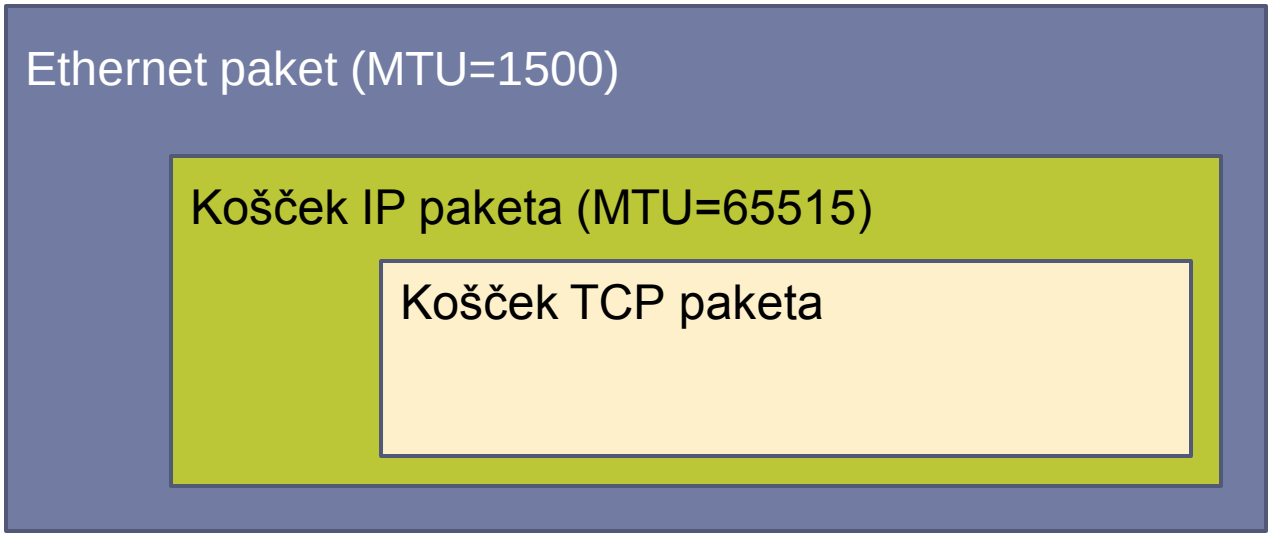
Procesorski sistemi v telekomunikacijah
Mrežni/komunikacijski procesorji

Paketni prenos podatkov

- Podatki se prenašaja po več 100 ali 1000 bytov naenkrat
- Taki enoti pravimo paket
- Paket je sestavljen iz
  glave (header) in koristne vsebine (payload)
- Primer: Ethernet paket

