
biokoda

biokoda®

SODOBNI KRIPTOGRAFSKI MEHANIZMI VAROVANJA PODATKOV

DENIS JUSTINEK
CTO, BIOKODA

Današnje teme

- Prioritete uporabnikov
- Začetki
- Predstavitev nekaterih izzivov na trivialnem šifrirnem mehanizmu
- Lastnosti kriptografskih mehanizmov
- Primer kripto. mehanizma: 3DH + Double Ratchet
- Napredno varovanje TLS povezav

biokoda®

“A security system is only
as strong as its weakest link. “

Cryptography Engineering
Ferguson, Schneier, Kohno

Vir: http://missukoai.xyz/chain-link-fence-lock/

Prioritete

- Uporabniki, podjetja, organizacije imamo veliko izbiro različnih produktov, ki implementirajo različne varnostne mehanizme za zagotavljanje zasebnosti

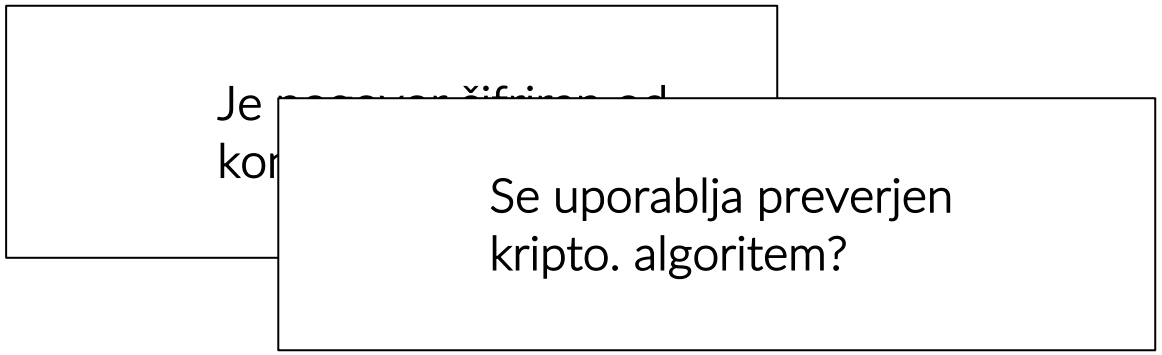
- Ali se pri uporabi vprašamo …

Je pogovor šifriran od konca do konca?

Prioritete

- Uporabniki, podjetja, organizacije imamo veliko izbiro različnih produktov, ki implementirajo različne varnostne mehanizme za zagotavljanje zasebnosti

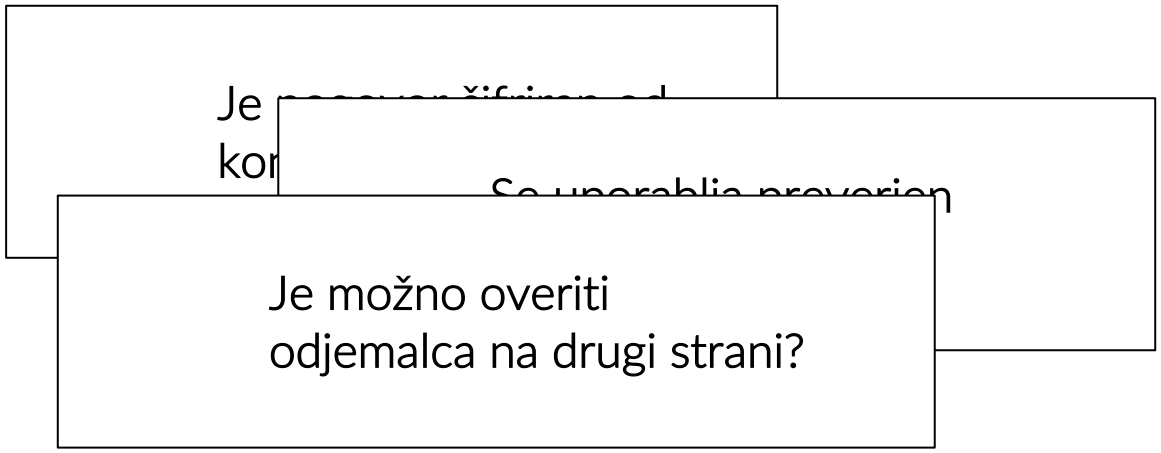
- Ali se pri uporabi vprašamo …



Prioritete

- Uporabniki, podjetja, organizacije imamo veliko izbiro različnih produktov, ki implementirajo različne varnostne mehanizme za zagotavljanje zasebnosti

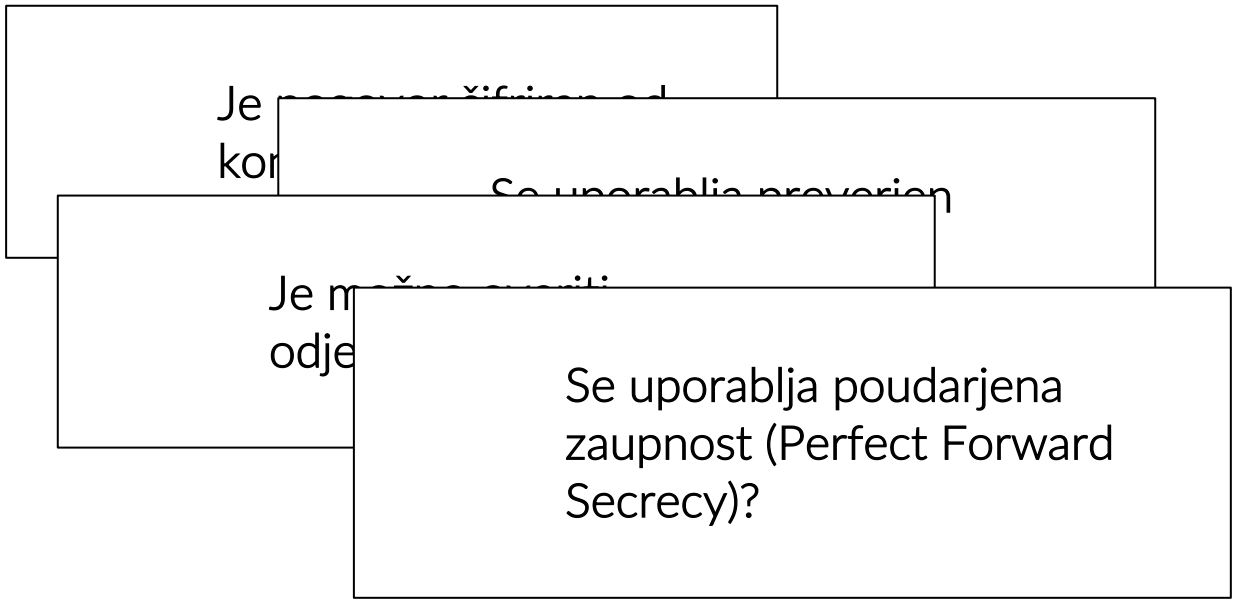
- Ali se pri uporabi vprašamo …



Prioritete

- Uporabniki, podjetja, organizacije imamo veliko izbiro različnih produktov, ki implementirajo različne varnostne mehanizme za zagotavljanje zasebnosti

