Preddiplomski studij

Računarstvo

Komunikacijske mreže

10.

Osnove sigurnosti mreža, usluga i aplikacija – sigurnost u Internetu

Ak.g. 2011./2012.

Sadržaj predavanja

- Sigurnost, prijetnje i zahtjevi
- Osnovno o kriptografiji
  - simetrična kriptografija
  - asimetrična kriptografija
  - digitalni potpis i sažetak poruke
  - infrastruktura javnog ključa
- Sigurnosna arhitektura Interneta
  - sigurnosno proširenje protokola IP – IPsec
  - sloj sigurnih priključnica SSL

Problem …

A → Alice

uljez (engl. intruder)

prisluškivanje (engl. evesdropping, eavesdropping,)

B → Bob

… i definicije

Sigurnost (engl. *security*)

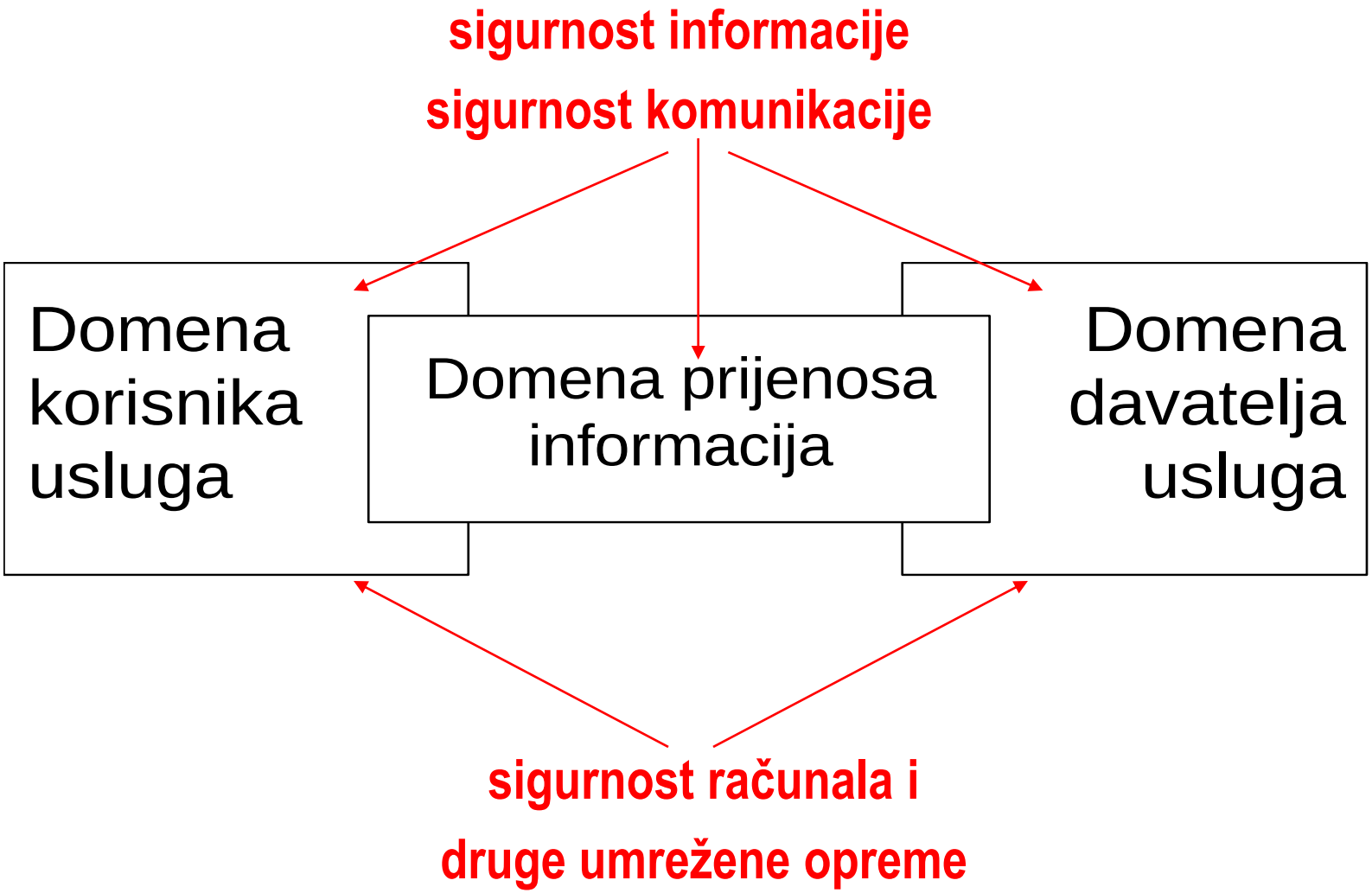
- Sposobnost mreža, sustava, usluga i aplikacija da se suprotstave neočekivanim slučajnim događajima i zlonamjernim aktivnostima koje mogu narušiti i kompromitirati raspoloživost, vjerodostojnost, cjelovitost i povjerljivost informacije i komunikacije

Prijetnja u mrežnom okružju

- okolnost, stanje ili događaj koji može naškoditi osoblju ili mrežnim i računalnim resursima u obliku uništavanja, razotkrivanja ili modifikacije podataka, uskrate usluge, prijevare i zlouporabe

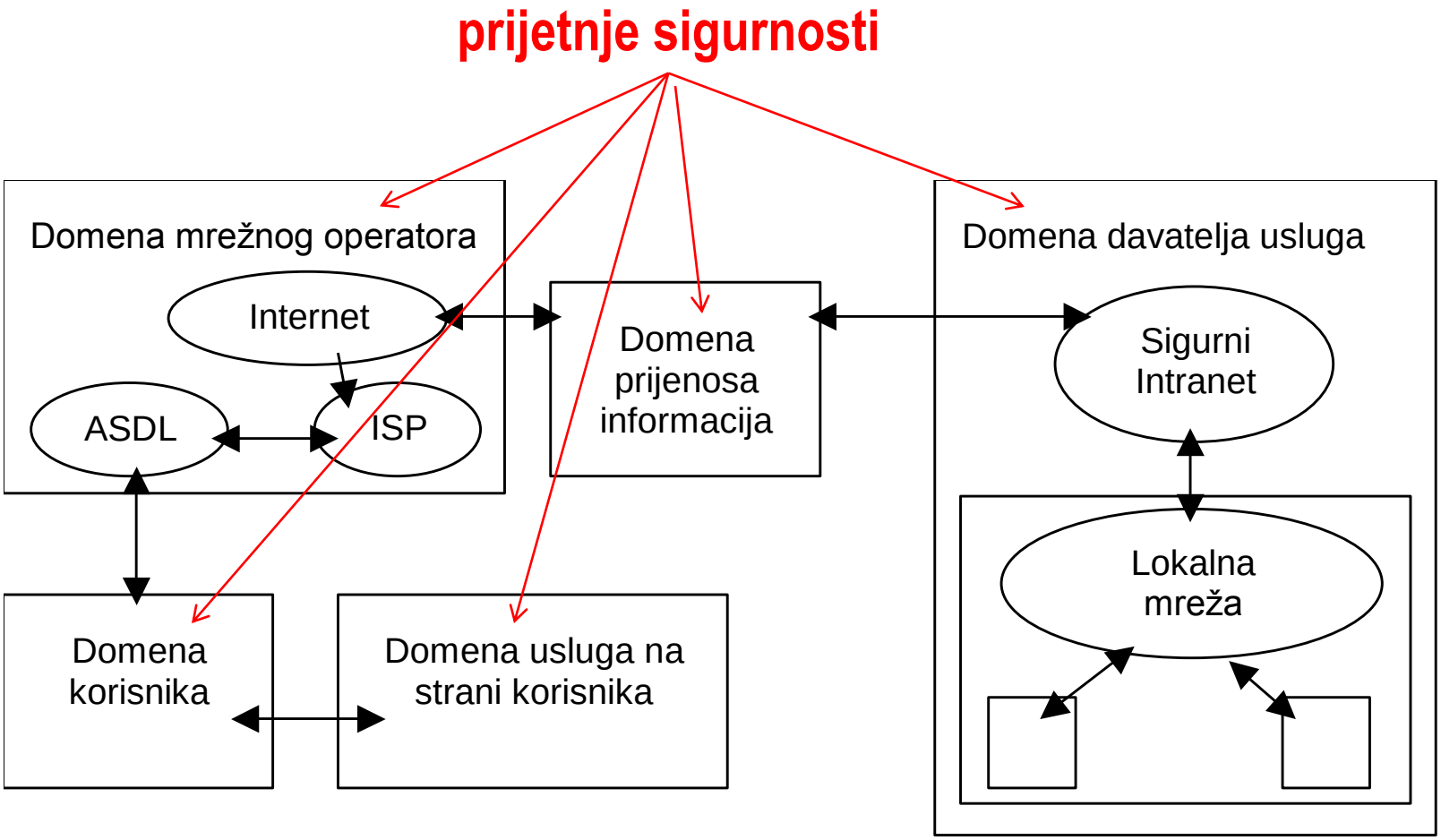
Sigurnost, prijetnje i zahtjevi

Sigurnost u mrežnom okružju (1)



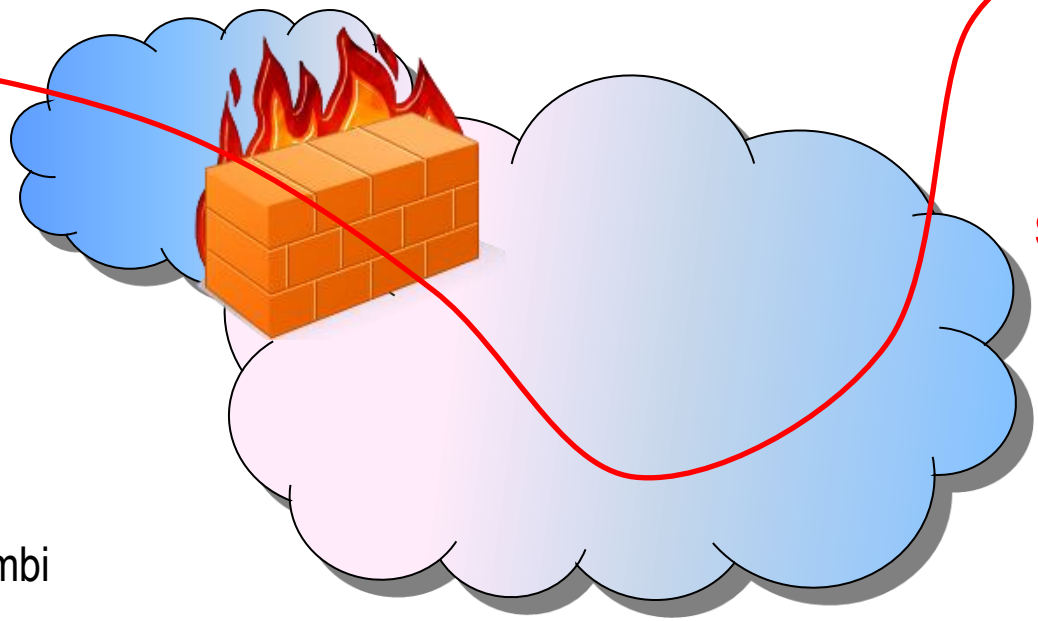
Sigurnost u mrežnom okružju (2)

Primjer: pristup internetskim uslugama putem javne mreže



Sigurnosne prijetnje i rješenja

sigurnost mreže



sigurnost usluge i aplikacije

- virus
- *hoax*
- *malware*
- *spyware*
- *adware*
- *dialer*
- trojanac

- crv
- zombi
- skener

PRIJETNJE

sigurnost usluge i aplikacije

- ranjivost
- uskraćivanje usluge
- lažno sjedište
- pogađanje lozinke

- antivirus

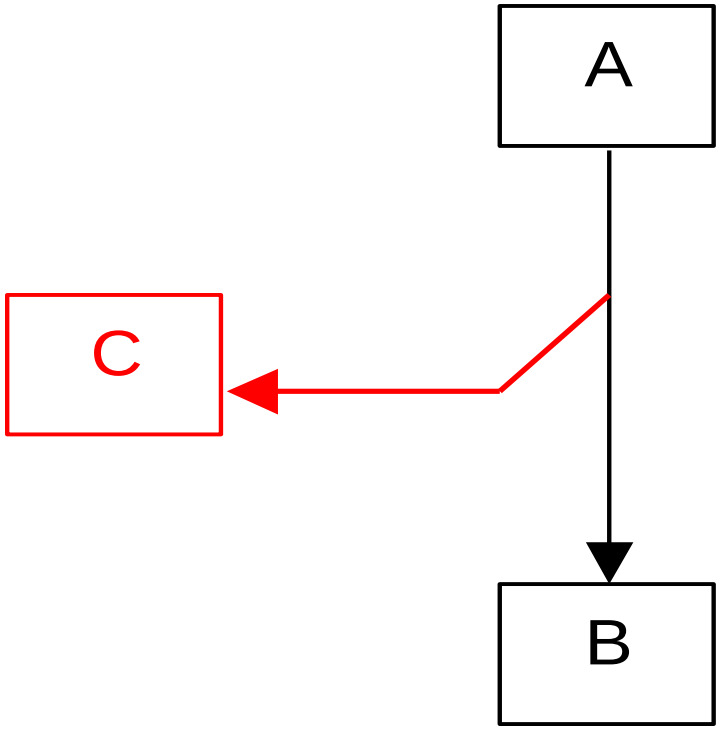
- vatrozid (*firewall*)
- *sustav za otkrivanje upada* (*Intrusion Detection System*)