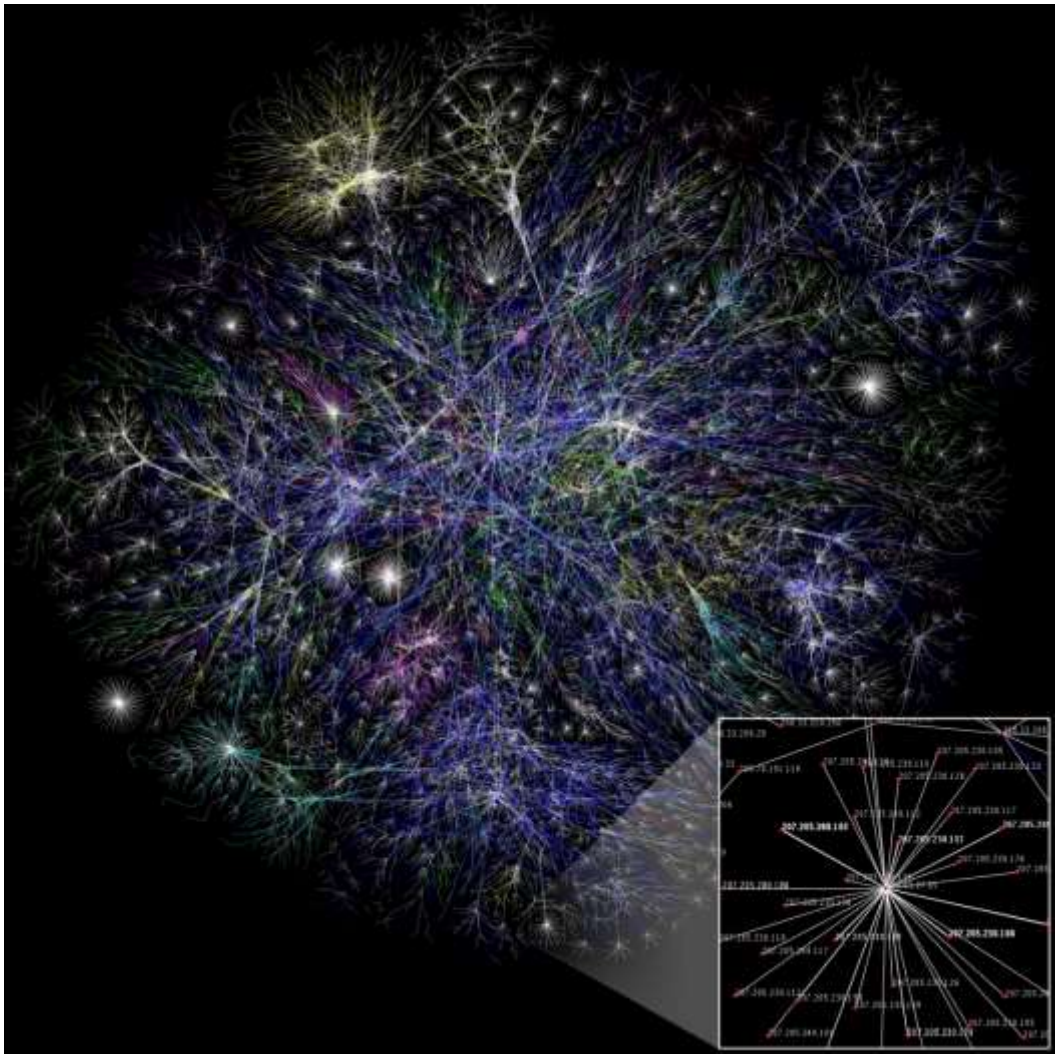
Paket v paketu v paketu v ...

- Vsebina paketa protokola A je lahko spet nek paket B.
- Paket protokola A lahko nosi največ MTU (Maximum Transmission Unit) bytov
- Če je paket B večji kot MTU, se razdeli in potuje v večih paketih protokola A (fragmentacija).
- Primer: paketi protokola TCP potujejo v paketih protokola IP, ki potujejo v Ethernet paketih



Internet

- Hrbtenica interneta so optične povezave
- Hitrosti povezav 2007 do 40Gb/s
- Februar 2010 Japonska-ZDA 300Gb/s



Slika 30% interneta (15.1.2005). Vir: Wikipedia, opte.org. Vsaka točka predstavlja en IP naslov.

Mrežni/komunikacijski procesorji

- Obdelava take količine informacij je prehuda naloga za klasične mikroprocesorje.
- Mrežni/komunikacijski procesorji imajo podsklope za obvladovanje velikih pretokov podatkov.

