SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 4:
Sigurnosni protokoli

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Sigurnosni protokoli

- Sadržaj poglavlja i predavanja:
  - 4.1 Šta su kriptografski protokoli i čemu služe?
  - 4.2 Protokol Secure Sockets Layer (SSL)
  - 4.3 IPSec
  - 4.4 Protokoli za proveru identiteta
  - Dodatak: Diffie-Hellman Key Exchange

Quote

If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.

—*The Art of War*, Sun Tzu

Potrebna predznanja

- Matematika
- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Internet

4.1 Šta su kriptografski protokoli i čemu služe

- **Protokol** je skup pravila i konvencija koji definiše komunikacioni okvir između dva ili više učesnika u komunikaciji
  - Uspostava veze
  - Održavanje veze
  - Raskid veze
  - Oporavak u slučaja prekida veze

- **Kriptografski protokoli** se upotrebljavaju za uspostavljanje sigurne komunikacije preko nepouzdanih globalnih mreža i distribuiranih sistema.
  - Oslanjaju se na kriptografske metode zaštite kako bi korisnicima obezbedili osnovne sigurnosne usluge poverljivosti, integriteta i neporecivosti.

Sigurnostni protokoli na različitim TCP/IP slojevima

- Sloj aplikacije – OpenPGP
- Transportni sloj – TLS (Transport Layer Security)
- Mrežni sloj – IPSec
- Sloj veze – šifrovanje, različiti mehanizmi

Poznati sigurnosni protokoli

- IPSec – IP Security
- SSL – Secure Sockets Layer

- TLS – Transport Layer Security
- TTLS - Tunneled Transport Layer Security

- EAP (Extensible Authentication Protocol)
- EAP TTLS – EAP Tunneled TLS Authentication Protocol

Usluge specifične za određene primene

- PGP - Pretty Good Privacy
- S/MIME - Secure/Multipurpose Internet Mail Extensions
- SET – Secure Electronic Transaction
- Kerberos
- SSL/HTTPS

4.2 Protokol Secure Sockets Layer (SSL)

- Obezbeđuje mehanizme za identifikaciju dva sagovornika povezana računarskom mrežom i zaštićeni prenos podataka između njih

- Projektovan da zadovolji sledeće ciljeve
  - Kriptografska zaštita
  - Nezavisnost od softvera i hardvera
  - Proširivost
  - Efikasnost

Zadatak SSL protokola

- Zadatak protokola Secure Sockets Layer (SSL) jeste da ostvari zaštićeni prenos podataka kroz mrežu.
- SSL obezbeđuje mehanizme za identifikaciju servera, identifikaciju klijenta i šifrovanu razmenu podataka između njih, što čini potpuni sistem zaštićene komunikacije dva mrežna entiteta.
- Za ostvarivanje zaštićenog prenosa, protokol SSL moraju podržavati i klijent i server.

Svojstva SSL-a

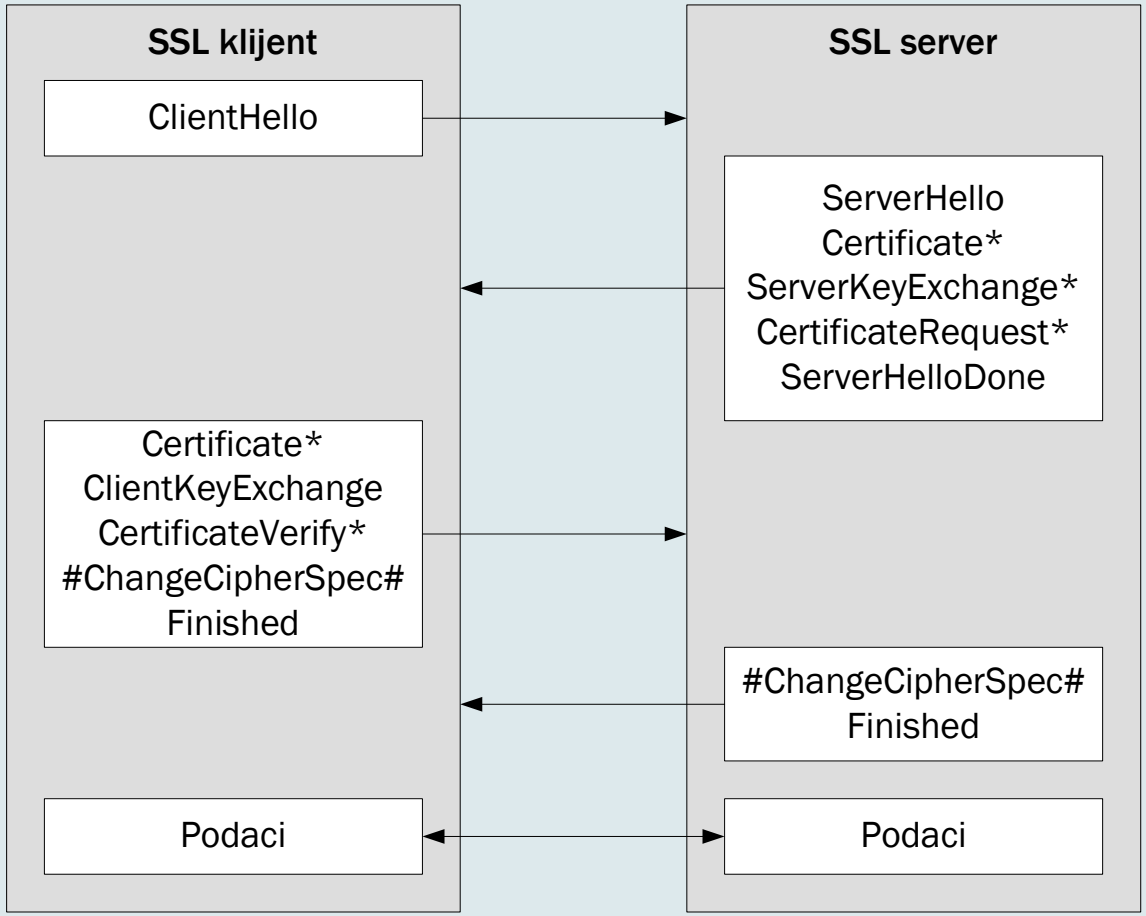
- Privatnost
- Mogućnost provere identiteta
- Pouzdanost

SSL u skupu protokola

SSL protokoli

- SSL se sastoji od dva protokola:
  - **SSL Handshake protokol** (protokol za rukovanje, tj. uspostavljanje sesije) koji omogućuje klijentu i serveru međusobnu identifikaciju i razmenu parametara za prenos (odabir algoritma i ključeve).
  - **SSL Record protokol** (protokol za zapise) koji je zadužen za šifrovanje i prenos poruka.

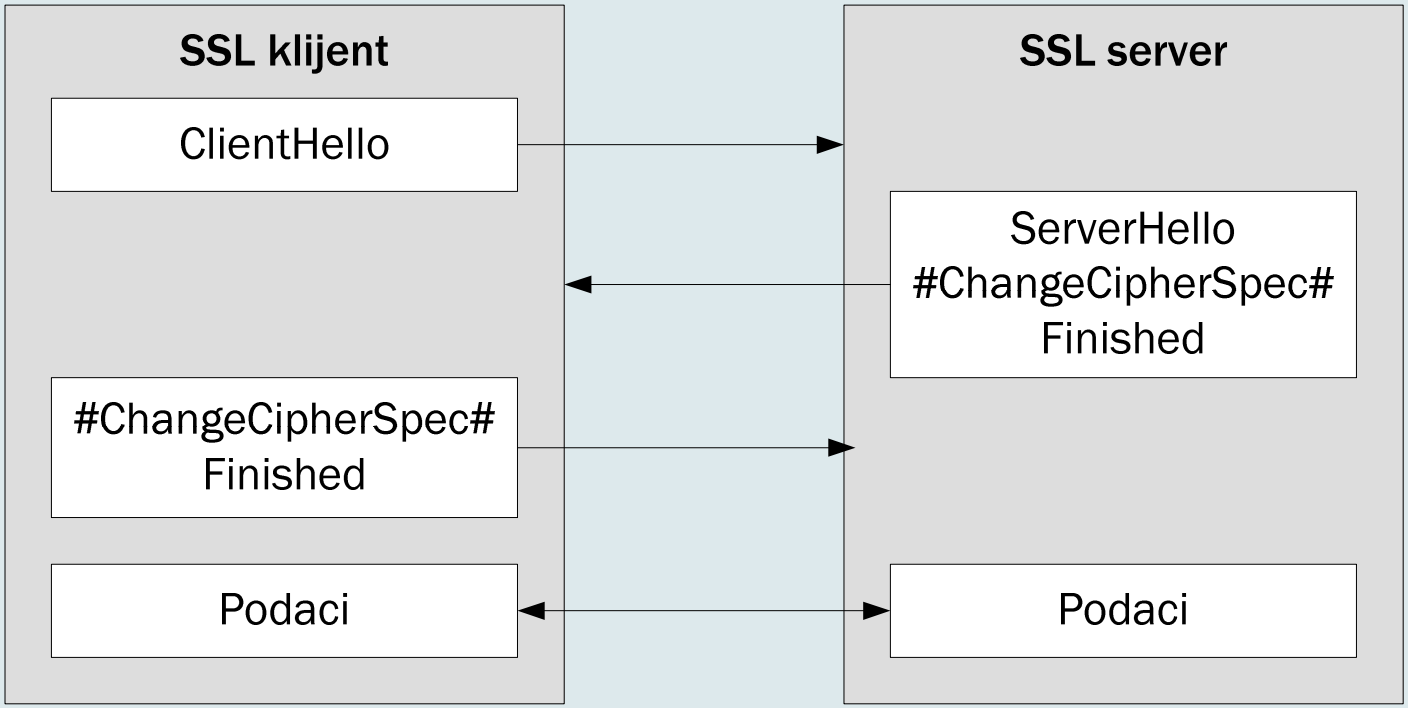
SSL protokol za rukovanje



Atributi SSL sesije i veze

- Svaka SSL sesija opisana je sledećim atributima:
  - Identifikator sesije
  - Potvrda entiteta
  - Metoda kompresije
  - Šifrovanje
  - Tajna
  - Proširivost

Obnavljanje SSL sesije



SSL protokol za zapise

- SSL protokol za zapise prima podatke s višeg sloja u blokovima proizvoljnih veličina, ne interpretira ih, već ih deli na delove odgovarajuće veličine, kriptografski štiti i šalje sagovorniku, gde se odvija obrnuti proces.

