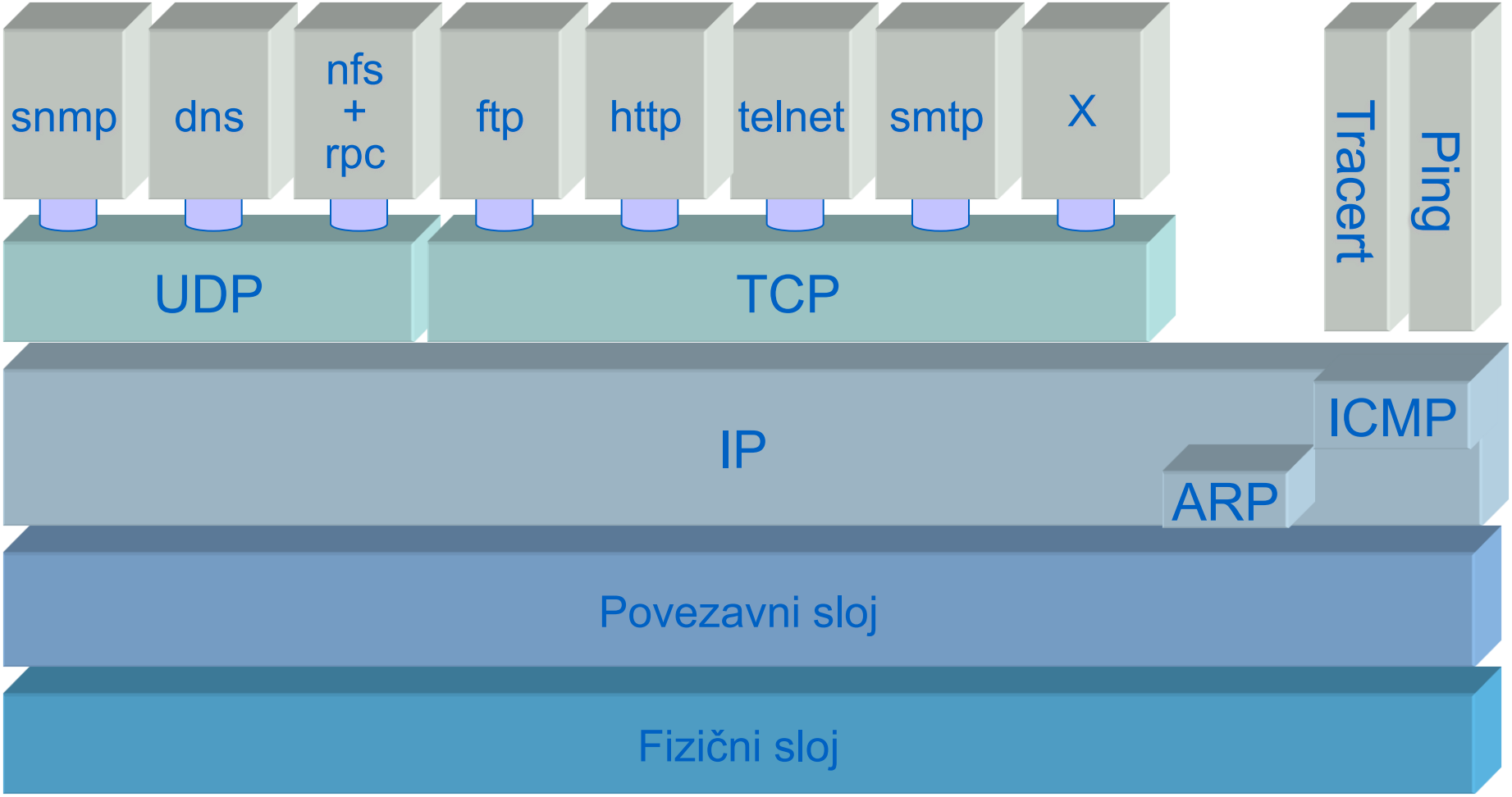
Varnostne storitve v omrežjih IP

Kazalo

- Varnostne storitve
- Varnostni mehanizmi
- Protokol IPSec

Tehnologija Ethernet

Protokoli sklad TCP/IP



Značilnosti tehnologije Ethernet

- Tehnologija razvita za okolja LAN
- Deluje po princip ˝Plug and Play˝
  - nič ni potrebno nastaviti, vse se zgodi avtomatsko ☺
- Odprt storitveni model
  - vsak lahko komunicira z vsakim
  - za vse uporabnike se predvideva, da so legitimni
  - ni avtentikacije oddajnika in sprejemnika
    - brez preverjanja izvornih in ponornih naslovov MAC
  - ni enkripcije prenosnega kanala Ethernet
- Podatkovna in kontrolna ravnina združeni
  - stikalo Ethernet zgradi tabelo MAC na osnovi posredovalne funkcije
- Ethernet napadi
  - poplavljanje tabel MAC
  - zastrupljanje tabel ARP
  - napadi na kontrolne mehanizme STP, RSTP, MSTP

Okvir Ethernet in 802.3

- **Preamble – niz potreben za sinhronizacijo (1010 ...)**
  - **združljivost za nazaj – 10 Mbit Ethernet (asinhron)**
  - **SFD (Start Frame Delimiter) – konec sinhronizacije (niz 10101011)**
- **Destination/source**
  - **ciljni/izvorni naslov MAC**
- **Length/Type**
  - **vrednost manjša od 600 HEX – polje Length**
  - **vrednost enaka ali večja od 600 HEX - polje Type**
  - **0800HEX = IPv4, 806HEX = ARP**
- **PAD – polnilni biti**
- **FCS – polje za zapis izračunane vrednosti CRC**

Okvir IEEE 802.3

Preamble 7	SFD 1	Destination 6	Source 6	Length/ Type 2	Data 46 do 1500	Pad	FCS 4

Okvir Ethernet II – DIX v2

preamble 8	destination 6	source 6	Type 2	Data 46 do 1500	Pad	FCS 4

Protokol TCP/IP

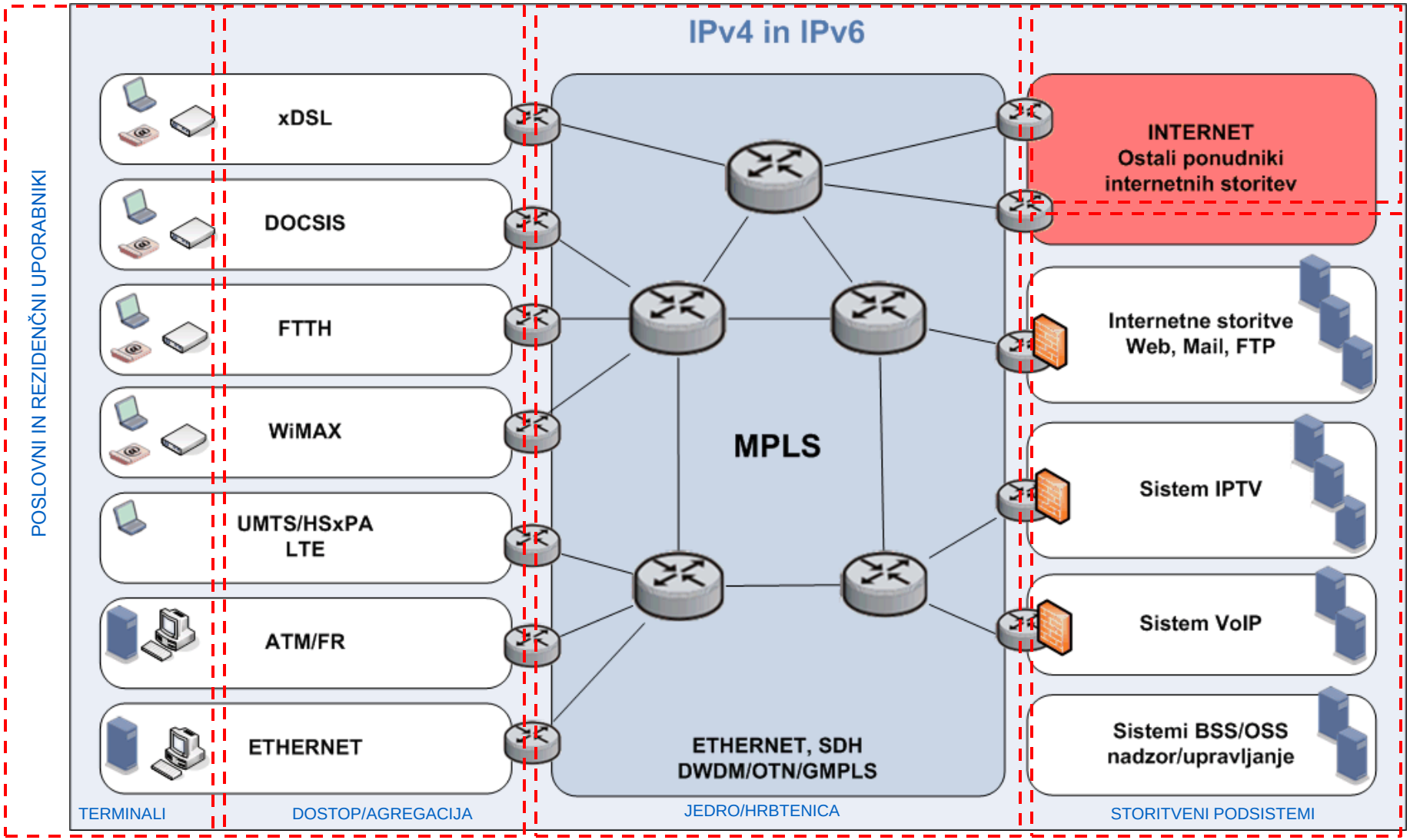
Značilnosti protokolov TCP/IP

- Značilnosti protokola IP
  - odprt storitveni model
    - vsak lahko komunicira z vsakim
    - za vse uporabnike se predvideva, da so legitimni
    - ni avtentikacije oddajnika in sprejemnika
      - brez preverjanja izvornih in ponornih naslovov
    - ni enkripcije prenosnega kanala IP
- Značilnosti protokola UDP
  - enak princip delovanja kot IP
- Značilnosti protokola TCP
  - vzpostavitev zveze
  - brez varnostnih mehanizmov
- Napadi na TCP/IP
  - DoS (ICMP poplavljanje, TCP syn, UDP flood)
  - prisluškovanje komunikacijskemu kanalu
  - IP spoofing
  - napadi na DHCP, poplavljanje ARP

Glava paketa IPv4

0	4	8	16	24	31
Ver	IHL	Type of service	Total lenght		
Identification			Flags	Fragment offset	
TTL		Protocol	Header checksum		
Source address					
Destination address					
Options				Padding	

Sodobna omrežja



Pasti javnih omrežij

- Prisluškovanje komunikacijskemu kanalu in prestrezanje informacij
  - sniffing, snooping
- Ponarejanje informacij
- Pretvarjanje
  - spoofing
- Onemogočanje uporabe virov omrežja
  - Denial of service, DDoS
- Nepooblaščena uporaba virov omrežja
- Nepooblaščeno razkrivanje informacij
- Delitev nevarnosti:
  - notranje
    - 80 % vdorov se zgodi znotraj omrežja (Computer Security Institute – 2002)
  - zunanje

Koncept zagotavljanja varnosti

- **V fizičnem svetu:**
- **V elektronskem svetu:**

V fizičnem svetu		V elektronskem svetu
osebni dokument s sliko, geslo, podpis	← overjanje integriteta →	tehnike digitalnega podpisovanja, certifikati, gesla, zgoščevalne funkcije
zaupni pogovori, zapečatena pisma	← zasebnost →	šifriranje
ključavnice, video nadzor	← omejevanje dostopa →	filtriranje prometa, sistemi AAA
ograja, vrata, ključavnica	← naprave →	stikalo, usmerjevalnik, požarni zid, sistem IDS

Varnostne storitve

- Avtentikacija uporabnikov, naprav/aplikacij (Authentication)
  - zajamči točnost izvora podatkov z vidika, kdo in od kod
- Nadzor dostopa (Access Control)
  - preprečuje neavtoriziran dostop do omrežnih virov/storitev
- Zaupnost/zasebnost podatkov (Confidentiality)
  - preprečuje prebiranje in kopiranje podatkov, ko se prenašajo prek javnega omrežja
- Celovitost/avtentičnost podatkov (Integrity)
  - zagotavlja, da podatki niso bili kakor koli spremenjeni od svojega nastanka
- Nezatajljivost (Non-repudiation)
  - onemogoča zanikanje izvora podatkov ter vključenost v opravljane storitve
- Preprečevanje onemogočanja dostopa do virov in storitev
  - omrežni viri oziroma storitve morajo biti uporabnikom na razpolago vedno, kadar jih ti želijo uporabiti
- Časovni žigi (Timestamping)
- Zagotavljanje avtorskih pravic

Varnostni koncepti v Ethernet in TCP/IP

- Implementacija varnostnih funkcij na omrežnih elementih
  - Filtri na stikalih in usmerjevalnikih – “stateless” filtri
  - Požarne pregrade – “stateful” filtri
  - Proxy naprave in aplikacijski prehodi – emulacija odjemalcev
  - Naprave IDS/IPS – detekcija nelegitimnih omrežnih operacij
- Zaščita na nivoju transportnih protokolov
  - HTTPS, SSH, S-MIME, PGP
  - TLS/SSL
  - IPSec
  - WPA2
- Zaščita vsebin na nivoju aplikacij
  - Sistemi DRM, CA