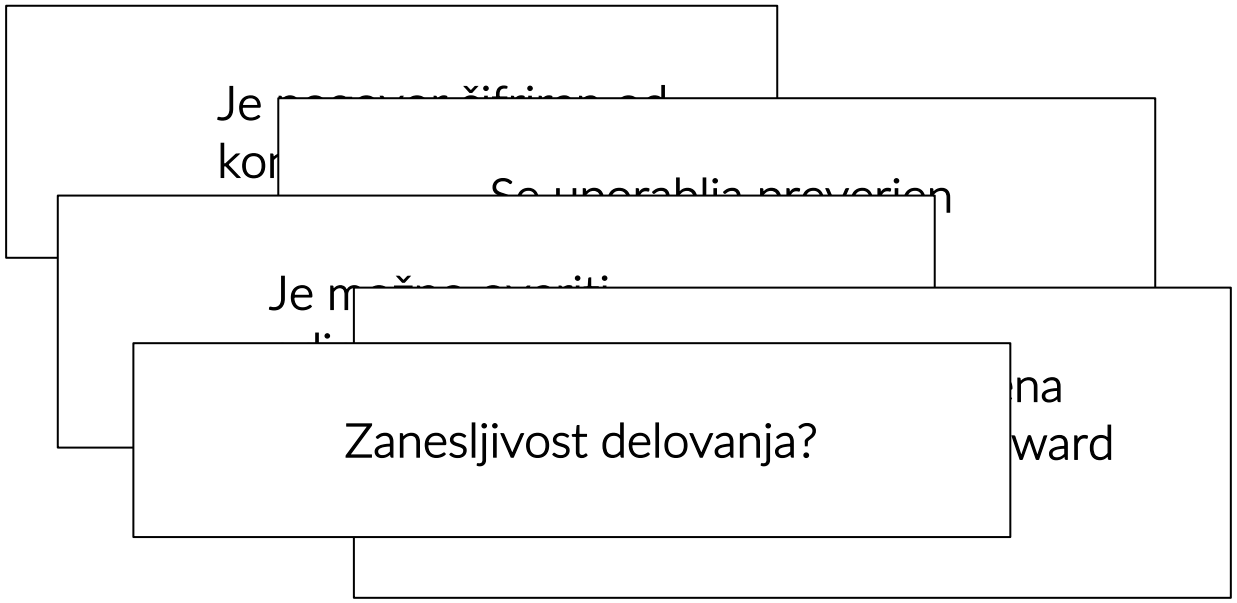
- Ali se pri uporabi vprašamo …



Prioritete

- Uporabniki, podjetja, organizacije imamo veliko izbiro različnih produktov, ki implementirajo različne varnostne mehanizme za zagotavljanje zasebnosti

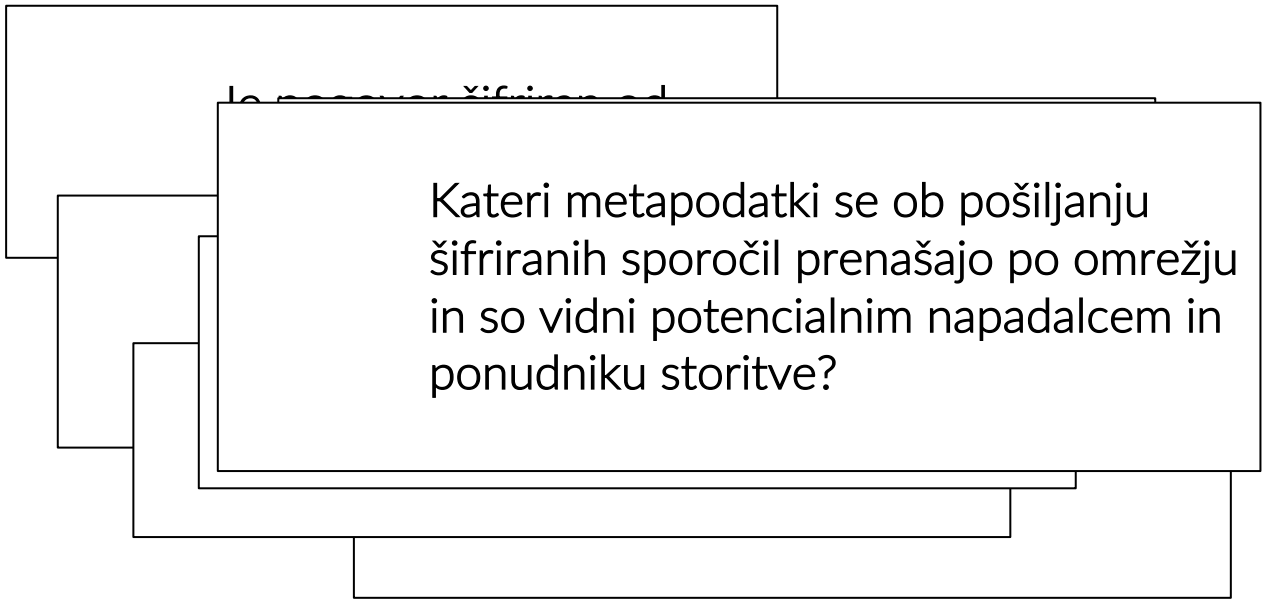
- Ali se pri uporabi vprašamo …



Prioritete

- Uporabniki, podjetja, organizacije imamo veliko izbiro različnih produktov, ki implementirajo različne varnostne mehanizme za zagotavljanje zasebnosti