Izveštaji

- Neočekivana poruka
- Neispravna MAC vrednost
- Greška prilikom dekompresije
- Greška u fazi uspostavljanja sesije
- Greške vezane za sertifikate
  - Nema sertifikata
  - Neprikladan sertifikat
  - Nevažeći sertifikat
  - Poništen sertifikat
  - Loš sertifikat
  - Neprihvatljiv sertifikat
- Nevažeći parametar

Primena SSL-a

- SSL se najčešće koristi za plaćanje robe kreditnom karticom, gde se zaštićeno prenosi samo broj kreditne kartice. Za takve, a i mnogo zahtevnije zadatke, SSL je zadovoljavajuće rešenje.

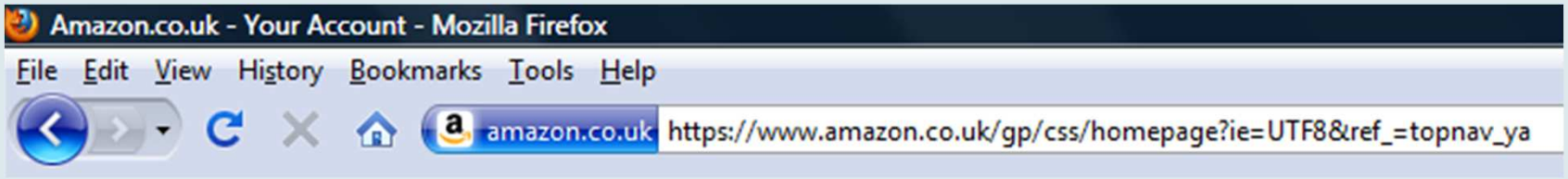
- SSL nije standardizovao IETF (Internet Engineering Task Force) pomoću RFC dokumenata, već je opisan u publikaciji koju je objavila kompanija Netscape Communications. SSL je relativno brzo postao *de facto* standard za sigurnu komunikaciju, a www konzorcijum (www.w3.org) odobrio je SSL kao zvaničan standard.

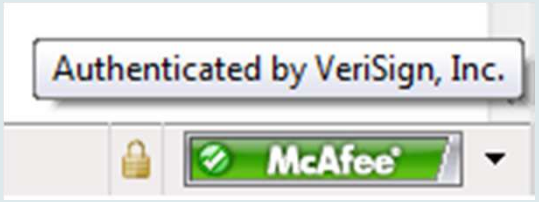
Implementacije SSL-a

- Hardverske
- Softverske

Hardware: SSL accelerator cards

In Web browser





OpenSSL

- OpenSSL je besplatan kriptografski alat koji implementira sigurnosne protokole SSL verzije 2 i 3 i TLS v1, kao i ostale kriptografske standarde koji se odnose na ove protokole (na primer, 3DES, AES i RSA). OpenSSL omogućava da se s komandne linije pozivaju razne kriptografske funkcije ugrađene u zbirke datoteka programskog paketa OpenSSL

- Programski paket OpenSSL može se besplatno preuzeti sa Web stranice www.openssl.org.

Druga rešenja

- Neka od drugih rešenja koja koriste arhitekturu i principe slične onima koji postoje u protokolu SSL jesu:
  - S/MIME (Secure/MIME)
  - SSH (Secure Shell)
  - PCT (Private Communication Technology)
  - OpenPGP.

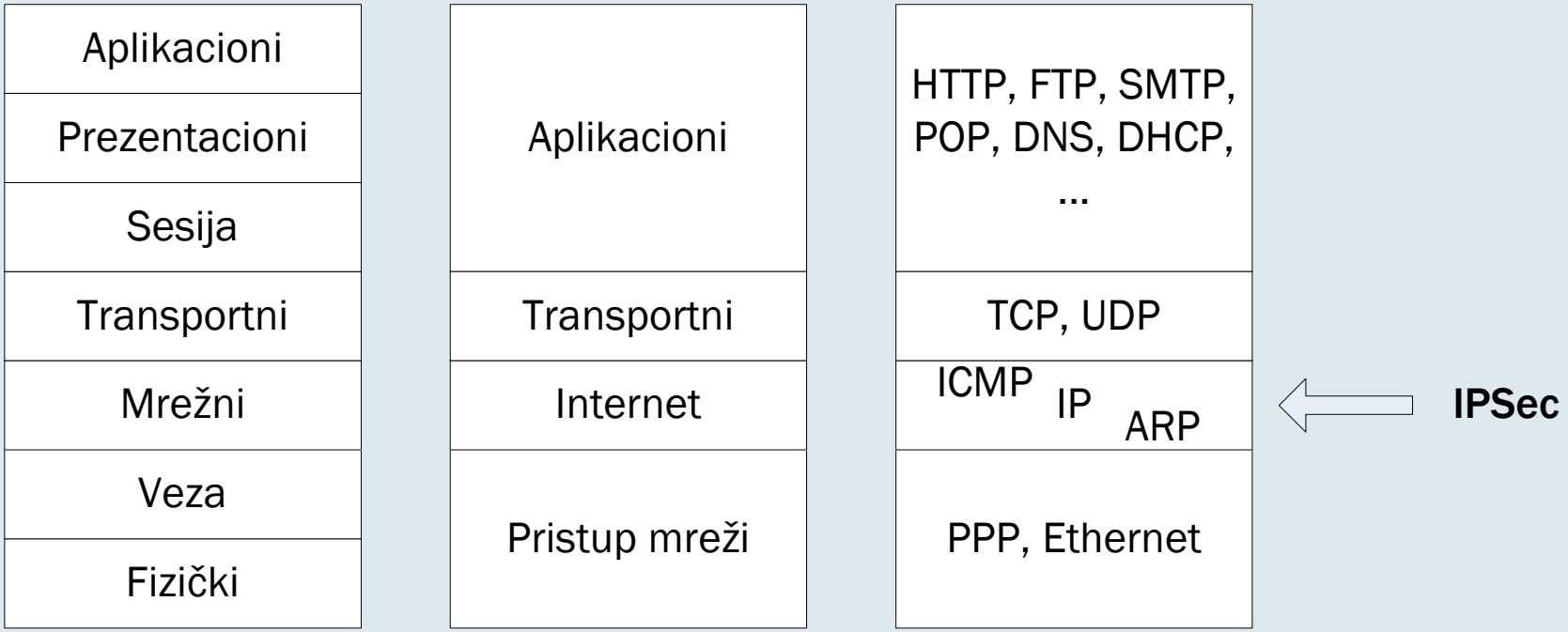
SSH

- Secure Shell (SSH) je popularan protokol za šifrovanje komunikacionih kanala, koji se najčešće koristi za obezbeđivanje sigurnih sesija udaljenog prijavljivanja na sistem.
- Arhitektura SSH je dvoslojna (engl. *two-tier*) klijent-server arhitektura.
- SSH server je softver koji prima ili odbija dolazeće veze ka računaru.
- SSH klijentski softver instaliran je na udaljenim računarima
- SSH šifruje sve podatke koji se prenose preko mreže, a samo šifrovanje je transparentno (nevidljivo) za korisnika

4.3 IPSecurity (IPSec)

- IPSec nije jedan protokol
- IPSec pruža skup sigurnosnih algoritama i plus opšti okvir (engl. *framework*) koji omogućava paru entiteta koji komuniciraju da koriste algoritme koje žele da bi obezbedili odgovarajuću sigurnost komunikacije