Kazalo

- Varnostne storitve
- Varnostni mehanizmi
- Protokol IPSec

Kazalo – varnostni mehanizmi

- Uvod
- Enkripcijski algoritmi
- Zgoščevalni algoritmi
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Kriptologija

- Znanost o prevajanju nezaščitenih podatkov v zaščitene in obratno
- Delitev
  - kriptografija
    - metode za šifriranje in zakrivanje podatkov
  - kriptoanaliza
    - metode za razkrivanje šifriranih podatkov

Razvoj kriptografije

- ~ 2000 p. n. št. – Egipčani
- 1970: začetki ˝digitalne˝ kriptografije
  - IBM – g. Feistel
- 1976: dokument ˝New Directions in Cryptography˝
  - g. Diffie in g. Hellman
  - kriptografija na osnovi javnih ključev
- 1977: standard DES (Data Encryption Standard)
- 1978: postopek RSA
  - g. Rivest, g. Shamir in g. Adleman
  - prvi praktično delujoči asimetrični kriptografski postopek
- 1985: ElGamal
- 1991: prvi mednarodni standard za digitalno podpisovanje dokumentov (ISO/IEC 9796)
  - temelji na algoritmu RSA

Cezarjev algoritem

- Premik abecede za določeno število znakov
- Primer: šifriranje ukaza NAPAD (čistopis)

```
ABCČDEFGHIJKLMNOPRSŠTUVZŽ
↓   ↓           ↓  ↓
VZŽABCČDEFGHIJKLMNOPRSŠTU
```

Postopek enkripcije:

$$f(a) \mapsto (a-k) \bmod 25$$

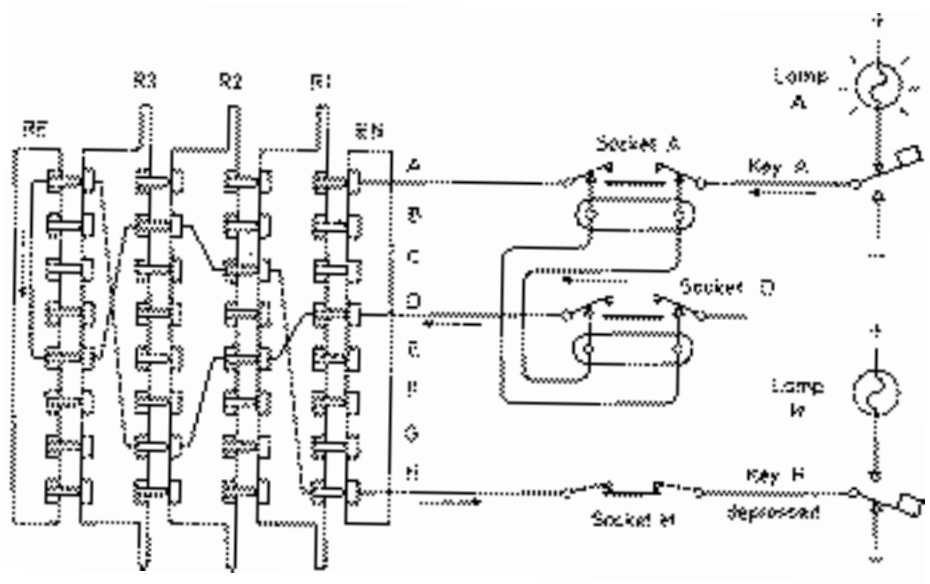
KVMVB

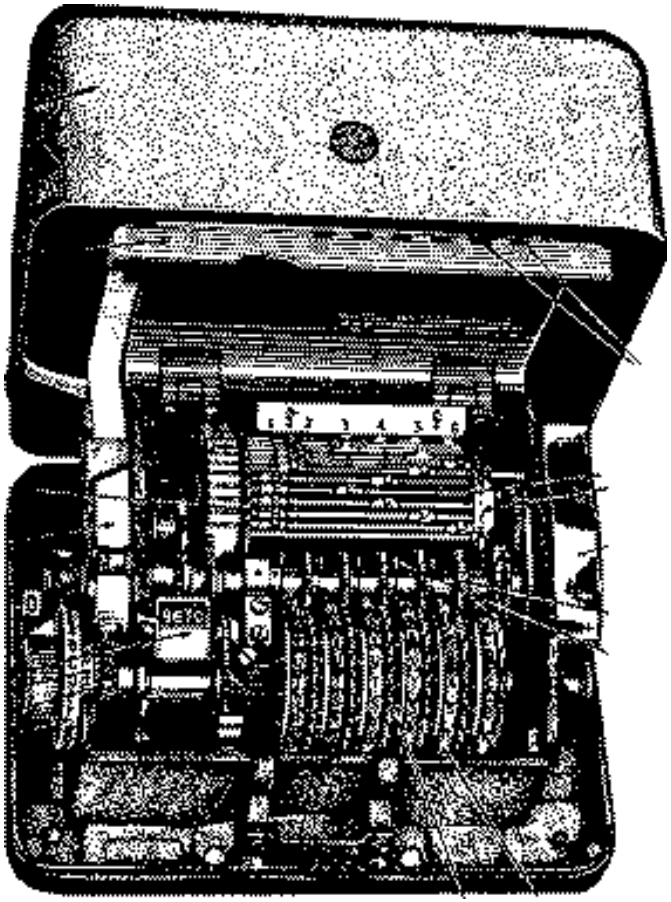
(kriptogram)

ključ: $k = 3$

- Vaja: šifrirajte svoje IME in PRIIMEK

Enigma Rotor Machine

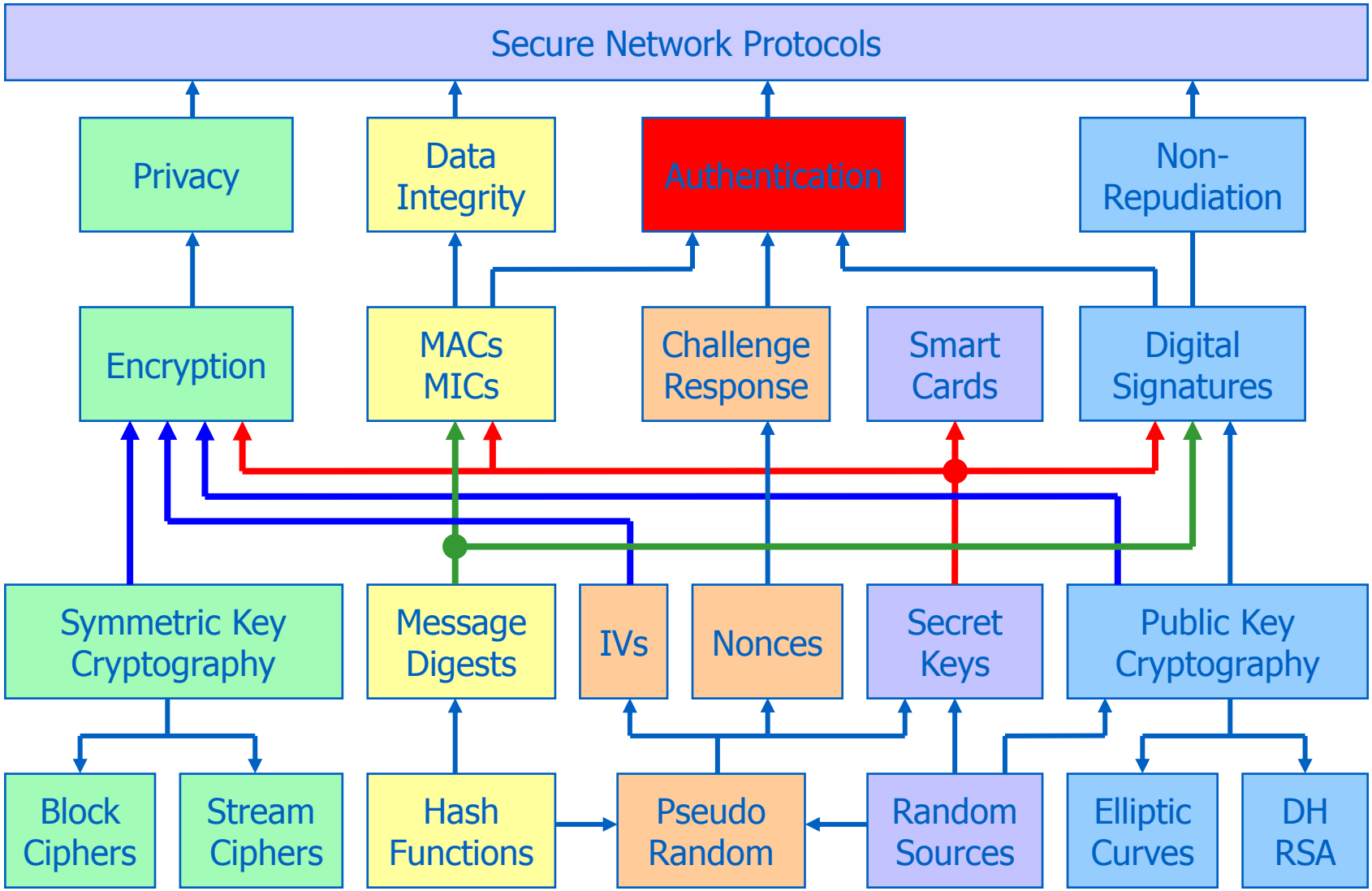




Delitev varnostnih mehanizmov

- Mehanizmi za enkripcijo
  - simetrični
  - asimetrični
  - hibridni
- Mehanizmi za zagotavljanje celovitosti
- Mehanizmi za elektronsko podpisovanje
- Mehanizmi za izmenjavo ključev
- Mehanizmi za nadzor dostopa
  - avtentikacija
  - avtorizacija
  - beleženje
- Mehanizmi za zaznavanje vdorov

Delitev varnostnih mehanizmov



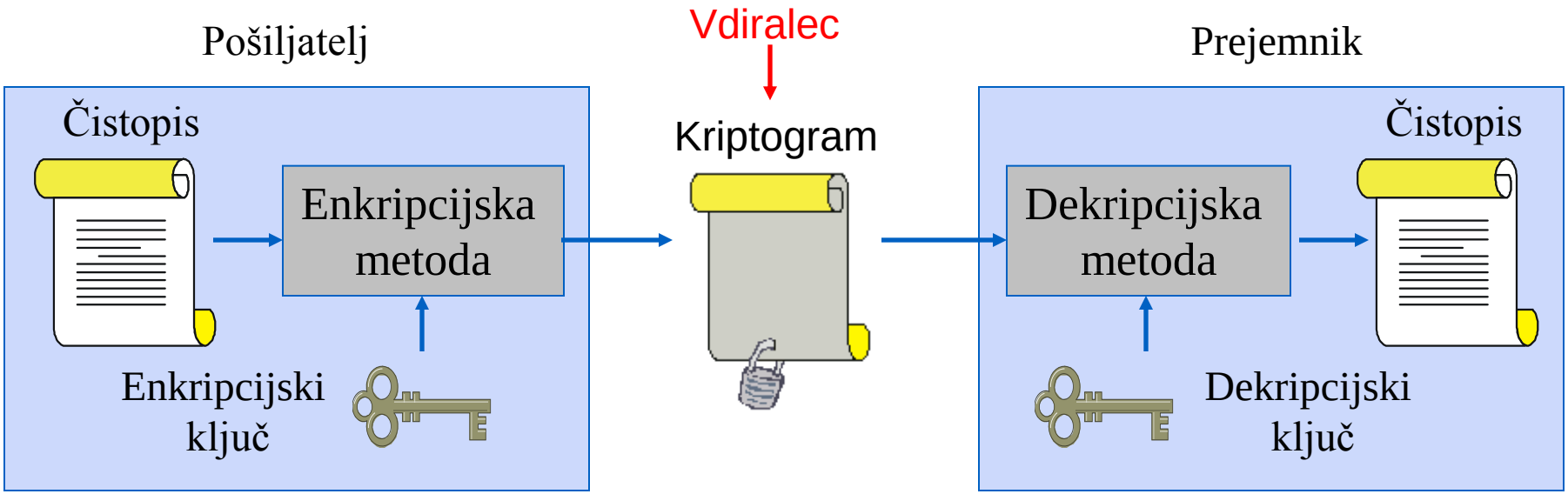
Vir: *Zurcher Hochschule Winterthur*

Kazalo – varnostni mehanizmi

- Uvod
- **Enkripcijski algoritmi**
- Zgoščevalni algoritmi
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Enkripcija