RJEŠENJA

- IPsec
- demilitarizirana zona
- virtualna privatna mreža

- **kriptografija**

Sigurnosne prijetnje: presretanje, prisluškivanje



Presretanje (engl. *interception*)

Prisluškivanje (engl. *evesdropping*)

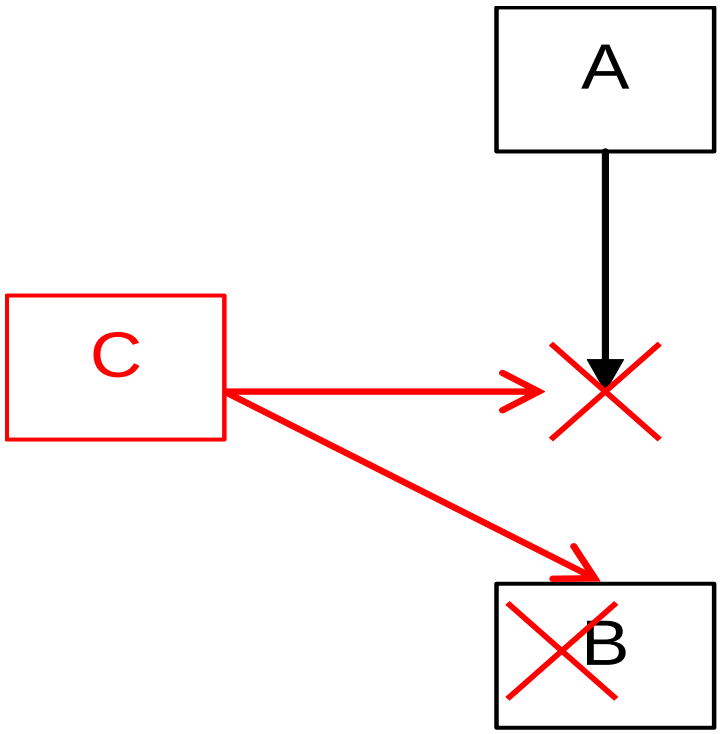
Prisluškivanje na vodu (engl. *wiretapping*)

- elektronička komunikacija se presreće i preuzima informacija
- neovlaštena uporaba podataka
- narušavanje privatnosti

Zakonski regulirano

(engl. *lawfull interception*)

Sigurnosne prijetnje: prekidanje, uskraćivanje



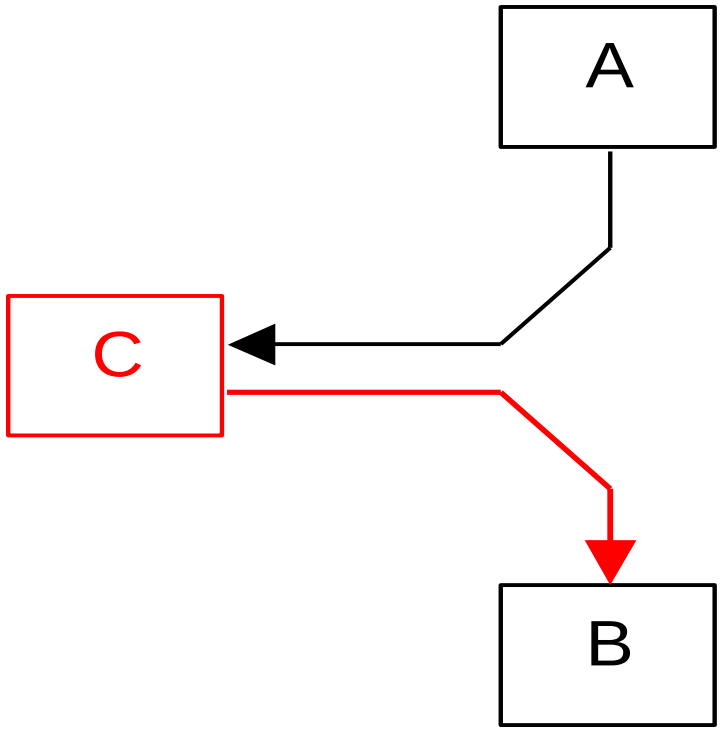
Prekidanje (engl. *interruption*)

- prekidanje normalnog tijeka komunikacije, usluge ili aplikacije

Uskraćivanje usluge (engl. *denial of service*)

- onemogućavanje usluge izazivanjem preopterećenja mreže ili umreženog sustava

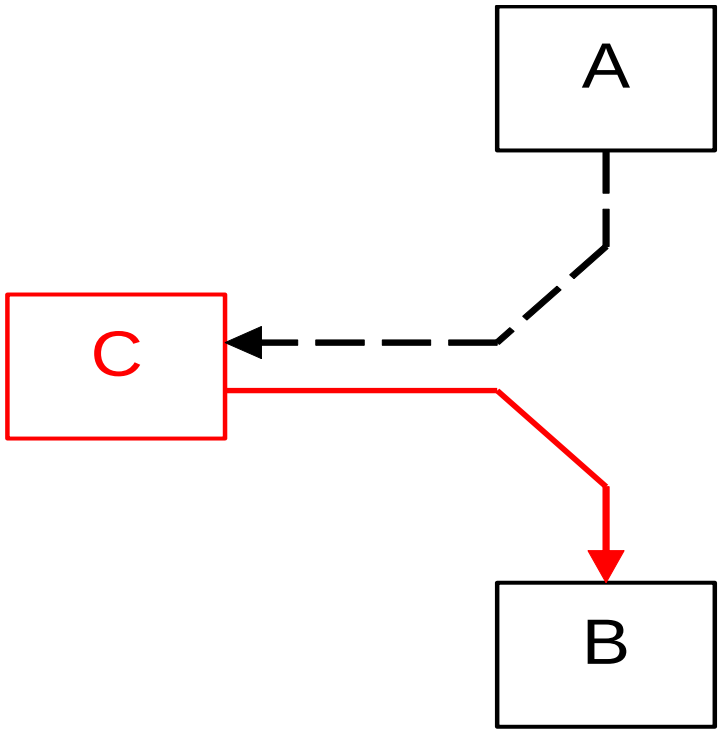
Sigurnosne prijetnje: promjena, kašnjenje



Promjena (engl. *modification, tampering*)

- promjena ili uništenje informacije
- kašnjenje može izazvati isti učinak – informacija postaje nevažna

Sigurnosne prijetnje: fabrikacija, ponavljanje



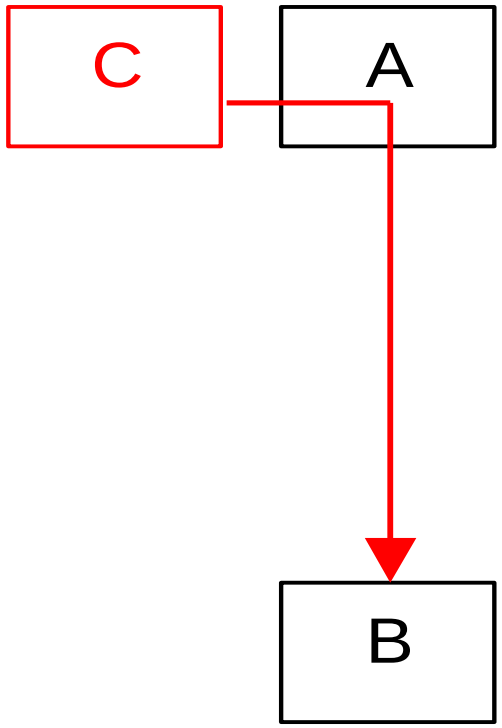
Fabrikacija (engl. *fabrication*)

- ubacivanje zlonamjerne informacije

Ponavljanje (engl. *replay*)

- ubacivanje informacije prethodno preuzete presretanje

Sigurnosne prijetnje: lažno predstavljanje



Lažno predstavljanje

maskiranje (engl. *masquerade*)
utjelovljenje (engl. *impersonation*)

- preuzimanje identiteta i uloge korisnika

Sigurnosni zahtjevi (1)

- **autentičnost** (engl. *authenticity*)
  - potvrda identiteta korisnika; ovjera vjerodostojnosti (autentifikacija) sudionika komunikacije
- **cjelovitost, integritet** (engl. *integrity*)
  - jamstvo da su informacije poslane, primljene ili pohranjene u izvornom i nepromijenjenom obliku
- **povjerljivost** (engl. *confidentiality*), **tajnost** (engl. *secrecy*)
  - razmijenjene poruke trebaju biti razumljive samo pošiljatelju i namjeravanom primatelju; zaštita komunikacije ili pohranjenih informacija od uvida neovlaštenim korisnicima
- **neporecivost** (engl. *nonrepudiation*)
  - sudionici ne mogu poreći akciju u kojoj su sudjelovali, npr. nemogućnost naknadnog odricanja odaslane poruke

Sigurnosni zahtjevi (2)

- **kontrola pristupa** (engl. *access control*)
  - ograničavanje pristupa informacijama i ograničavanje provođenja akcija
- **raspoloživost** (engl. *availability*)
  - informacije moraju biti raspoložive, a sustavi i usluge u stanju operativnosti, usprkos mogućim neočekivanim i nepredvidljivim događajima, primjerice nestanku struje, prirodnim nepogodama, nesrećama i zlonamjernim napadima
- **radna sigurnost** (engl. *operational security*)
  - (aktivno) suprotstavljanje napadima na mrežu i računala neke organizacije

Osnovno o kriptografiji

Kriptologija, kriptografija i kriptoanaliza

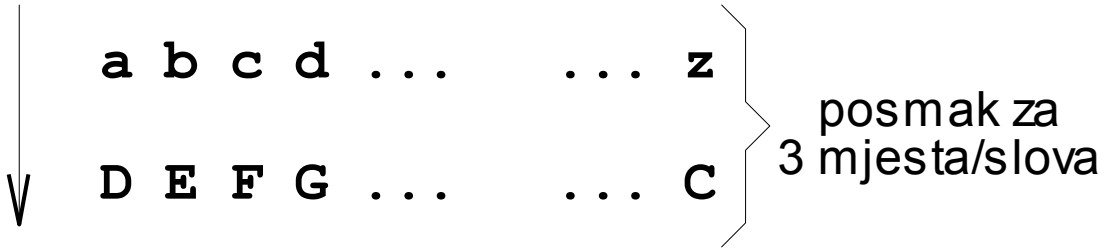
Temelj svake sigurnosti je tajna!

- kriptologija (engl. *cryptology*): znanost o šifriranju i dešifriranju, odnosno kriptiranju i dekriptiranju, koja obuhvaća dvije discipline:
  - kriptografija (engl. *cryptography*):
    skup postupaka pretvorbe izvornih podataka u oblik nečitljiv za uljeza - umješnost izmišljanja šifri
  - kriptoanaliza (engl. *cryptoanalysis*):
    skup postupaka “probijanja” tako zaštićenih podataka - umješnost razbijanja šifri

Primjer iz povijesti: Cezarova šifra

Zamjenska šifra (engl. *substitution cypher*):

- zamjena znakova drugim znakovima
- *Cezarova šifra*:
  - zamjena abecede (za *p* = 3 mjesta) *posmaknutom* abecedom

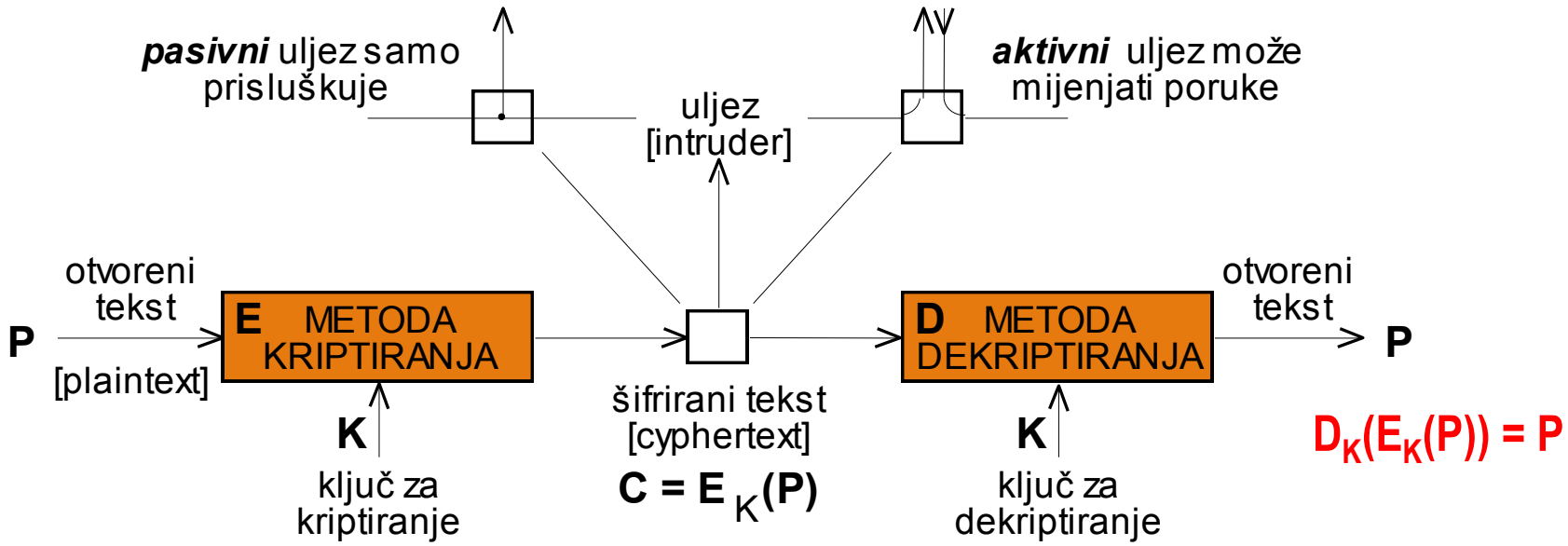


  - kriptografija: posmak za *p* mjesta/slova, ključ = *p*
  - kriptoanaliza: odrediti posmak *p* (lako probijanje → kružno posmaknuta abeceda)
- složenije zamjenske šifre: jedno ili višeabecedna zamjena