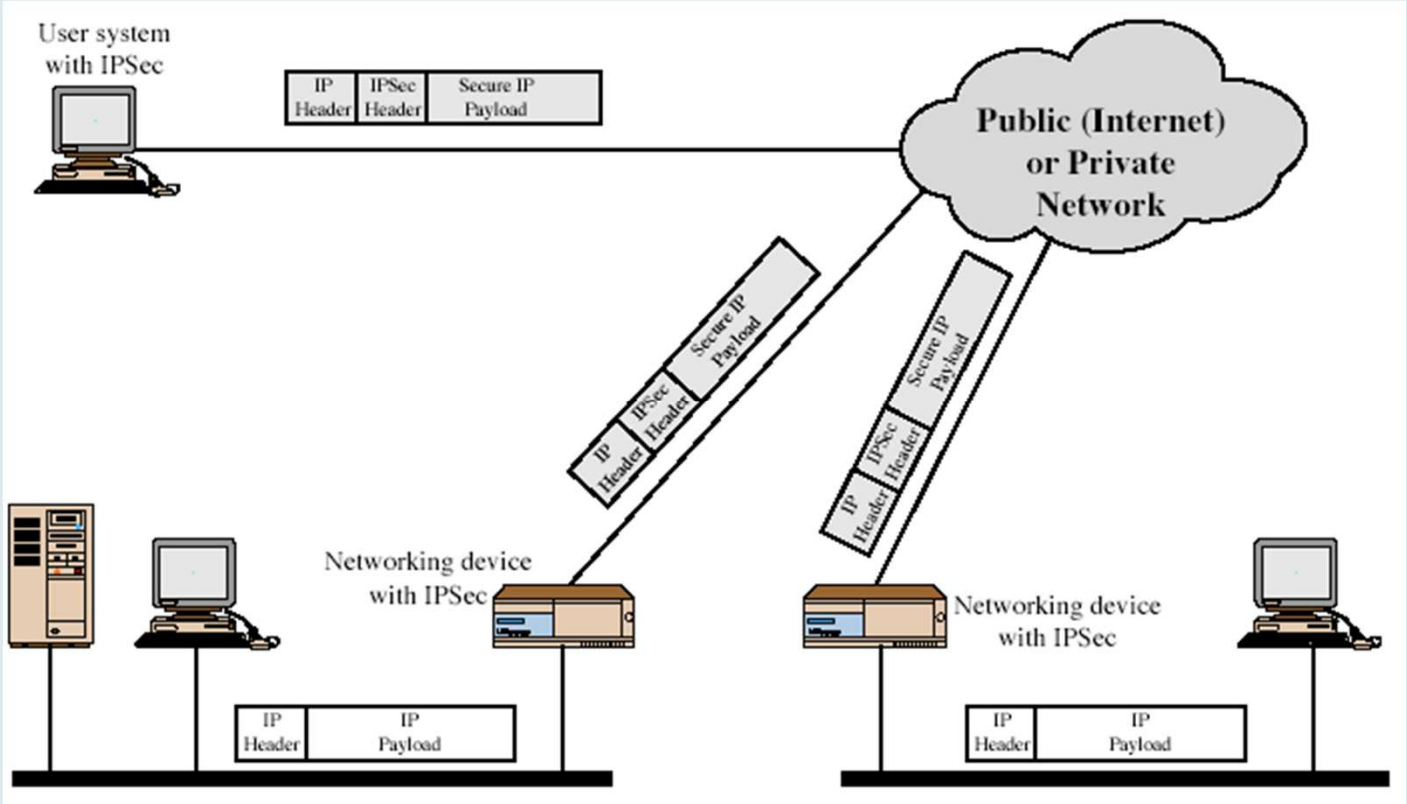
Mesto IPSec u skupu protokola



Primena IPSec-a

- Povezivanje udaljenih ogranaka firme sa centralom sigurnom vezom, a preko javnih (nesigurnih) mreža
- Siguran pristup sa udaljenih lokacija preko javne mreže (Internet)
- Uspostavljanje extranet i intranet veza sa partnerima
- Povećanje sigurnosti elektronske trgovine

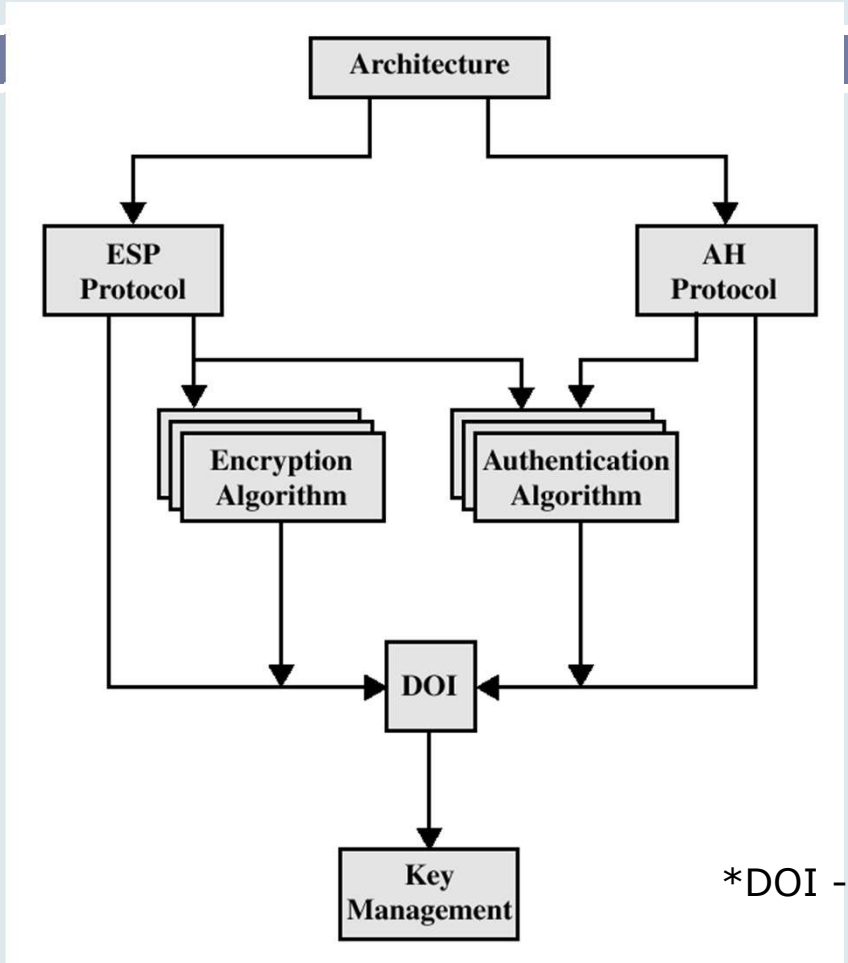
Primena IPSec-a...



Kratak pregled

- Internetworking and Internet Protocols
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combinations of Security Associations
- Key Management

Pregled IPSec dokumenata



*DOI - **D**omain **O**f **I**nterpretation

IPSec

- Generalni sigurnosni mehanizmi koje pruža IPSec
  - Provera identiteta (engl. *authentication*)
  - Poverljivost (engl. *confidentiality*)
  - Upravljanje ključevima (engl. *key management*)

- Može se koristiti preko LAN i (privatnih i javnih), Interneta

IPSec paketi i standardi

- IPSec definiše informacije koje se moraju dodati IP paketu kako bi se obezbedili privatnost, integritet i provera identiteta, kao i način šifrovanja sadržaja paketa.
- Pri radu, IPSec koristi sledeće protokole i standarde:
  - Diffie-Hellmanov protokol za razmenu ključeva između dva učesnika u komunikaciji
  - Algoritme za digitalno potpisivanje komunikacije pri Diffie-Hellmanovoj razmeni ključeva
  - DES, 3DES (i u novije vreme, AES) simetrične algoritme za šifrovanje
  - HMAC (*Hashing Message Authentication*) u sprezi sa algoritmima MD5 i SHA
  - Digitalne sertifikate koje je potpisao odgovarajući autoritet.

IPSec protokoli

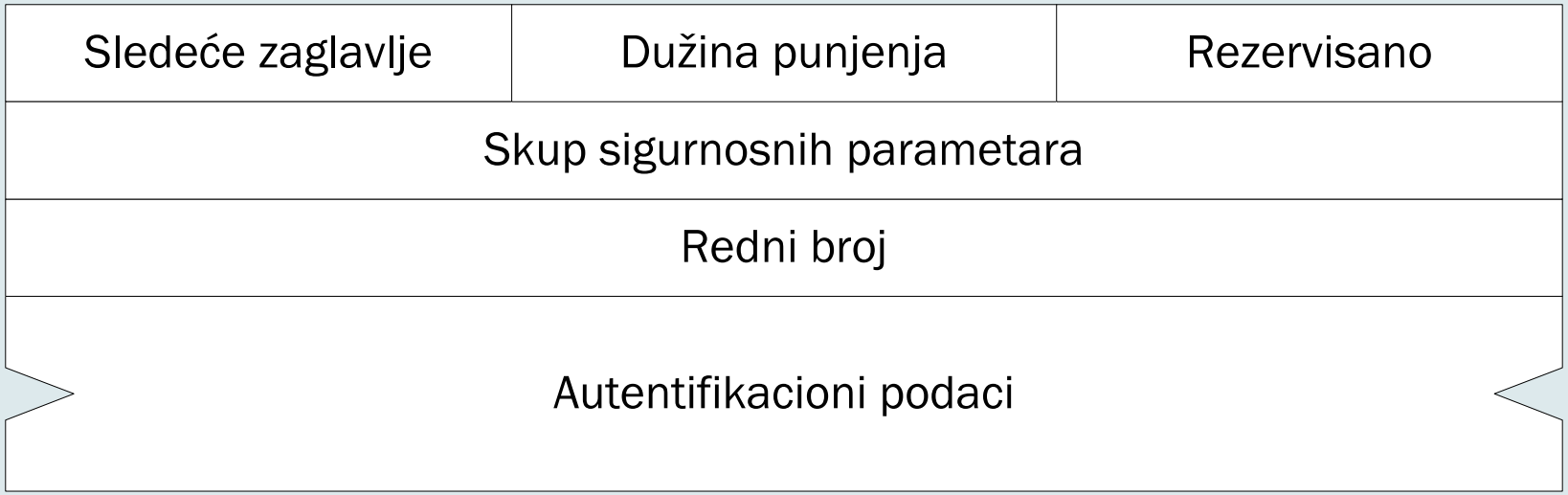
- AH (*Authentication Header*)
- ESP (*Encapsulated Security Payload*)

Standardni oblik IP paketa

Protokol AH

- Protokol AH definisan je dokumentom RFC 2402. AH obezbeđuje sigurnosne usluge provere identiteta, integriteta i neporecivosti IP paketa, ali ne može obezbediti privatnost.