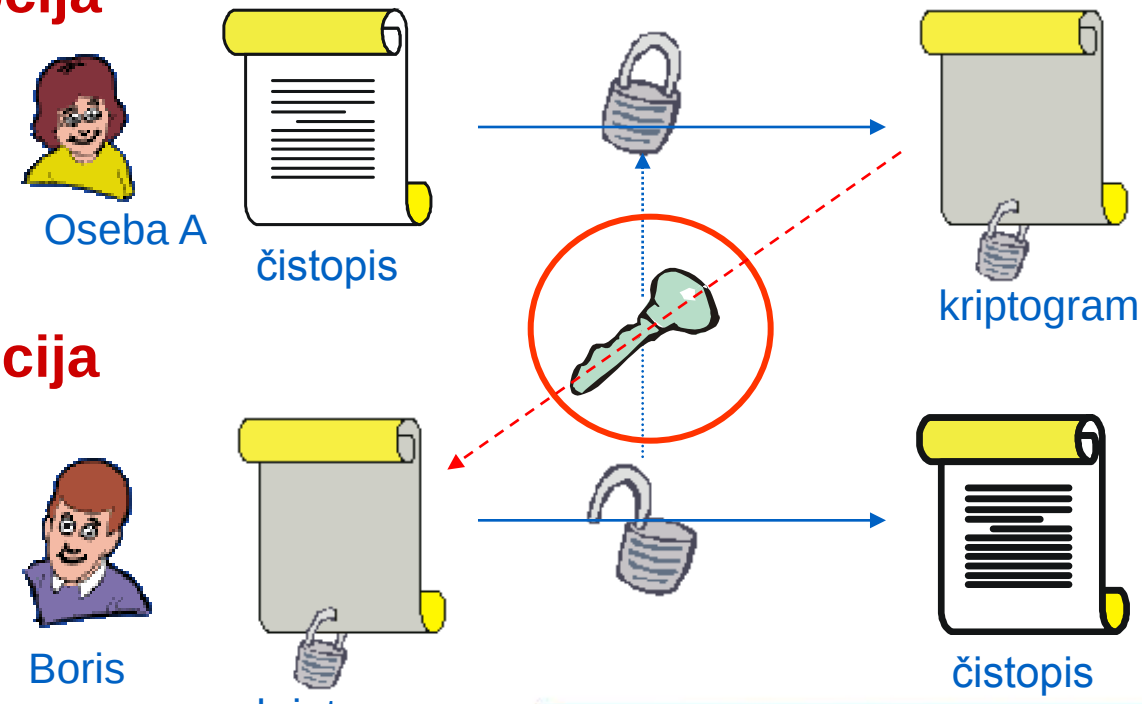
- Enkripcija/šifriranje je spreminjanje berljivih podatkov ˝čistopis˝ v obliko ˝kriptogram˝, ki onemogoča njihovo razumevanje
- V preteklosti so bile enkripcijske metode tajne
- Danes uporabljane enkripcijske metode so javne, stopnja zaščite je odvisna le od dolžine ključa



Simetrični postopki

- Za komunikacijo med dvema osebama se uporablja samo en ključ
  - enak ključ za enkripcijo in dekripcijo
- Ključ mora pošiljatelj podatkov na varen način posredovati naslovniku

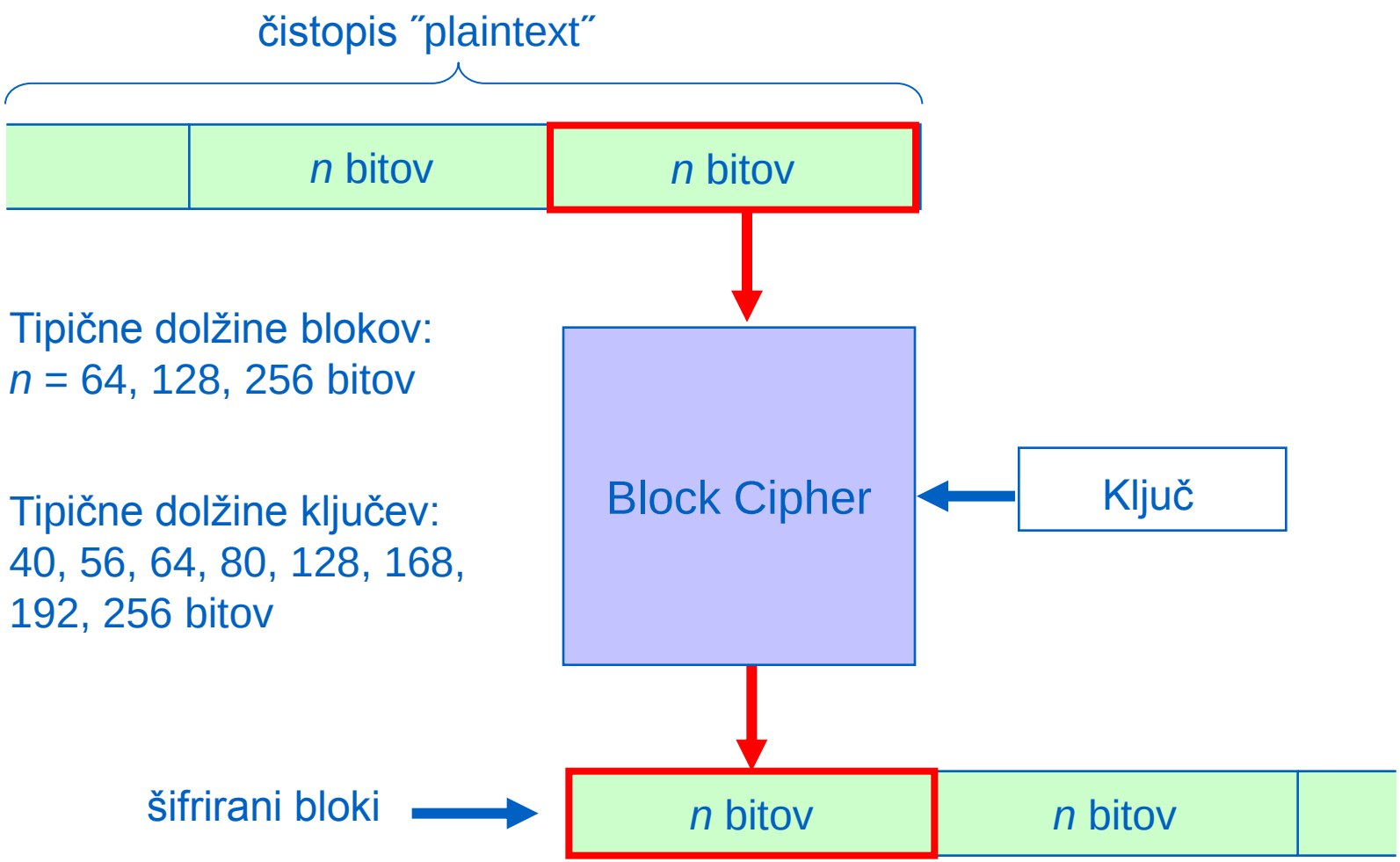
1. Enkripcija



2. Dekripcija

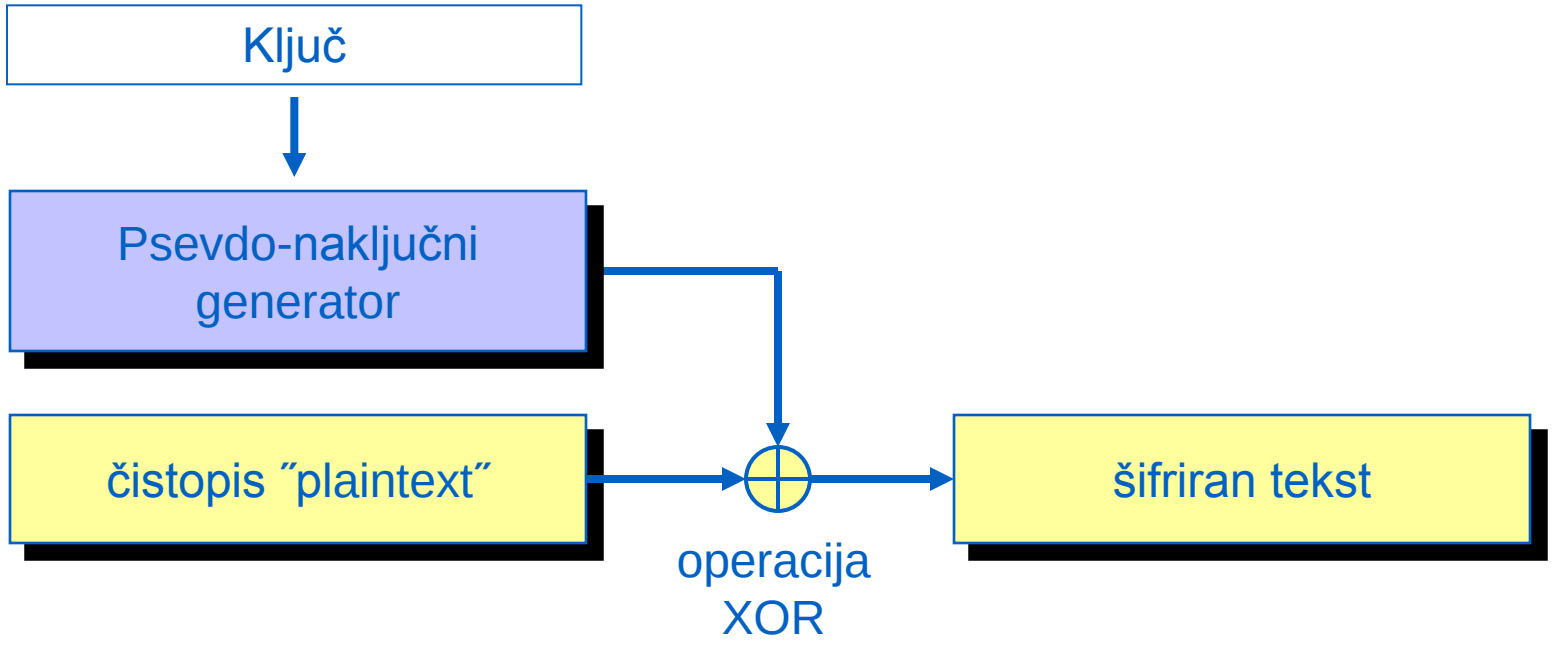
Simetrični postopki – Block Cipher

- **Princip delovanja**



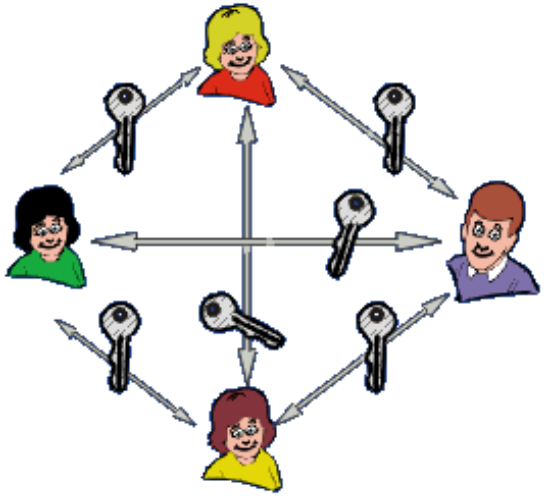
Simetrični postopki – Stream Cipher

- **Princip delovanja**

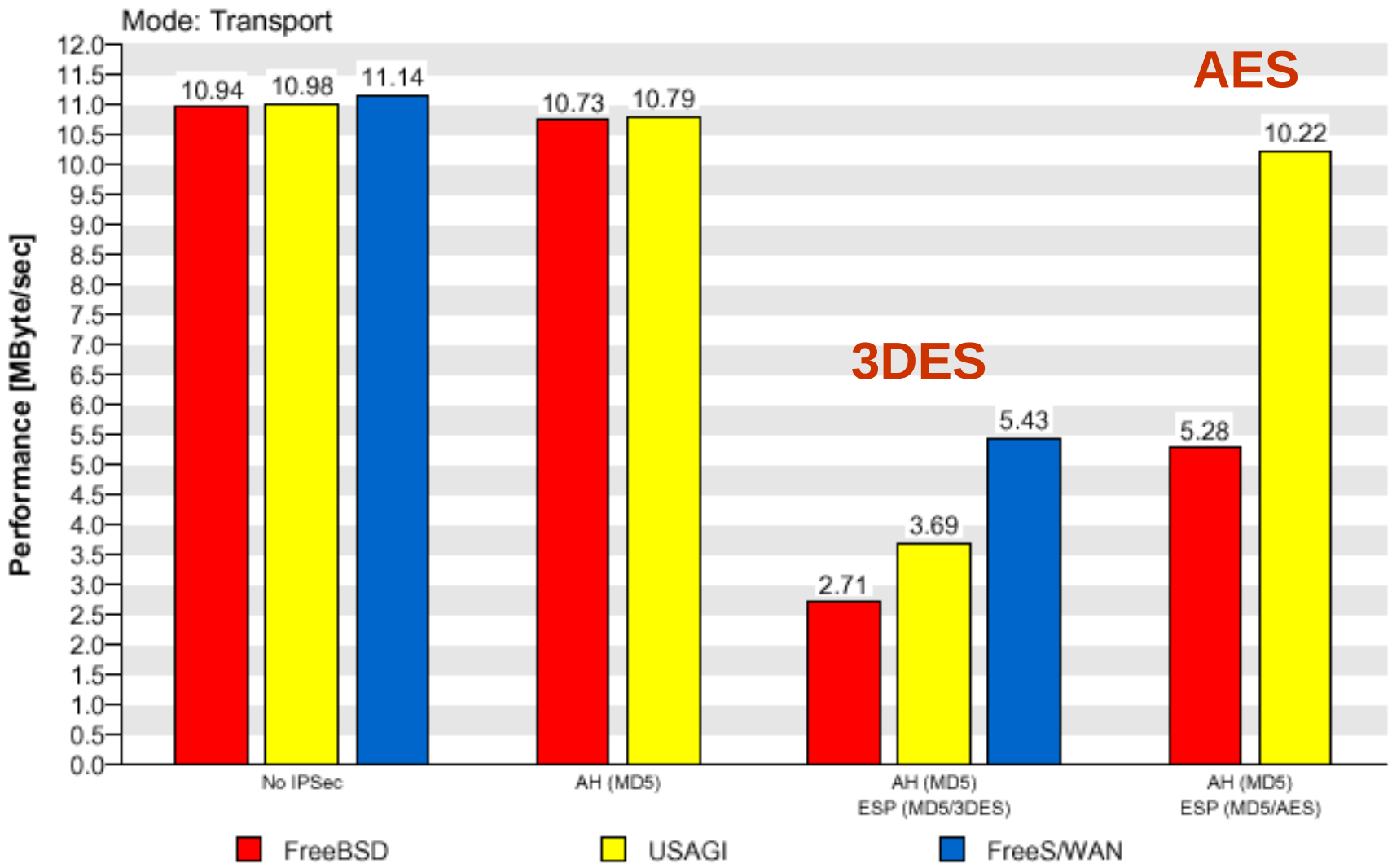


Lastnosti simetričnih postopkov

- **Prednosti**
  - hitrost
- **Slabosti**
  - težave z “varno” izmenjavo ključa med pošiljateljem in naslovnikom
  - kopičenje ključev: drugačen ključ za vsakega novega “sogovornika”
- **Primeri algoritmov**
  - DES (Data Encryption Standard)
    - dolžina ključa 56 bitov
  - 3DES
    - dolžina ključa 168 bitov (učinkovita 112 bitov)
  - AES (Advanced Encryption Standard)
    - dolžina ključa 128, 192, 256 bitov
  - RC2, RC4, RC5 (Rivest’s Cipher)
    - variabilna dolžina ključev
  - IDEA (International Data Encryption Algorithm)
    - dolžina ključa 128 bitov
  - enkratni ščit (velikost ključa enaka dolžini podatkov)



