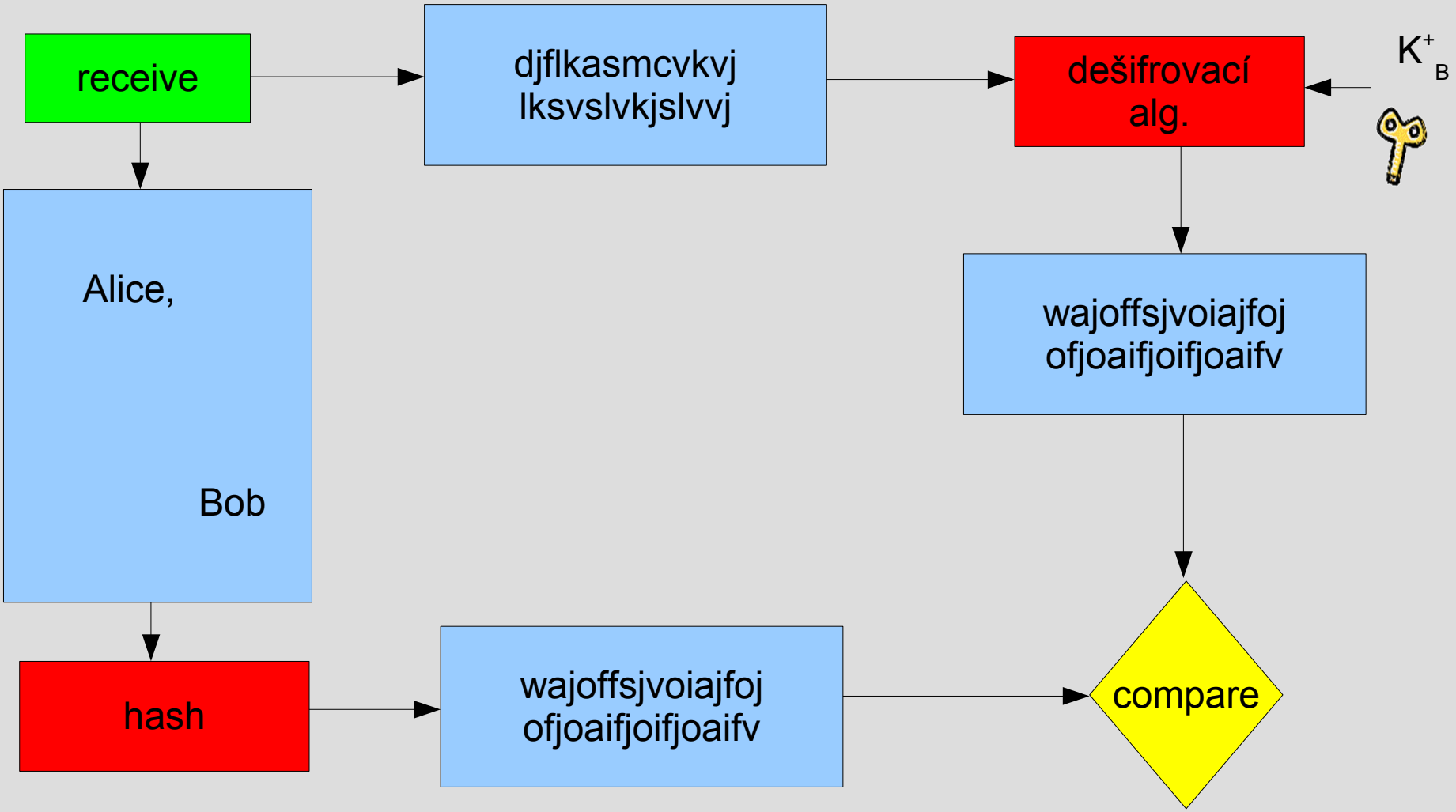
Podpis

- šifrujeme celý dopis - zbytečně náročné
- použití otisku
  - vytvoření otisku
  - zašifrování otisku
  - dešifrování otisku
  - vytvoření a porovnání otisku
  - využití hashovacích funkcí
  - problém kolizí (řízených)

Podpis


Alice,
Bob
hash
wajoffsjvoiajfoj
ofjoaifjoifjoaifv
šifrovací
alg.
K-B
djflkasmcvkvj
lksvslvkjslvvj
send

