12. Bezpečnost počítačových sítí

Typy útoků:

- odposlech při přenosu
- falšování identity (Man in the Middle, namapování MAC, …)
- automatizované programové útoky (viry, trojské koně, …)
- buffer overflow, …
- přetížení či zahlcení zdrojů (spamming, DoS, DDoS, …)
- získávání soukromých informací
- podvržení informace
- spyware, adware, …

Obrana:

- znemožnění odposlechu apod. – šifrovat
- blokovat útoky – firewall
- detekovat a zneškodnit útoky – IDS
- znemožnit přístup – VLAN, VPN

Integrita dat

- protokoly: detekce, duplicita, ztráta, záměna pořadí
- kontrolní součty (parita, CRC, ..)
- kryptografické kontrolní součty (MD5, SHA,..)

Zabezpečení LAN:

- seznam povolených IP, MAC
- omezení počtu MAC (obrana proti přepnutí do HUB modu)

Firewall

- zabezpečení rozhraní veřejná síť / soukromá síť (PC)
- definice pravidel přístupu
- omezení přístupu na části vnitřní sítě
- omezení protokolů a služeb
- kontrola přístupu a zaznamenávání statistik

neřeší: vnitřní útok, virová ochrana, alternativní cesty, odposlech či modifikace dat

Paketový filtr: filtrace podle adres : síťová vrstva (IP, číslo protokolu, …), transportní vrstva (porty, příznaky komunikace – ack, ….)

Aplikační brána: filtruje na úrovni aplikací, vytvoření proxy a povolení konkrétních služeb, analýza paketů …

IDS – Intrusion detection systém (odhaluje útoky a informuje firewall)

- paket signature – pro známé typy útoků, zjišťování řetězce v datech, (často falešný poplach)
- statefull signature – vylepšení – hledá řetězec jen v kontextu okolních informací
- traffic/protocol snímaly detection – i pro neznámé útoky

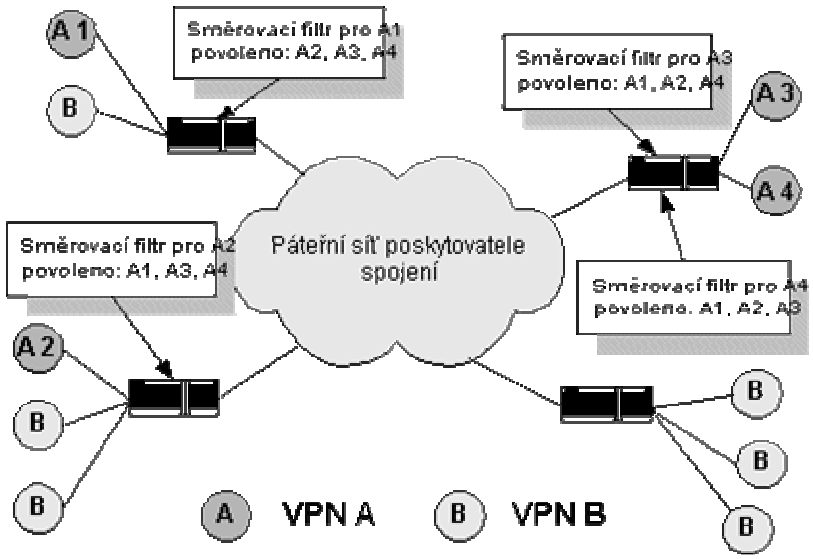
VLAN

Virtual LAN – členství v sítí na základě ne fyz. topologie ale

- portů
- mac adres
- ip adres, protokolů, …
- skupinového vysílání

VPN – virtual private network

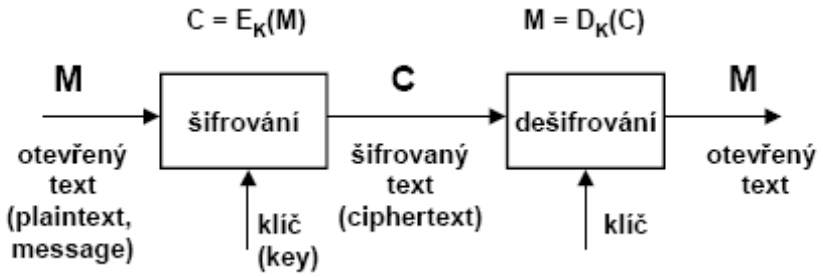
- při nahrazení soukromých linek internetem je třeba zabezpečení vlastní sítě
- tunelování
-