Primerjava algoritmov 3DES in AES



Vir: C. Karg, Research Establishment for Applied Science
http://www.dodccrp.org/Activities/Symposia/7thICCRTS

Asimetrični postopki

- Kriptografija z javnim ključem
- ˝Odpravlja˝ problem varne izmenjave ključev in kopičenja ključev simetričnega šifriranja
- Razvila sta ga Diffie in Hellman, algoritem je javno dostopen od leta 1976
- Enkripcijski in dekripcijski ključ sta različna
  - javni ključ uporabljen za šifriranje
  - zasebni ključ uporabljen za dešifriranje

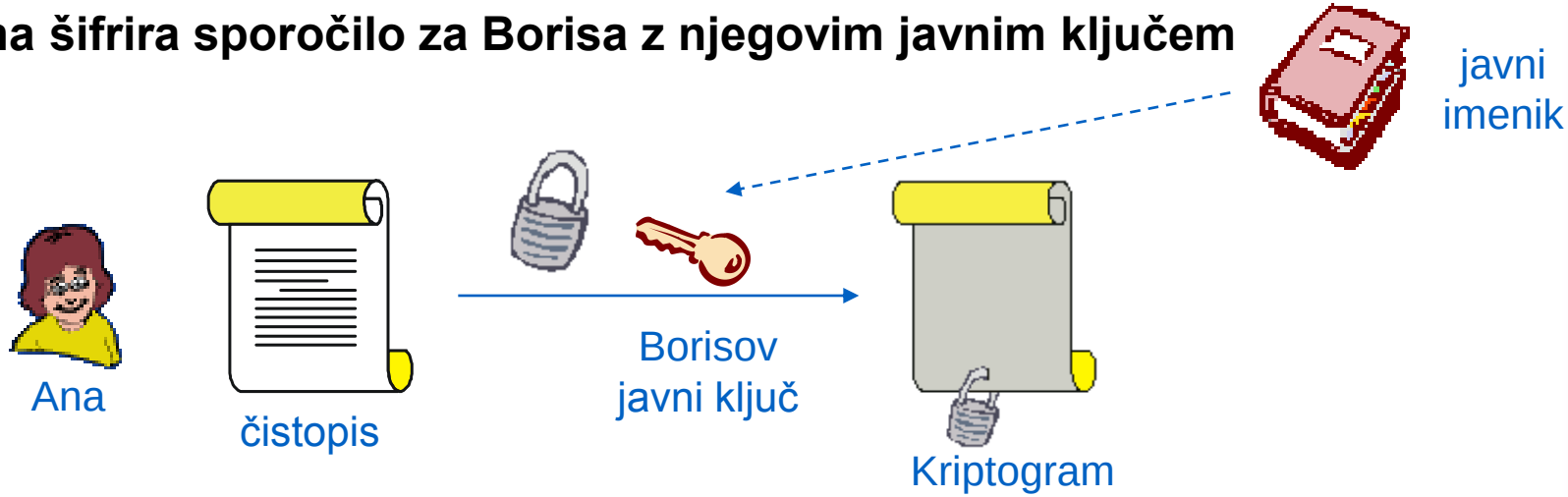
par ključev za enkripcijo

javni ključ
za enkripcijo

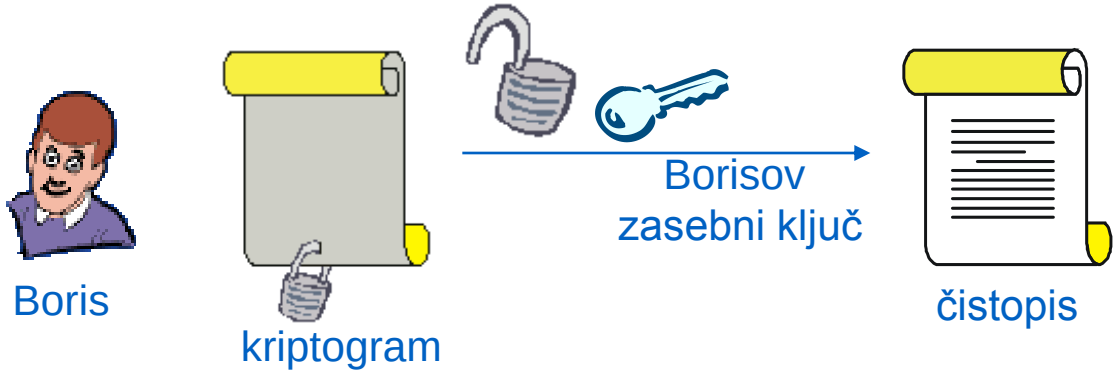
zasebni ključ
za dekripcijo

Asimetrični postopki

- **Postopek šifriranja**
  - **Ana šifrira sporočilo za Borisa z njegovim javnim ključem**



- **Postopek dešifriranja**
  - **Boris dešifrira sporočilo s svojim zasebnim ključem**



Lastnosti asimetričnih postopkov

- Ključa sta enoumno povezana
- Če poznamo javni ključ, je praktično nemogoče matematično izračunati zasebnega
- Vsak posameznik ima svoj par ključev, od katerih je eden javni, drugi pa zasebni
- Ključa izvajata inverzni operaciji
  - eden enkripcijo, drugi dekripcijo
- Če je en ključ v paru uporabljen za enkripcijo, potem ne more biti isti ključ uporabljen tudi za dekripcijo

Lastnosti javnega in zasebnega ključa

- Lastnosti javnega ključa
  - javno dostopen
  - vedno je povezan z določeno osebo/terminalom/aplikacijo
    - lastnikom para ključev
  - ponavadi je objavljen v javnem imeniku
- Lastnosti zasebnega ključa
  - ima ga samo lastnik
  - vedno je povezan z določeno osebo/terminalom/aplikacijo
    - lastnikom para ključev
  - lastnik je odgovoren skrbeti za varno hranjenje ključa
- Primeri
  - Diffie-Hellman
    - dolžina ključa 512, 768, 1024, 2048
  - RSA
    - dolžina ključa 512, 1024, 2048, 3072, 4096
  - algoritmi na osnovi eliptičnih krivulj
    - dolžina ključa 112, 160, 224, 256, 384, 512

Primerjava postopkov

- **Simetrični postopki**
  - hitrost
  - primerni za zaščito lokalno shranjenih podatkov
  - težave z izmenjavo ključev
  - število ključev narašča z $N(N-1)/2$
    - problem N^2
- **Asimetrično postopki**
  - enostavna izmenjava ključev
  - število ključev narašča linearni
  - počasnost
  - kompleksnost algoritmov
  - problem generiranja naključnih praštevil

Primerjava dolžine ključev 1/2

- Priporočilo – RSA Laboratories (6 maj, 2003)
  - tehnologija iz leta 1996 (vredna 10 M $) je omogočala razbiti 56 bitni ključ DES v 6 minutah
  - tehnologija iz leta 2003 (vredna 10 M $) je omogoča razbiti 56 bitni ključ DES v 14 sekundah
    - Moor-ov zakon – hitrost strojne obdelave/$ se podvoji vsakih 18 mesecev
- Primerjava dolžine asimetričnih in simetričnih ključev (algoritma RSA in DES)
  - 1024-bitni asimetrični ekvivalenten 80-bitnem simetričnem
    - uporaben za podatke, ki potrebujejo učinkovito zaščito do leta 2010
  - 2048-bitni asimetrični ekvivalenten 112-bitnem 3DES
    - uporaben za podatke, ki potrebujejo učinkovito zaščito do leta 2030
  - 3072-bitni asimetrični ekvivalenten 128-bitnem simetričnem
    - uporaben za podatke, ki potrebujejo učinkovito zaščito po letu 2030

Primerjava dolžine ključev 2/2

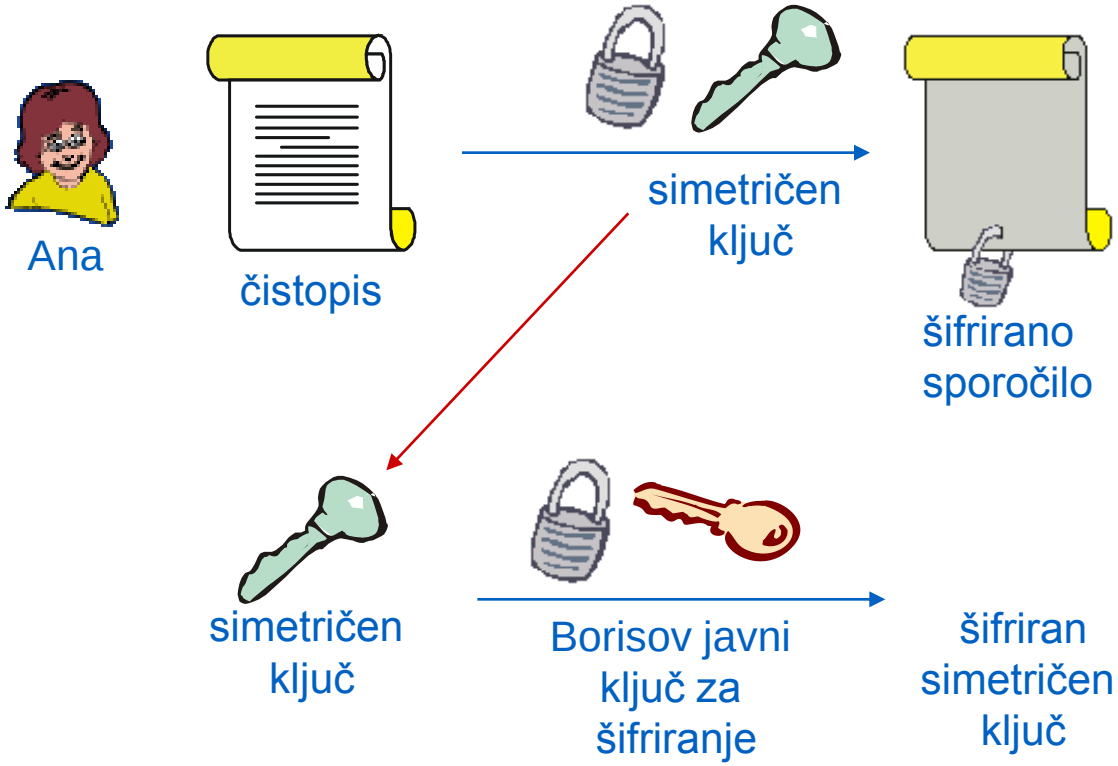
Postopek/dolžina ključa	K[bit]	K[bit]	K[bit]	K[bit]	K[bit]	K[bit]
Simetrični	56	80	112	128	192	256
Asimetrični (RSA)	512	1024	2048	3072	7680	15360
Asimetrični (na osnovi eliptičnih krivulj)	112	160	224	256	384	512
Razmerje RSA/eliptični	5:1	6:1	9:1	12:1	20:1	30:1

Hibridni postopki

- Kombinacija simetričnih in asimetričnih postopkov
- Za enkripcijo se uporablja simetrični postopek (hitra enkripcija)
- Za izmenjavo ključev simetričnega postopka pa se uporablja asimetrični postopek (varna izmenjava ključev)
- Primer uporabe:
  - PGP (Pretty Good Privacy)