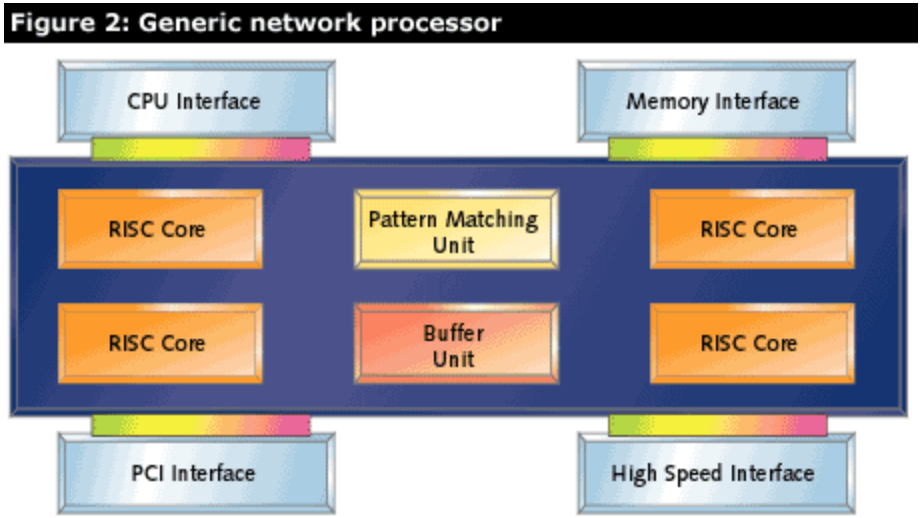
Hitrost (Mb/s)	Čas na voljo za obdelavo 64-bytnega paketa (ns)
1.5	340 000
45	11 000
155	3 000
622	820
2 500	200
9 500	51

Intel IXP425

Naloge

- Iskanje vzorcev v paketih podatkov, npr. za filtriranje vsebin
- Iskanje po tabelah - usmerjanje prometa na osnovi naslova
- Manipulacija bitov v paketih
- Razvrščanje paketov v čakalne vrste (queueing)
- Enkripcija/dekripcija vsebine paketov
- Kompresija/dekompresija podatkov

Ponavadi imajo mrežni procesorji več RISC jeder

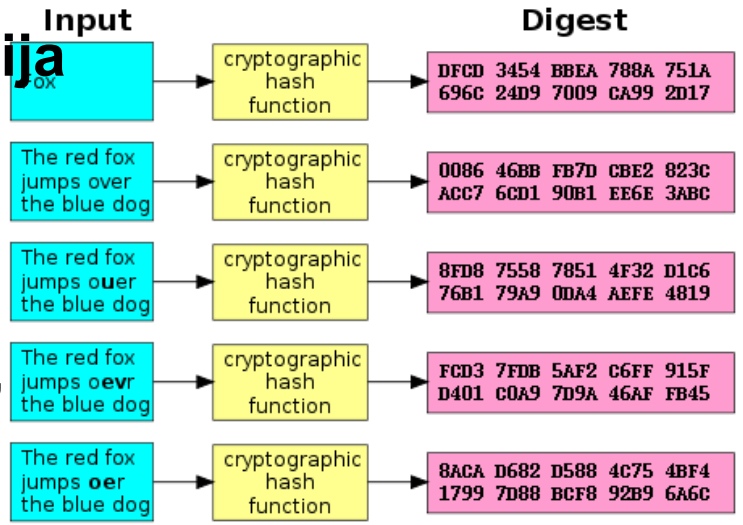


Uporaba

- Mrežna stikala in usmerjevalniki
- Sistemi za zagotavljanje kakovosti storitve za izbrane protokole (QoS, Quality of Service)
- Sistemi za kontrolo dostopa do omrežja
- Pomoč mikroprocesorju pri izvedbi protokolov, npr. TCP/IP
- V RAID krmilnikih (Redundant Array of Independent

Postopki v mrežnih procesorjih
Zgoščevalna funkcija (Hash function)

- Priredi kratko število poljubno dolgemu nizu bitov
  Primer: 8-bitna vsota bytov v nizu – kontrolna vsota
- Dva različna niza... (običajno) dve različni vrednosti funkcije
- Uporaba: hitra primerjava nizov, asociativne (hash) tabele, kontrola pravilnosti podatkov (npr. CRC), ...
- Primer: kontrolne vsote, ciklične redundančne kode (CRC32, ...), ...
- **Kriptografska zgoščevalna funkcija**
  Podobni nizi dajo močno različne vrednosti zgoščevalne funkcije
- Primer: MD4, MD5, SHA-512, ...
- Uporaba: za avtentikacijo podatkov, hranjenje gesel uporabnikov, generiranje naključnih števil, ...