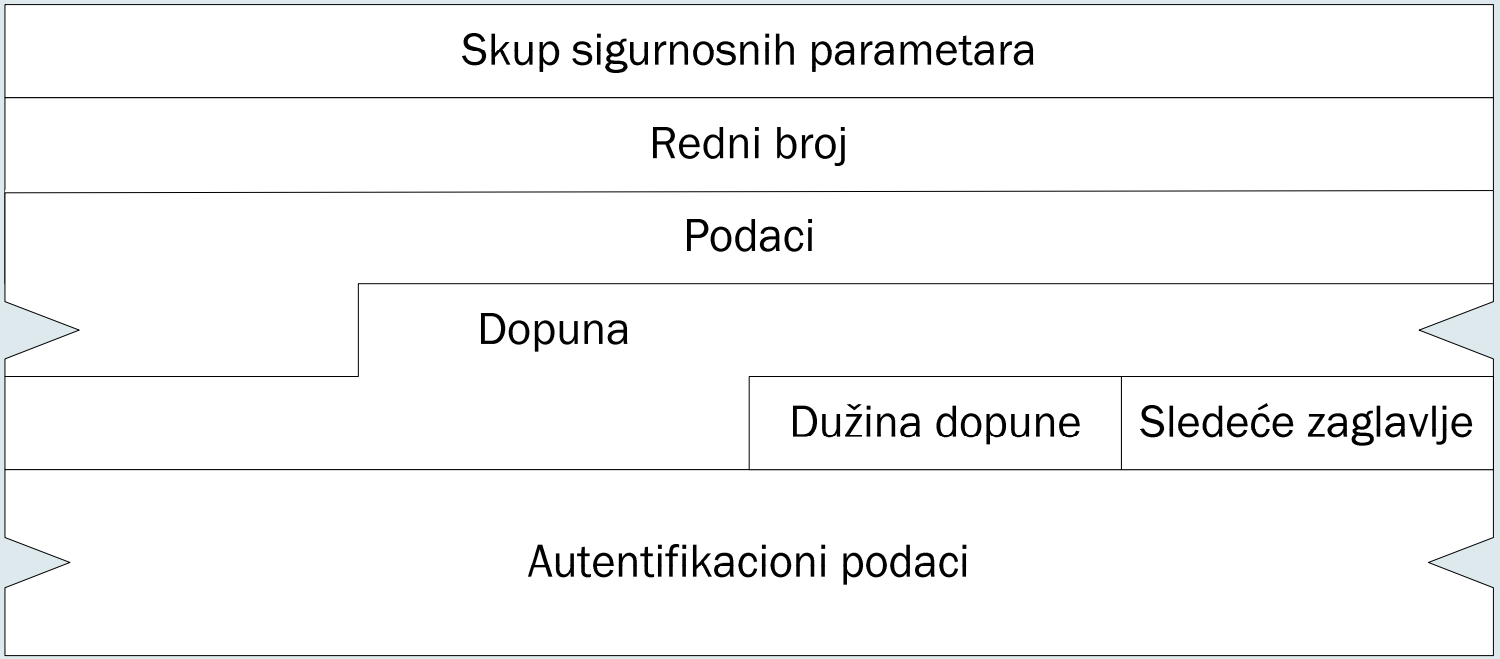
AH zaglavlje



Protokol ESP

- Protokol ESP definisan je dokumentom RFC 2406. ESP obezbeđuje sigurnosne usluge provere identiteta, integriteta, neporecivosti i privatnosti podataka.

ESP paket



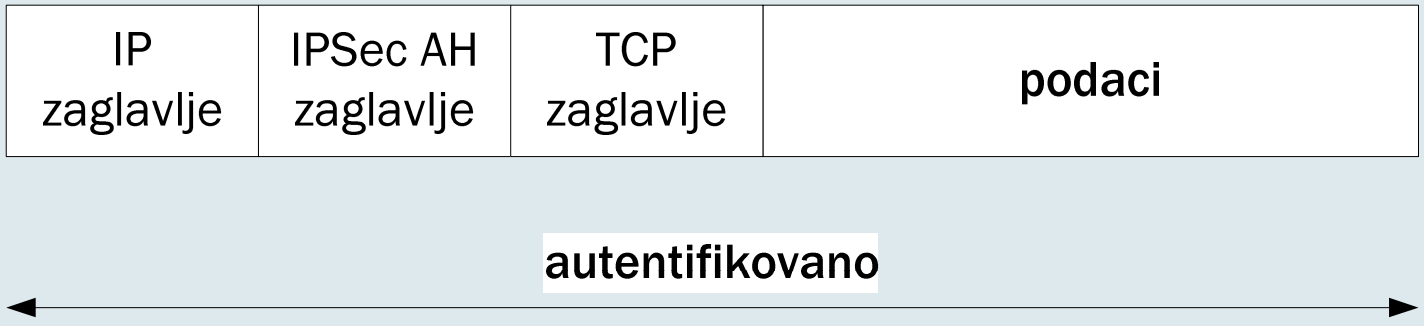
IPSec režimi rada

- IPSec podržava dva režima rada:
  - prenosni (engl. *transport mode*)
  - tunelovanje (engl. *tunnel mode*).

Transportni režim rada

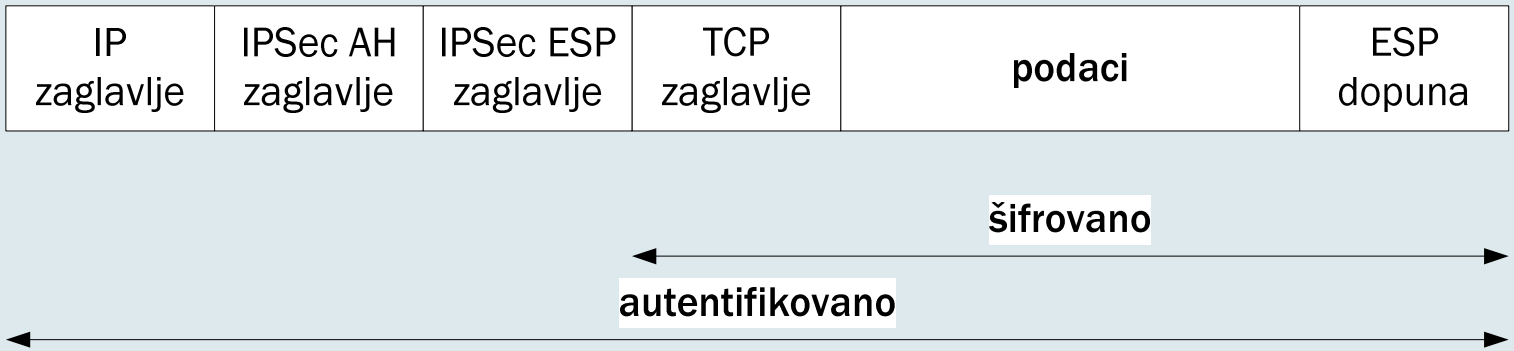
- Transportni režim rada namenjen je prvenstveno za uspostavljanje sigurne komunikacije između dva entiteta, tj. za komunikaciju računar-računar u privatnim LAN ili WAN računarskim mrežama. Za transportni način rada potrebno je da obe krajnje tačke komunikacije (izvor i odredište) podržavaju IPSec.