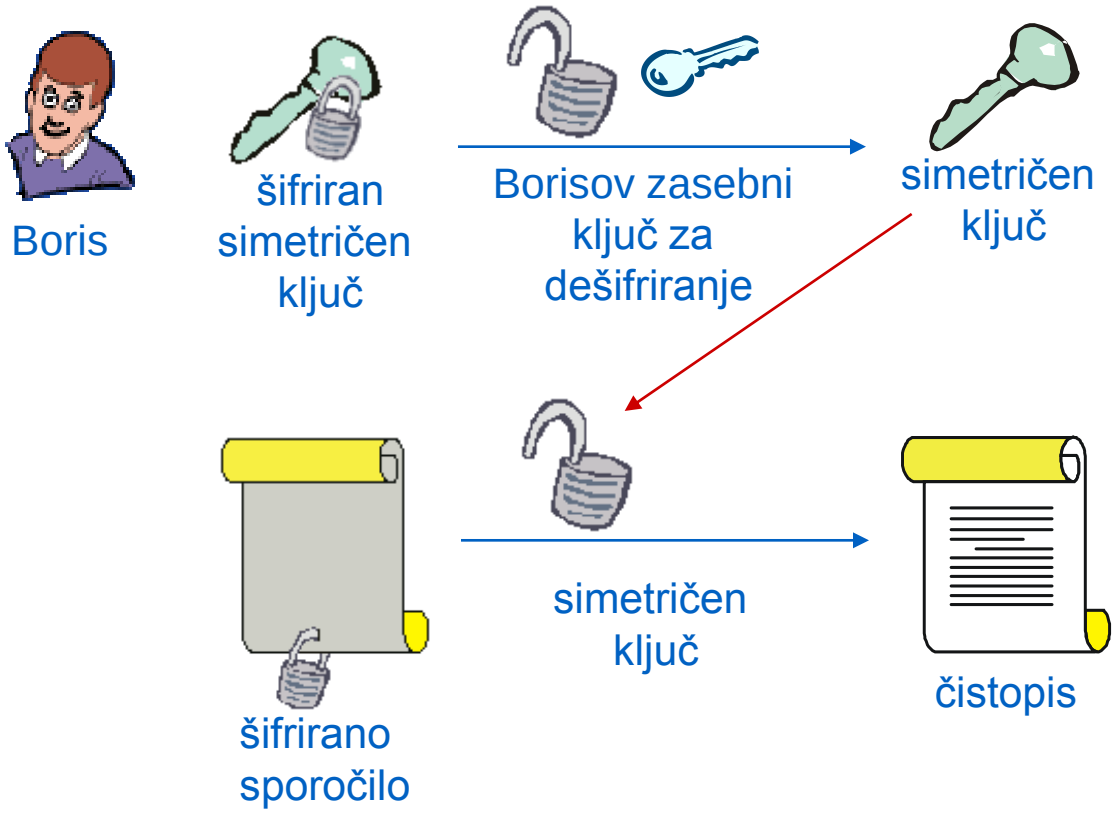
Hibridni postopki 1/2

- **Šifriranje**
  - **Ana šifrira sporočilo za Borisa s simetričnim ključem**
  - **simetričen ključ šifrira z Borisovim javnim ključem**
  - **Ana pošlje Borisu šifrirano sporočilo in šifriran simetrični ključ**



Hibridni postopki 2/2

- **Dešifriranje**
  - **Boris dešifrira simetričen ključ s svojim zasebnim ključem**
  - **z dešifriranim simetričnim ključem dešifrira sprejeto sporočilo**



Algoritem Diffie-Hellman

- **Omogoča varno izmenjavo tajnega ključa brez predhodno izmenjanih skrivnosti**
  - **algoritem definira dva parametra *p* in *g*, ki sta javna**
    - ***p* – praštevilo**
    - ***g* – celo število manjše od p; za vsak *n* = [1, ..., *p*-1] mora obstajati število *k*, da velja enačba** $n = g^k \bmod p$
- **Ranljiv na napad ˝man-in-the-middle˝**

Uporabnik A		Uporabnik B
	Nezaščiten prenosni kanal	
1. Generiranje tajnega ključa A $A \in \{1, \ldots, p-2\}$		Generiranje tajnega ključa B $B \in \{1, \ldots, p-2\}$
2. Izračun javnega ključa X $X = g^A \bmod p$		Izračun javnega ključa Y $Y = g^B \bmod p$
	X → Izmenjava javnih ključev ← Y	
3. Izračun deljene skrivnosti $k = Y^A \bmod p$		Izračun deljene skrivnosti $k = X^B \bmod p$

Kazalo – varnostni mehanizmi

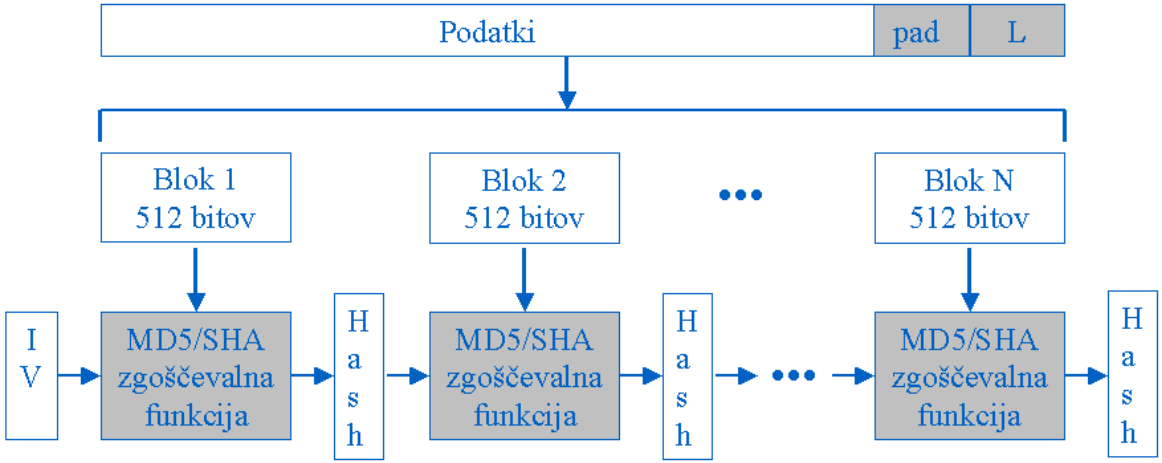
- Uvod
- Enkripcijski algoritmi
- **Zgoščevalni algoritmi**
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Zgoščevalni postopki

- **Zgoščevalni postopek (*One-way Hash Function*) preslika poljubno dolg niz znakov v blok konstantne dolžine, ki predstavlja nekakšen "prstni odtis" oziroma povzetek vhodnega niza (*Message Digest*)**
- **Lastnosti zgoščevalnih postopkov**
  - **nemogoče je najti dve različni sporočili, ki bi ju algoritem preslikal v enak povzetek**
  - **niz podatkov se vedno preslika v enak povzetek**
  - **iz povzetka ni mogoče dobiti originalen, vhodni niz podatkov (od tu ime "*One-way Hash Function*")**
  - **vsaka sprememba vhodnega niza povzroči spremembo povzetka**
- **Najbolj znani zgoščevalni postopki**
  - **MD5 (*Message Digest*)**
  - **SHA-1, SHA-2 (*Secure Hash Algorithm*)**

Blok diagram algoritma HASH

- Vhodne podatke razdelimo na bloke konstantne dolžine
- Zadnji blok dopolnimo do polne dolžine (*padding*)
- Obdelujemo blok za blokom
  - za obdelavo prvega bloka uporabimo zgoščevalno funkcijo in vektor
- Rezultat predstavlja zadnji povzetek (*Hash*)
  - povzetek na izhodu zgoščevalne funkcije je vedno enake dolžine



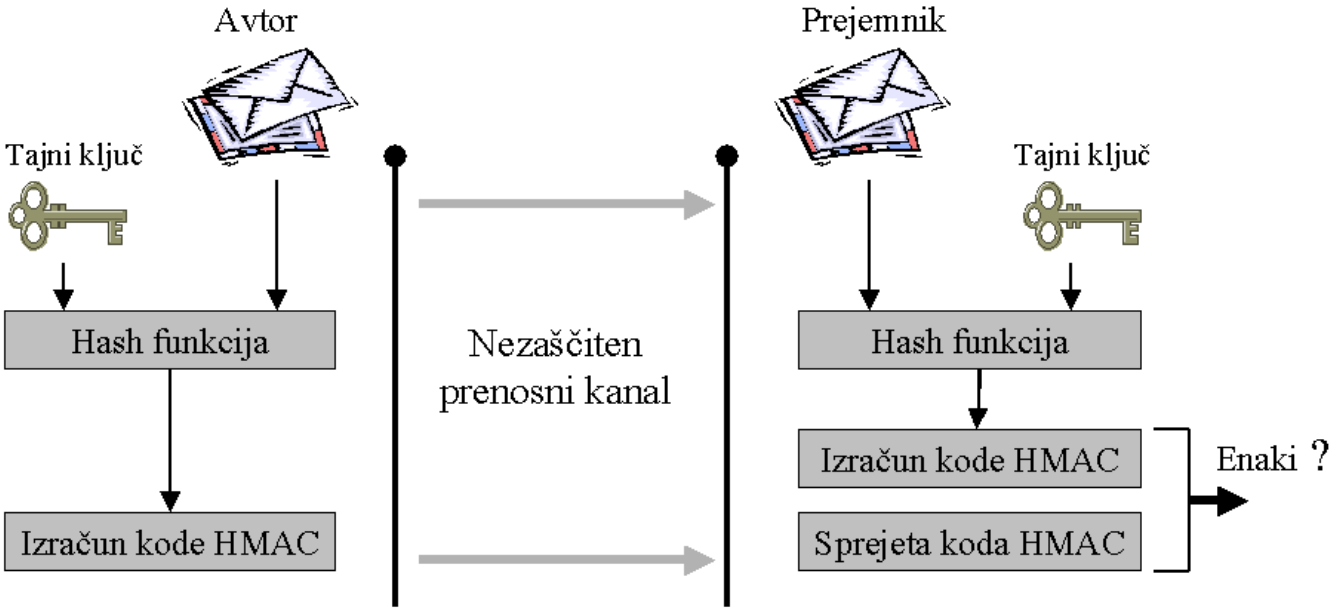
L – Dolžina vhodnih podatkov

Vektor IV – Inicializacijski vektor je standardiziran vhodni niz, katerega dolžina je odvisna od velikosti izhodnega povzetka (128/160/256/384/512 bitov)

Hash – povzetek na izhodu zgoščevalne funkcije (128/160/256/384/512 bitov)

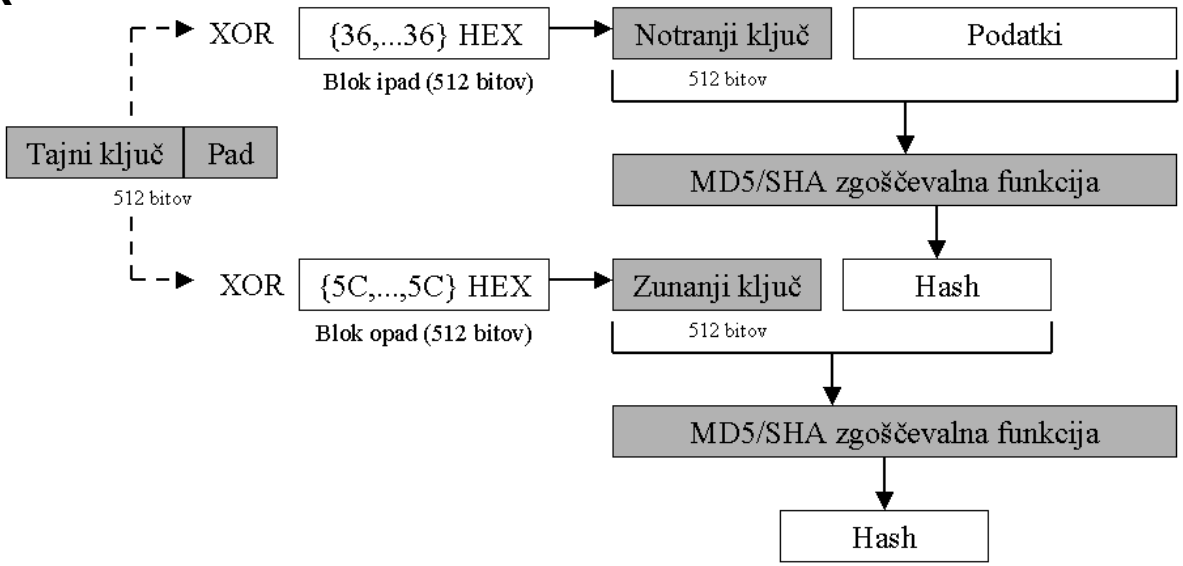
Mehanizemi MAC

- Message Authentication Codes
- Zagotavljajo celovitost podatkov na osnovi tajnega ključa
- Mehanizem HMAC (Hash MAC)
  - mehanizem MAC, ki za svoje delovanje uporablja zgoščevalne funkcije (MD5, SHA-1, SHA-2)
  - HMAC-MD5 oziroma HMAC-SHA-1
- HMAC se uporablja za zagotavljanje celovitosti podatkov



Blok diagram mehanizma HMAC

- **Princip delovanja**
  - **tajni ključ razširimo do dolžine 512 bitov**
  - **z operacijo XOR med tajnim ključem in blokom ipad dobimo notranji ključ**
  - **sestavljen niz obdelamo z zgoščevalno funkcijo**
  - **z operacijo XOR med tajnim ključem in blokom opad dobimo zunanji ključ, ki ga dodamo vmesnemu povzetku**
  - **sestavljen niz ponovno obdelamo z zgoščevalno funkcijo, ki da končni povzetek**



Kazalo – varnostni mehanizmi

- Uvod
- Enkripcijski algoritmi
- Zgoščevalni algoritmi
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Digitalni/elektronski podpis