Model kriptiranja (1)

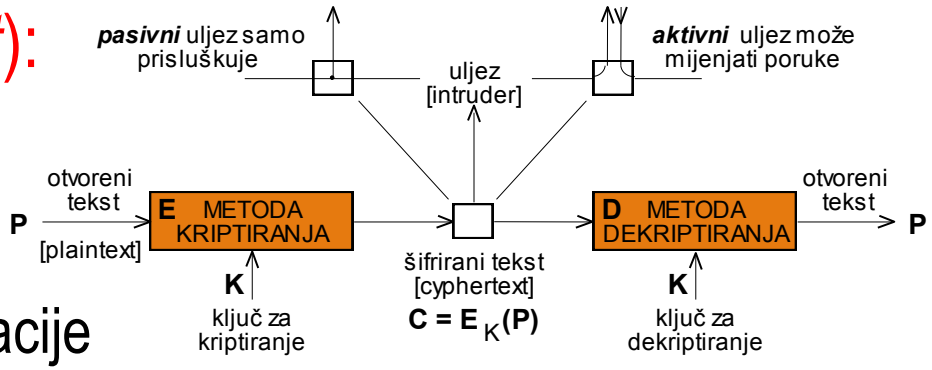
Šifra (engl. *cypher*):

transformacija izvornog teksta, bez obzira na njegovu lingvističku strukturu



Model kriptiranja (2)

- otvoreni tekst (engl. *plaintext*):
  - poruka koju treba kriptirati
- ključ (engl. *key*):
  - parametar funkcije transformacije
  - tajan i lako promjenjiv, duljina osigurava neprobojnost šifre!
- šifrirani tekst (engl. *cyphertext*), kriptogram (engl. *cryptogram*):
  - rezultat procesa kriptiranja
- uljez (engl. *intruder*):
  - pasivni: samo prisluškuje
  - aktivni: modificirati poruke, ponoviti memorirane ili ubaciti svoje poruke



Model kriptiranja (3)

Simetrična kriptografija:

- identični ključ za kriptiranje i dekriptiranje
- primjeri standarda: DES, AES

Asimetrična kriptografija:

- različiti ključevi za kriptiranje i dekriptiranje
- kriptografija javnog ključa
- primjer algoritma: RSA

Simetrična kriptografija (1)

- tradicionalna kriptografija temelji se na *simetričnim* algoritmima:
  - identični tajni ključ (engl. *secret key*) za kriptiranje i dekriptiranje
  - duljina ključa određuje snagu zaštite
- tipična primjena u mreži:
  - kriptiranje pojedine sjednice (aplikacijskih procesa) ili dijelova sjednice

    ~ “dijalog” ograničene duljine/trajanja
- problemi:
  - kako pojačati snagu kriptiranja?
  - kako ubrzati proces kriptiranja/dekriptiranja?
  - kako sigurno dostaviti tajni ključ sudionicima komunikacije?

    postupak za razmjenu ključeva (*Diffie-Hellman key exchange*)

Simetrična kriptografija (2)

Snaga kriptiranja

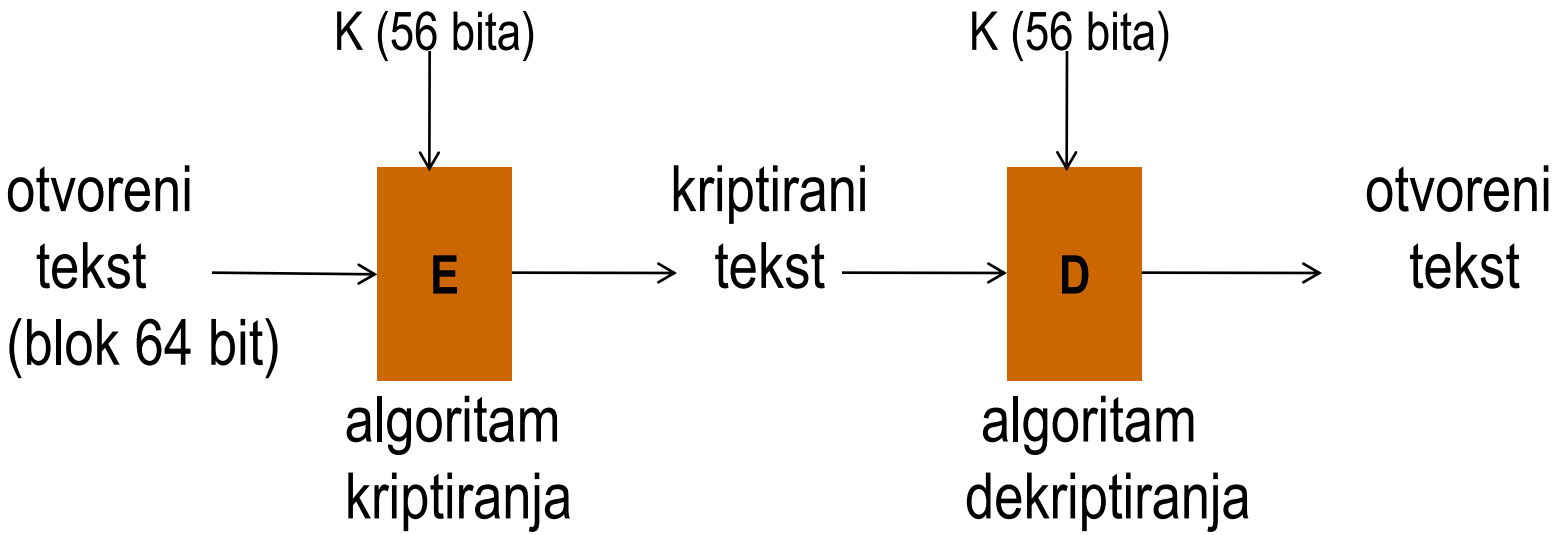
- složenost algoritma kriptiranja
- snaga kriptiranja povećava se *kaskadiranjem* većeg broja transformacija: produktna šifra (engl. *product cypher*)
- kriptiranje *n*-bitnih blokova otvorenog teksta – blokovske šifre (engl. *block cyphers*):

Ubrzanje procesa kriptiranja/dekriptiranja

- sklopovska implementacija: brzina
- programska implementacija: fleksibilnost

Standard DES

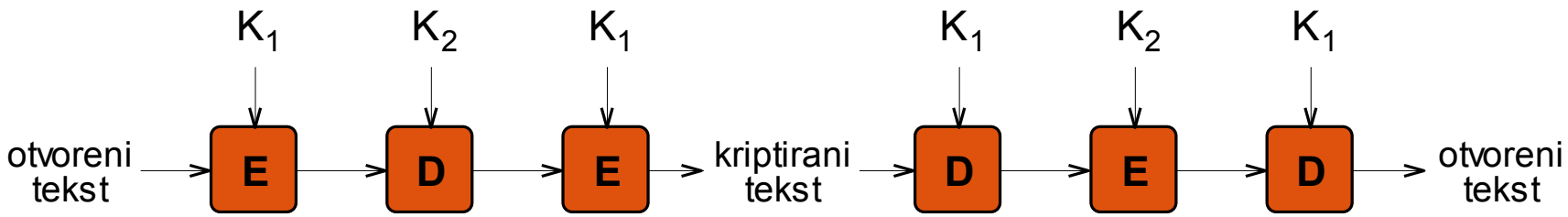
DES (engl. *Data Encryption Standard*), 1977.



- simetrična blokovska šifra:
  - šifra temeljena na jednoabecednim zamjenama (16 puta) za 64-bitne blokove
  - ključ (K) prekratak - može se probiti "grubom silom" (engl. *brute force*)

Standard utrostručeniDES

Utrostručeni DES (engl. *Triple DES*), 1979.



- snaga kriptiranja DES pojačava se *kaskadiranjem*:
  - tri ključa (K_1, K_2, K_3) – 168 bita
- podesiva snaga kriptozaštite:
  - primjer: EDE/DED s 2 ključa (K_1, K_2, $K_3 = K_1$ 1) - 112 bitova (na slici)
- primjena: elektronička pošta (PGP, S/MIME)

Standard AES

AES (engl. *Advanced Encryption Standard*)

- razvijen prema sljedećim zahtjevima (zamjena za DES):
  - simetrična blokovska šifra: blok 128 bita
  - ključevi duljine 128, 192 i 256 bita
  - moguća programska i sklopovska izvedba
  - javno objelodanjeni dizajn
  - javni ili nediskriminatorno licencirani algoritam
- odabrani algoritam: Rijndael (autori Rijnmen i Daemen, 2001.)
  - duljine ključeva i blokova u rasponu 128-256 bita, u koracima od po 32 bita
  - odabir duljina ključeva i blokova *nezavisan*
  - dizajn za sigurnost, ali i *veliku brzinu*!

Bolji od *Triple* DES!

Asimetrična kriptografija javnog ključa (1)

Kriptografija javnog ključa (engl. *public key cryptography*)

- svaki sudionik ima dva ključa: javni ključ i tajni privatni ključ
- sudionik objavljuje javni ključ koji se kombinira s tajnim privatnim ključem:
  - kriptiranje i dekriptiranje s različitim ključevima ~ *asimetrični* postupak
  - E: algoritam kriptiranja, s *javnim ključem* E(P)
  - D: algoritam dekriptiranja, s *privatnim ključem* D(E(P)) = P
- zahtjevi :
  - izrazito teško izvesti D iz E, a E se ne može probiti metodom odabranog otvorenog teksta
  - objaviti algoritam kriptiranja

Asimetrična kriptografija javnog ključa (2)

Postupak kriptiranja i dekriptiranja:

1. svaki sudionik, A i B, objavljuje svoj javni ključ, E_A i E_B :

   $A \sim E_A$, $B \sim E_B$

2. kriptiranje:

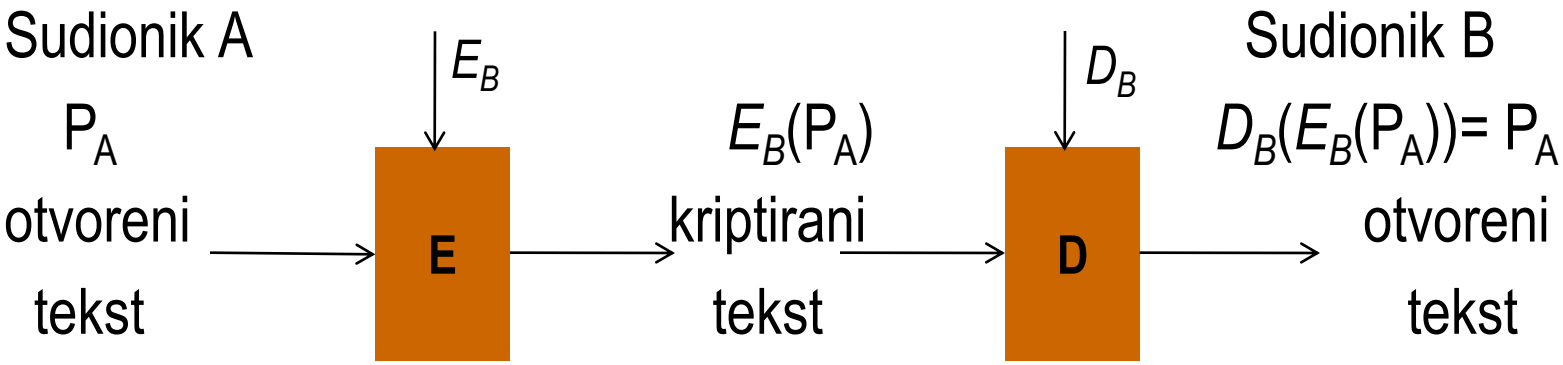
   $A \rightarrow B$: $E_B(P_A)$ javni ključ E_B

   $B \rightarrow A$: $E_A(P_B)$ javni ključ E_A

3. dekriptiranje:

   B: $D_B(E_B(P_A)) \equiv P_A$ privatni ključ D_B

   A: $D_A(E_A(P_B)) \equiv P_B$ privatni ključ D_A



Algoritam RSA

Algoritam RSA (Rivest, Shamir, Adleman; MIT, 1978)