IPSec – řešení neřešené ochrany dat při přenášení IPv4
Sada hlaviček přidávaná před hlavičky 4. vrstvy obsahující informace o zabezpečení, vytváří šifrovaný tunel

Kryptologie = kryptografie + kryptoanalýza

- klasická (steganografie, substituční, transpoziční) - předpočítačová
- moderní (bezpečnost musí být závislá na klíči ne na algoritmu)



Symetrická – tajný klíč
Asymetrická – veřejný a soukromý klíč

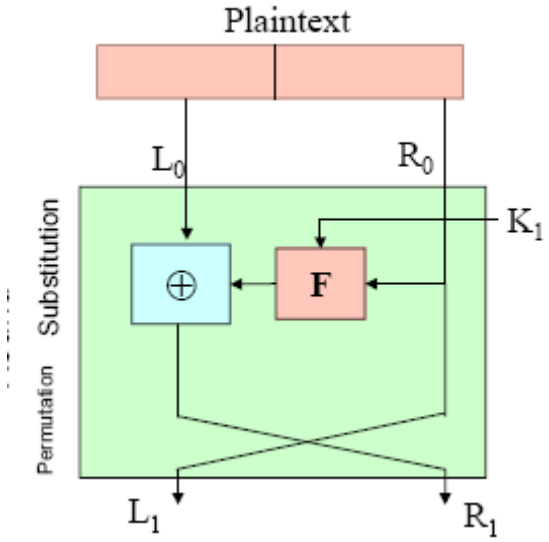
Co potřebujeme zaručit? : (ne každé šifrování zaručuje všechny položky)

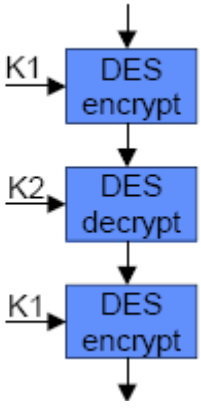
Důvěrnost
Autentizace
Integrita
Nepopiratelnost

- útok silou – nejlepší známý útok

SYMETRICKÉ

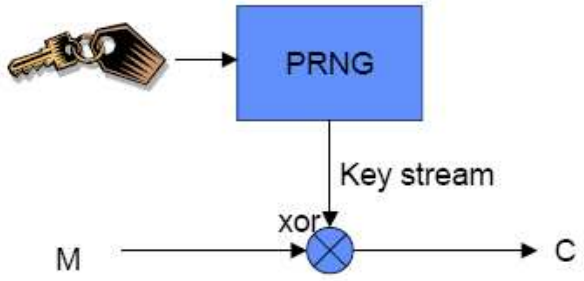
blokové: DES – 64b bloky, 56b klíč, Feistelova šifra
3DES (DES-EDE) 112b klíč
IDEA, ….





- **Moorův zákon**
  - Každých 18 měsíců se zdvojnásobí rychlost a paměťová kapacita
  - Každého 1.5 roku získáváme schopnost luštit navíc jeden bit klíče
- **Pokud dnes je 56bitový klíč rozlomen distribuovaným útokem za asi jeden den, 100bitový bude rozlomen za jeden den za cca 70 let**

Proudové: šifrování se provádí bit po bitu (Byte po byte)



ASYMETRICKÉ

- nelze vyrobit na zakázku
- faktorizace čísel, eliptické křivky, knapsack, …
- pomalejší
- 1024,2048, … b klíče, blokové šifry

RSA:

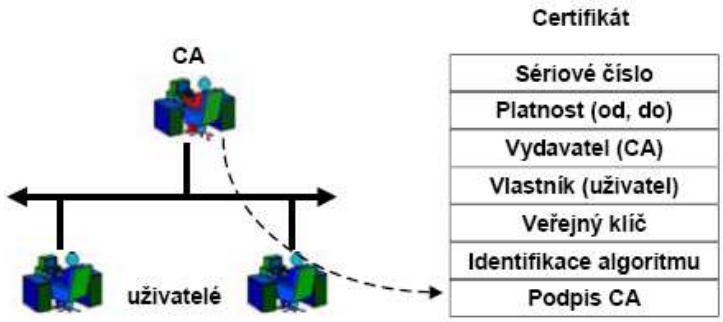
Klíče
– *n*: veřejný modulus
– *e*: veřejný exponent (typicky 3 nebo $2^{16}+1$)
– *d*: soukromý exponent
– *p*,*q*: činitele (factors) modulu n
» $n = p \times q$
– Musí platit vztah
» $d \times e \bmod (p-1)(q-1) = 1$
• Veřejný klíč je (*n*,*e*).
• Soukromý klíč je (*n*,*d*).

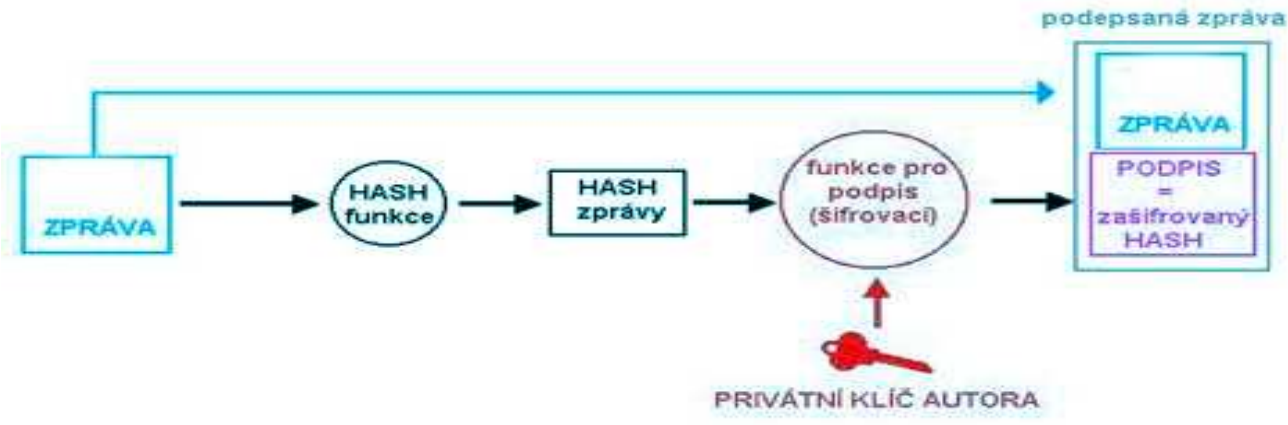
Šifrování - $c = m^e \bmod n$
Dešifrování - $m = c^d \bmod n$
Podpis – $s = m^d \bmod n$
Ověření – $m = s^e \bmod n$

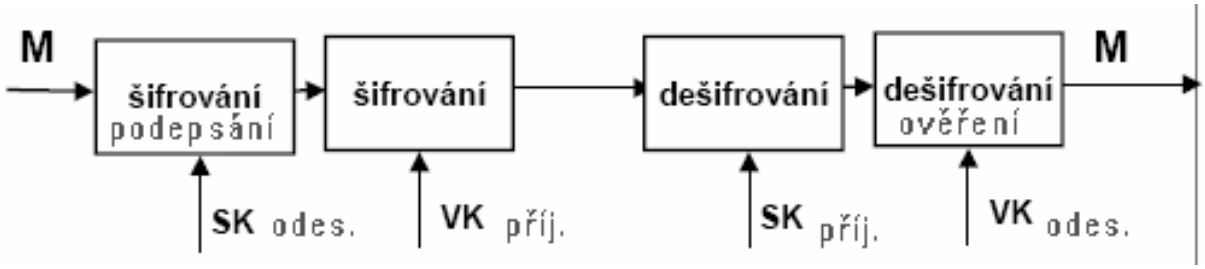
HASH

- jakýkoliv vstup → výstup konstantní délky (128,256b …) pro jiný vstup jiný výstup, jednocestná funkce
- SHA-1, MD5, SHA-2, …

EL. PODPIS – digitální podpis (založen na kryptografických mechanismech)