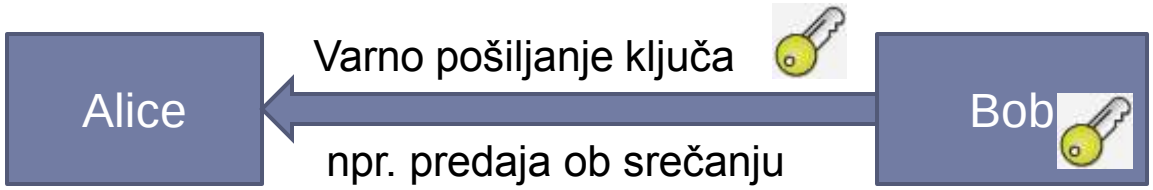
Postopki v mrežnih procesorjih
Primer: avtentikacija z SHA-512

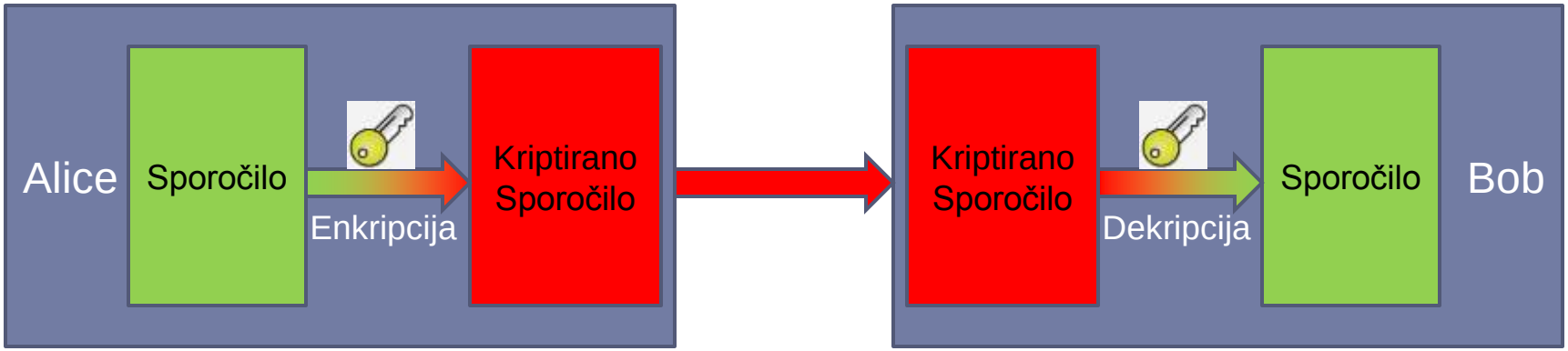
- Geslo uporabnika je “bicikel”
- Računalnik hrani SHA-256 vrednost gesla “bicikel”:
  74f87ed882981104a48436b2d4f4b096d17f14e331d9bd0b39b1b73ca4c8588b
- Če kdo vdre v računalnik, bo dobile le SHA-256 vrednost gesla, ne pa tudi samega gesla.
- Recimo, da se uporabnik poskuša prijaviti z geslom “tricikel”. Računalniku pošlje geslo “tricikel”. Računalnik izračuna SHA-256 za “tricikel”:
  ac15178a769f799ad38d732fb67e136f14b8dc7c4b6fbecad34dea2d5d6041b1
- Računalnik primerja obe SHA-256 vrednosti in ugotovi, da je geslo napačno.
  Uporabnik ne dobi dostopa.

- Če uporabnik pošlje geslo “bicikel”, računalnik izračuna SHA-256 in dobi

Postopki v mrežnih procesorjih
Simetrična kriptografija

- Za enkripcijo in dekripcijo se uporablja enak ključ
- Problem: varna izmenjava ključev (brez prisluha tretje osebe)
- Postopki:
  DES (56 bitni ključ), 3DES (168, 112 ali 56 biten ključ)
  RC4 (40-2048 bitni ključ) – v SSL protokolih, WEP protokol (WLAN)
  AES (128, 192 ali 256 bitni ključ) – naslednik DES, uporaba v WPA2 (WLAN)