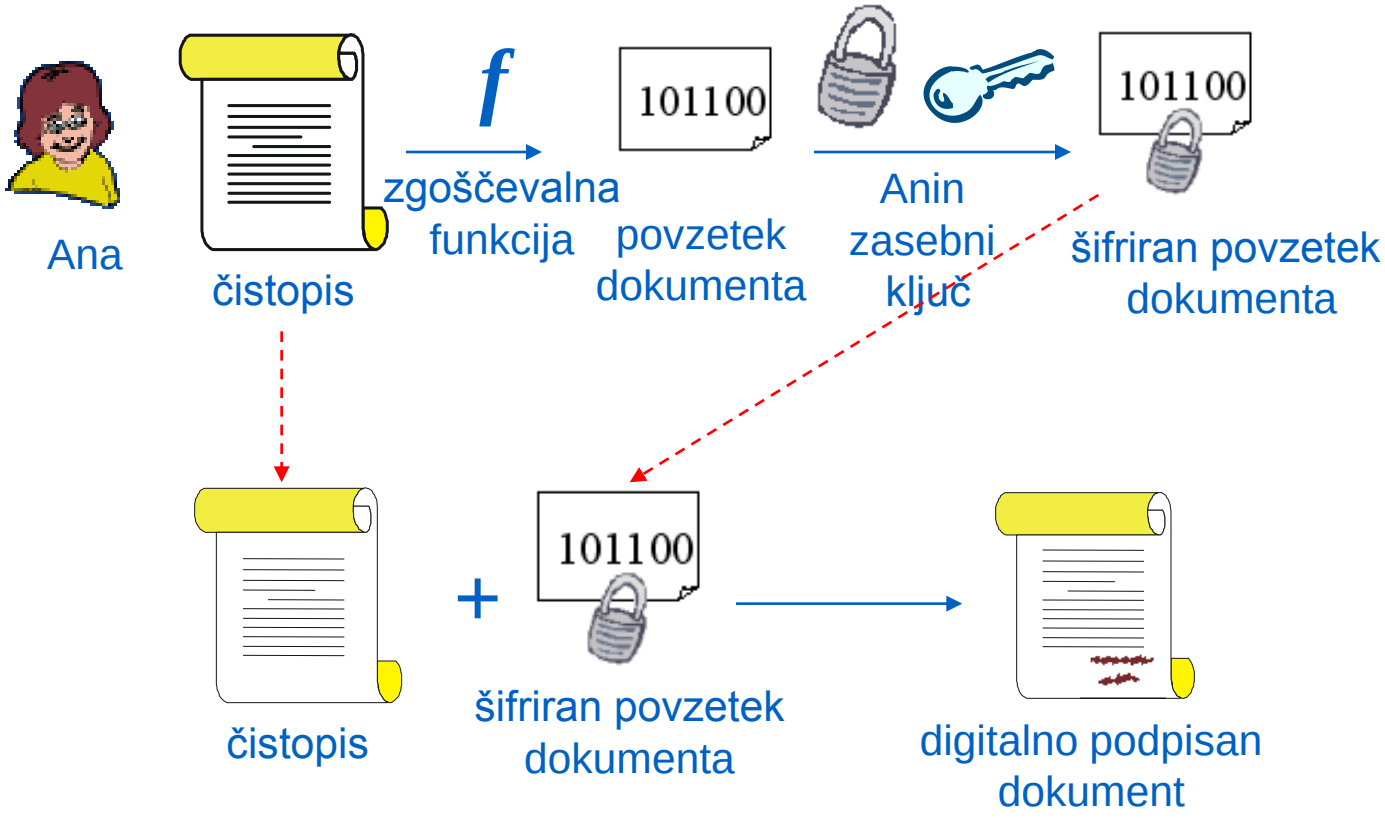
- Povzetek dokumenta (HASH) šifriran z avtorjevim zasebnim ključem (asimetrični postopek)
- Elektronski podpis omogoča:
  - overjanje
    - identificira pošiljatelja
  - celovitost
    - možnost identifikacije spremembe od trenutka, ko so podatki digitalno podpisani
  - nezatajljivost
    - podpisovalec svojega podpisa ne more zanikati
  - čas nastanka dokumenta
    - uporaba časovnih žigov
  - digitalni podpis nam ne zagotavlja zasebnosti podatkov
    - potrebna je kombinacija z enkripcijo

Digitalno podpisovanje 1/3

- **Pri digitalnem podpisovanju uporabimo postopek asimetričnega šifriranja zgoščenih podatkov ravno v obratnem vrstnem redu**
  - **izkorišča lastnosti šifriranja z javnim ključem, ki omogoča, da podatke šifriramo tudi z zasebnim ključem in dešifriramo z javnim ključem**
  - **izračunamo povzetek podatkov (zgoščevalni algoritem)**
  - **povzetek podatkov podpisovalec šifrira z lastnim zasebnim ključem → digitalni podpis**
  - **verodostojnost prejetih podatkov prejemnik preveri z javnim ključem pošiljatelja**

Digitalno podpisovanje 2/3

- **Podpisovanje dokumenta**
  - **Ana naredi povzetek dokumenta in ga šifrira s svojim zasebnim ključem**
  - **čistopis z dodanim šifriranim povzetkom predstavlja digitalno podpisan dokument**



Digitalno podpisovanje 3/3

- **Preverjanje digitalnega podpisa**
  - **Boris iz čistopisa izračuna povzetek dokumenta**
  - **iz pripetega povzetka dobi originalni povzetek (dešifriranje pripetega povzetka)**
  - **v primeru enakosti obeh povzetkov je digitalni podpis veljaven**

Hranjenje zasebnega ključa

- Na disku
  - nikoli naj ne bo shranjen na disku v nešifrirani (plain text) obliki
  - šifriran z uporabo varnega gesla
- Na pametni kartici (Smart Card)
- Na napravah TR (Tamper-Resistant)
  - najvišja stopnja varnosti
  - onemogočen dostop do zasebnega ključa (omogočena je le uporaba ključa)
  - tipično se uporabljajo se za hranjenje zasebnih ključev overitelje

Kazalo – varnostni mehanizmi

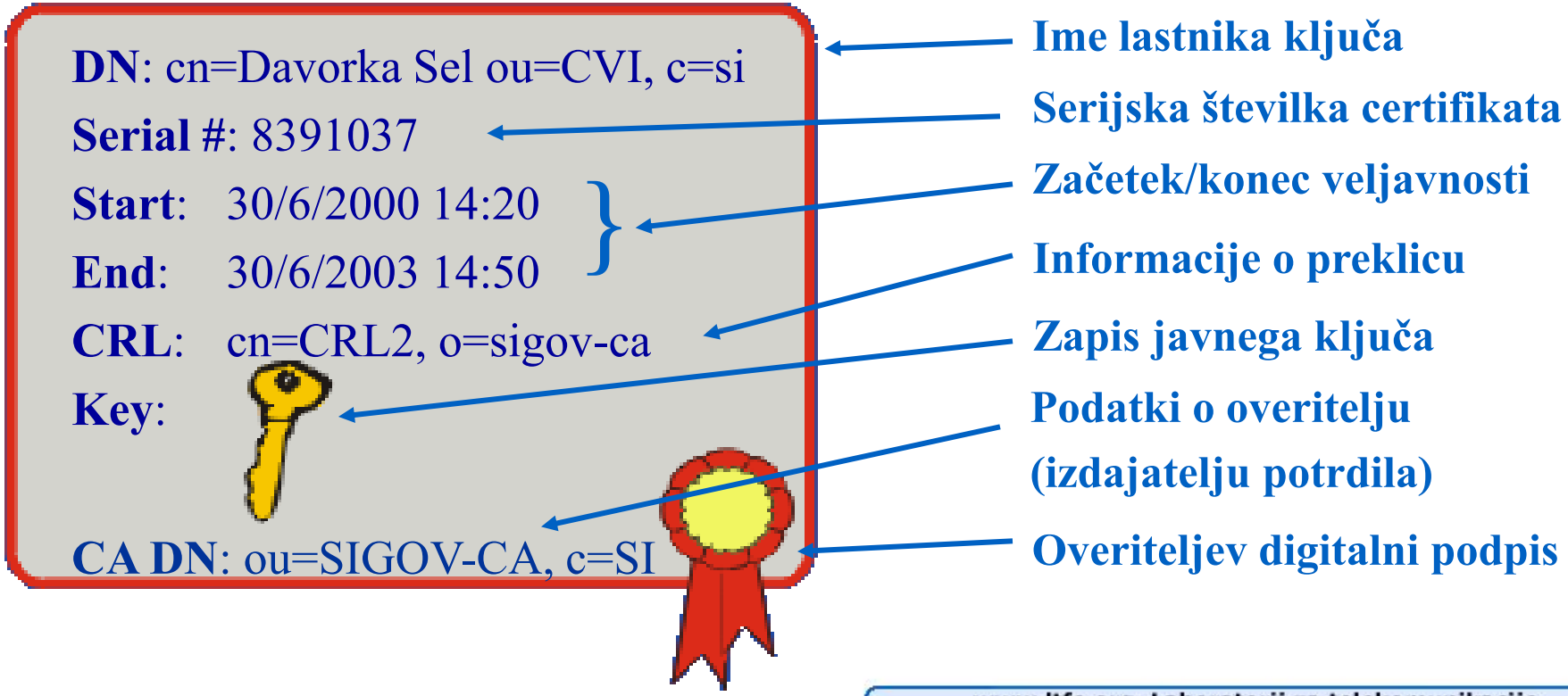
- Uvod
- Enkripcijski algoritmi
- Zgoščevalni algoritmi
- Varna izmenjava ključev
- Digitalni podpis
- Digitalno potrdilo, Sistemi PKI
- Sistemi AAA

Digitalna potrdila 1/3

- Digitalna potrdila (certifikati) zagotavljajo verodostojnost javnih ključev
- ISO/IEC 9594-8/ITU-T Recommendation X.509
- Digitalna potrdila vsebujejo:
  - javni ključ
  - podatke o lastniku javnega ključa
  - podpis overitelja, ki je potrdilo izdalo
  - ostale potrebne parametre
- Overitelj (CA – Certifying Authority, RA – Registration Authority) je ustanova, ki je pooblaščena za izdajanje in upravljanje z digitalnimi potrdili (javnimi ključi)
- Za uporabnike predstavlja točko zaupanja
- Overitelj jamči za istovetnost podatkov v digitalnem potrdilu o imetniku

Digitalna potrdila 2/3

- **Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP)**
  - **člen 15: "Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost."**

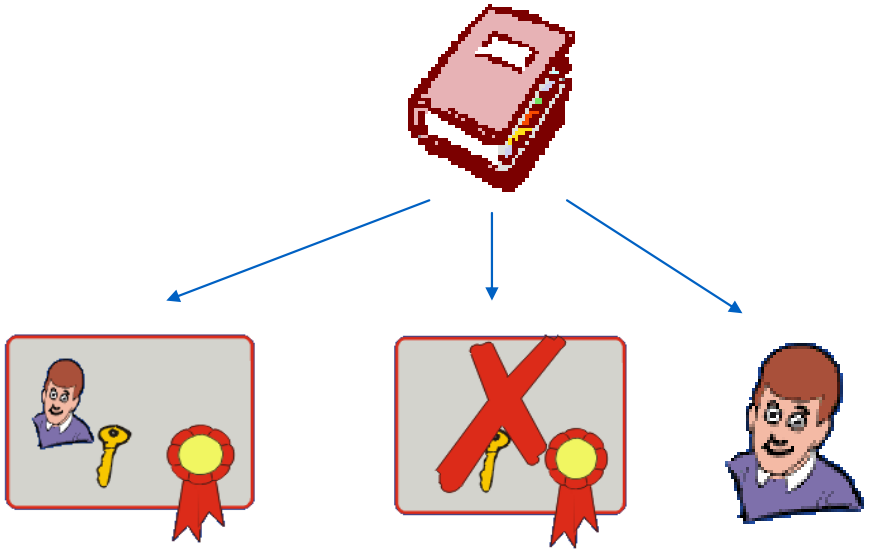


Digitalna potrdila 3/3

- Digitalno potrdilo (javni ključ) omogoča:
  - šifriranje podatkov (šifriranje z javnim ključem)
  - digitalno podpisovanje dokumentov
- S stališča celotnega koncepta varnosti v elektronskem poslovanju nam digitalna potrdila nudijo naslednje varnostne storitve
  - zaupnost, ki je zagotovljena s šifriranjem podatkov
  - overjanje pošiljatelja, zagotovljena z digitalnim podpisom
  - Nezatajljivost lastništva poslane informacije oziroma pošiljatelja
  - celovitost sporočila, kar pomeni, da samo del sporočila ni bil spremenjen ali drugače popravljen brez vednosti pošiljatelja
- Digitalno potrdilo lahko pripada različnim entitetam
  - osebi
  - organizaciji
  - podjetju
  - napravi/aplikaciji

Javni imeniki

- Javni imeniki shranjujejo izdana potrdila
  - pri njih dobimo javni ključ izbranega uporabnika
  - vodijo seznam preklicanih digitalnih potrdil
  - vodijo seznam podatkov o uporabnikih, katerim so izdali digitalna potrdila
    - ime, priimek
    - elektronski naslov
  - vodijo evidenco o politikah delovanja z digitalnimi potrdili



Infrastruktura javnih ključev

- PKI (Public Key Infrastructure)
- Koncept PKI določa
  - vrsto storitev
  - postopke ugotavljanja identitete
  - algoritme in protokole za varno upravljanje z javnimi ključi
  - koncept delovanja overitelja (Certifying Authority, Registration Authority)
- Tipične storitve, ki jih omogoča PKI
  - ugotavljanje istovetnosti entitet
  - izbira/določitev javnega ključa
  - registracija javnih ključev
    - izdaja novih certifikatov
  - preklic izdanih certifikatov
  - overjanje izdanih certifikatov

Kazalo

- Varnostne storitve
- Varnostni mehanizmi
- **Protokol IPSec**

Umestitev protokola IPSec

- **Aplikacijski sloj**
  - **SSH, PGP, S/MIME, Kerberos**
- **Transportni sloj**
  - **SSL, TLS, WTLS**
- **Omrežni sloj**
  - **IPSec**
- **Povezavni sloj**
  - **CHAP, PPTP, L2TP, WEP (WLAN)**
- **Fizični sloj**
  - **Frequency Hopping, HW šifriranje**

Protokoli TCP/IP	
HTTP, SNMP, SMTP, FTP, TFTP, IKE, ...	
TCP	UDP
IP, IPSec	
Ethernet, FR, ATM, PSTN, ...	