AH u transportnom režimu rada



ESP u transportnom režimu rada

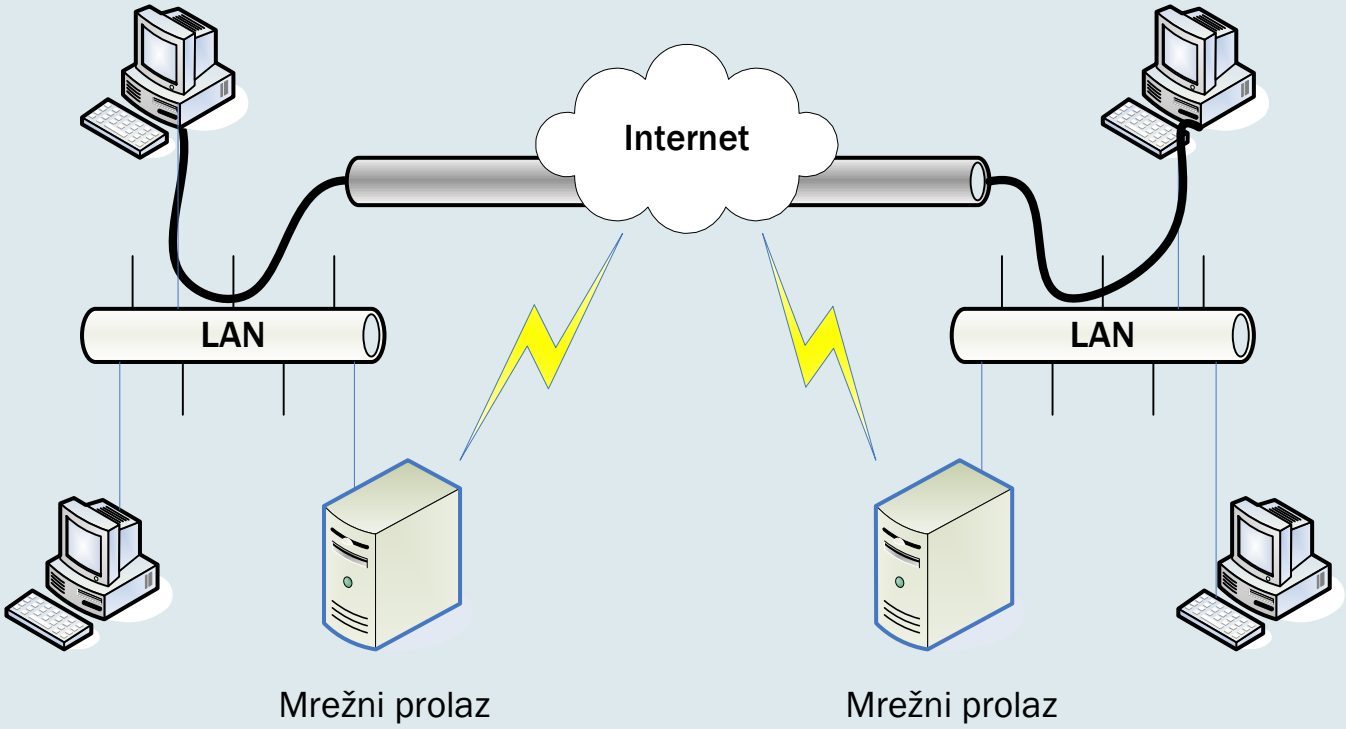
ESP + AH u transportnom režimu rada



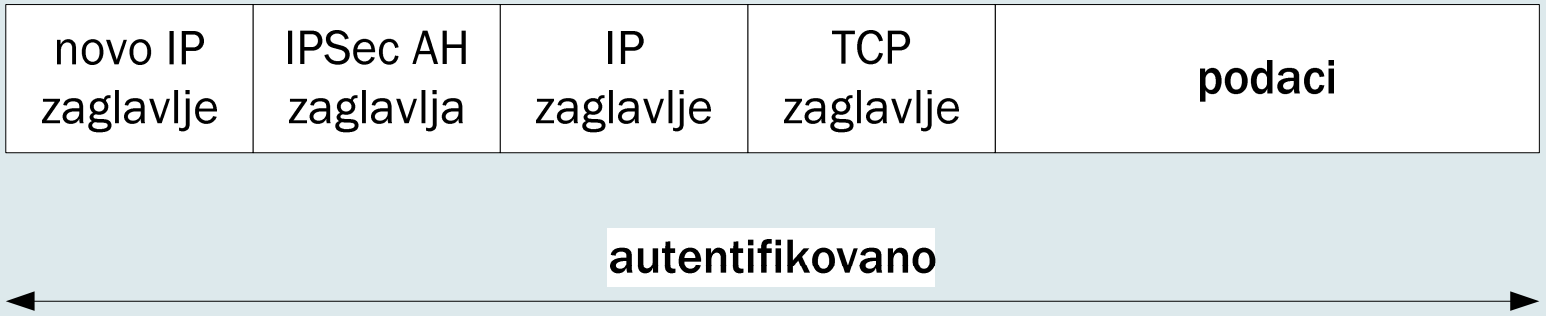
Tunelovanje

- Tunelovanje je drugi režim rada IPSec protokola, u kome IPSec služi za uspostavljenje sigurne komunikacije između mrežnih prolaza (engl. *gateway*) na udaljenim mrežama (engl. *gateway-to-gateway*), obezbeđujući tako virtuelnu privatnu komunikaciju, tj. uspostavljajući VPN mrežu (*Virtual Private Network*) između udaljenih lokacija. U ovom slučaju krajnji entiteti u komunikaciji ne moraju da podržavaju IPSec.