- asimetrični algoritam temeljen na faktorizaciji velikih brojeva:
  - vrlo snažan i siguran algoritam za šifriranje i digitalno potpisivanje
  - zasniva se na teoriji brojeva:
    nalaženje prim-brojeva ($> 10^{100}$) prilikom faktorizacije velikih brojeva
  - sigurnost zasnovana na vrlo velikom vremenu potrebnom za faktorizaciju, npr. za 200-znamenkasti broj oko $4 \cdot 10^9$ godina na računalu s $t_{instr} = 1\ \mu s$
  - glavni nedostatak: za dobru sigurnost potrebni *dugi* ključevi (≥ 1024 bita), tako da je izračunavanje dosta sporo
- opći nedostatak asimetričnih algoritama: sporost, pogotovo kod velikih količina podataka (100 - 1000 puta sporiji od simetričnih)

Digitalni potpis

- zamjena za vlastoručne potpise u porukama
- sustav koji podržava sljedeće zahtjeve:
  - primatelj može provjeriti identitet pošiljatelja
    ~ ovjera (engl. *authentication*) pošiljatelja
  - pošiljatelj ne može kasnije poreći sadržaj poruke
    ~ neporecivost (engl. *nonrepudiation*) poruke
  - primatelj nije mogao "izmisliti" poruku
- mogućnosti ostvarivanja digitalnih potpisa:
  - potpis sa simetričnim ključem
  - potpis s javnim ključem
  - sažetak poruke

Potpis sa simetričnim ključem (1)

- postoji *središnji autoritet* koji zna sve tajne ključeve i kojem svi vjeruju:
  - pošiljatelj šalje središnjem autoritetu kriptiranu poruku za primatelja i dodatne podatke (vremensku oznaku i slučajni broj poruke)
  - središnji autoritet ustanovljuje identitet pošiljatelja,

    dodaje informaciju o pošiljatelju kriptiranu *svojim tajnim* ključem (*potpisana poruka*)

    prosljeđuje primatelju *proširenu* poruku kriptiranu *primateljevim* ključem
- primatelj:
  - može pročitati poruku, jer je kriptirana njegovim ključem
  - siguran je u identitet pošiljatelja
  - posjeduje potpis koji on nije mogao izmisliti

Potpis sa simetričnim ključem (2)

A, B: imena sudionika

K_A, K_B, K_{BB}: tajni ključevi

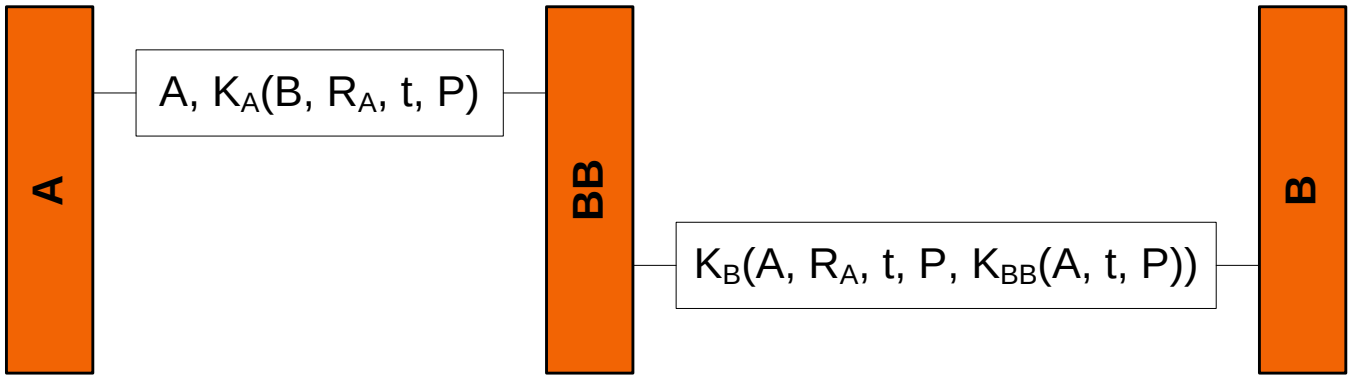
P: poruka

R_A: slučajni broj, t: vremenska oznaka

Potpisane poruke: $K_A(B, R_A, t, P)$, $K_{BB}(A, t, P)$

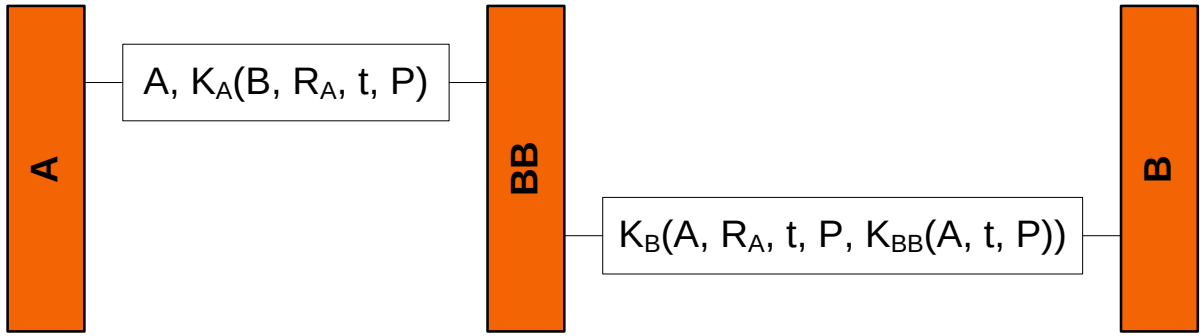
BB: bilježnik

BB zna K_A, K_B i $K_{BB)}$



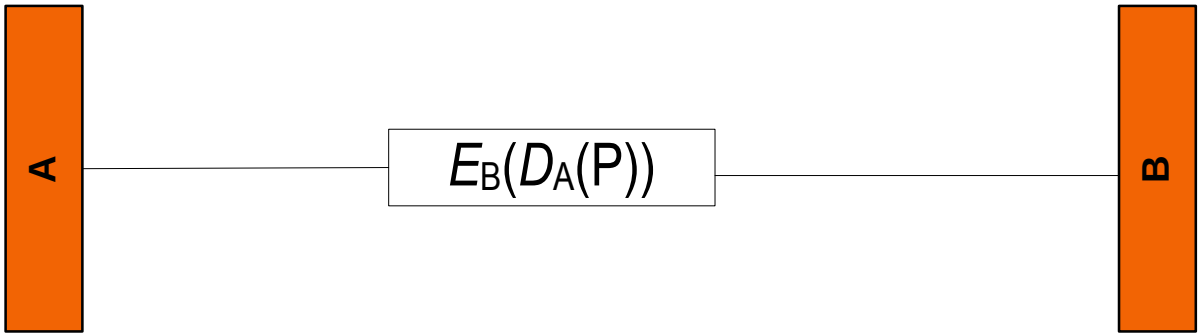
Potpis sa simetričnim ključem (3)

- osiguranje neporecivosti *(engl. nonrepudiation)*
  - BB prihvatio poruku od A, jer je kriptirana tajnim ključem K_A
  - BB kriptirao podatke od A: $K_{BB}(A, t, P)$, tako da ih B nije mogao izmisliti
- sprječavanje *napada ponavljanjem* (engl. *replay attack*):
  - t ukazuje na "stare" poruke
  - R_A ukazuje na već "iskorištene" poruke



Potpis s javnim ključem

- izbjegava se središnji autoritet kojem svi vjeruju (a koji im čita poruke!)
- od algoritma javnog ključa, uz $D(E(\mathrm{P})) = \mathrm{P}$, dodatno se zahtijeva $E(D(\mathrm{P})) = \mathrm{P}$ (zadovoljava algoritam RSA):
  - kriptiranje kod A: $E_B(D_A(\mathrm{P})) = \mathrm{C}$
  - dekriptiranje kod B: $E_A(D_B(\mathrm{C})) = E_A(D_B(E_B(D_A(\mathrm{P})))) = \mathrm{P}$
- neporicanje: samo A mogao je kriptirati privatnim D_A !



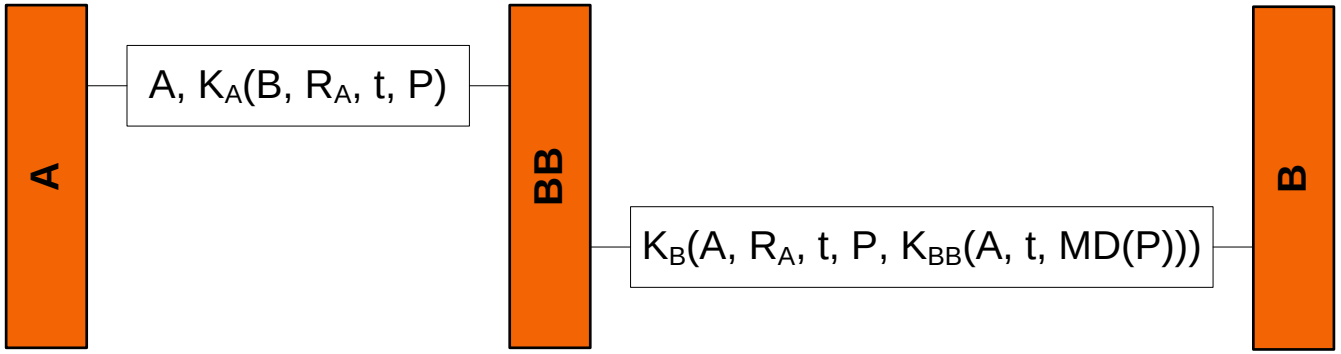
Sažetak poruke (1)

Sažetak poruke (engl. *message digest*, MD)

- potpisivanje poruke jedinstvenim kratkim uzorkom bita fiksne duljine:
  - izbjegava se kombiniranje dviju različitih funkcija (ovjere i tajnosti)
- jednosmjerna *hash* funkcija MD koja iz proizvoljno dugog teksta generira niz bita fiksne duljine, sa sljedećim svojstvima
  - lako izračunati MD(P)
  - gotovo nemoguće izračunati P iz MD(P)
  - za dani P nemoguće izračunati P' ~ MD(P') = MD(P): osigurati da je *hash* > 128 bita
  - promjena od samo 1 bita daje *vrlo različit* rezultat: *hash* mora "temeljito izmiješati" bitove

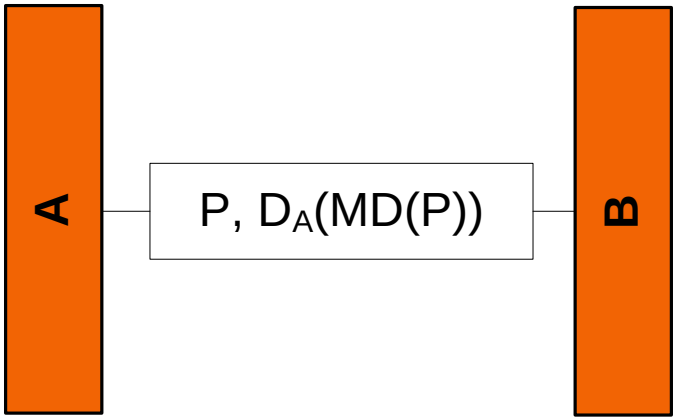
Sažetak poruke (2)

- primjena sažetka poruke kod potpisa sa *simetričnim* ključem:
  - zamjena P s MD(P):
    brža obrada (kriptiranje) i prijenos!
  - dekriptiranjem potpisane poruke $K_{BB}(A, t, MD(P))$:
    uspoređuju se P i MD(P)



Sažetak poruke (3)

- primjena sažetka poruke kod potpisa s *javnim* ključem:
  - kriptira se *samo* MD(P):
    puno brža obrada (kriptiranje) i prijenos
  - sigurno otkrivanje eventualne zamjene P s P' djelovanjem aktivnog uljeza provjerom usklađenosti P' i MD(P) kod B



Algoritmi sažetka

- *Secure Hash Algorithm* (SHA-1), 1995.
  - algoritam američke vlade, vjerojatno najsigurniji
  - daje *hash* vrijednost duljine 160 bita
- *Message Digest Algorithm 5* (MD5), 1992.
  - daje *hash* duljine 128 bita
  - prethodnik MD4 probijen, postoje problemi i s MD5
- *Digital Signature Algorithm* (DSA), 1991
  - u okviru *Digital Signature Standard* (DSS)
  - samo za potpisivanje, 80 bita
  - koristi SHA-1 za izračunavanje *hasha*

Sigurna komunikacija - što se želi postići …

Integritet i autentičnost:

- digitalno potpisivanje poruke tajnim privatnim ključem, provjera potpisa javnim ključem – asimetrična kriptografija

Tajnost (povjerljivost):

1. razmjena tajnog sjedničkog ključa kriptirana javnim ključem – asimetrična kriptografija
2. kriptiranje poruke tajnim sjedničkim ključem – simetrična kriptografija

Neporecivost:

- digitalno potpisivanje i drugi mehanizmi

Kontrola pristupa

… i što je problem

- Kako riješiti sigurnosne zahtjeve za veliki broj korisnika, u različitim mrežama i organizacijama, za različite oblike elektroničkog poslovanja (trgovina, plaćanje, …)?
- Kako dostaviti javni ključ, odnosno razmijeniti javne ključeve, naročito između sudionika koji se ne poznaju?
- Kako uspostaviti povjerenje između različitih organizacija da bi njihovi korisnici sigurno komunicirali?
- Kako spriječiti prijetnju ubacivanja uljeza u komunikaciju koji preuzima javni ključ?