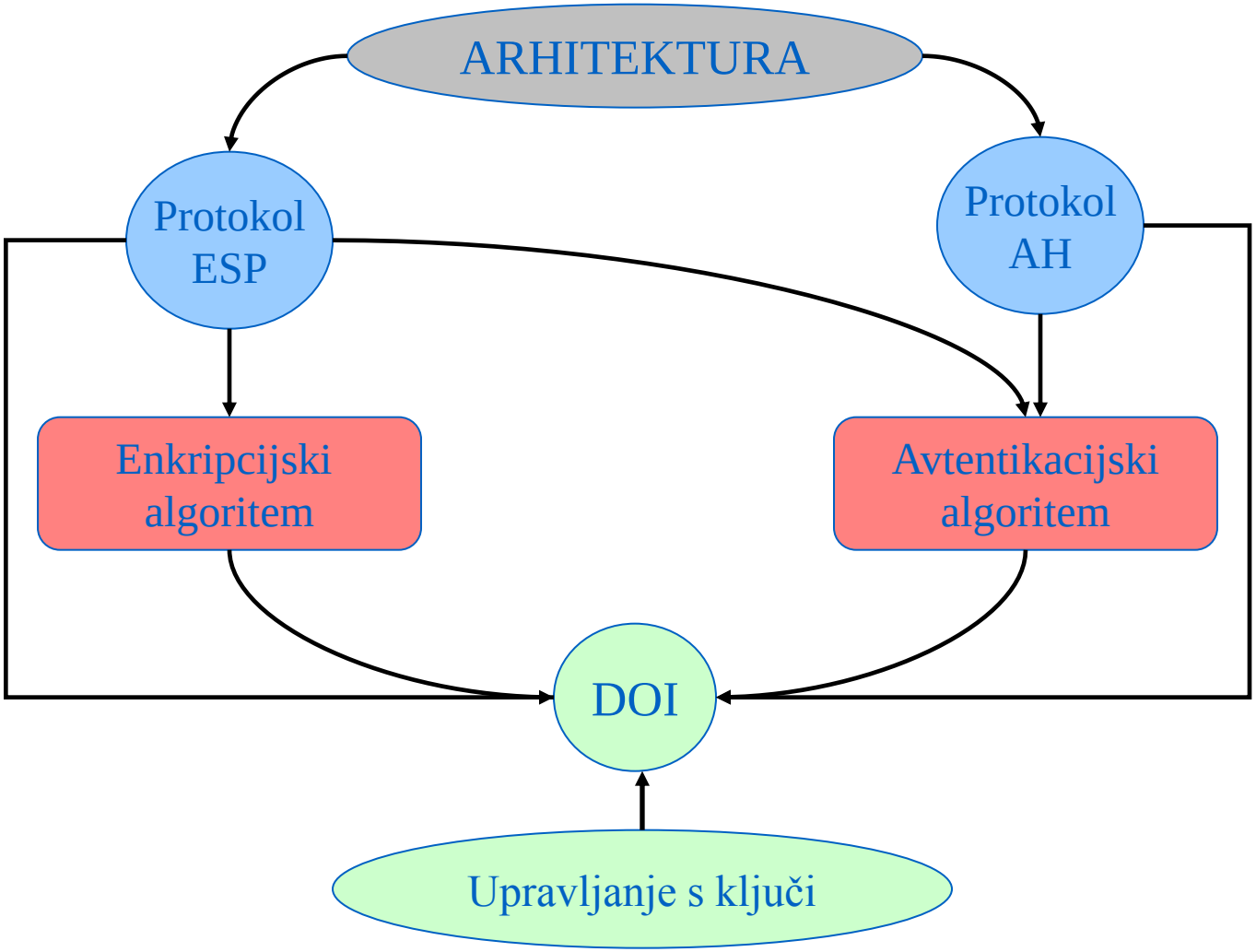
IPSec – Internet Protocol Security

- Začetek razvoja leta 1992 v IETF, kot del standarda IPv6
- Trenutno se vgrajuje v produkte, ki podpirajo IPv4
- Definiran z dokumentom RFC 2401
- Razlogi za IPSec:
  - TCP/IP nima lastnih varnostnih mehanizmov
    - zasebnost
    - celovitost podatkov
    - avtentikacija sodelujočih
- Osnovna vodila razvoja:
  - zagotoviti zaščito podatkov na omrežnem sloju
  - protokol naj bo transparenten za uporabnika in aplikacije
  - temelji naj na znanih kriptografskih mehanizmih
  - dosežen nivo varnosti naj bo odvisen le od uporabljenih kriptografskih mehanizmov
- Ključna aplikacija, za katero se danes uporablja protokol IPSec, so navidezna zasebna omrežja

Varnostne storitve

- Avtentikacija izvora podatkov
- Zaupnost podatkov
- Celovitost podatkov
- Nadzor dostopa
- Delno prekrivanje prometnega pretoka
- Zaščita pred podvajanjem datagramov IP
  - zaščita pred DoS, DDoS
- Dodatna storitev: stiskanje (kompresija) podatkov

Arhitektura



Protokola varnosti

- **Protokol AH (Authentication Header)**
  - **definiran z RFC 2402**
  - **varnostne storitve**
    - **avtentikacija izvora podatkov**
    - **celovitost podatkov**
    - **zaščita pred podvajanjem paketov**

    } **Avtentikacija podatkov** (HMAC-MD5, HMAC-SHA-1 ...)

- **Protokol ESP (Encapsulation Security Payload)**
  - **definiran z RFC 2406**
  - **varnostne storitve**
    - **zaupnost podatkov** → **Enkripcija podatkov** (DES, 3DES ...)
    - **avtentikacija izvora podatkov**
    - **nepovezavna celovitost podatkov**
    - **delno prekrivanje prometnega pretoka**
    - **zaščita pred podvajanjem paketov**

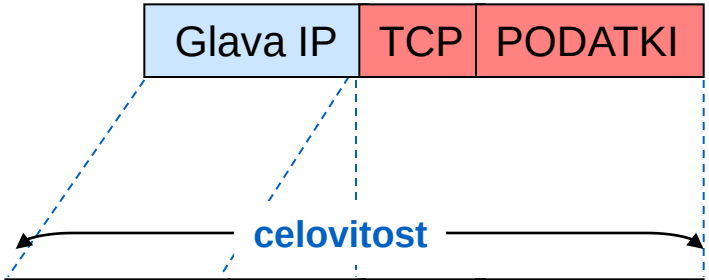
    } **Avtentikacija podatkov** (HMAC-MD5, HMAC-SHA-1 ...)

Varna zveza

- Varna zveza (SA – Security Association)
  - je enosmerna logična povezava med dvema napravama IPSec
  - zagotavlja varnostne storitve prenašanemu prometu
  - varni zvezi nudi varnostne storitve protokol AH ali ESP
    - v okviru ene varne zveze je lahko vzpostavljen le en protokol varnosti!
  - torej, v primeru dvosmerne komunikacije med napravama IPSec sta vzpostavljeni dve varni zvezi
- Varno zvezo definirajo trije parametri:
  - identifikator varnosti (SPI – Security Parameter Index)
  - naslov IP ponorne naprave
  - identifikator protokola varnosti (identifikator protokola AH oziroma ESP)
- Tipi varnih zvez oziroma prenosni načini:
  - transportni način – zaščiti podatke višje ležečih protokolov
  - tunelski način – zaščiti celoten paket IP

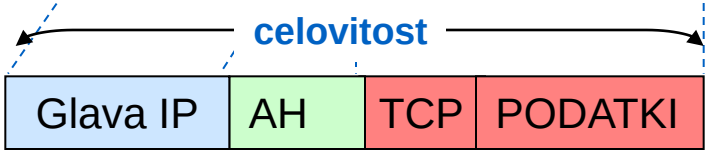
Prenosni načini

Originalni paket IP

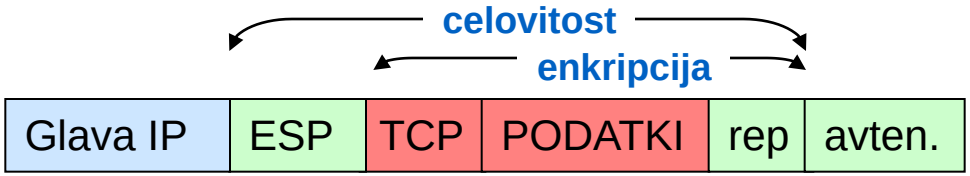


Transportni način

Protokol AH



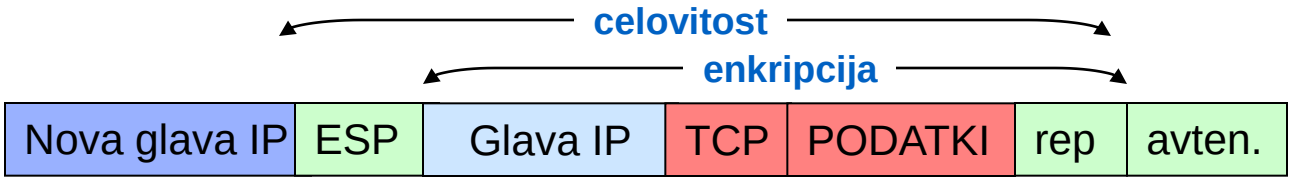
Protokol ESP



Tunelski način

Protokol AH

Protokol ESP



Naprave IPSec

- Terminali – so izvori in ponori prometa
- Varnostni prehodi – prenašajo in usmerjajo promet
- Med dvema gostiteljema je možen transportni in tunelski način prenosa

- Tunelski način prenosa je vedno obvezen, kadar je vsaj eden izmed udeležencev varne zveze varnostni prehod

Upravljanje varnih povezav

- Ročno vnesemo potrebne parametre oziroma dogovorjene vrednosti
  - identifikator varnosti, uporabljene protokole in algoritme, ključe za avtentikacijo in enkripcijo
- Avtomatsko s protokolom IKE (Internet Key Exchange)
  - definiran z RFC 2409 (v postopku standardizacije je IKEv2)
  - namenjen je za:
    - vzpostavljanje, vzdrževanje in rušenje varnih povezav IPSec
  - skrbi za:
    - avtentikacijo sodelujočih strani
    - izmenjavi enkripcijskih ključev
    - izmenjavo parametrov, ki so potrebni za vzpostavitev varnih zvez IPSec
  - princip delovanja:
    - 1. FAZA – vzpostavitev varne zveze IKE (dvosmerna povezava)
      - enkripcijski algoritem, zgoščevalni algoritem, avtentikacijska metoda, parametri za izvajanje algoritma Diffie – Hellman, ostali atributi varne zveze IKE
    - 2. FAZA – vzpostavitev varnih zvez IPSec (enosmerne povezave)
      - protokol AH oziroma ESP, enkripcijski algoritem, zgoščevalni algoritem, ostali atributi varne zveze IPSec