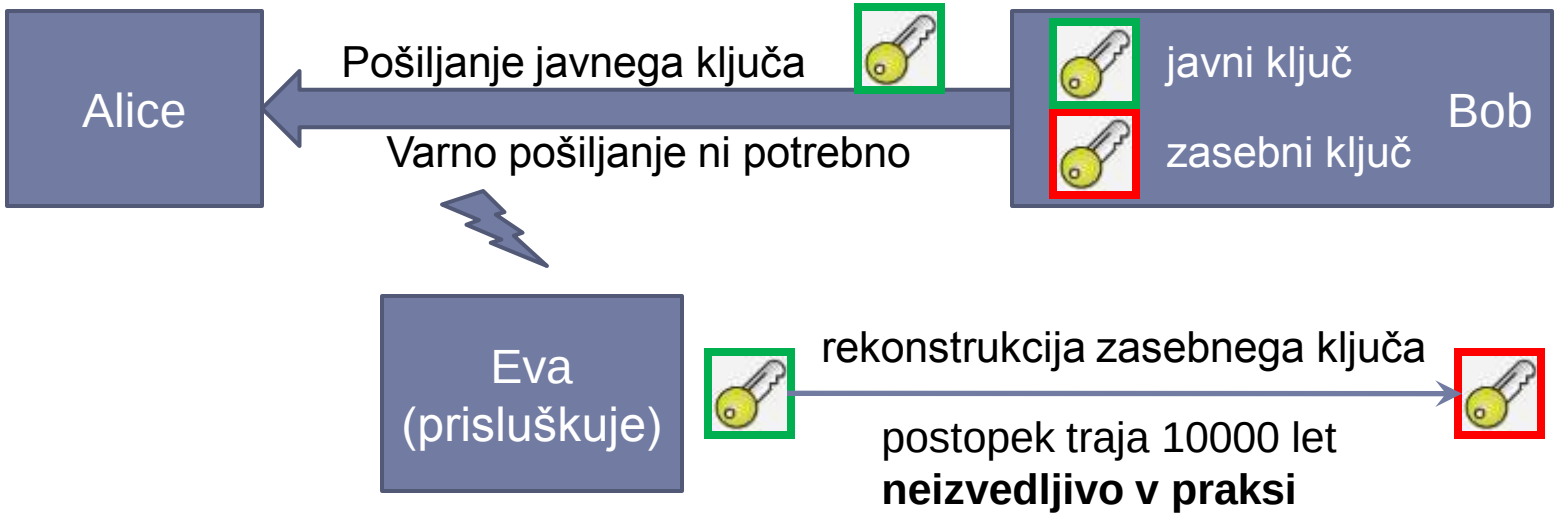


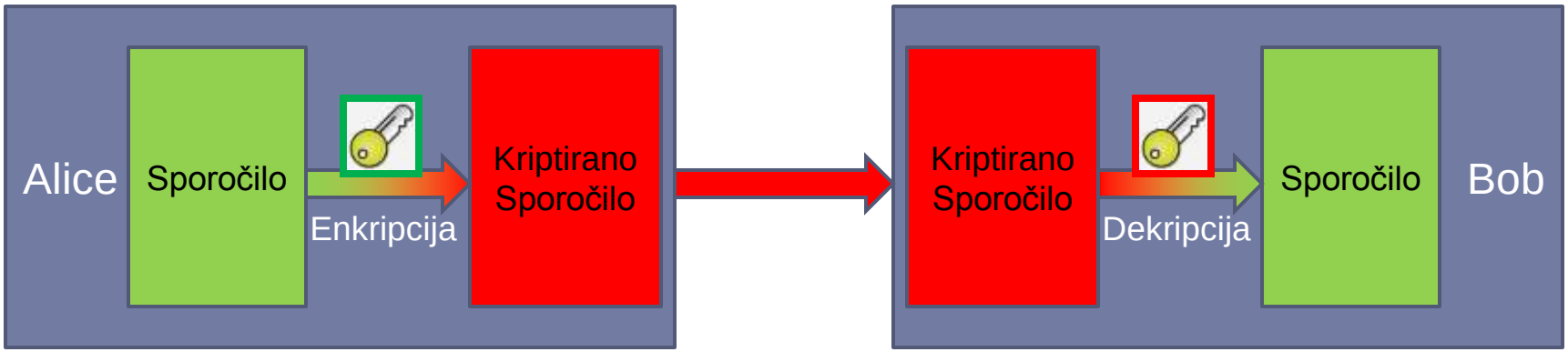


Postopki v mrežnih procesorjih Asimetrična kriptografija...