Sustavno rješenje: infrastruktura javnog ključa

(engl. *Public Key Infrastructure*, PKI)

Infrastruktura javnog ključa (1)

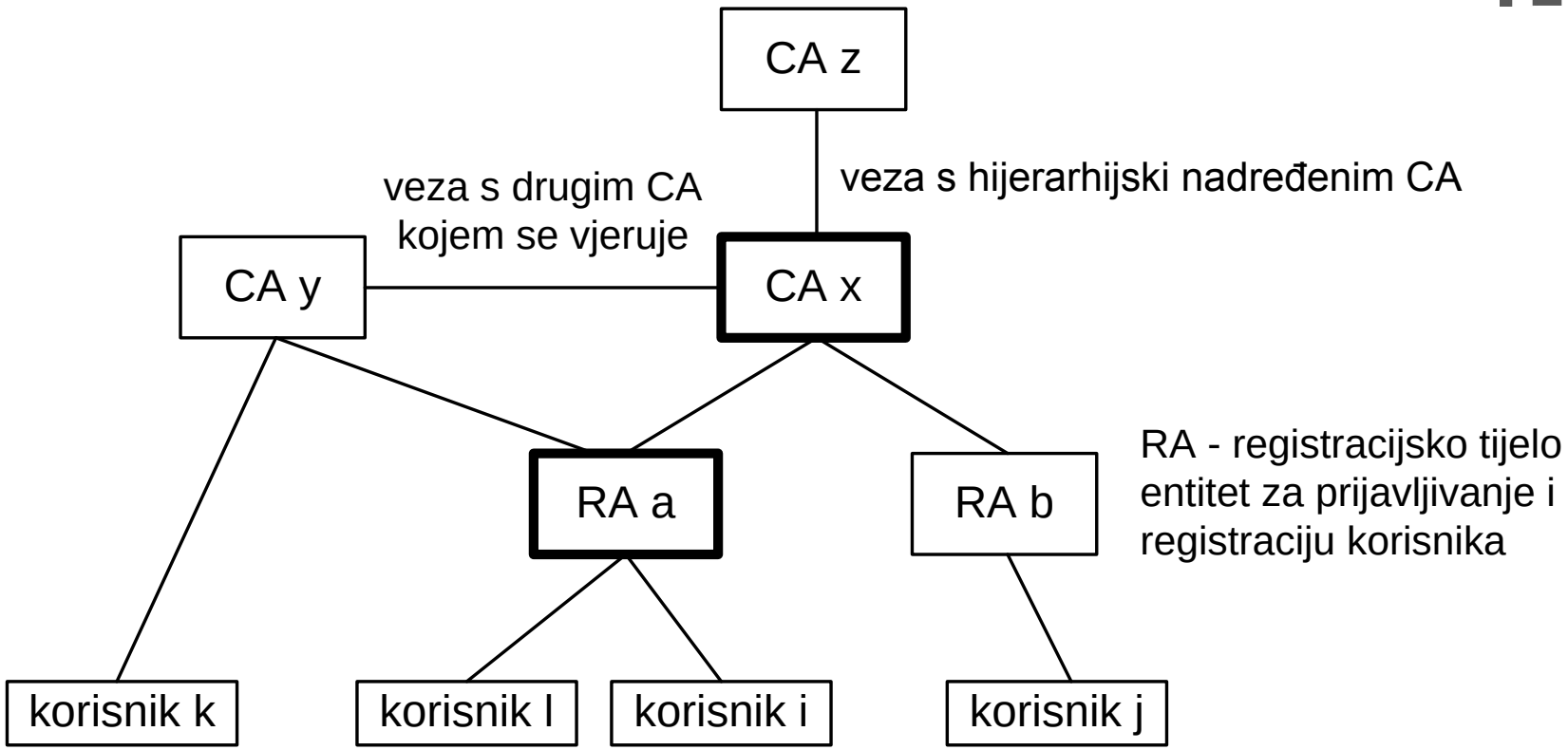
Identitet korisnika dokazuje se digitalnim certifikatom:

- digitalni certifikat (engl. *digital certificate*) digitalno potpisana izjava kojom se potvrđuje da je korisniku – vlasniku certifikata dodijeljen njegov javni ključ

Izdavanje, provjeru i povlačenje digitalnog certifikata obavlja se infrastrukturom javnog ključa u čijem su sastavu:

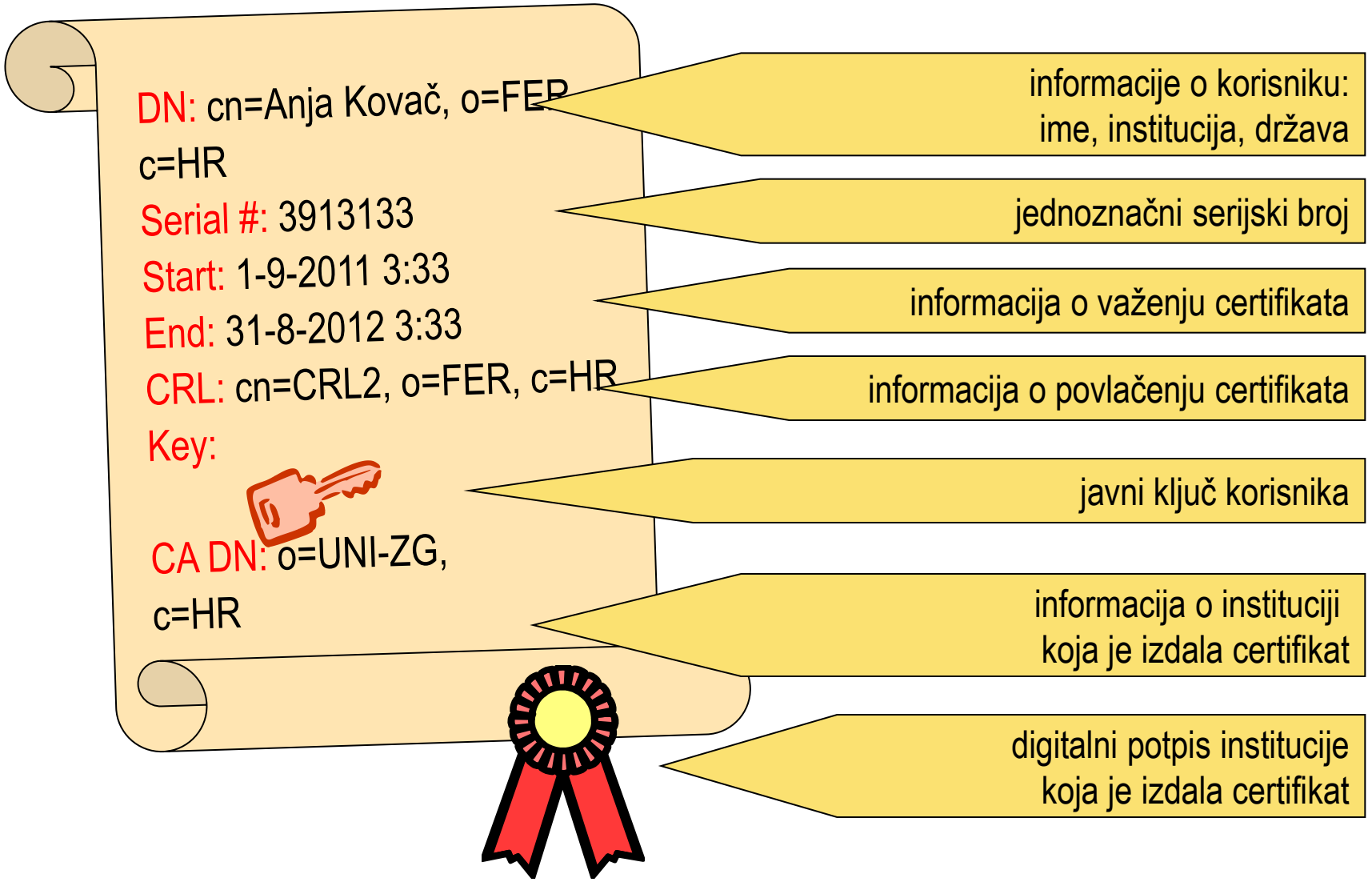
- registracijsko tijelo (engl. *Registration Authority*, RA)
  - provjerava identitet korisnika, ustanovljava sadržaj certifikata te registrira korisnika – vlasnika certifikata u ime CA
- certifikacijsko tijelo (engl. *Certification Authority*, CA)
  - izdaje i povlači certifikat, održava i objavljuje informacije o stanju certifikata, omogućuje provjeru izdanih certifikata
  - ima vlastiti certifikat i povezan je s drugim certifikacijskim tijelima

Infrastruktura javnog ključa (2)

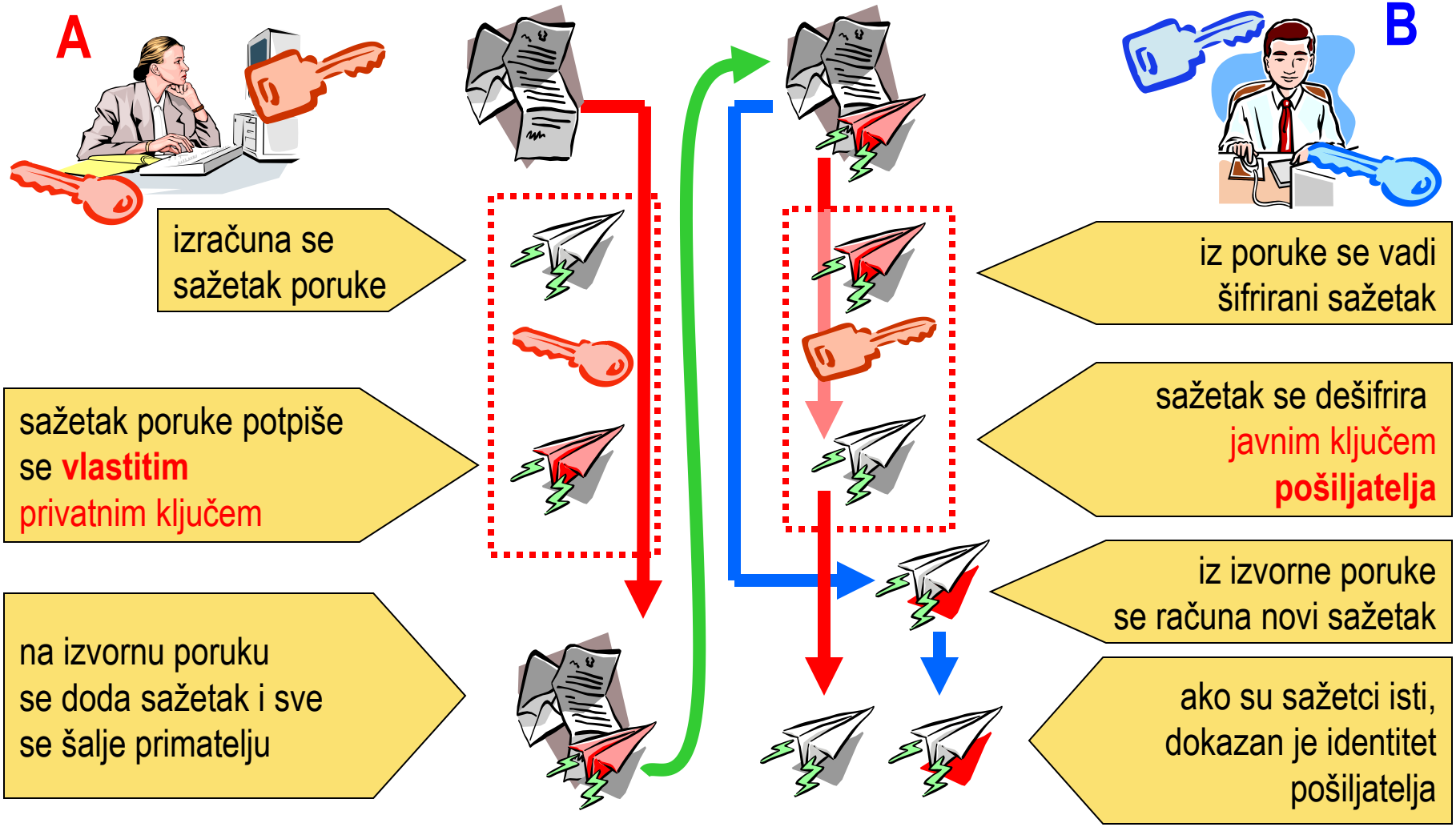


- međusobno povjerenje certifikacijskih tijela (CA_x i CA_y) koja jamče za svoje korisnike ($korisnik_j$ i $korisnik_k$)
- hijerarhijski nadređeni CA (CA_z) potpisuje certifikate za sebi podređene CA (CA_x) i jamči za njih