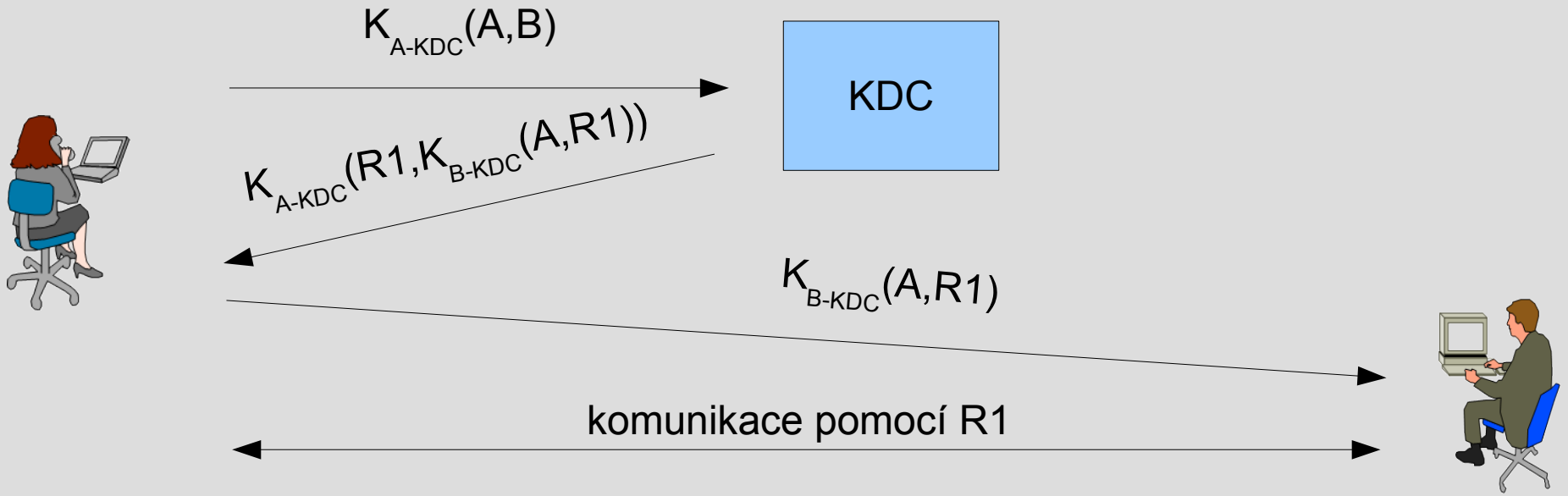
Podpis - ověření



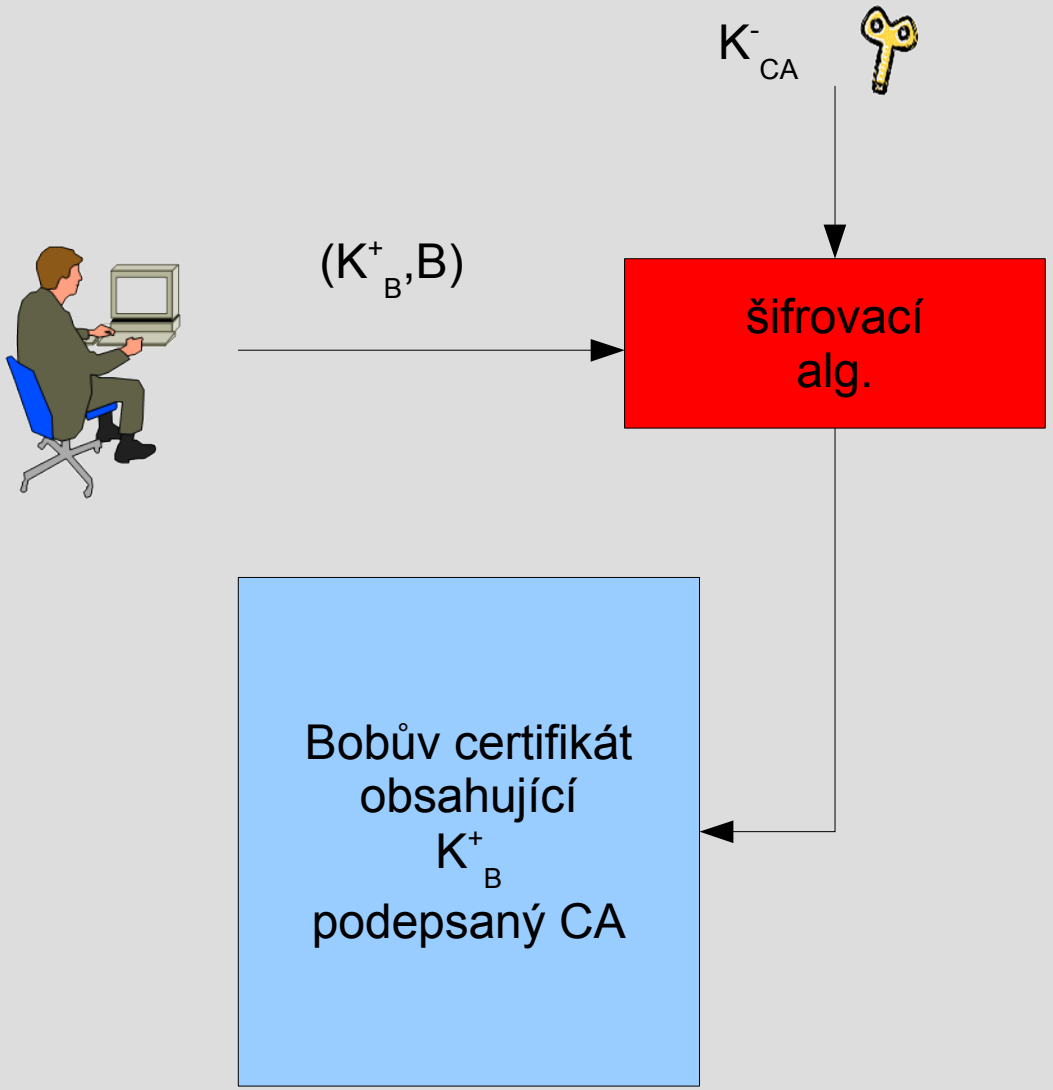
Distribuce klíčů

- symetrické i asymetrické řešení
- symetrické
  - KDS (Key Distribution Center)
  - Kerberos
  - každý uživatel má vlastní klíč
  - Kerberos přiděluje dočasné komunikační klíče
- asymetrické
  - CA (Certification Authority)
  - ověření uživatele
    - průkaz totožnosti, ...
    - vystavení certifikátu podepsaného CA
  - průkaznost CA
    - obecně známá
    - osobní kontakt
    - doporučená důvěryhodným prostředníkem

KDC


$K_{A\text{-}KDC}(A,B)$
KDC
$K_{A\text{-}KDC}(R1,K_{B\text{-}KDC}(A,R1))$
$K_{B\text{-}KDC}(A,R1)$
komunikace pomocí R1