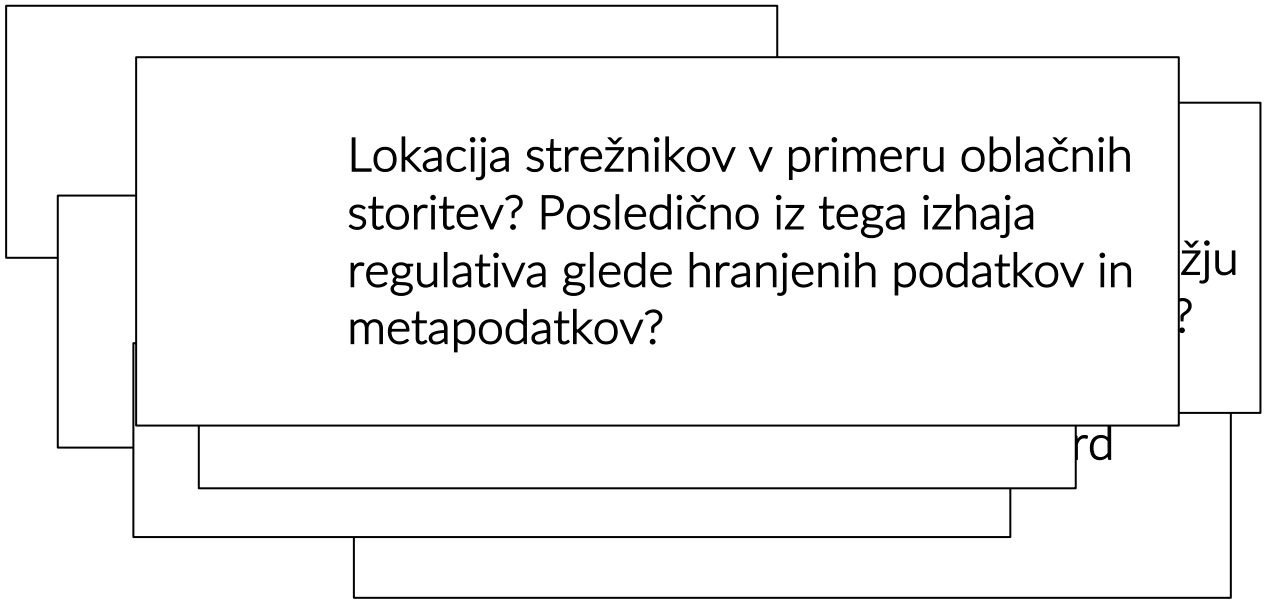
- Ali se pri uporabi vprašamo …



Prioritete

- Uporabniki, podjetja, organizacije imamo veliko izbiro različnih produktov, ki implementirajo različne varnostne mehanizme za zagotavljanje zasebnosti

- Ali se pri uporabi vprašamo …



Prioritete

- Uporabniki, podjetja in organizacije imamo veliko izbiro različnih produktov, ki implementirajo različne varnostne mehanizme za zagotavljanje zasebnosti

- Uporabnike sicer v večini primerov zanima samo …

  - Velikost socialnega omrežja? (*So prijatelji prisotni?*)
  - Enostavnost uporabe?
  - Dostopnost sistema?
  - Dodatne storitve, ki jih sistem ponuja?

Nekaj trenutkov iz zgodovine …

- Cezarjeva šifra

  Šifrirano besedilo: GDQ LQIRUPDFLMVNH YDUQRVWL

- Carl Friedrich Gauss [1800] – modularna aritmetika

- …

- Auguste Kerckhoffs [1883]: ”*The system must not require secrecy and can be stolen by the enemy without causing trouble.*”

- Kriptologija

  - Kriptografija – tajnost, šifriranje, zakrivanje sporočil

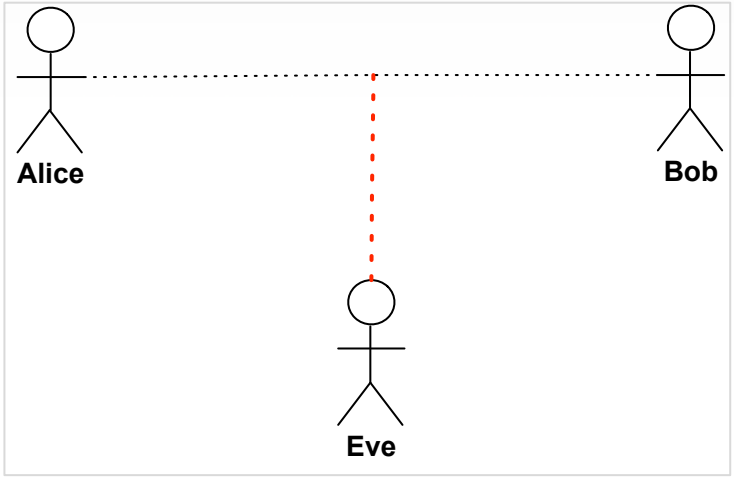
  - Kriptoanaliza – razkrivanje, razbijanje tajnih podatkov

- Za lažje razumevanje nadaljevanja bomo na primeru *slabega* šifrirnega sistema poskušali razumeti lastnosti modernih kriptografskih mehanizmov

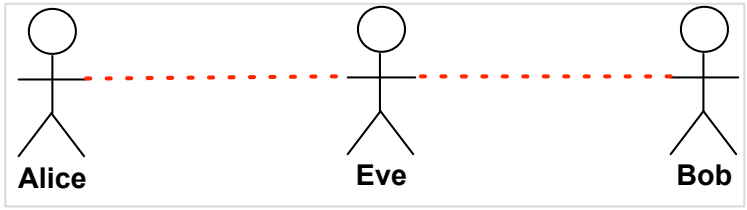
Izvorno besedilo: ???

Šifrirano besedilo: GDQ LQIRUPDFLMVNH YDUQRVWL

- **Alice, Bob** - osebi, ki varno komunicirata
- **Eve** – napadalec



Eve v vlogi pasivnega napadalca



Eve v vlogi aktivnega napadalca (*napad s posrednikom*)

- Za lažje razumevanje nadaljevanja bomo na primeru *slabega* šifrirnega sistema poskušali razumeti lastnosti modernih kriptografskih mehanizmov

Izvorno besedilo: DAN INFORMACIJSKE VARNOSTI

Šifrirano besedilo: GDQ LQIRUPDFLMVNH YDUQRVWL

- Predpostavimo, da Eve izve kako sistem deluje. Kot pasivni napadalec ima Eve posnetek celotne varovane komunikacije. Katere informacije so ogrožene?

  Izvorno besedilo: DAN INFORMACIJSKE VARNOSTI

  Šifrirano besedilo: GDQ LQIRUPDFLMVNH YDUQRVWL

  (D+3 = G, A+D =D, N+3=Q, I+3=L,…)

  Dolžine besed, ponavljanje, frekvenčna analiza,

- Preteklost celotne komunikacije.
- Prihodnost celotne komunikacije.
- Prisotnost napada ni mogoče zaznati.
- Eve lahko spreminja sporočila.
- …

Lastnosti pod drobnogledom

- Poudarjena zaupnost (*perfect forward secrecy*)
  - Varovanje preteklosti komunikacije
- Zaupnost prihodnosti * (*future secrecy*)
  - Varovanje prihodnosti komunikacije
- Preprečevanje/zaznavanje napada s posrednikom (*Man-in-the-middle attack prevention*)
- Preverljivost komunikacije

Za razumevanje nadaljevanja

- Zgoščevanje (*hashing*)
  - SHA256 vrednost niza "DAN INFORMACIJSKE VARNOSTI") je "bbe027cf90e9fcc17449813b5fd71bba134e2fb6b0a721865680f77a5e6d439a“
  - Ireverzibilna operacija. Iz končnega izračuna ni moogoče sklepati kaj je bil vhod.
- Simetrično šifriranje (bločne funkcije, pretočne funkcije)
  - S pomočjo zasebnega ključa (skrivnosti) transformiramo vhodni niz v šifriran niz.
  - Temelji na deljeni skrivnosti.
- Asimetrično šifriranje
  - Temelji na zasebnih in javnih šifrirnih ključih. Za komuniciranje med točkama A in B mora biti predhodno opravljena izmenjava javnih ključev (*key exchange*). Izračun šifrirnega ključa oz. deljene skrivnosti se izvede s pomočjo zasebnih ključev ter izmenjanih javnih ključev.
- Overjanje podatkov

Pudarjena zaupnost (PFS)

- Poudarjena zaupnost – angl. Perfect forward secrecy
- Ključno vprašanje: ali je v primeru, da so zasebni ključi zlorabljeni, preteklost, po trenutku zlorabe varna?
- V primeru šifrirnega, mehanizma, ki ustreza zahtevam PFS je odgovor na takšno vprašanje **pritrdilen**.