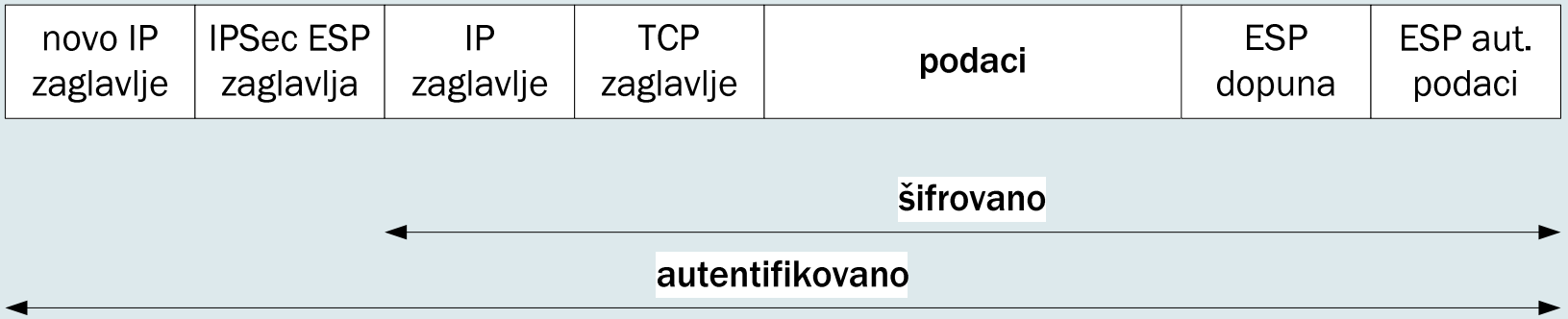
Tunelovanje



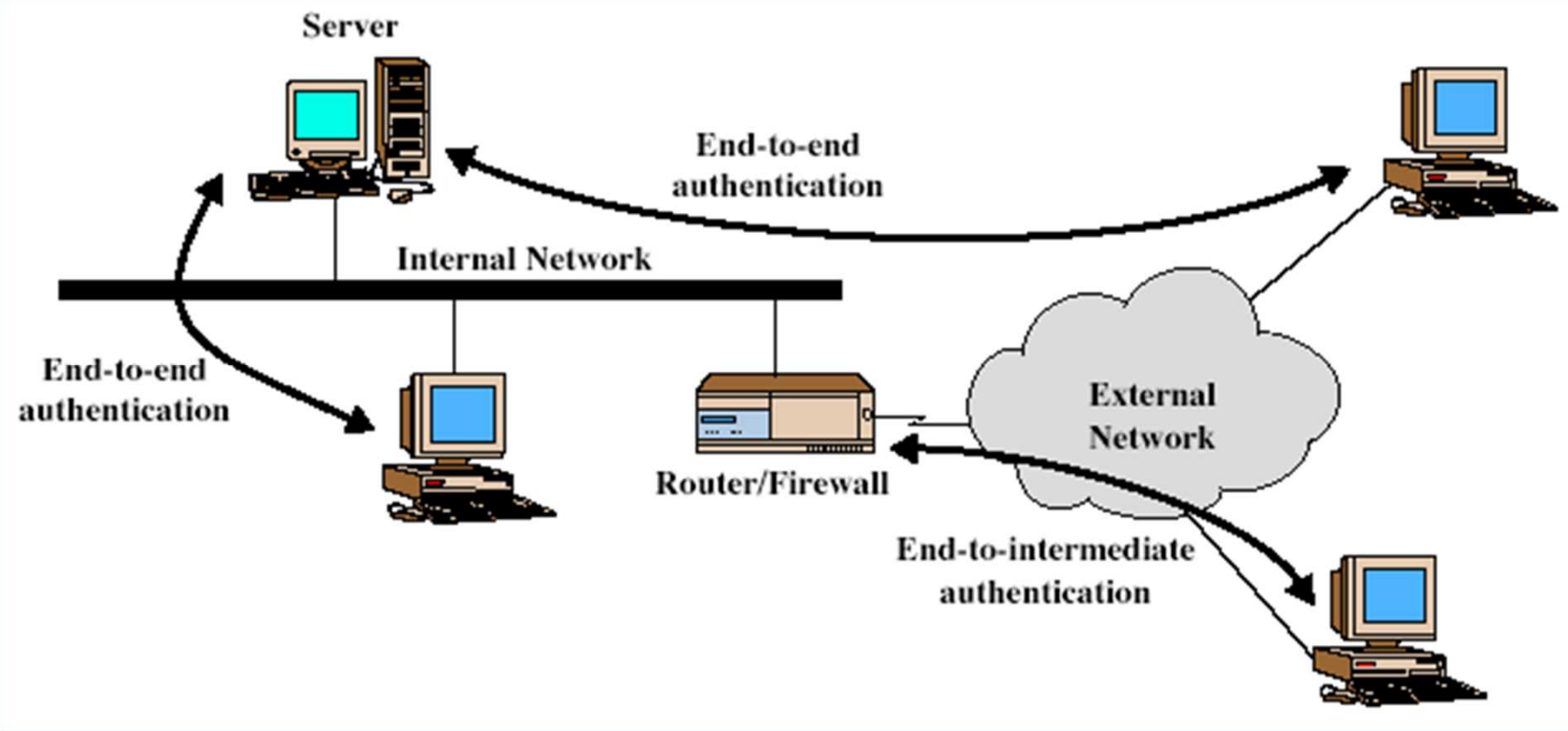
AH tunelovanje



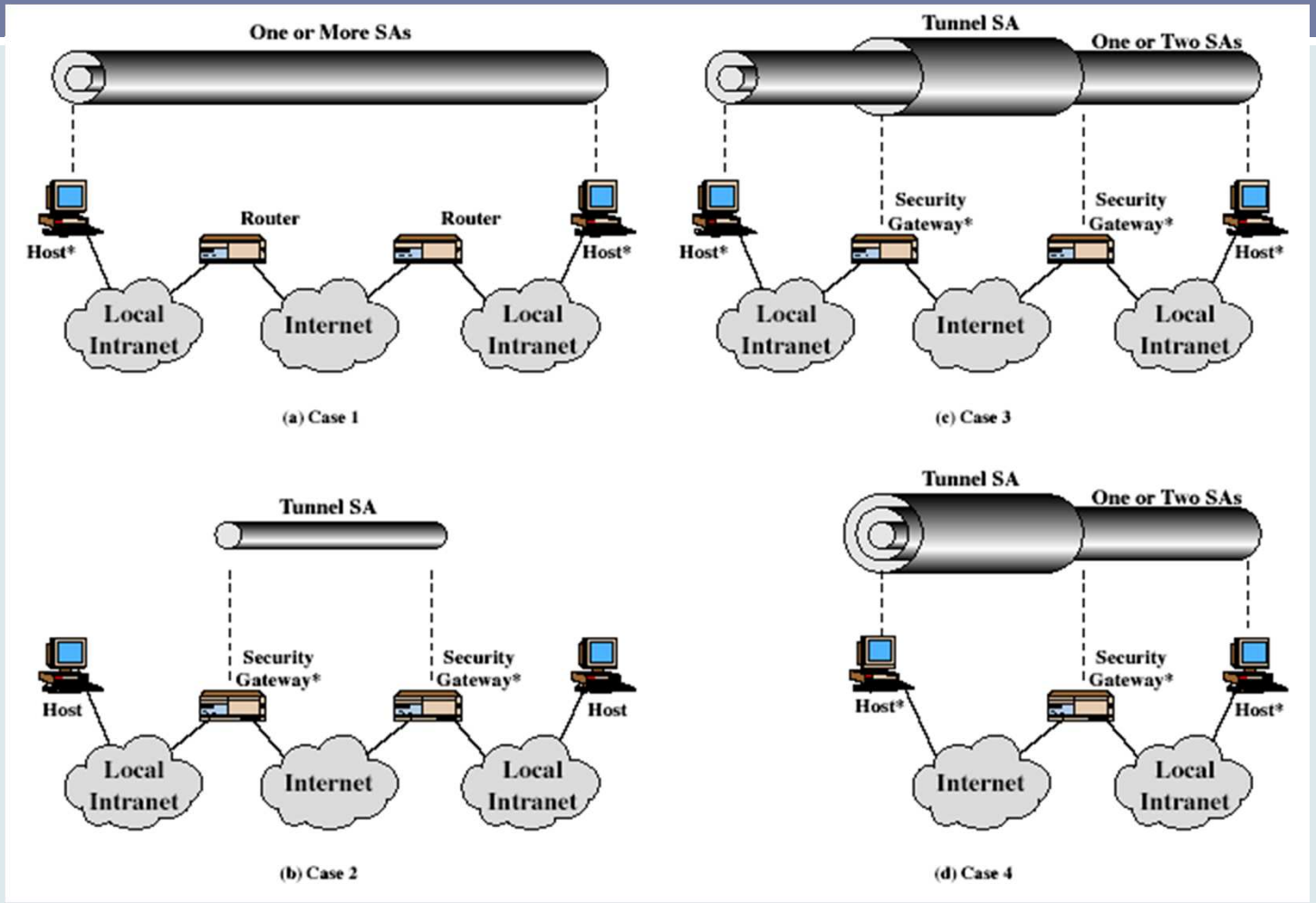
ESP tunelovanje



Režimi provere identiteta



Kombinovanje sigurnosnih parametara komunikacije



Uspostavljanje IPSec komunikacije

- ISAKMP (*Internet Security Association and Key Management Protocol*)
- IKE (*Internet Key Exchange*)
  - Uspostavljanje IKE SA
  - Uspostavljanje IPSec SA
- Oakley
  - Protokol za razmenu ključeva
  - Baziran na Diffie-Hellmanovom protokolu
  - Dodaje funkcije koje rešavaju neke od slabosti

Uspostavljanje IPSec komunikacije...

- Teoretski je moguće ručno podešavanje skupa sigurnosnih parametara.
- Postoji nekoliko formalnih metoda koje se već koriste ili su predložene za uspostavljanje IPSec komunikacije.
- Protokoli Photuris i SKIP (*Simple Key management for Internet Protocols*) zasnovani su na Diffie-Hellmanovom protokolu za razmenu ključeva i mogu se koristiti u tu svrhu.

4.4 Protokoli za proveru identiteta

- **Provera identiteta** je sigurnosna usluga kojom se od svakog korisnika zahteva da se predstavi sistemu pre nego što nešto uradi. Cilj provere identiteta je da obezbedi odgovarajući mehanizam pomoću koga će se potvrditi da je objekat zaista „ono za šta se izdaje“.

- Primeri:
  - Kerberos
  - RADIUS

Kerberos

- Kerberos je jedan od najpoznatijih protokola za proveru identiteta korisnika.
- Ime je dobio po Kerberu, zato što centar za distribuciju ključeva, poput mitskog bića, ima tri „glave“: bazu, server za proveru identiteta i server za izdavanje karata.

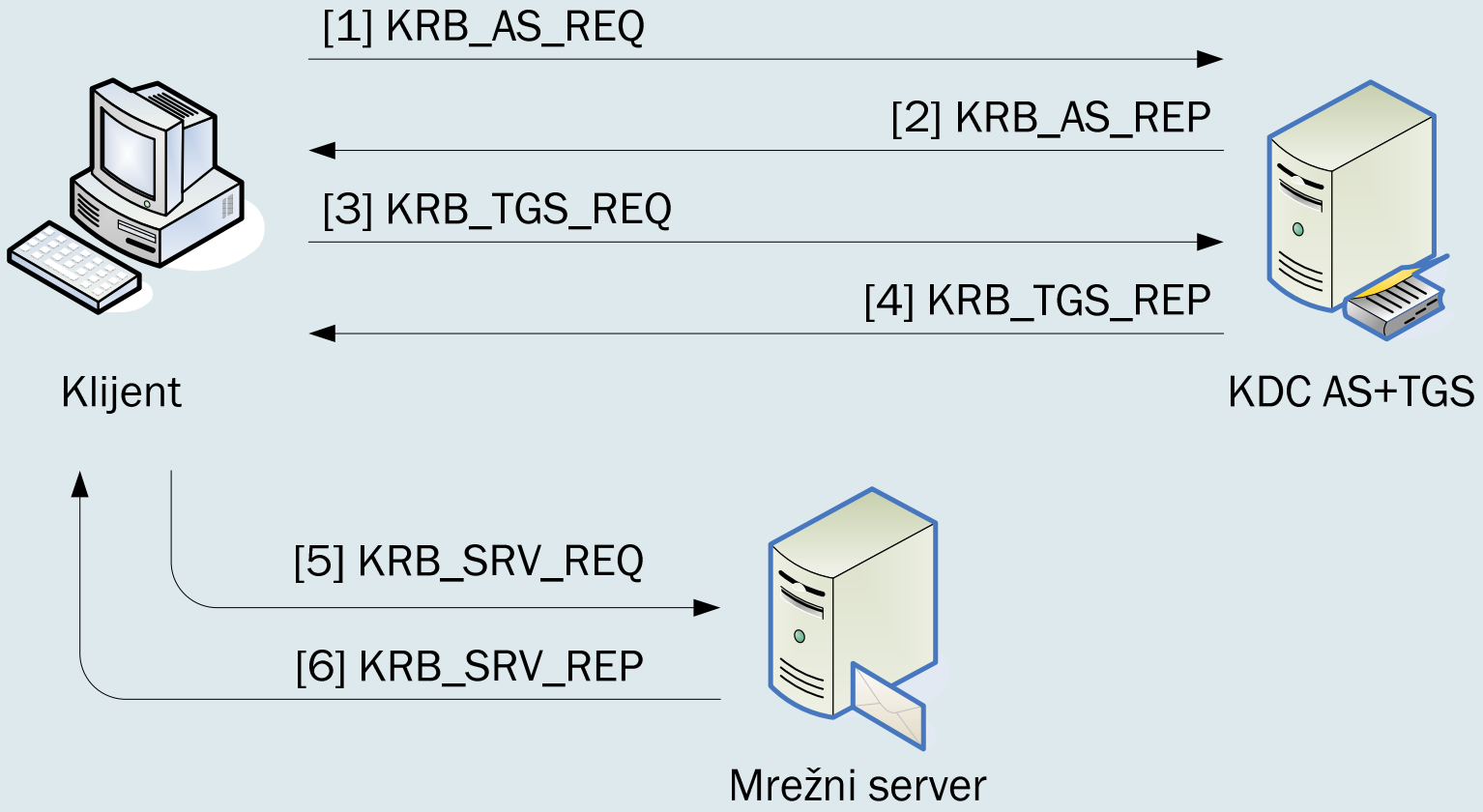
*Kerber (grč. *Κέρβερος*, Krberos, što znači demon iz jame) u grčkoj mitologiji predstavlja troglavog psa čuvara ulaza u podzemlje (Had)

Kerberos

- Kerberos jeste takozvano prijavljivanje tipa „prijavi-se-samo-jednom“ (engl. *Single Sign On*), koje korisnicima omogućava da se samo jednom prijave na sistem i da nakon toga, u skladu sa svojim ovlašćenjima, imaju pristup svim resursima u sistemu (ili mreži).