- Kriptografija z javnim ključem
- **Javni ključ za enkripcijo, zasebni ključ za dekripcijo**
- Naslovnik generira par javni-zasebni ključ
- Naslovnik pošlje javni ključ pošiljatelju sporočila, zasebni ključ ostane na varnem pri naslovniku
- Pošiljatelj kriptira sporočilo z javnim ključem in ga pošlje naslovniku
- Naslovnik dekriptira sporočilo z zasebnim ključem
- Ni izmenjave (zasebnega) ključa za dekripcijo
- **Postopki s pomočjo katerih bi iz javnega ključa rekonstruirali zasebni ključ so dolgotrajni in v praksi neuporabni, če je ključ dovolj dolg.**
- Postopki: RSA, Diffie-Helman, McEliece, ...

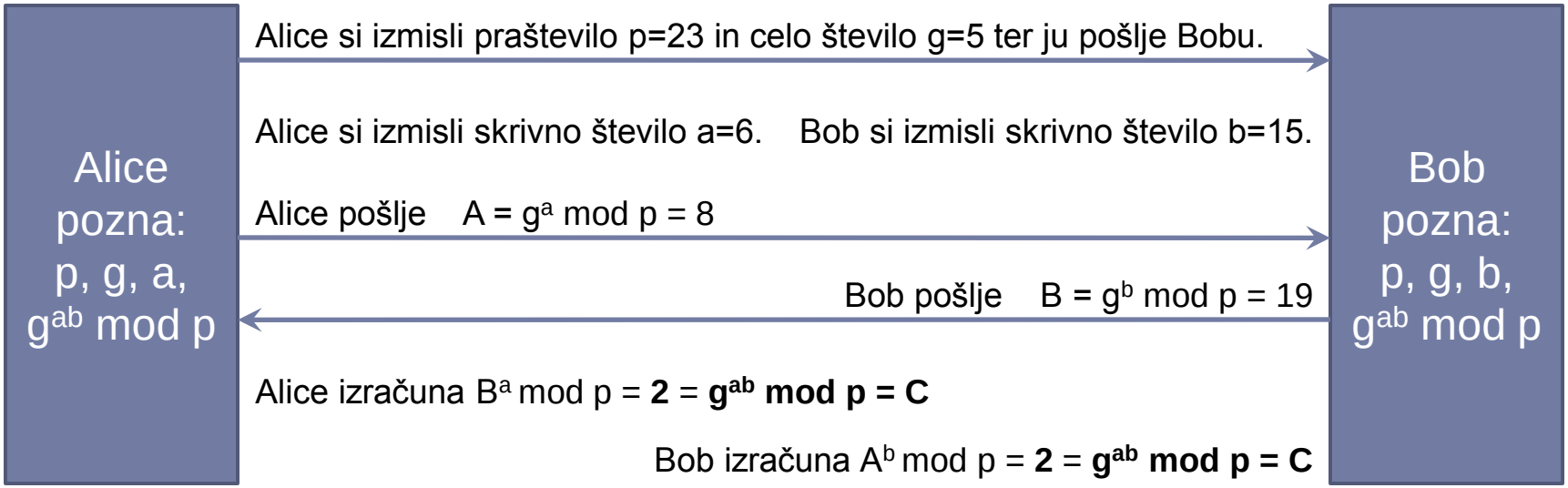
Postopki v mrežnih procesorjih ... asimetrična kriptografija