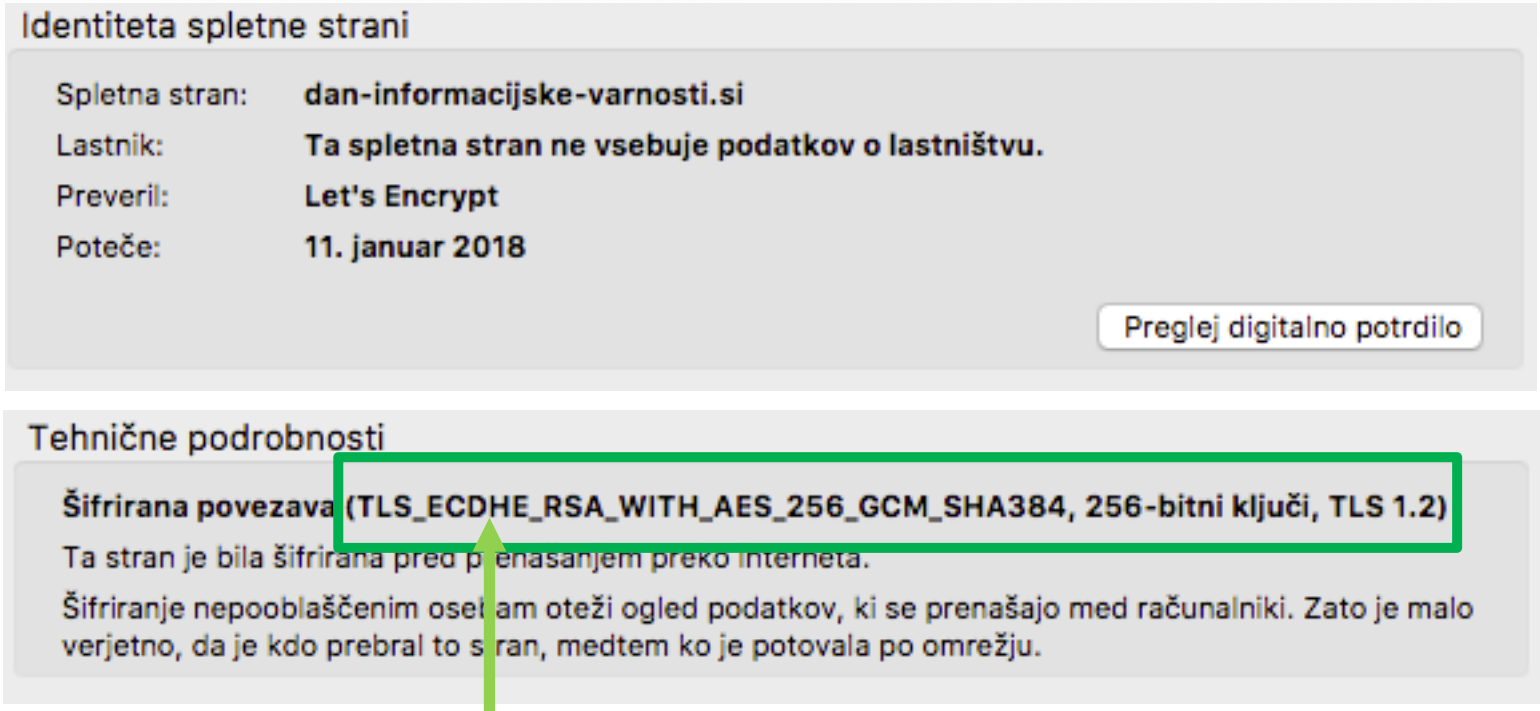
Poudarjena zaupnost (PFS)

- Lastnost komunikacijskega protokola, kjer zloraba dolgotrajnih šifrirnih ključev ne kompromitira pretekle komunikacije (sej)

- Sistem, ki uporablja infrastrukturo javnih ključev ustreza lastnosti PFS takrat, ko je rezultat izmenjave ključev naključni šifrirni material, ki ni posledica deterministčnih izračunov

Poudarjena zaupnost (PFS)

- Kako vem ali je pri komunikaciji s spletnimi strežniki uporabljen šifrirni mehanizem, ki zagotavlja PFS?



ECDHE – Elliptic Curve Diffie Hellman Ephemeral

- Zaupnost prihodnosti

- Sicer nestandardno poimenovanje, uporabljeno pri implementaciji mehanizma Double Ratchet (dvosmerna raglja) pri Open Whisper Systems

- Ključno vprašanje: v primeru da je ob nekem trenutku kratkotrajni šifrirni material zlorabljen ali se lahko zagotovi zaupnost podatkov v prihodnosti?

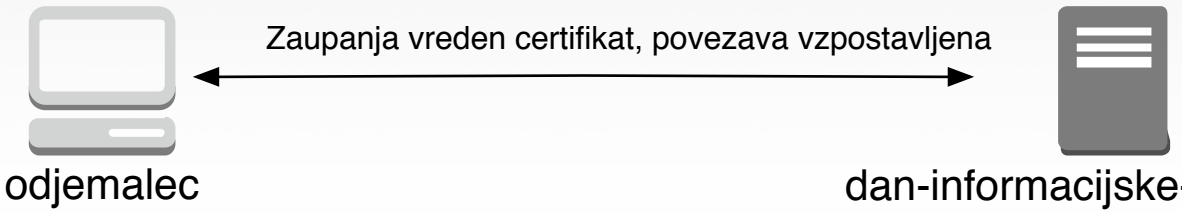
Vir: https://signal.org/blog/advanced-ratcheting/

- Preprečevanje MITM
  - End-to-end šifrirni mehanizmi: preverljivost šifrirnega kanala
  - HPKP - HTTP Public Key Pinning
  - TLS Pinning

- SSL/TLS – kako preprečiti napade s ponarejenimi ali napačno-izdanimi certifikati za vaše spletno mesto?

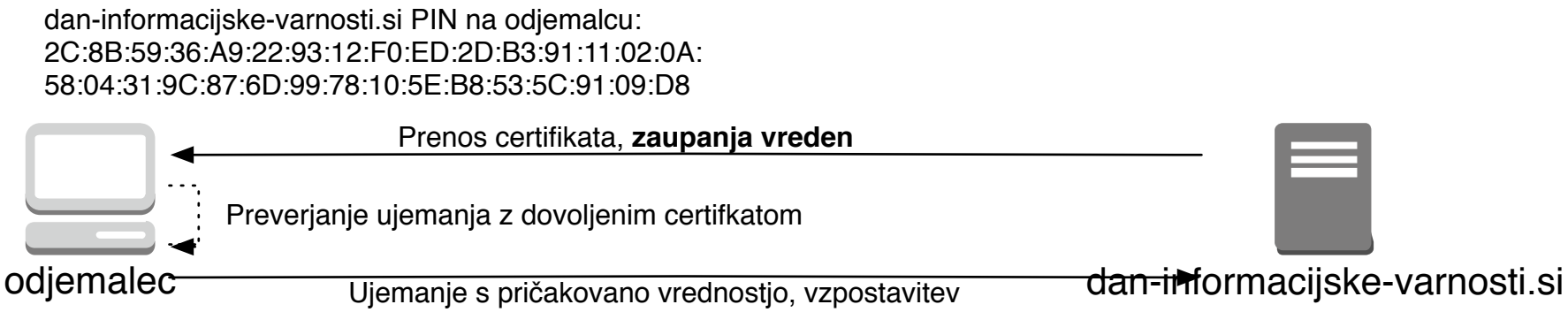
- TLS Pinning – odjemalci se povežejo samo na zaupanja vredne strežnike. (*Preverjanje komunikacije iz strani odjemalca*)