Primjer 1: digitalni certifikat



Primjer 2: digitalno potpisivanje poruke

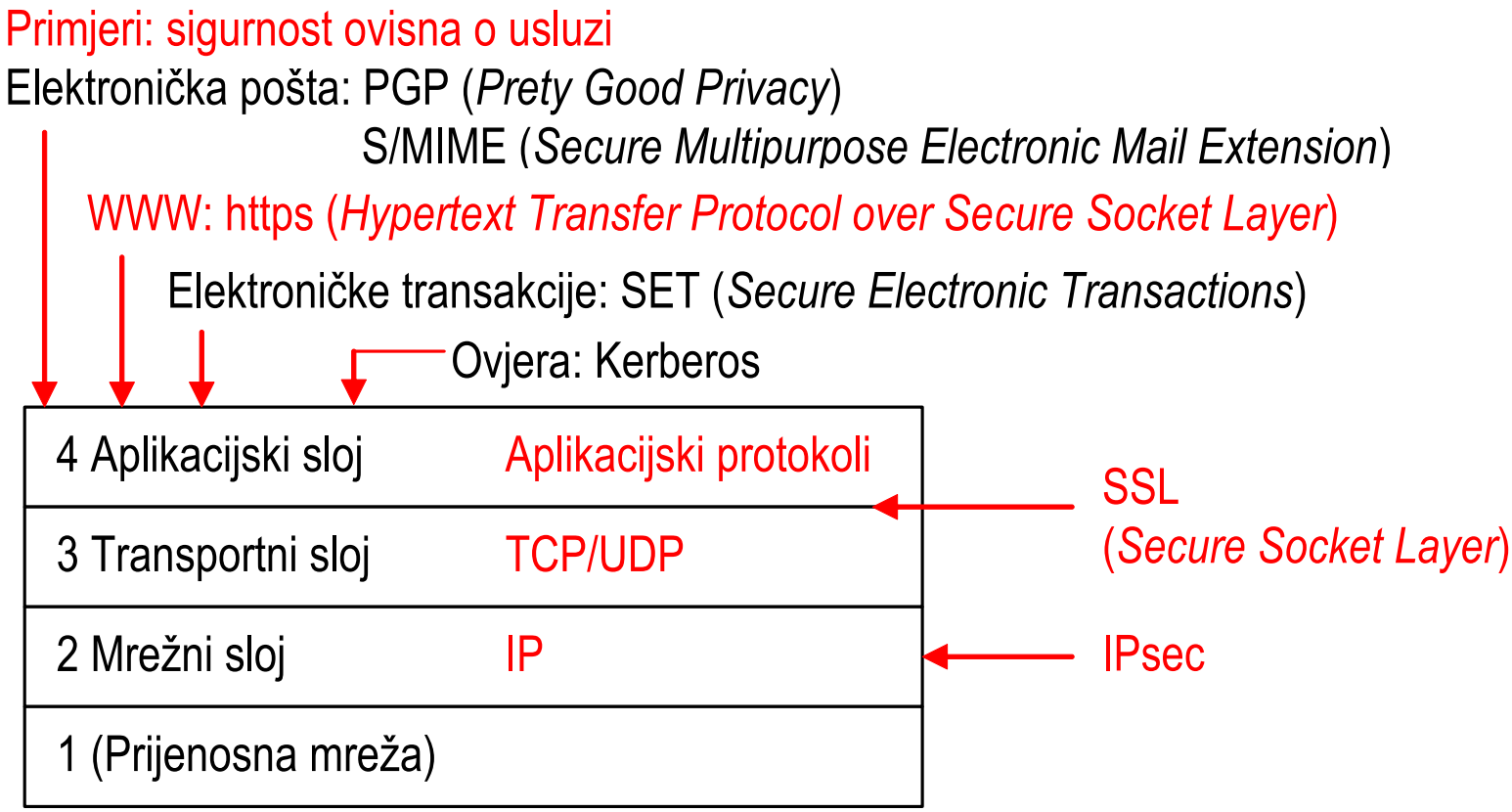


Sigurnosna arhitektura Interneta

Sigurnosni protokoli: IPsec, SSL

Sigurnosni protokoli

Niz protokola koji se primjenjuju za pružanje sigurnosnih usluga u Internetu



IPsec (1)

Sigurnost za IP (engl. IP *security*, IPsec)

- sigurnosni mehanizmi u mrežnom sloju u kojima se primjenjuje simetrična kriptografija s tajnim ključem*:
  - zaglavlje autentičnosti (engl. *Authentication Header*, AH): integritet datagrama, autentičnost izvora, neponavljanje
  - sigurnosno ovijeni podaci (engl. *Encapsulating Security Payload*, ESP): tajnost i integritet datagrama, autentičnost izvora
  - sigurnosno udruživanje, stvaranje i upravljanje tajnog ključa (engl. *Internet Key Exchange*, IKE)
- moguća primjena različitih algoritama, kao i promjena algoritama, nakon kompromitiranja duže korištenih algoritama

* simetrična kriptografija zbog dobrih performansi!

IPsec (2)

- IPsec je spojno orijentiran, s time što se “spoj” odnosi na sigurnosno udruživanje (engl. *Security Association*, SA) sudionika.
- Postupak:
  1. Definiraju se krajnje točke sigurne komunikacije, krajnje računalo ili mrežni uređaj - sigurnosni prilaz (SG – *Security Gateway*) i odabire način rada, transportni ili tunelski
  2. Uspostavlja se sigurnosno udruživanje tijekom kojeg se dogovaraju sigurnosne usluge omogućene s AH i ESP (integritet, tajnost, autentičnost) i stvara tajni ključ
  3. Sigurno se prenose datagrami s AH ili ESP-zaglavljem

Sigurnosno udruživanje

Sudionici uspostavljaju sigurnosnu asocijaciju* da bi se omogućila sigurna komunikacija:

- dogovaraju se sigurnosne usluge koje pružaju AH i ESP (integritet, tajnost, autentičnost)
- dogovaraju se krajnje točke (IP-adrese) između kojih će se ostvariti sigurna komunikacija i utvrđuje način rada
- sigurno se dostavlja dijeljena tajna temeljem koje sudionici stvaraju tajni ključ
- tajni ključ se povremeno osvježava

*sigurnosno udruživanje je jednosmjerno, tako da su potrebne dvije asocijacije za dvosmjernu razmjenu podataka

Transportni način rada IPsec

(engl. *transport mode*)

Zaštita polja podatka izvornog IP-datagrama - korisnog tereta (TCP-segment)

Umetanje zaglavlja IPsec (AH ili ESP) iza IP-zaglavlja:

- zaglavlje IPsec (AH ili ESP) postavlja se *ispred* zaglavlja višeg protokola (TCP)
- mijenja se “oznaka višeg protokola” u IP-zaglavlju (IPsec umjesto TCP)
- štiti se polje podataka izvornog datagrama i nepromjenjivi dio IP-zaglavlja

Tunelski način rada IPsec

(engl. *tunnel mode*):

Zaštita cijelog izvornog IP-datagrama

Tunel!

Formiranje novog datagrama:

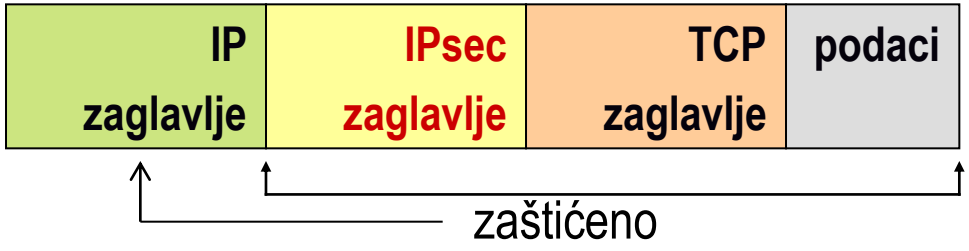
- izvorni IP-datagram smješta se u polje podataka *novog* IP-datagrama s *novim* zaglavljem IP i zaglavljem IPsec (AH ili ESP):
- *novo* IP-zaglavlje sadrži adresu izvora i odredišta (krajnje točke sigurne komunikacije) između kojih se prenosi novi IP-datagram
- štiti se cijeli izvorni IP-datagram i nepromjenjivi dio *novog* IP-zaglavlja (samo AH)

Sigurna komunikacija uz IPsec

izvorni IP-datagram

Transportni način: štiti podatke protokola viših slojeva (od transportnog na više)

datagram zaštićen transportnim načinom

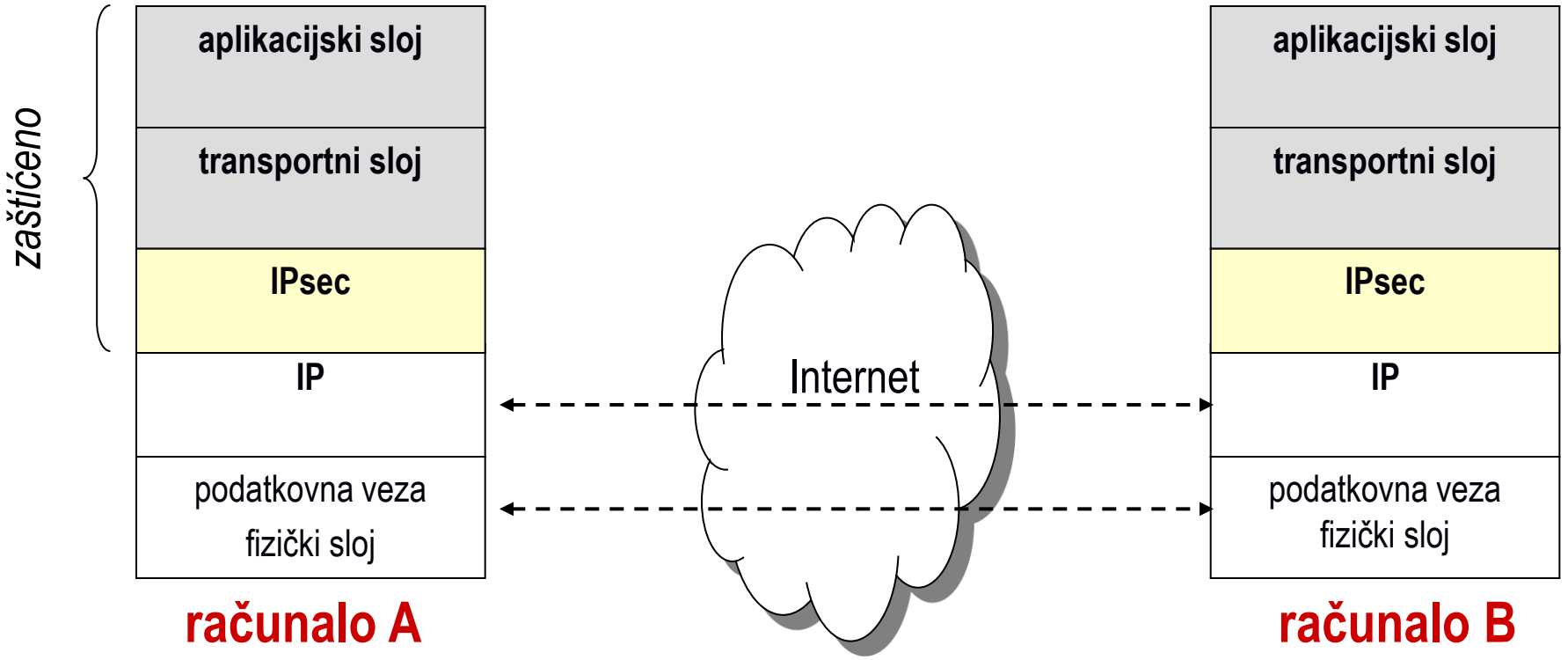


Tunelski način: štiti cijeli izvorni IP-paket

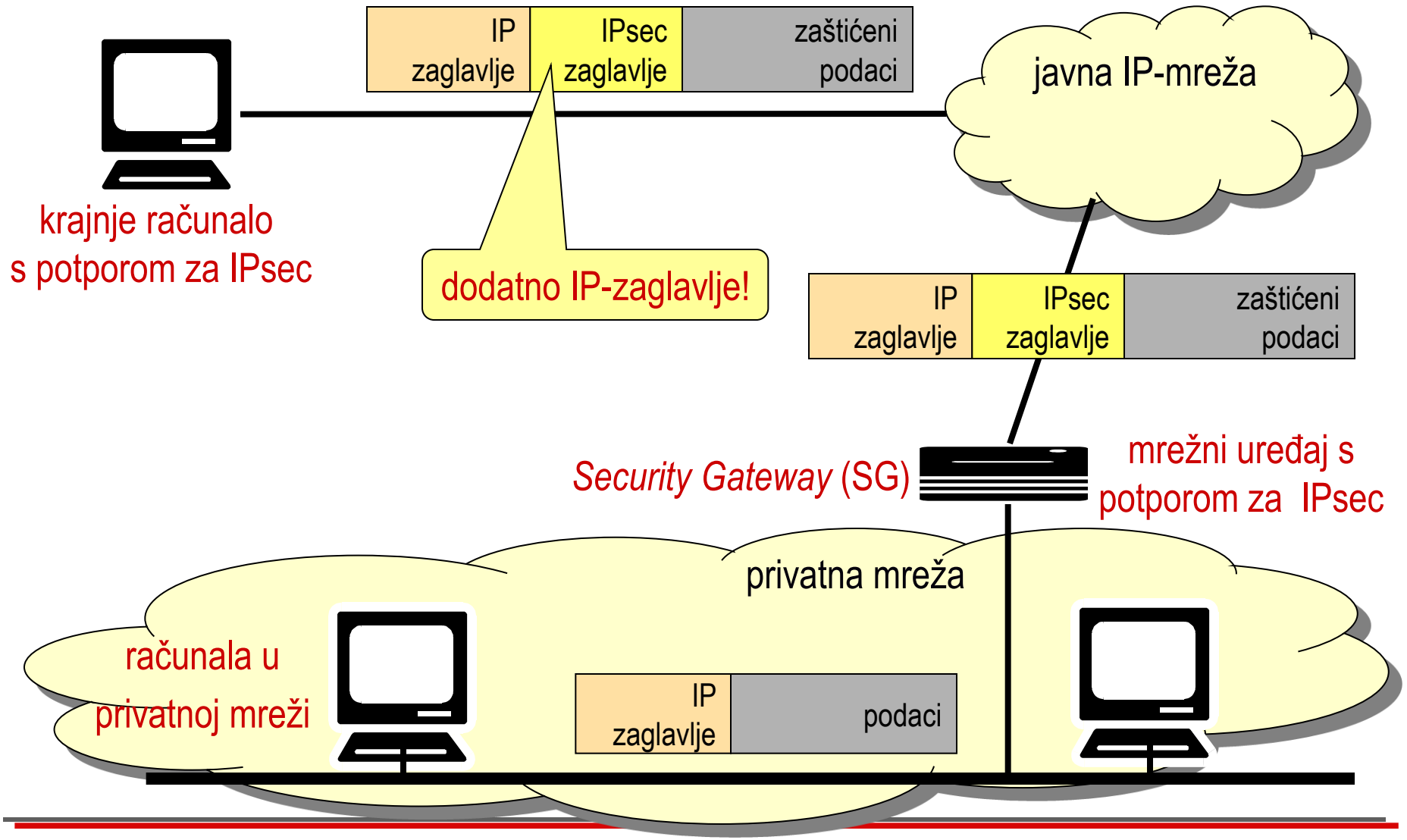
datagram zaštićen tunelskim načinom

Transportni način, primjer uporabe (1)