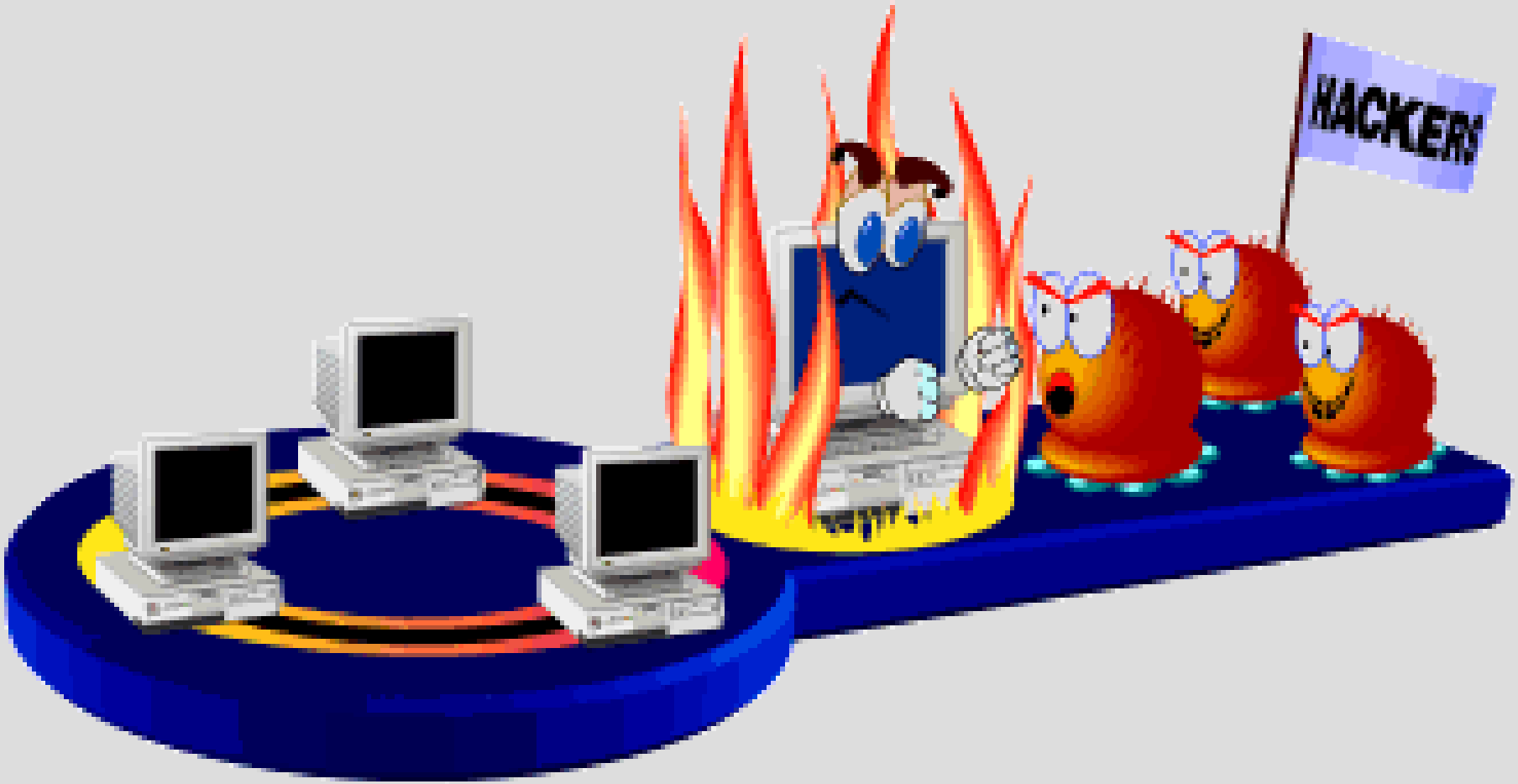
CA - vytvoření certifikátu



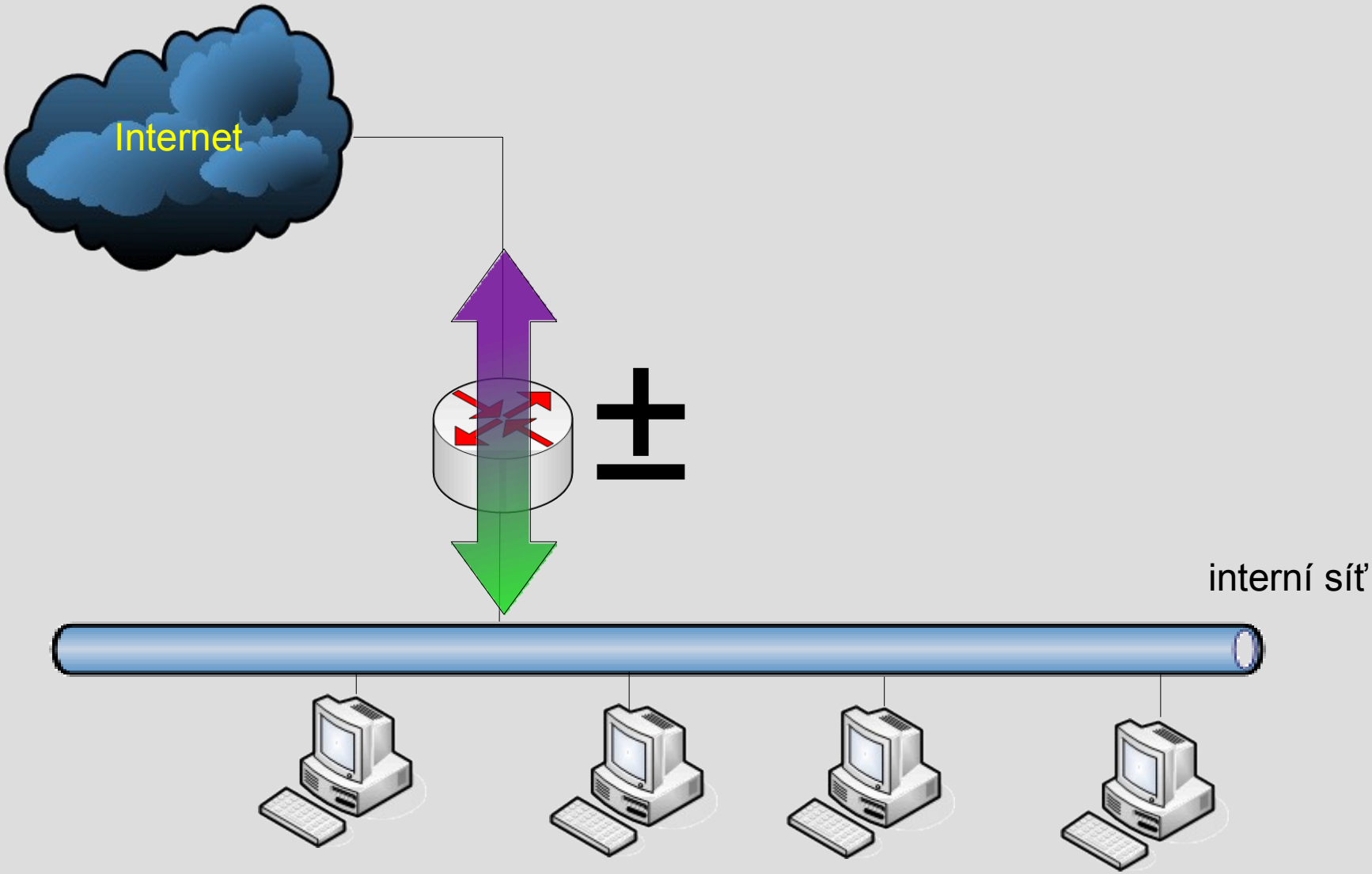
Řízení přístupu

- zamezení útočníkům v přístupu k prostředkům
- ochrana ve vstupním bodě – firewall
- firewall
  - HW prostředky
  - SW prostředky
  - pravidla
  - politika
- vlastnosti
  - zahazování, akceptace a forwardování paketů
  - logování
- paketové filtry
  - rozhodují se jen podle obsahu paketu
- kontextové filtry
  - rozhodují se podle kontextu spojení
- aplikační brány
  - speciální aplikace (např. proxy)