- Brez TLS pinning ali HPKP:

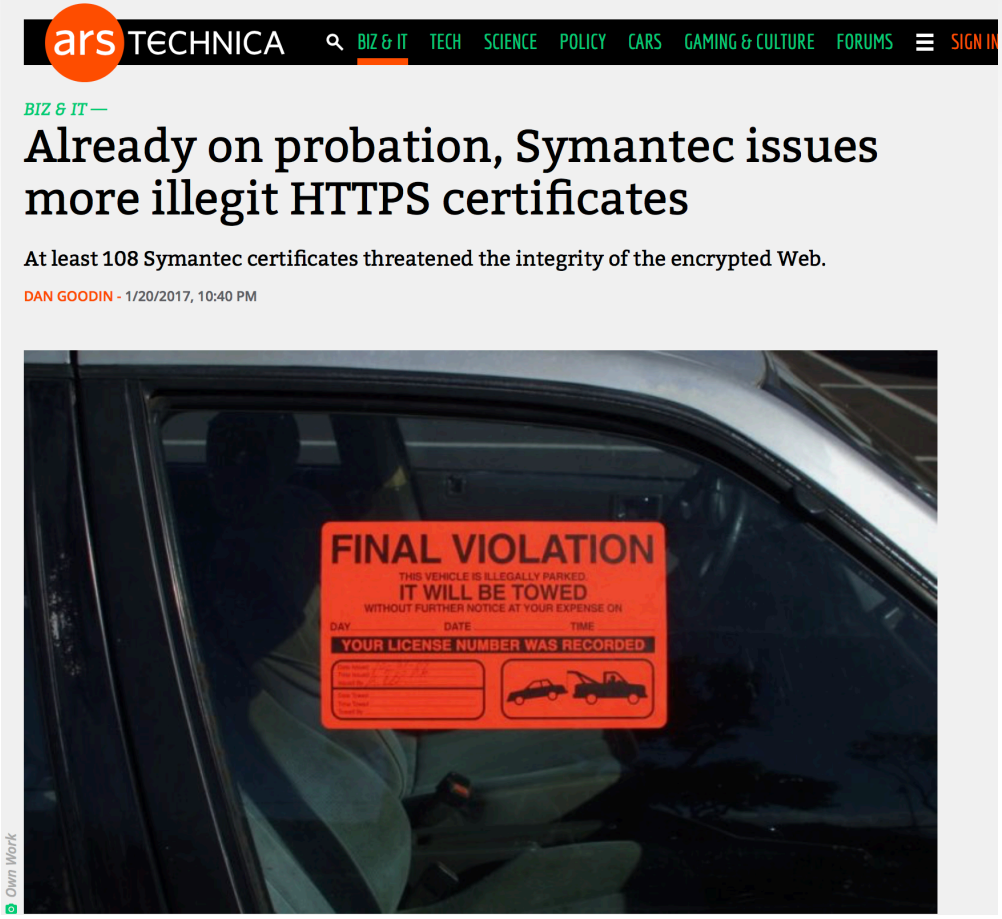


Odjemalec zaupa certifikatom iz CA repozitorija za povezovanje na ciljne točke.

- S TLS pinning ali HPKP:



Zakaj HPKP ali TLS pinning?



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS SIGN IN

BIZ & IT —

Already on probation, Symantec issues more illegit HTTPS certificates

At least 108 Symantec certificates threatened the integrity of the encrypted Web.

DAN GOODIN - 1/20/2017, 10:40 PM

X3DH + Double Ratchet

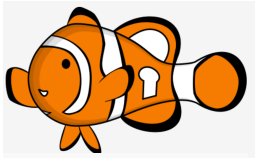
- Sodobni mehanizem v praksi – 3DH + Double Ratchet
- Implementacije za namene varovanja medčloveške komunikacije
- Cilj: zagotovitev PFS, future secrecy, preprečevanje napada s posrednikom, enostavnost vzpostavitve varovanega kanala za komuniciranje, možnost preverjanja varnega kanala (seje)
- Poenostavljena predstavitev