- krajnje točke: krajnje računalo A – krajnje računalo B

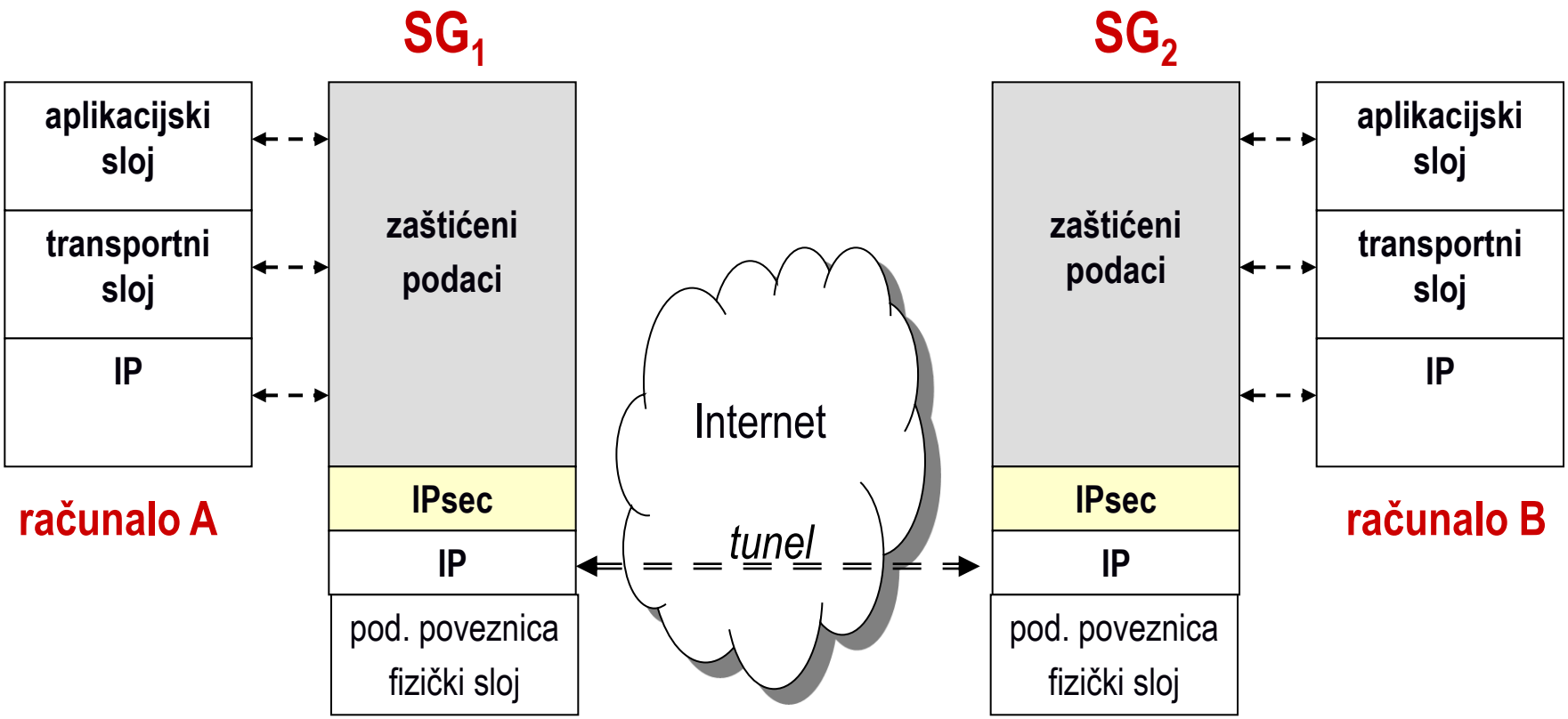


Transportni način, primjer uporabe (2)



Tunelski način, primjer uporabe (3)

- krajnje točke: dva mrežna uređaja SG_1-SG_2



sigurnosni prilaz (engl. *Security Gateway*, SG)

Zaglavlje AH – primjer: transportni način

Sigurnosne usluge:

- integritet: polje podataka nepromijenjeno
- autentičnost: integritet nepromjenjivih polja IP-zaglavlja (onemogućeno falsificiranje izvora paketa - pošiljatelja)
- zaštita od napada ponavljanjem (engl. *antireplay security*): redni broj paketa unutar sigurnosnog zadruživanja
- *ne* i tajnost: nema kriptiranja podataka!

Integritet i autentičnost osigurava se kodom vjerodostojnosti poruke izvedenim tajnim ključem (engl. *Hashed Message Authentication Code, HMAC*) koji se uključuje u AH-zaglavlje.

Zaglavlje ESP – primjer: tunelski način

Sigurnosne usluge:

- tajnost: cijeli izvorni datagram (IP-zaglavlje i polje podataka)
- integritet: cijeli izvorni datagram nepromijenjen
- autentičnost: integritet izvornog IP-zaglavlja (onemogućeno falsificiranje izvora paketa - pošiljatelja)
- zaštita od napada ponavljanjem: redni broj paketa unutar sigurnosnog zadruživanja

Sloj sigurnih priključnica

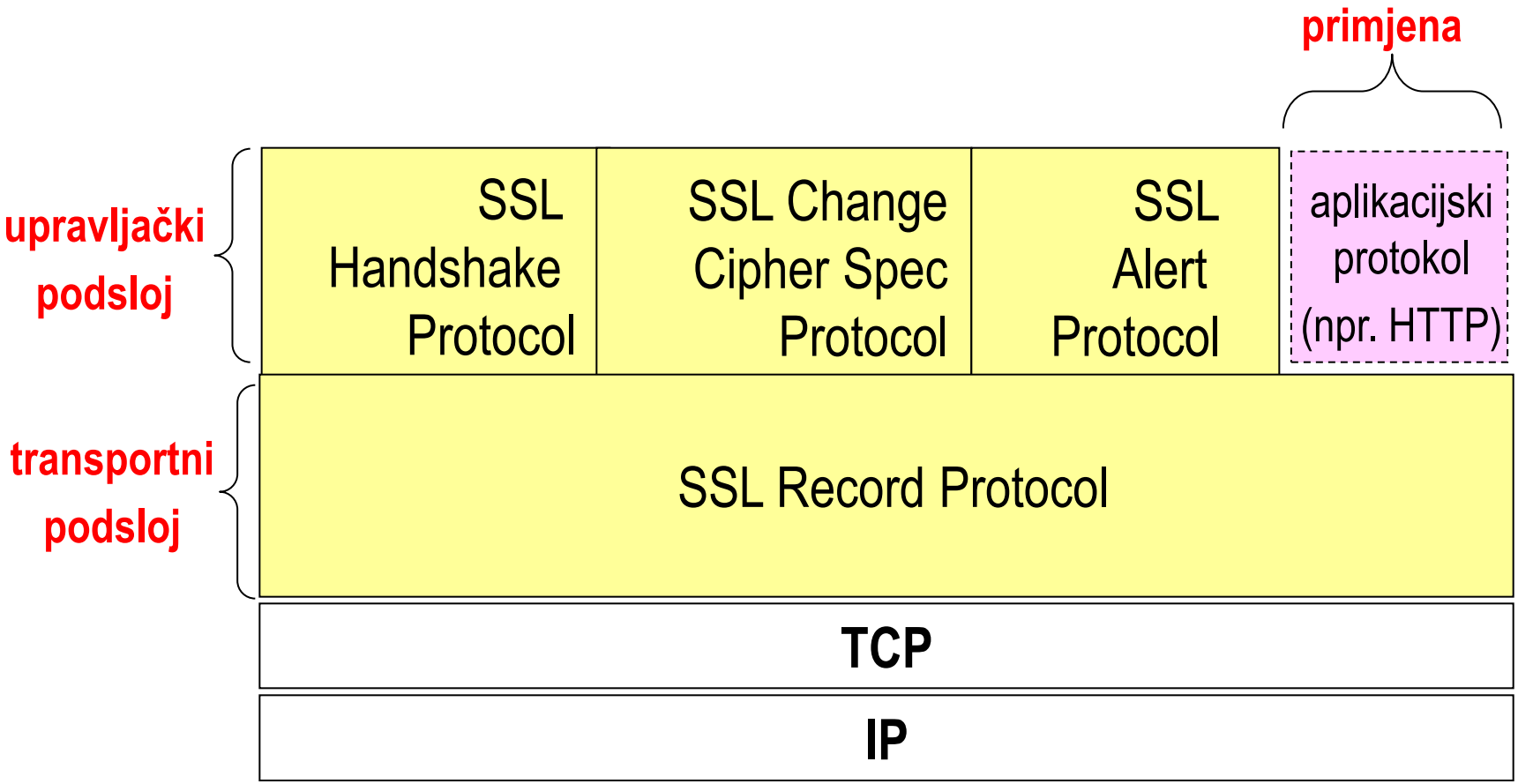
SSL (engl. *Secure Sockets Layer*)

- sigurnosni mehanizmi u transportnom sloju
- dvoslojni protokol koji se postavlja iznad transportnog protokola da bi pružio sigurnosne usluge integriteta i tajnosti aplikacijskom protokolu, npr. :
  - HTTP nad SSL: HTTPS (engl. *Secure* HTTP)

TLS (engl. *Transport Layer Security*)

- inačica SSL-a prihvaćena od IETF-a
- zadaće SSL/TLS:
  - uspostavljanje i održavanje sigurne komunikacije (SSL-sjednica)
  - kriptiranje uz moguće sažimanje (kompresiju) podataka

Arhitektura SSL-a (1)



Arhitektura SSL-a (1)

Transportni podsloj :

- SSL-protokol zapisa (engl. SSL *Record Protocol*): fragmentira i komprimira (opcija) poruku višeg sloja, dodaje kôd vjerodostojnosti poruke i sve zajedno šifrira

Upravljački podsloj:

- SSL-protokol rukovanja (engl. SSL *Handshake Protocol*): uspostava SSL-sjednice i dogovor parametara sigurne veze
- SSL-protokol promjene kripto-algoritma (engl. SSL *Change Cipher Spec Protocol*): označava promjenu ključa
- SSL-protokol uzbunjivanja (engl. SSL *Alert Protocol*): poruke upozorenja o narušenoj sigurnosti (indikacija za prekid SSL-sjednice)

Primjer sigurne sjednice klijent-poslužitelj

1. uspostavljanje SSL-sjednice i dogovor o sigurnosnim parametrima

   SSL-protokol rukovanja (asimetrična kriptografija)