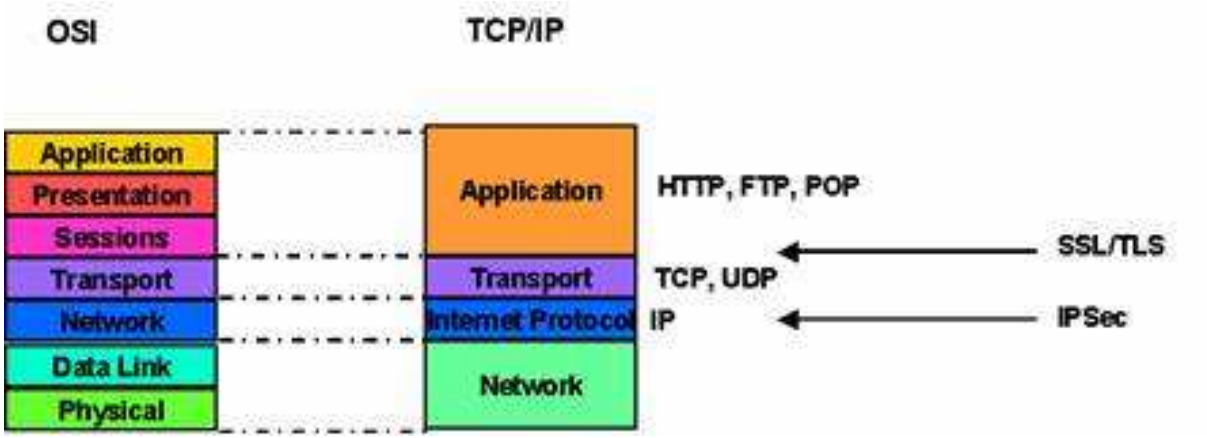
Pozn. Správa klíčů symetrické a asymetrické kryptografie ?! rozdíl

POUŽITÍ V SÍTÍCH:
Šifrování mezi dvěma počítači nebo mezi dvěma aplikacemi

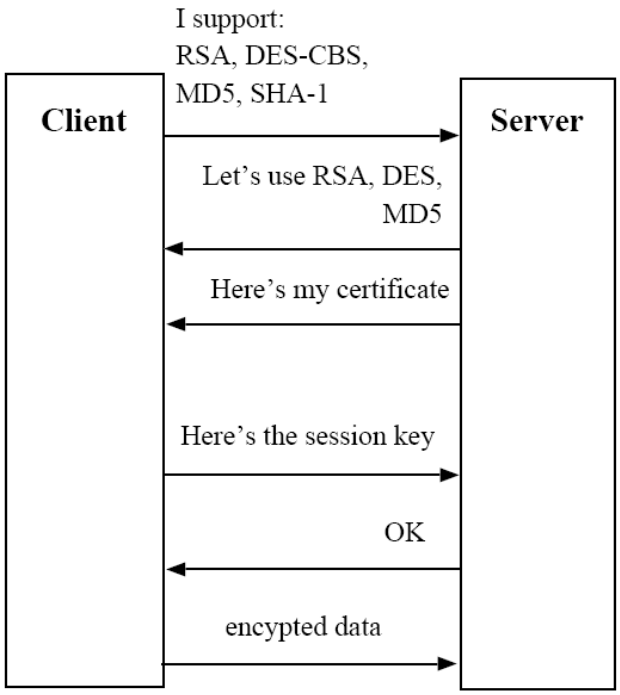
Linková vrstva: - šifruje se každý přenos zvlášť
- autentizace uzlů (počítačů)
- hw realizace, jeden klíč pro dva komunikující uzly

Presentační, Aplikační vrstva: - autentizace uživatelů
- lze aplikaci přizpůsobit algoritmus
- vytvoření kanálu mezi aplikacemi (např. SSL)

SSL:
mezi aplikační a transportní vrstvou (použití např https, …)
vytvoření zabezpečeného tunelu, nutná podpora od aplikace,



- mohou požadovat oboustrannou autentizaci
- klíč relace (session key) se vytváří z klíčového materiálu získaného od obou stran



SSH – RSA autentizace, dále DES, 3DES, IDEA, RC4, …