Princip delovanja IKE

1. PC 1 pošlje paket Varnostnemu prehodu 1

PAKET IP →

2. Varna prehoda izmenjata parametre za vzpostavitev varne zveze IKE

IKE SA ⟷ IKE FAZA 1 ⟷ IKE SA

3. Varna prehoda izmenjata parametre za vzpostavitev varnih zvez IPSec

IPSec SA ⟷ IKE FAZA 2 ⟷ IPSec SA

4. Paket potuje skozi tunelsko povezavo do PC2

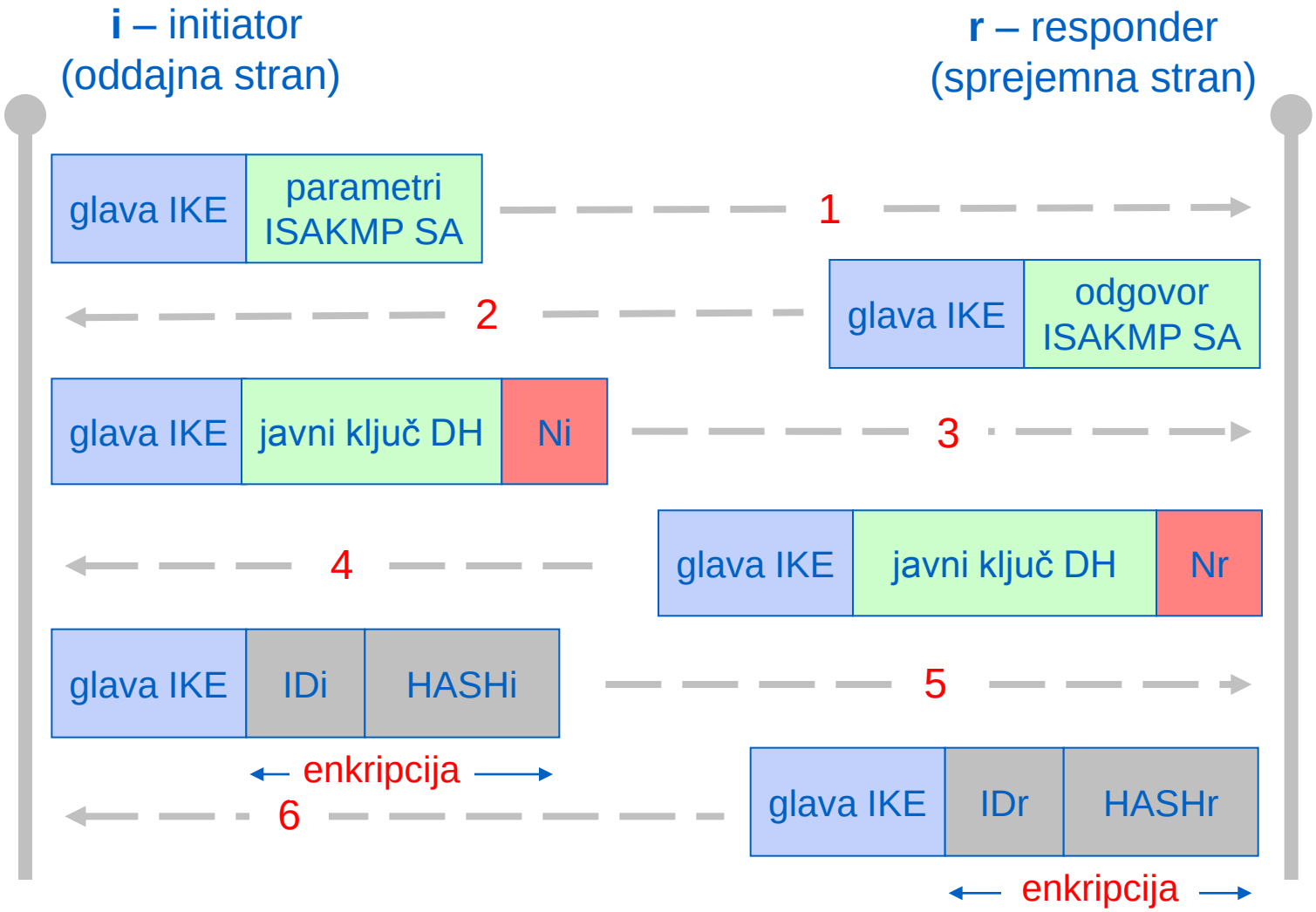
Tunelska povezava

PAKET IP →

5. Rušenje tunelske povezave

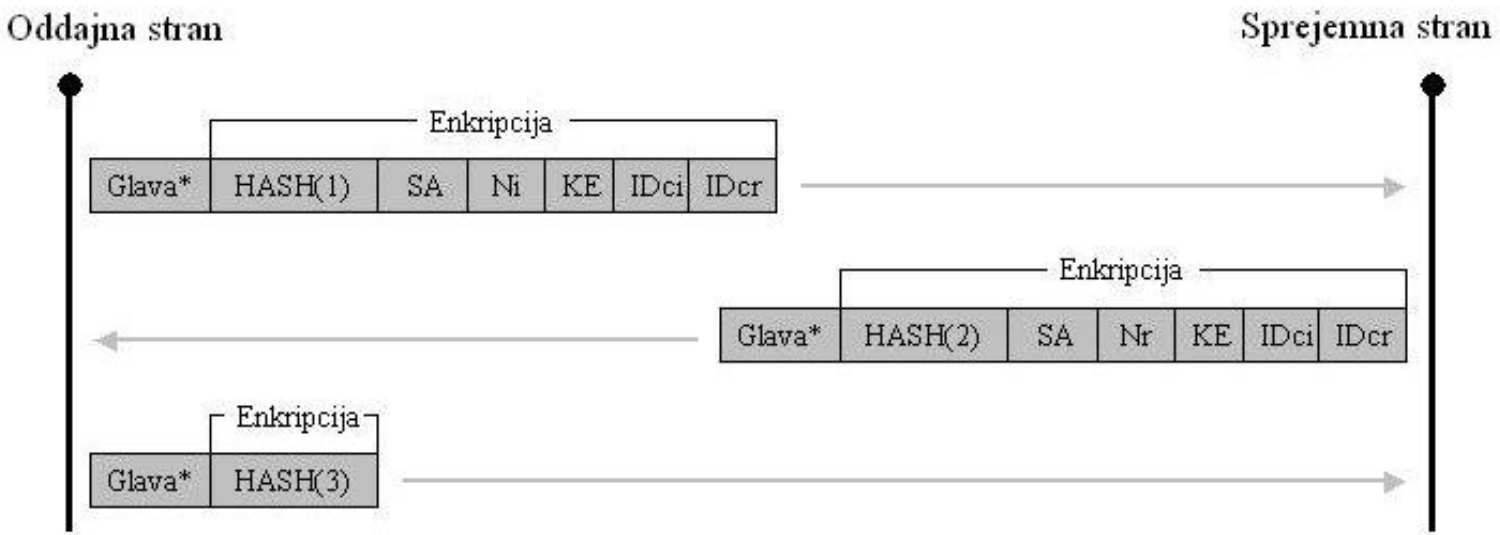
IKE faza 1 – Main Mode

- **Avtentikacija na osnovi predhodno izmenjanih skrivnosti**



IKE faza 2 – Quick Mode

- **Razlaga polj:**
  - **polje HASH prenaša povzetek zgoščevalnega postopka**
  - **polje SA prenaša podatke potrebne za pogajanje, oziroma že določene parametre varne zveze IPSec**
  - **polji Ni in Nr prenašata ostale potrebne podatke *(Nonce Payload)***
  - **opcijsko polje KE prenaša javne ključe**
  - **opcijski polji IDci in IDcr prenašata identifikacijske podatke**
    - **v primeru, ko varna prehoda ne vzpostavljata varne zveze za lasten promet (npr. tunelsko povezavo)**



Parametri varne zveze IKE

Parametri varne zveze IKE	Nabor razpoložljivih parametrov
Enkripcijski algoritem	DES-CBC, 3DES-CBC, IDEA-CBC, CAST-CBC, RC5-R16-B64-CBC, Blowfish-CBC
Zgoščevalni algoritem	MD5, SHA-1, Tiger
Avtentikacijska metoda	RSA podpis, DSS podpis, javni ključi RSA, izboljšani način javnih ključev, predhodno izmenjan ključ
Skupina matematičnih funkcij *(Group Description)*	768 - bitna MODP skupina, 1024 - bitna MODP skupina, EC2N skupina,
Tip matematične skupine *(Group Type)*	MODP, ECP, EC2N
Življenjski čas varne zveze - enota *(Life Type)*	Sekunde, kilobiti *(kilobytes)*
Psevdo naključna funkcija PRF	Ni še definirano
Dolžina enkripcijskega ključa	V primeru, če je njegova dolžina variabilna
Velikost skupine Diffie-Hellman	Velikost polja v bitih
Način vzpostavitve varne zveze IPSec	Hitri način, novi način *(New Group Mode)*

Parametri varne zveze IPSec

Parametri varne zveze IPSec	Nabor razpoložljivih parametrov	
Enkripcija s protokolom ESP	DES_IV64, DES, 3DES, RC5, IDEA, CAST, BLOWFISH, 3IDEA, DES_IV32, RC4, NULL	
Avtentikacija s protokolom AH	HMAC-MD5, HMAC-SHA-1, DES-MAC	
Kompresija podatkov *(IPCOMP)*	OUI, DEFLATE, LZS	
Atributi varne zveze *(SA attributes)*	Enota življenjskega časa	Sekunda, kilobiti *(kilobytes)*
	Življenjski čas varne zveze	V sekundah
	Oakly skupina potrebna za PFS	
	Prenosni način	Tunelski, transportni
	Avtentikacijski algoritem za protokol ESP	HMAC-MD5, HMAC-SHA-1, DES-MAC, KPDK, NULL
	Privatni kompresijski algoritem	Implementacija lastnih kompresijskih algoritmov
	Rezervirani atributi	

Primerjava med IKEv1 in IKEv2

- **Zakaj protokol IKEv2?**
  - **IKEv1 ne podpira avtentikacije uporabnika in ostalih avtentikacijskih mehanizmov**
  - **problem transparentnosti za naprave NAT**
  - **kompleksnost protokola IKEv1 (slabo dokumentiran)**

	IKEv1	IKEv2
Standardizacija	RFC 2407/2408/2409	draft
Delovanje protokola	Faza 1 (3. ali 6. sporočil) Faza 2 (3. sporočila)	Faza 1 (4. sporočila) Faza 2 (2. sporočili)
Avtentikacija	Digitalni podpis, predhodno izmenjani ključi, koncept javnih ključev	Digitalni podpis, predhodno izmenjani ključi
Prikrivanje identitete	Opcijsko	Vedno
Perfect Forward Secrecy	Opcijsko	Opcijsko
Zaščita pred DOS	-	Opcijsko
HASH	Del sporočila	Celotno sporočilo
Razširjena avtentikacija	-	EAP
DHCP	-	Da

NAT – Network Address Translation

- Omogoča prenaslavljanje izvornega/ponornega naslova IP v nek drug naslov IP
- V omrežja IP vpelje koncept odjemalec-strežnik
  - problemi z aplikacijami, ki prenašajo izvorne naslove IP v okviru aplikacijskih protokolov
  - problemi z aplikacijami, ki ne dovolijo spreminjanja vrednosti glave IP in TCP/UDP
- Delovanje:
  - statični NAT
    - sprememba polj v glavi IP
  - dinamični NAT/PAT
    - sprememba polj v glavi IP (NAT)
    - sprememba polj v glavi IP in TCP/UDP (PAT)
- Naprava, ki opravlja funkcijo NAT mora za pakete, katerim je bila spremenjena glava IP oziroma TCP, ponovno izračunati kontrolno vsoto ˝checksum˝
  - kontrolna vsota glave TCP/UDP se izračuna tudi na osnovi zapisov v poljih glave IP (izvorni/ponorni naslov IP, protokol)

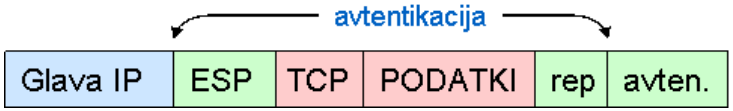
NAT in IPSec

- **Protokol AH**
  - zagotavlja celovitost celotnega paketa IP vključno z glavo
  - protokol AH (v tunelskem ali transportnem načinu prenosa) ne deluje skozi naprave, ki opravljajo funkcijo NAT

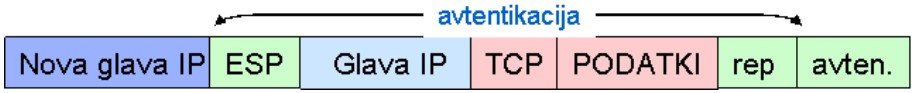
AH – transportni način

AH – tunelski način

- **Protokol ESP**
  - zagotavlja celovitost le prenašanih podatkov (brez zunanje glave IP)
  - sprememba vrednosti v zunanji glavi IP (NAT) ne vpliva na proces avtentikacije IPSec
    - še vedno pa je potreben ponoven izračun kontrolne vsote glave TCP/UDP?
    - izkop preverjanja kontrolne vsote glave TCP/UDP na strani sprejemnika?



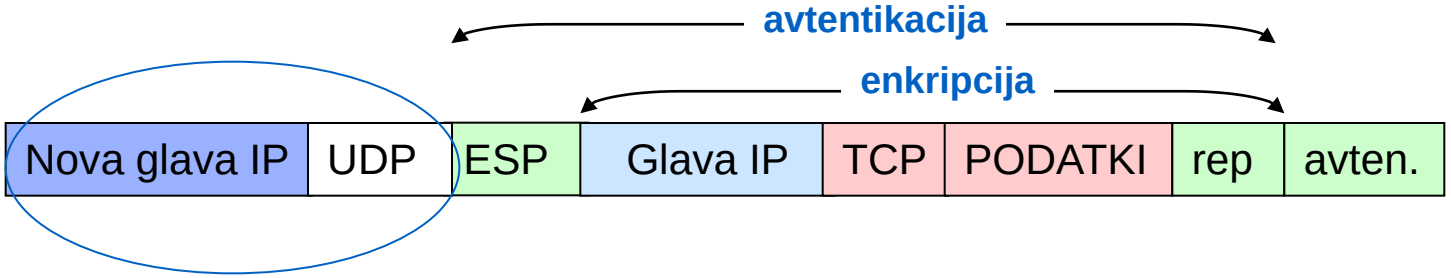
ESP – transportni način



ESP – tunelski način

IPSec NAT Traversal

- **Med zunanjo glavo IP in glavo ESP vstavimo glavo UDP**
  - **v primeru prenosa paketa skozi napravo, ki opravlja funkcijo NAT bo nova kontrolna vsota ˝checksum˝ zapisana v zunanji glavi IP in UDP**



spremenjena polja v primeru prenosa prek naprave NAT