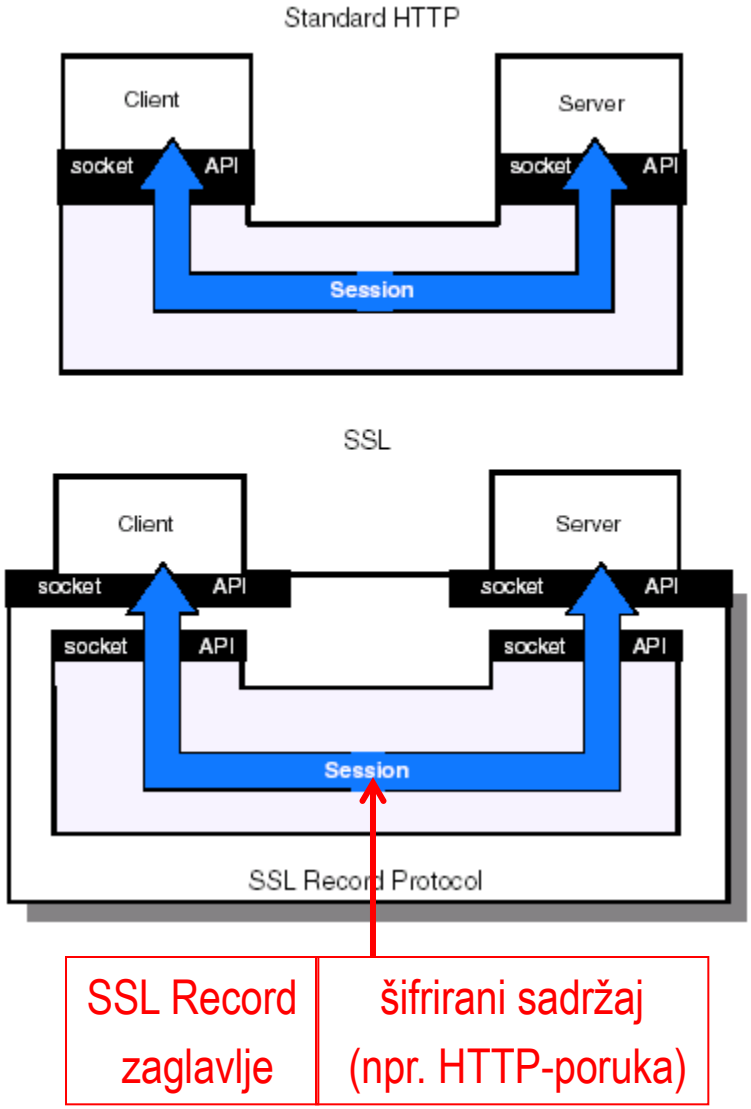
   autentifikacija poslužitelja ili

   autentifikacija poslužitelja i klijenta

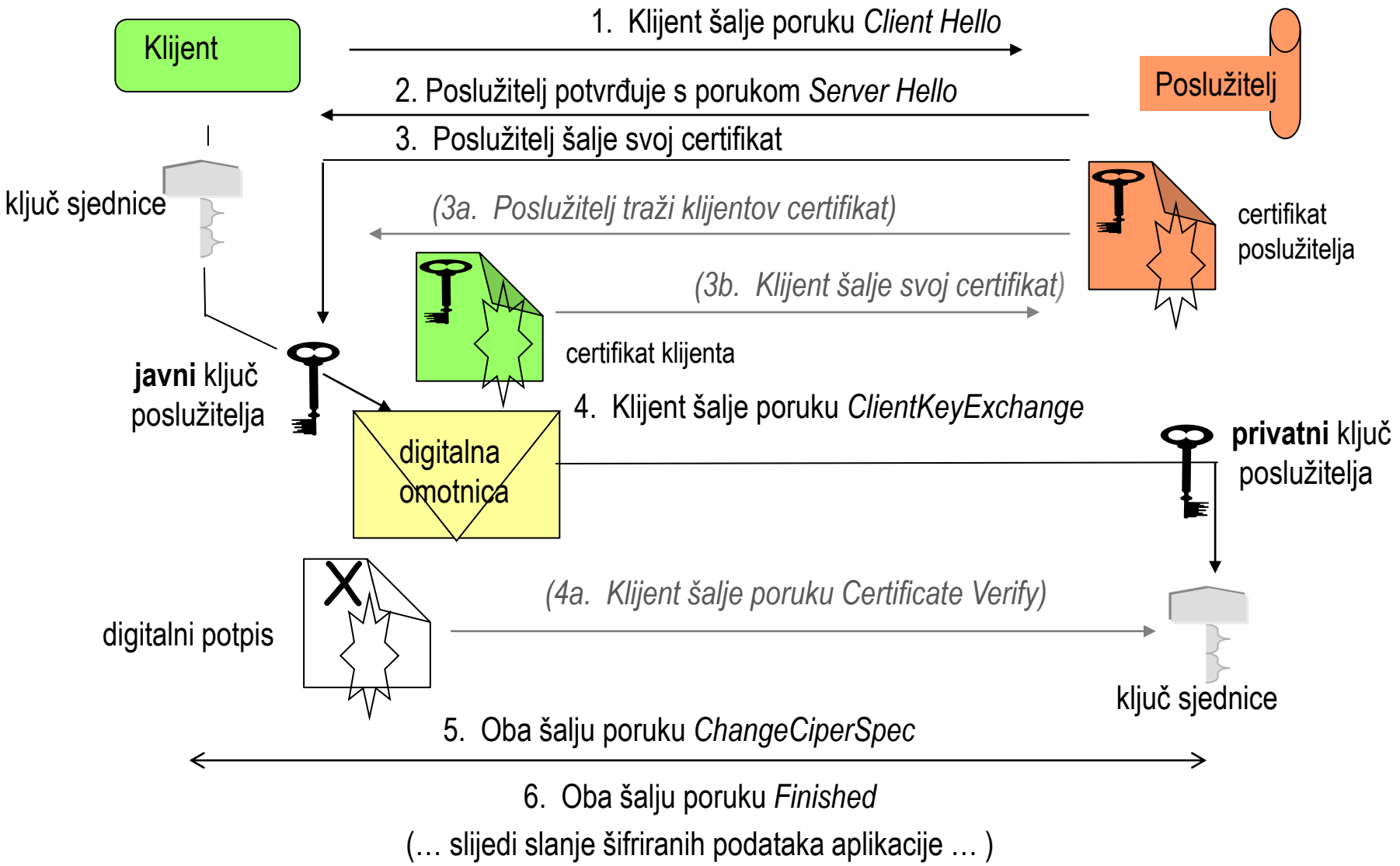
2. prijenos podataka tijekom SSL-sjednice

   SSL-protokol zapisa

   (simetrična kriptografija)



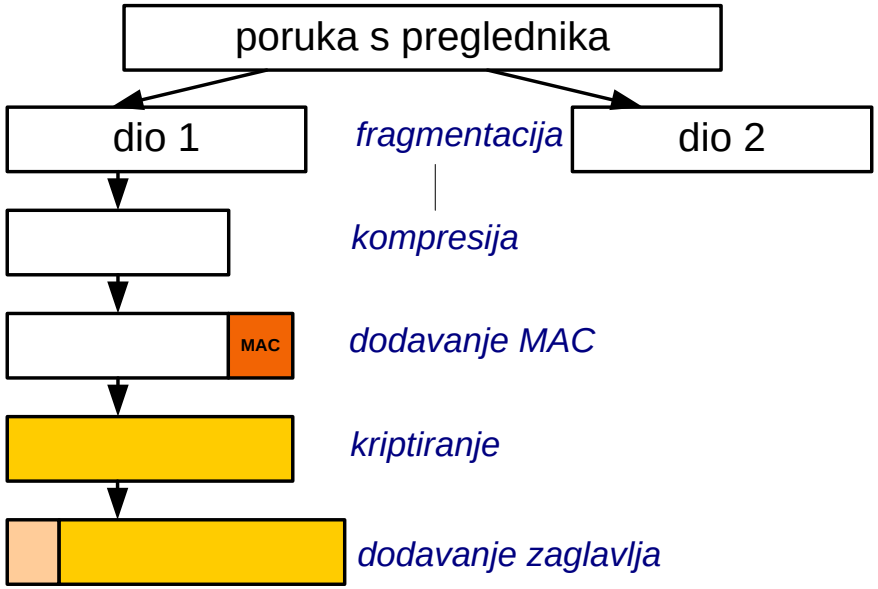
Uspostavljanje SSL-sjednice



Prijenos podataka tijekom SSL-sjednice

Protokol SSL-zapisa

- poruka (npr. s preglednika) dijeli se na jedinice od 16K
- svaka se jedinica komprimira
- dodaje se kod vjerodostojnosti (tipično MD5) komprimirane poruke i tajnog ključa
- sve se kriptira simetričnim algoritmom kriptiranja
- dodaje se zaglavlje

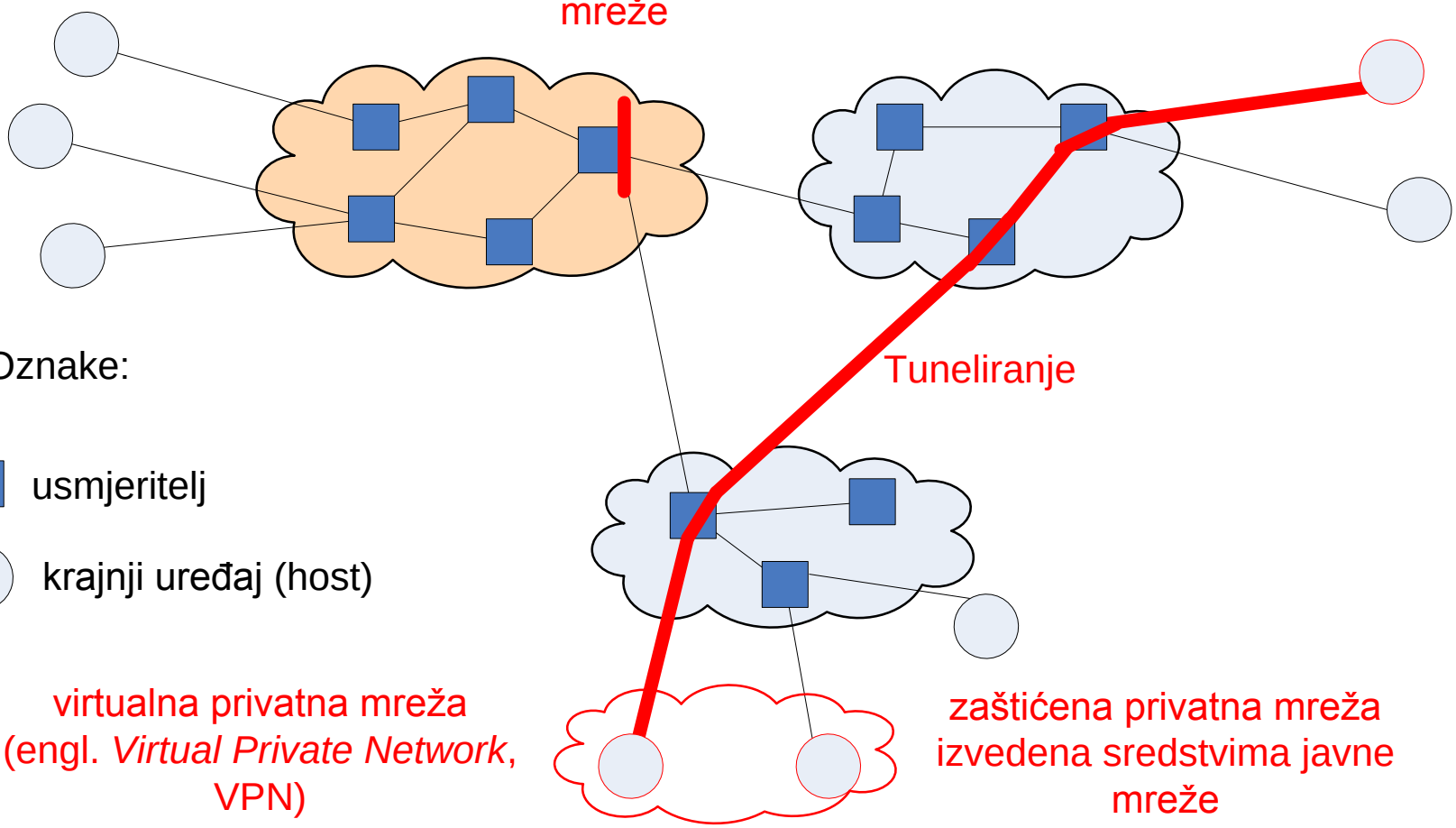


još malo o sigurnosnoj arhitekturi Interneta

sigurnosna zaštitna stijena,

virtualna privatna mreža

sigurnosna zaštitna stijena, vatrozid (engl. *firewall*)
filtriranje IP-datagrama na ulazu/izlazu privatne mreže



Pitanja za provjeru znanja

- Kako se može utvrditi autentičnost (vjerodostojnost) sudionika u komunikaciji?
- Kako se može očuvati cjelovitost (integritet) poruke?
- Kako se može postići povjerljivost (tajnost) poruke?
- Koje sigurnosne zahtjeve ne rješavaju kriptografski postupci?
- Kakve se sigurnosne usluge pruža i što se štiti zaglavljem AH u tunelskom načinu rada?
- Kakve se sigurnosne usluge pruža i što se štiti zaglavljem ESP u transportnom načinu rada?

Istraživački zadatak

Istražite pretraživanjem informacija dostupnih putem Interneta:

- Što obuhvaća pojam "*Authentication Authorisation Accounting*" (AAA) u Internetu?
- Kako su AAA usluge izvedene u CARnetu?
- Kad su Vam te usluge potrebne?

Dodatna literatura

- A. Bažant, Ž. Car, G. Gledec, D. Jevtić, G. Ježić, M. Kunštić, I. Lovrek, M. Matijašević, B. Mikac, Z. Skočir:

  "Telekomunikacije – tehnologija i tržište", 6. Sigurnost i privatnost, Element, Zagreb, 2007.
- L. Budin, M. Golub, D. Jakobović, L. Jelenković:

  "Operacijski sustavi", 11. Sigurnost računalnih sustava,

  Element, Zagreb, 2010.

- The Handbook of Applied Cryptography Online
  http://www.cacr.math.uwaterloo.ca/hac/
- An Overview of Cryptography
  http://www.garykessler.net/library/crypto.html