- Protokol Kerberos razvijen je još osamdesetih godina prošlog veka na MIT institutu (*Massachusetts Institute for Technology*) u okviru projekta Athena (u sklopu koga je, između ostalog, razvijano i grafičko radno okruženje za UNIX sisteme – X Window System)

Razmena poruka u Kerberos komunikaciji



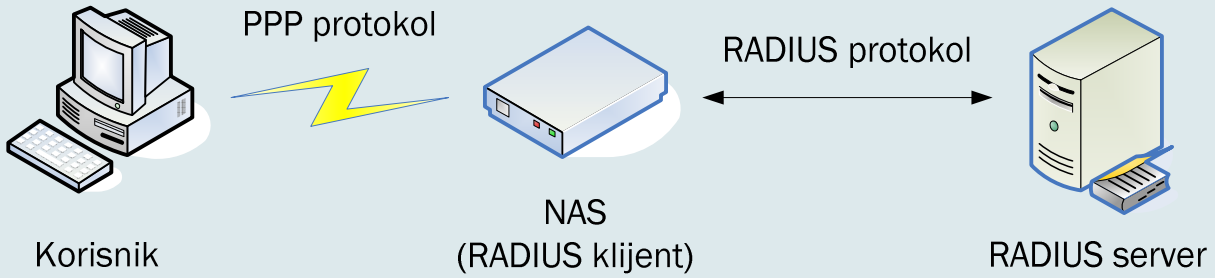
RADIUS

- RADIUS (*Remote Authentication Dial In User Service*) je AAA protokol, tj. protokol koji se koristi za proveru identiteta, autorizaciju i obračun usluga korisnika.
  - *AAA = *authentication, authorization and accounting*

RADIUS…

- Najčešće se koristi za proveru identiteta korisnika na mrežnim uređajima, poput rutera i modema, koji, zbog ograničenih hardverskih resursa kojima raspolažu, ne mogu da čuvaju veliki broj parametara za proveru identiteta različitih korisnika.
- RADIUS obezbeđuje i mehanizam centralizovanog administriranja korisnika, što je jako pogodno u okruženjima u kojima postoji potreba za administriranjem velikog broja korisnika.

RADIUS...



Literatura

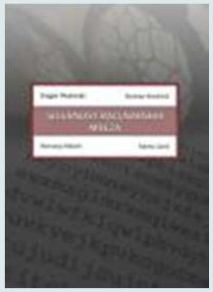
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

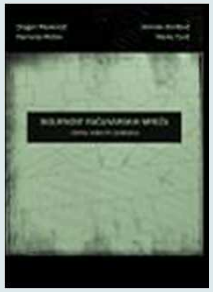
- Za predavanje 4:
  - Poglavlje 4: Sigurnosni protokoli
  - Dodatak A: Sigurnosni standardi i programi sertifikacije

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?

Dodatni slajdovi

- Diffie-Hellman Key Exchange - Mathematician's Explanation
- Diffie-Hellman Key Exchange - A Non-Mathematician's Explanation

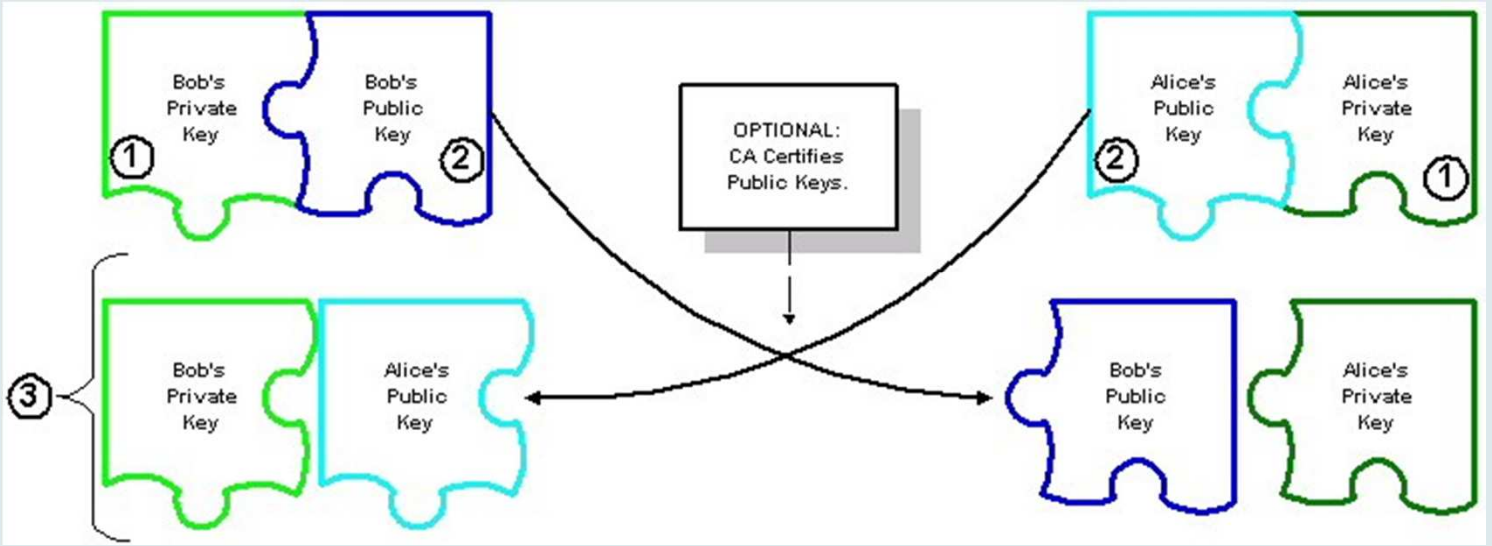
Diffie-Hellman Key Exchange - Mathematician's Explanation

Diffie-Hellman Key Agreement

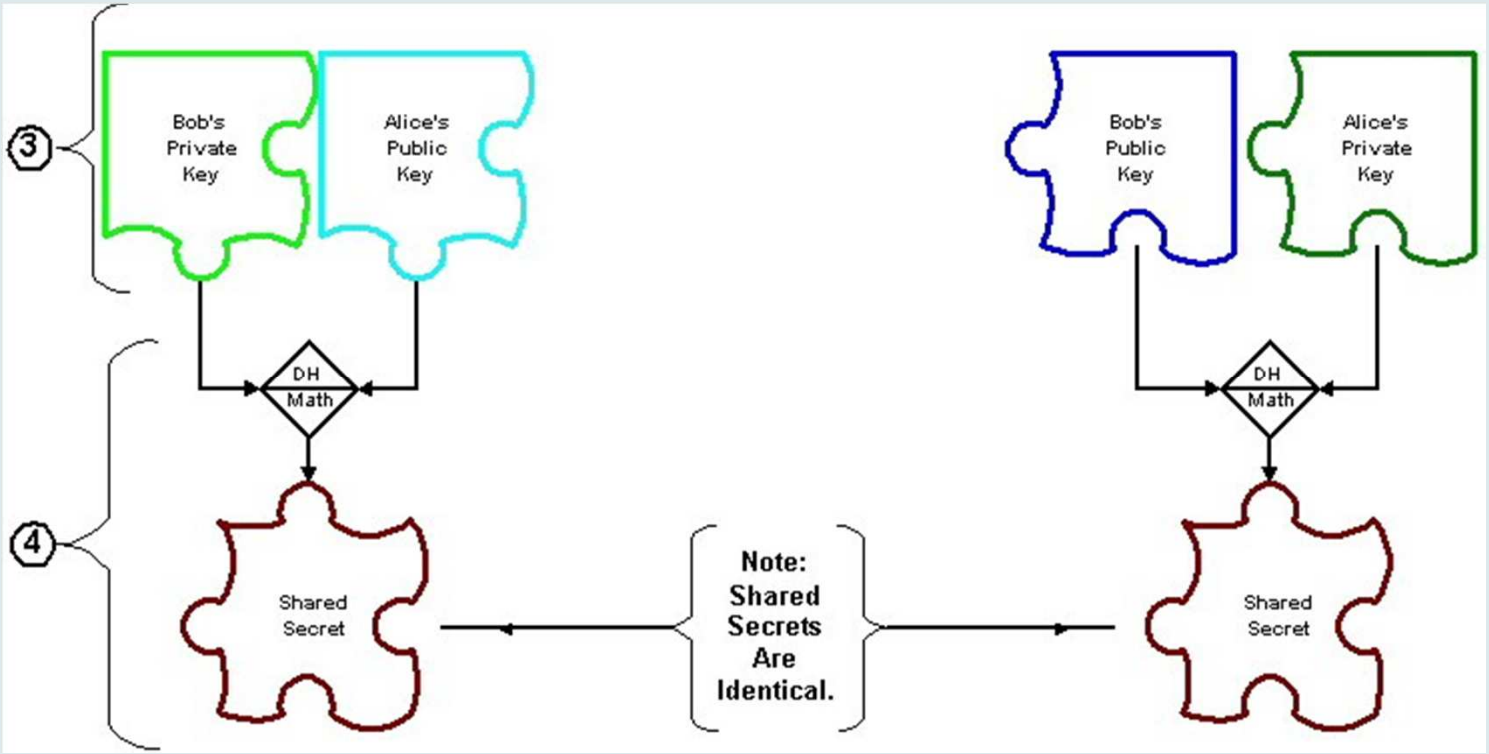
- **Peer A**
  - 1. Generate large integer p.
    Send p to Peer B.
    Receive q.
    Generate g.
  - 2. Generate private key X_A
  - 3. Generate public key $Y_A = g \text{ ^ } X_A \text{ mod } p$
  - 4. Send public key Y_A
  - 5. Generate shared secret number $ZZ = Y_B \text{^ } X_A \text{ mod } p$
  - 6. Generate shared secret key from ZZ (56-bit for DES, 168-bit for 3DES)