Asimetrična kriptografija
Primer: postopek Diffie-Hellman

- V osnovi je to postopek za varno izmenjavo ključa.
- Tretja oseba, ki prisluškuje izmenjavi, bi teoretično lahko rekostruirala ključ, ampak v praksi bi to predolgo trajalo.
- a mod b = ostanek pri deljenju a z b npr.: 27 mod 7 = 6



- Alice in Bob uporabita **$C=g^{ab}$ mod p** kot ključ za postopke simetrične kriptografije.
- Eva, ki je prisluškovala, pozna p, g, A in B, ne pa tudi C-ja. Lahko pa ga izračuna!!!
- Izračun C traja predolgo, če so p, a in b dovolj dolgi (cca. 300, 100 in 100

Postopki v mrežnih procesorjih
Digitalni podpis

- Digitalni podpis je kriptografska zgoščevalna funkcija, katere vrednost je odvisna od ključa in od vsebine sporočila
- Kot ključ uporabi podpisnik svoj zasebni ključ
- Podpis je odvisen od vsebine sporočila in od zasebnega ključa.
- Kdorkoli, ki ima javni ključ pošiljatelja lahko preveri avtentičnost sporočila s pomočjo javnega ključa pošiljatelja.
- Preverjanje opravi funkcija, ki iz sporočila, podpisa in javnega ključa izračuna ali se podpis ujema s sporočilom in ključem.
- Če je sporočilo neavtentično (spremenjeno) se podpis se ne ujema s sporočilom in javnim ključem.
- Tretja oseba ne more ponarediti digitalnega podpisa za spremenjeno sporočilo, ker nima pošiljateljevega zasebnega ključa – tega ima izključno le pošiljatelj.

Postopki v mrežnih procesorjih
Kompresija/dekompresija podatkov

- Kompresija – pretvorna niza A dolžine n v niz B dolžine m≤n
- Dekompresija – pretvorba niza B nazaj v niz A
- **Brezizgubna kompresija** – iz niza B lahko rekonstruiramo niz A
  Primer: algoritem LZ (Lempel-Ziv) - WinZIP, gzip, ...

  Iskanje ponavljajočih se vzorcev v nizu in učinkovit zapis teh vzorcev
  Primer: namesto abababababab v nizu A pišemo [ab]5 v nizu B

- **Izgubna kompresija** – iz niza B lahko niz A rekonstruiramo le delno, tako da so razlike do prvotnega niza A dovolj majhne
  Primer: stiskanje zvoka, slike in videa

  Odstranjevanje informacij, ki jih porabnik dekompresiranega niza ne opazi
  Npr. odstranjevanje maskiranih tonov (ki jih uporabnik ne more slišati), povečevanje šuma v frekvenčnih pasovih, ki vsebujejo glasen zvok

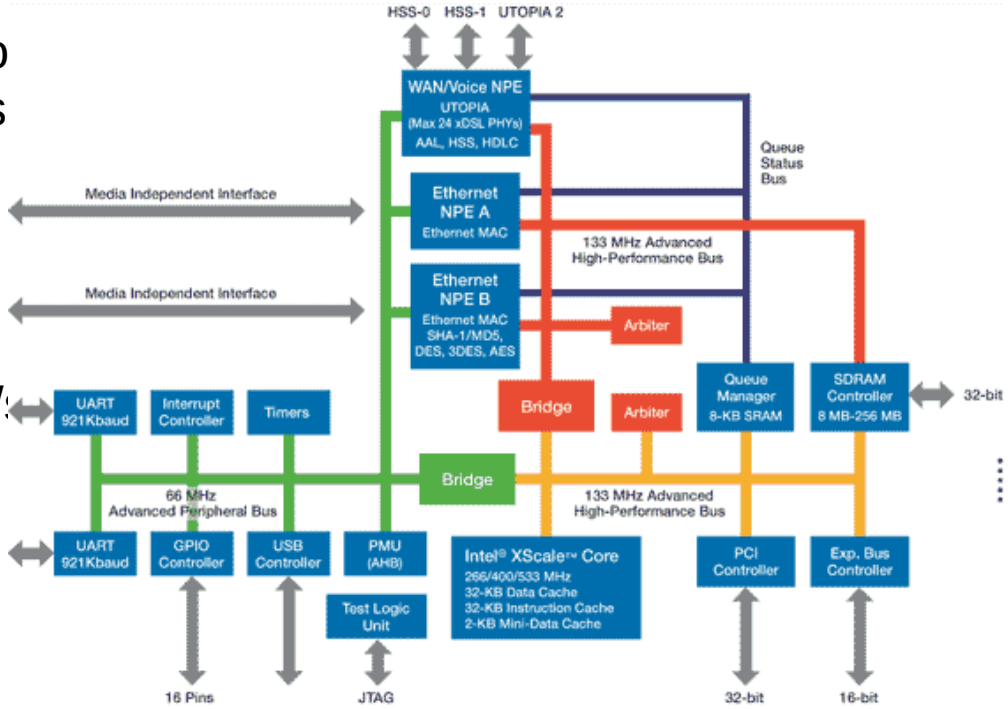
Postopki v mrežnih procesorjih
Regularni izrazi in razpoznavanje vzorcev