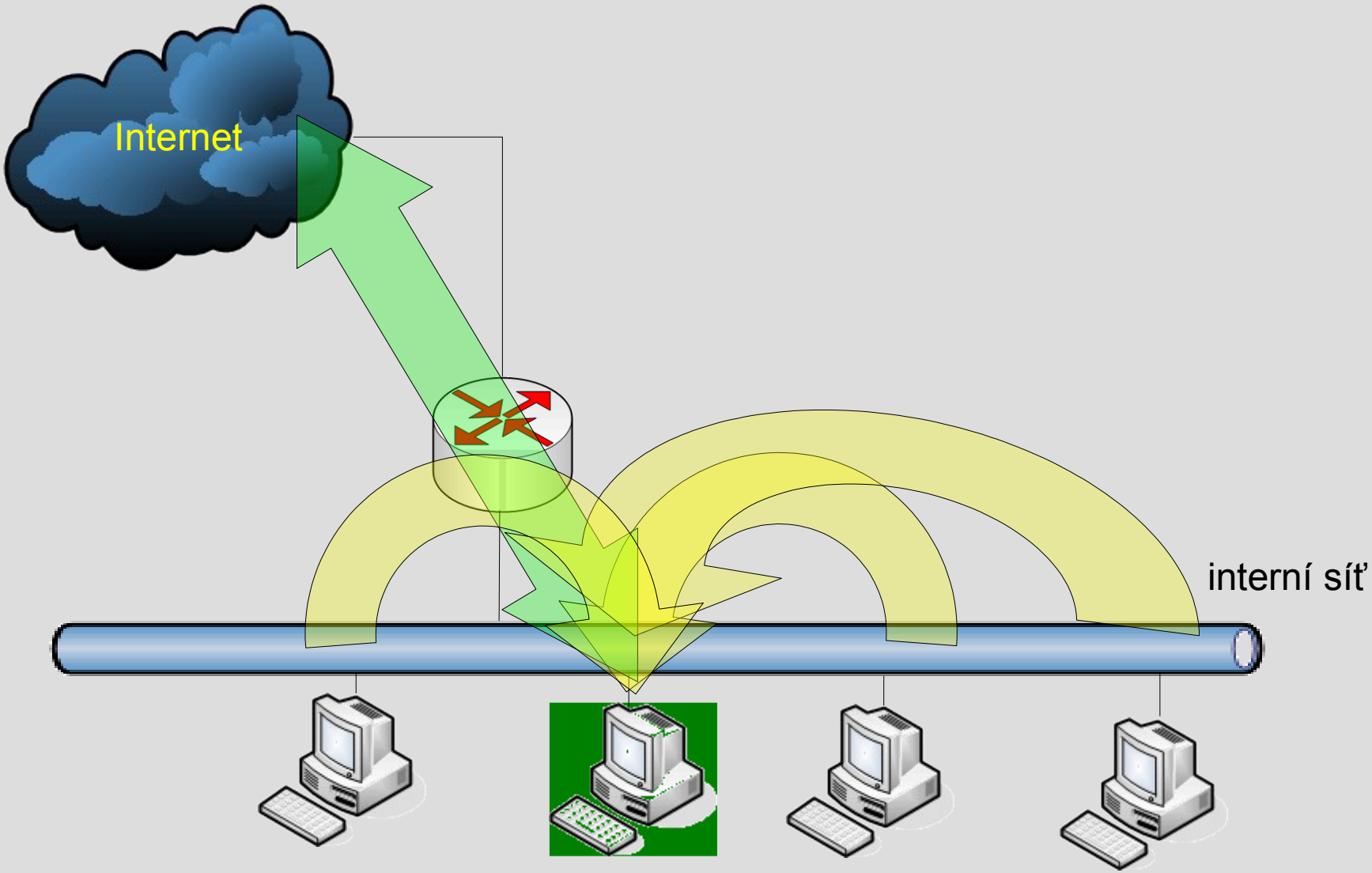
Fajrvol



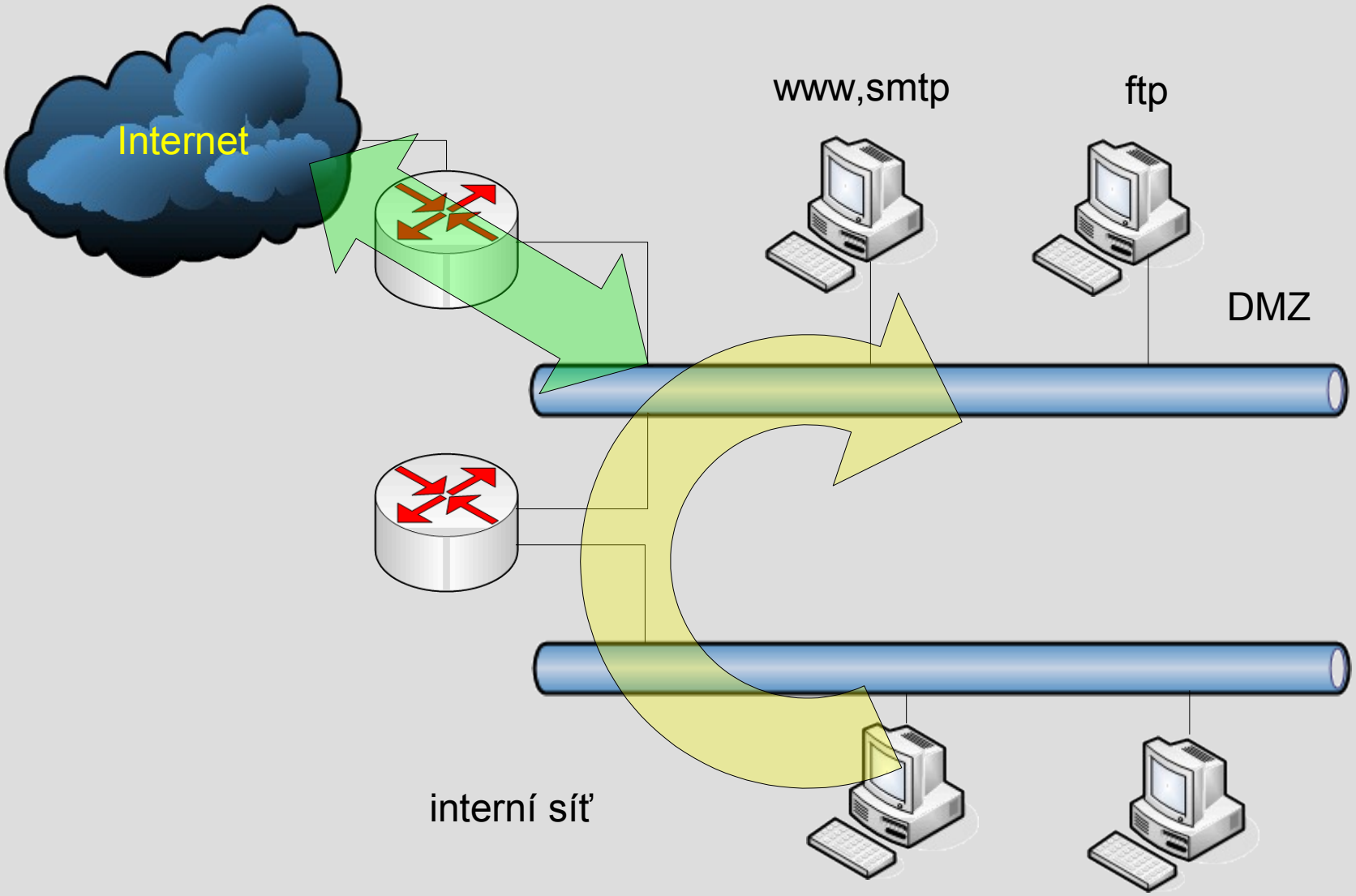
Filtr



Filtr a proxy



Filtry, proxy, DMZ



Typy útoků I

- mapování (mapping)
  - první fáze útoku, sběr informací, ping, portscanner
  - dobrý předpoklad pro DDoS
- odposlouchávání (sniffing)
  - možnost zjištění hesel
  - fyzický přístup k síti
    - zneužití směrování (přepínače i směrovače)
- podvrhnutí (spoofing)
  - podvrhnutí zdrojové adresy
  - poměrně jednoduše lze omezit na fw
- DoS(Denial-of-Service)
  - omezení dostupnosti služby pro legitimní uživatele
  - využívá chyby, nebo přetížení
    - SYN flooding attack – podvržený SYN paket, alokace zdrojů
    - smurf attack – podvržené ping pakety, zahlcení odpověďmi
    - dlouhý ping – využívá chybu v TCP/IP zásobníku

Typy útoků II

- DDoS (Distributed DoS)
  - velmi nebezpečná varianta DoS útoku
  - téměř bez možnosti obrany
- únos spojení (hijacking)
  - možnost ukradení navázaného spojení
  - šifrování tento problém řeší

Zabezpečení aplikací

- na více vrstvách
- aplikační vrstva
  - zabezpečení souboru např. PGP
- transportní vrstva
  - SSL Secure Socket Layer
  - zabezpečení spoje
- síťová vrstva
  - IPsec
  - zabezpečení mezi dvěma uzly
- linková vrstva
  - šifrování modemů, IEEE 802.11
  - zabezpečení linky
- šifrování může být na libovolné vrstvě, nižší vrstvy šifrují i hlavičky vyšších vrstev

co dál?

SSL, IPsec

pravidla pro firewally

bezpečnostní politiky

IDS

co po útoku

....

zase někdy jindy?