- Implementacije 3DH + DoubleRatchet z variacijami

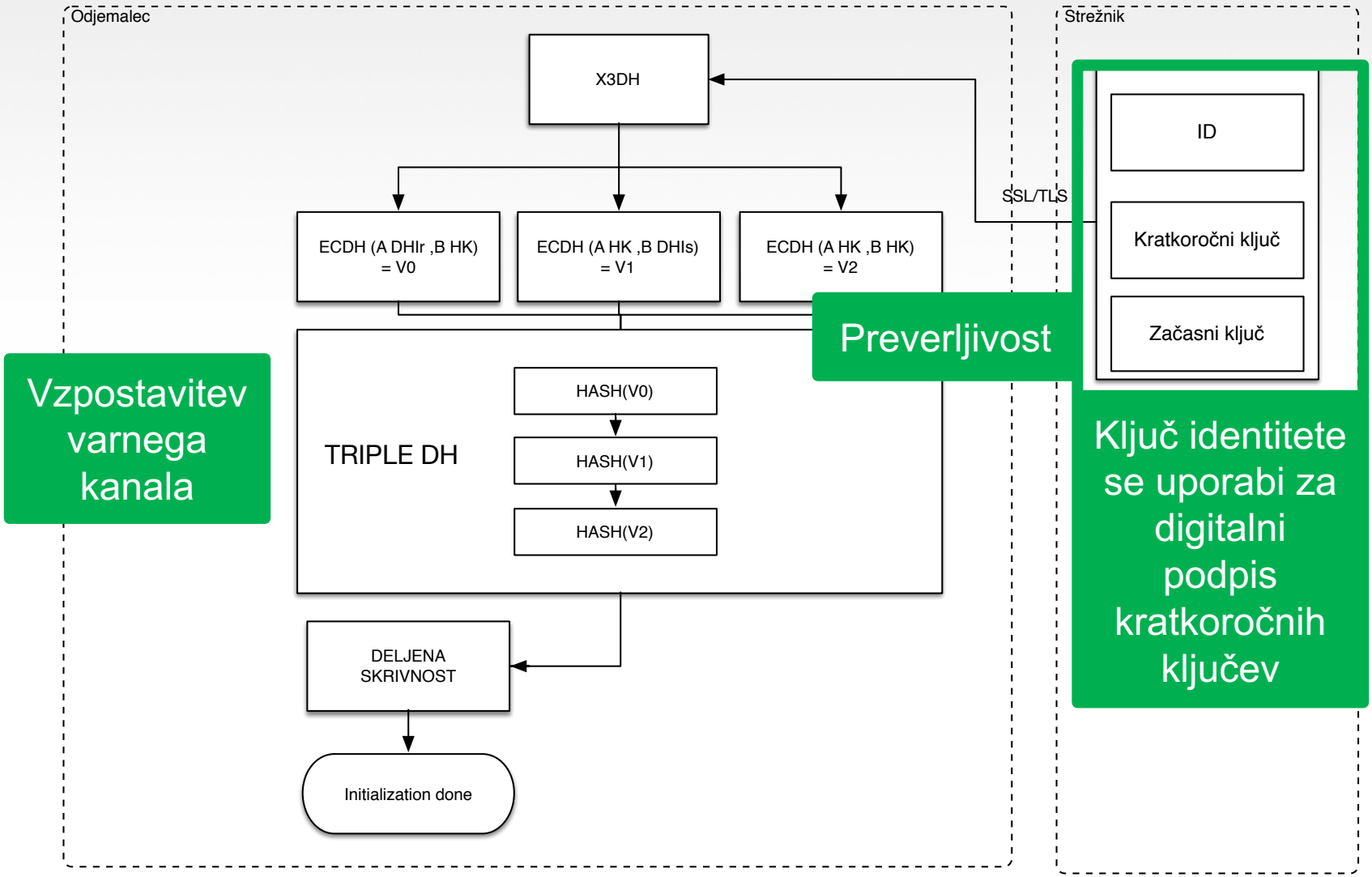
BIOCODED

Signal

wire



3DH in Double Ratchet



3DH: vzpostavitev varnega kanala

POENOSTAVLJEN OPIS

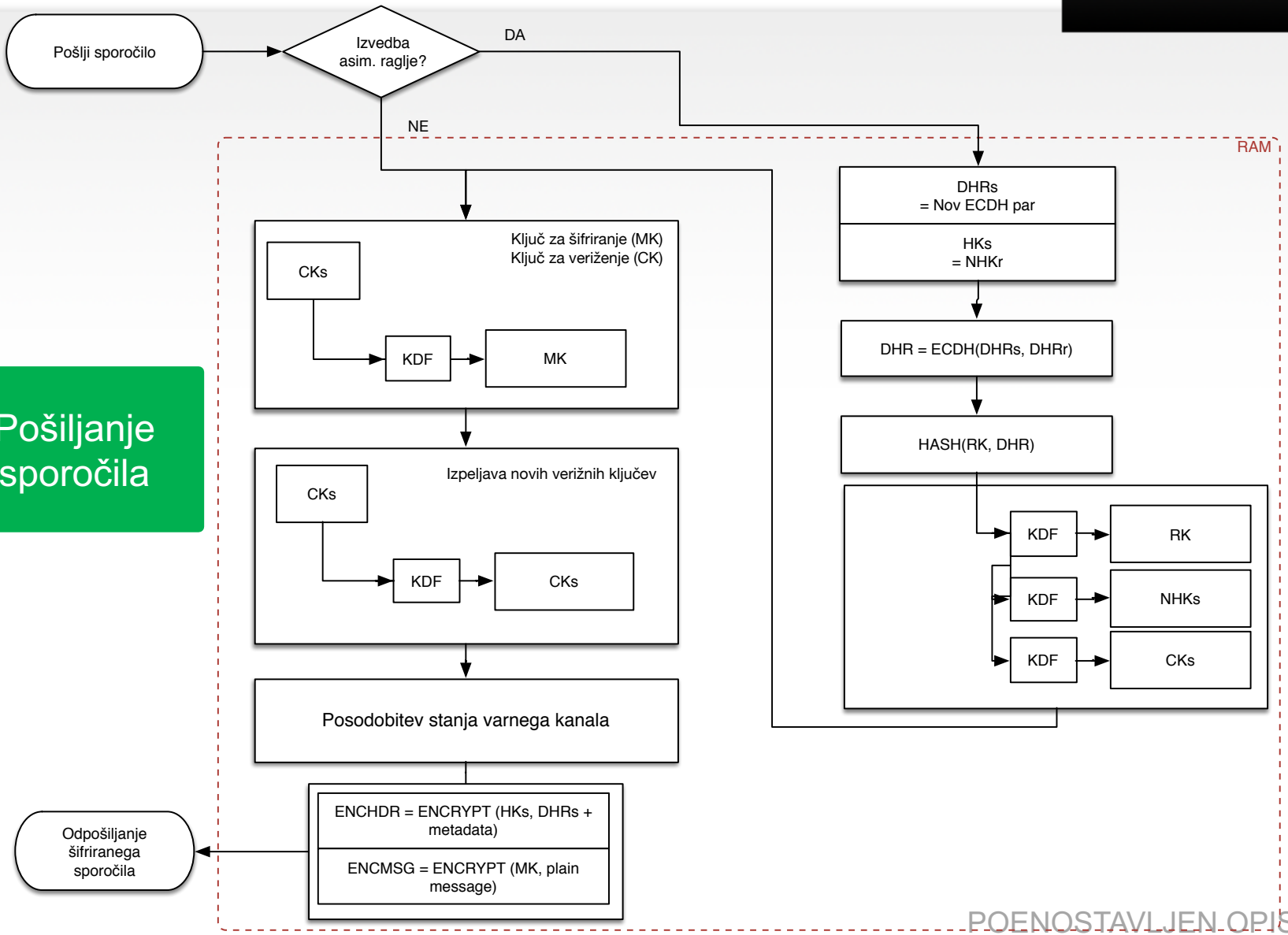
X3DH + Double Ratchet

- Od kod poimenovanje “Double Ratchet” oz. dvosmerna raglja?

- #1 Raglja: Simetrična raglja s pomočjo zgoščevanja izpeljuje nove zasebne ključe za šifriranje odposlanih sporočil

- #2 Raglja: Asimetrična raglja s pomočjo izmenjave ključev (ECDH) in izračuna deljene skrivnosti spreminja stanje varnega kanala iz katerega se izpeljujejo zasebni ključi #1 raglji.