- **Peer B**
  - 1. Generate large integer q.
    Send q to Peer A.
    Receive p.
    Generate g.
  - 2. Generate private key X_B
  - 3. Generate public key $Y_B = g \text{ ^ } X_B \text{ mod } p$
  - 4. Send public key Y_B
  - 5. Generate shared secret number $ZZ = Y_A \text{^ } X_B \text{ mod } p$
  - 6. Generate shared secret key from ZZ (56-bit for DES, 168-bit for 3DES)

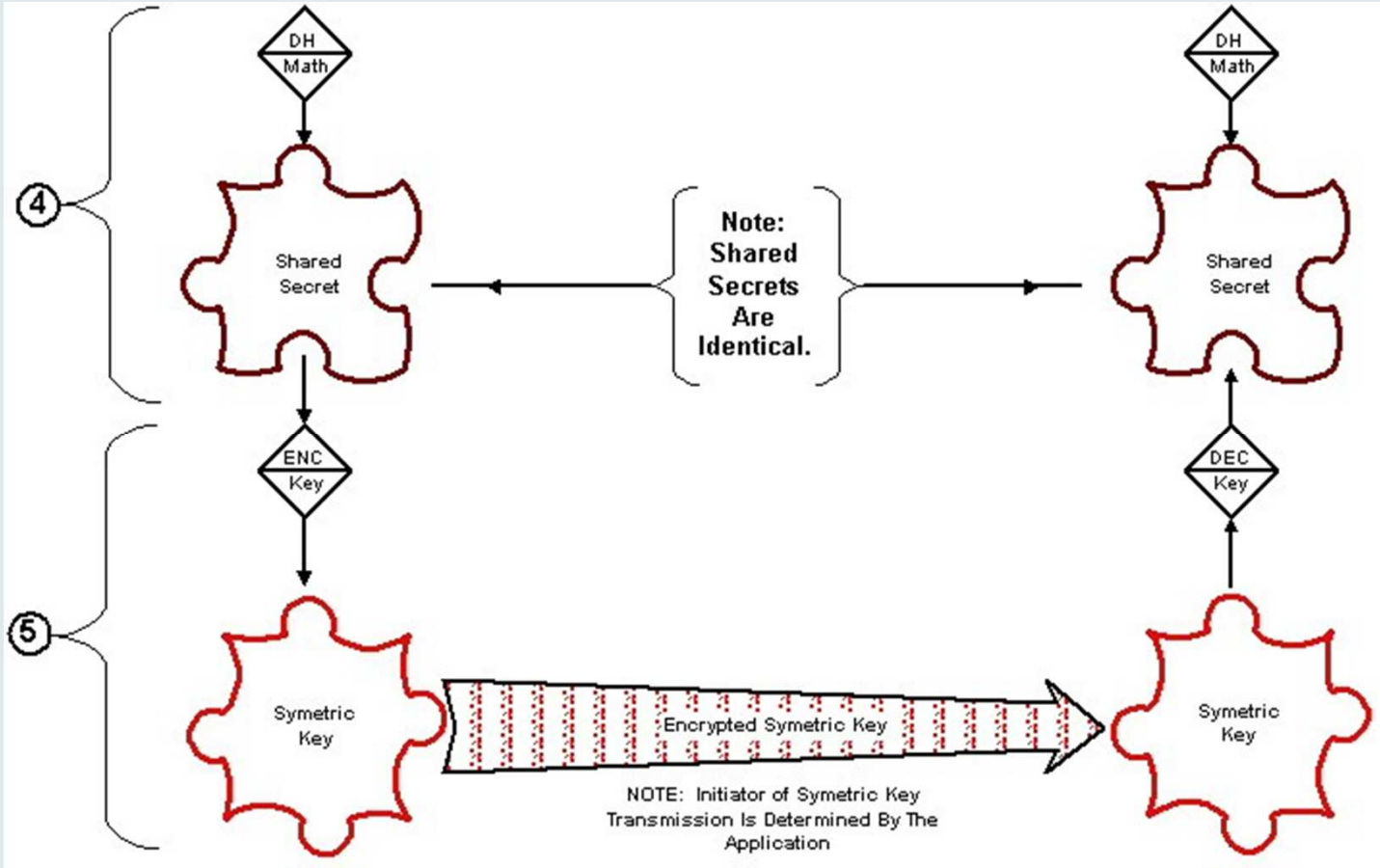
Diffie-Hellman Key Exchange - A Non-Mathematician's Explanation (1)



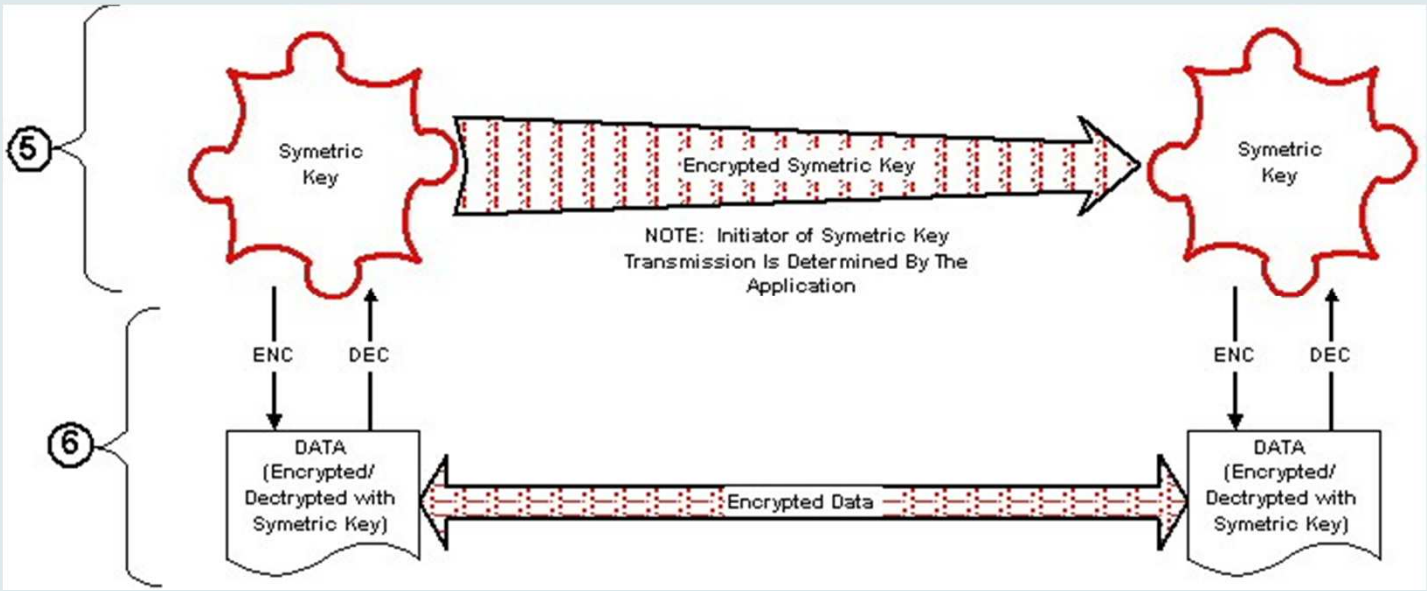
Diffie-Hellman Key Exchange - A Non-Mathematician's Explanation (2)



Diffie-Hellman Key Exchange - A Non-Mathematician's Explanation (3)



Diffie-Hellman Key Exchange - A Non-Mathematician's Explanation (4)



Diffie-Hellman Key Exchange - A Non-Mathematician's Explanation (5)