- Za opisovanje vzorcev
- Iskanje vzorca v toku podatkov opravlja avtomat.
- Avtomat je določen z regularnim izrazom.
- Obstaja več dogovorjenih formatov za regularne izraze

- Primer: regularni izrazi v jeziku Perl
  `Clinton|Bush|Reagan` ... najdi zaporedja znakov ‘Clinton’, ‘Bush’ ali ‘Reagan’
  `a.c` ... ‘a’, ki mu sledi en poljuben znak, nakar sledi znak ‘c’
  `a\.c` ... ‘a’, ki mu sledi pika, nakar sledi znak ‘c’
  `ab*c` ... ‘a’, ki mu sledi 0 ali več ‘b’-jev, nakar sledi znak ‘c’
  `[abc]` ... črke mali ‘a’, mali ‘b’ in mali ‘c’
  `[A-Z]` ... vse velike angleške črke
  `[Aa]bc` ... niz ‘Abc’ ali niz ‘abc’
  `ab{2,4}c` ... ‘a’, ki mu sledijo od 2 do 4 ‘b’-ji, nakar sledi znak ‘c’
  `[abc]+` ... niz dolg vsaj en znak, ki vsebuje le znake ‘a’, ‘b’ in ‘c’
  `[^abc]+` ... niz dolg vsaj en znak, ki ne vsebuje znakov ‘a’, ‘b’ in ‘c’

Primer: mrežni procesor Intel IXP425

- Do 533 MHZ, 32-bitno RISC jedro Intel XScale
  (Intel+Marvell izvedba arhitekture ARMv5 – i.MX27 je ARM926, ki je ARMv5)
- Vgrajeni algoritmi SHA-1, MD5, DES, 3DES, AES
- Dvoje hitrih serijskih (HSS) vrat
- Dva 10/100Mbit Ethernet vmesnika
- UTOPIA L2 vmesnik za povezavo
  z ADSL, G.SHDSL in VDSL vmes
- PCI v2.2 vmesnik (33/66 MHz)
- USB 1.1 krmilnik
- SDRAM krmilnik
- Dva UART vmesnika (do 921kbit/
- 16 splošnonamenskih priključkov
- 16-bitno razširitveno vodilo
- Poraba: 1-1.5W



Primer: mrežni procesor Freescale MPC8572E (PowerQUICC III)

- Dve e500 (32-bitni PowerPC) jedri, 1.5GHz, 32kB/1MB L1/L2 cache,
- Dva DDR2/DDR3 krmilnika
- Štirje 10/100/1000Mbit Ethernet vmesniki
- Vezje za razpoznavanje vzorcev
- Vezje za iskanje po tabelah
- Hiter serijski vmesnik
- Vmesnik PCI Express
- Dva DMA krmilnika
- Dva I^2C vmesnika
- Algoritmi DES, 3DES, MD5, SHA-1/2, AES, RSA, ...
- Poraba: 25W