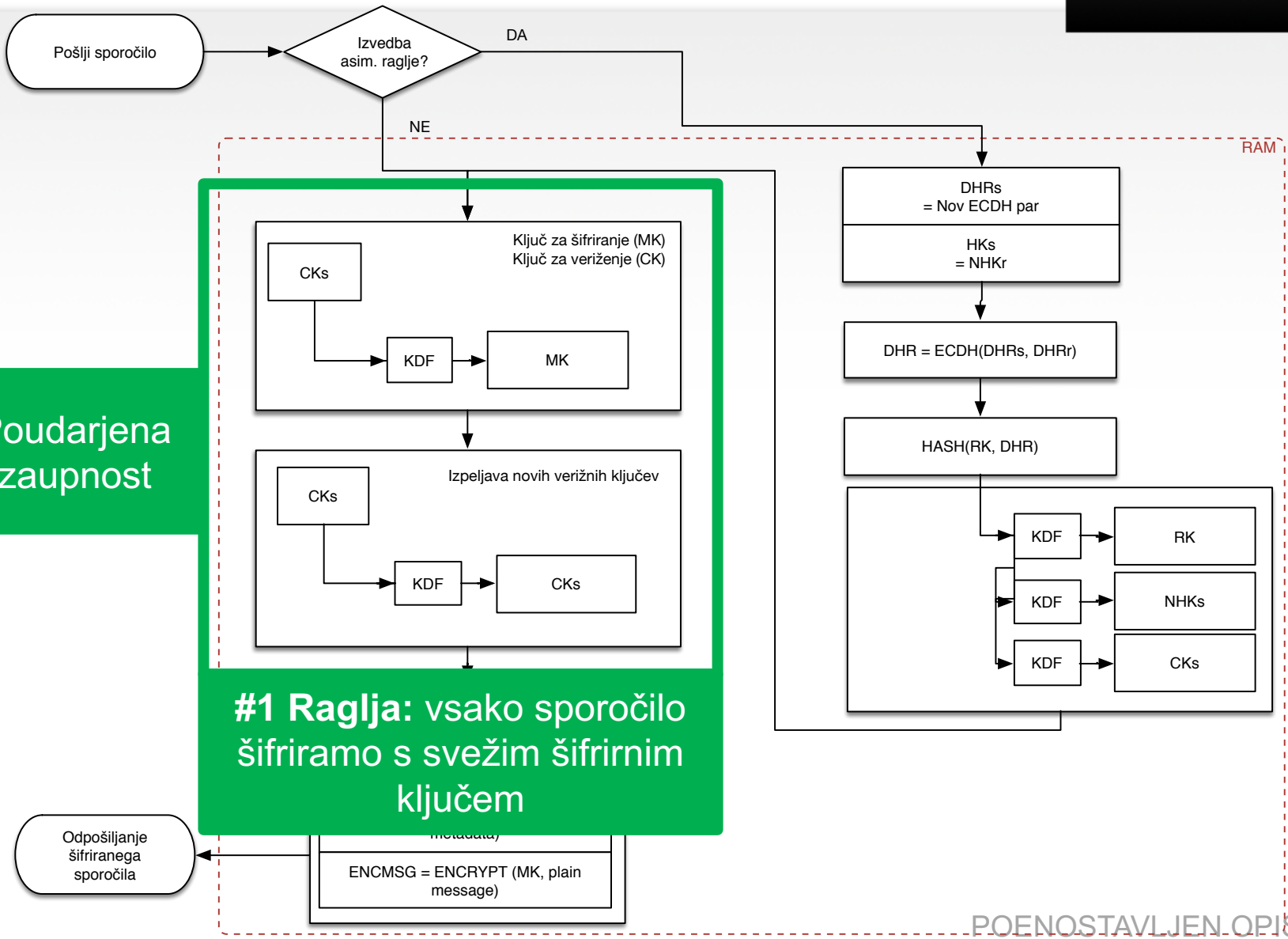
X3DH in Double Ratchet



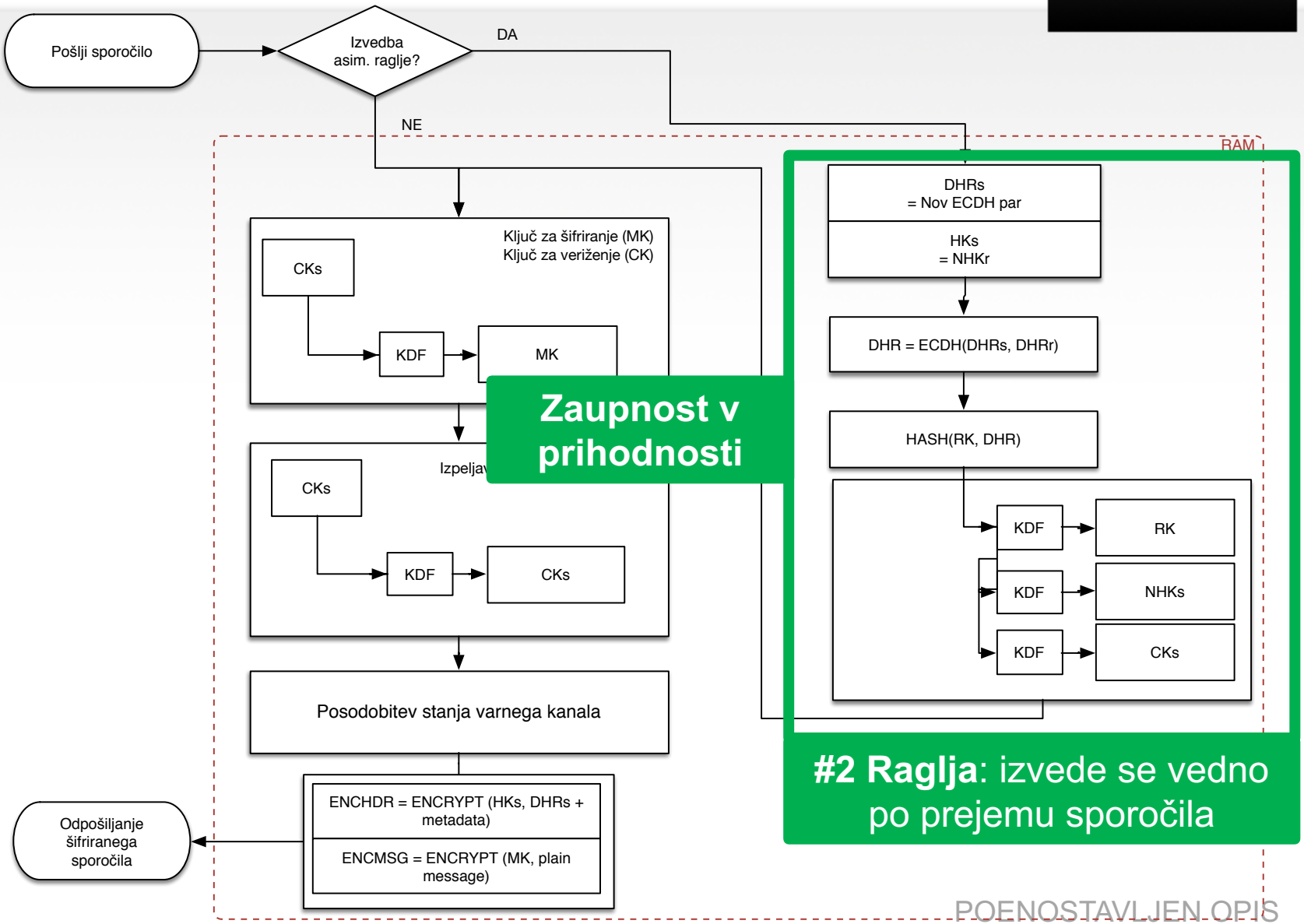
Pošiljanje sporočila

POENOSTAVLJEN OPIS

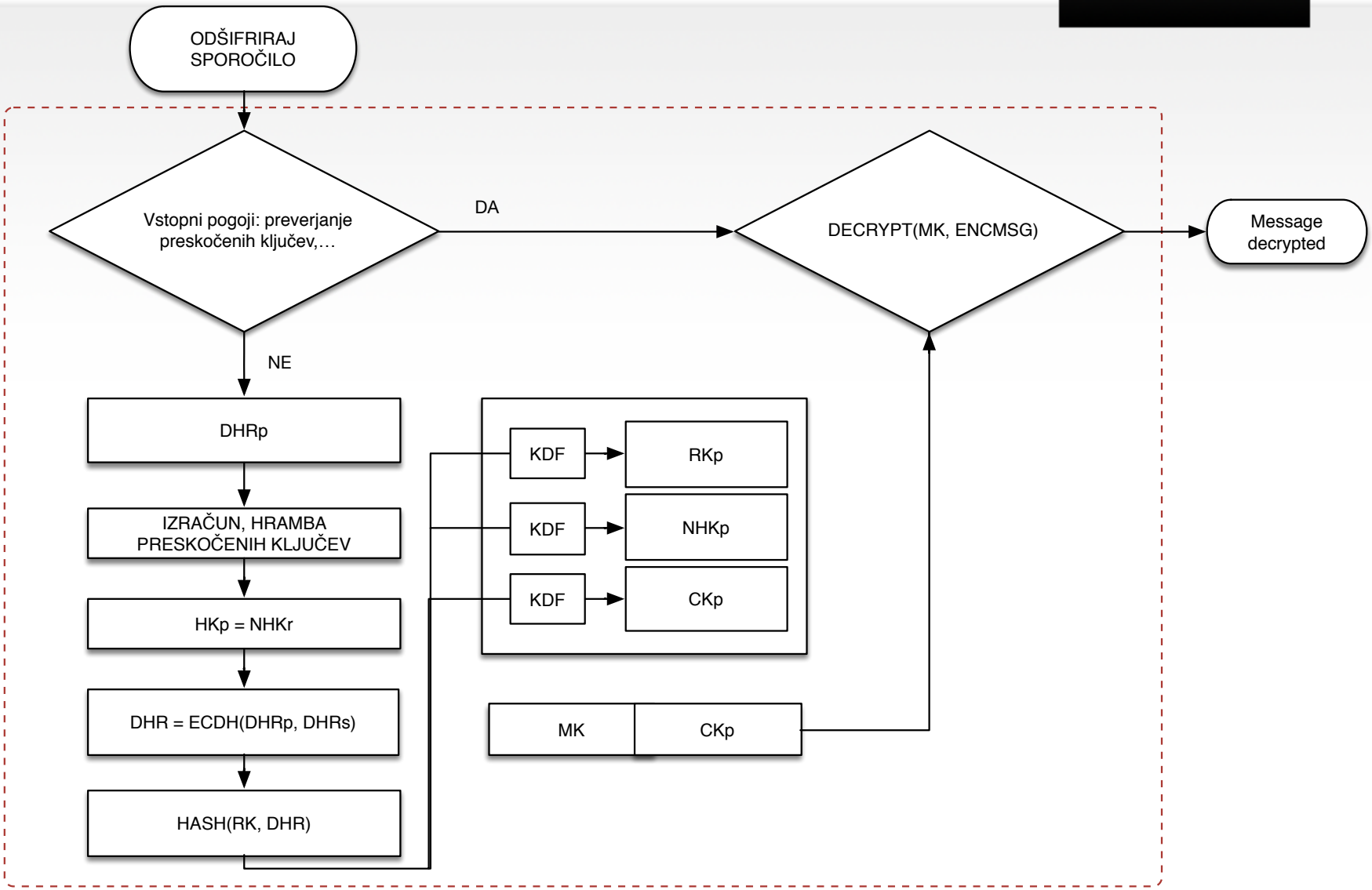
X3DH in Double Ratchet



X3DH in Double Ratchet



X3DH in Double Ratchet



POENOSTAVLJEN OPIS

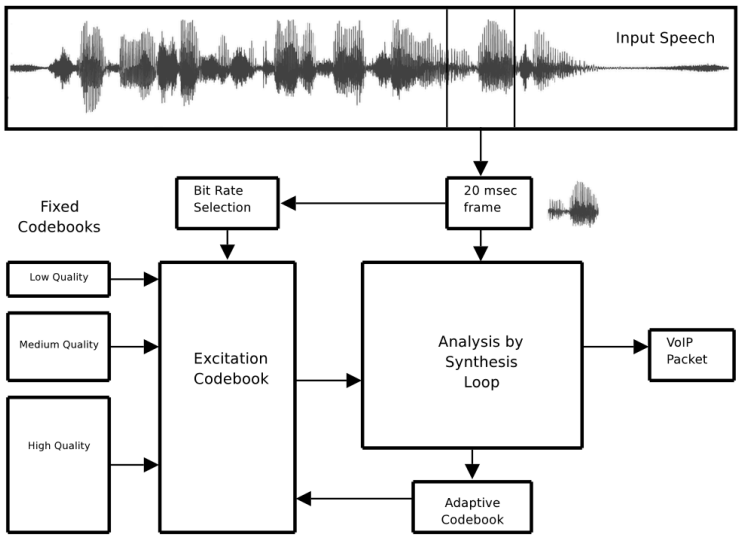
Šifriranje zvoka

- Kdaj je zvočni pogovor zaseben?
  - Vprašanje šifriranja

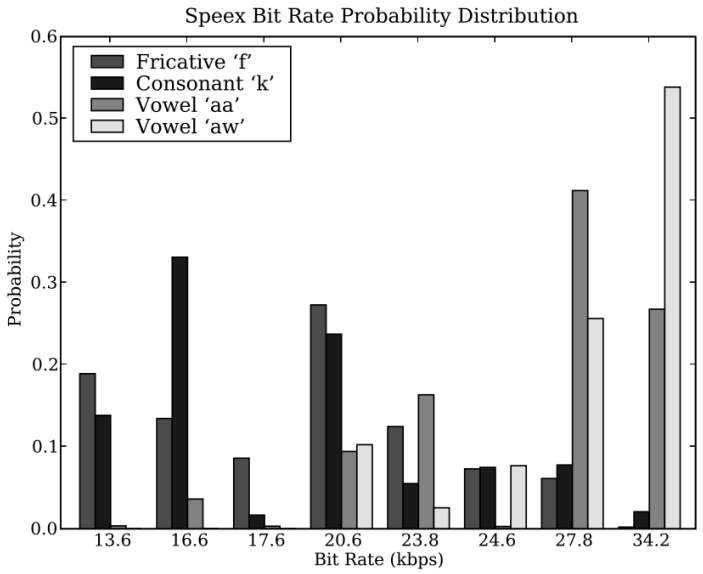
    IN

  - Vprašanje kodiranja zvoka (kompresija,...)

Šifriranje zvoka



Opazujemo bitne hitrosti kodiranja.



Vir: http://www.cs.unc.edu/~fabian/papers/tissec2010.pdf

- Šifriranje zvoka

- Kdaj je zvočni pogovor zaseben?

Neglede na stopnjo šifriranja se iz velikosti kompresiranih zvočnih paketov lahko opravi analiza pogovora.

Na podlagi analize posnetega zvočnega pogovora se lahko do 50% natančnostjo analizirajo krajše besede in z do 90% natančnostjo daljše besede.

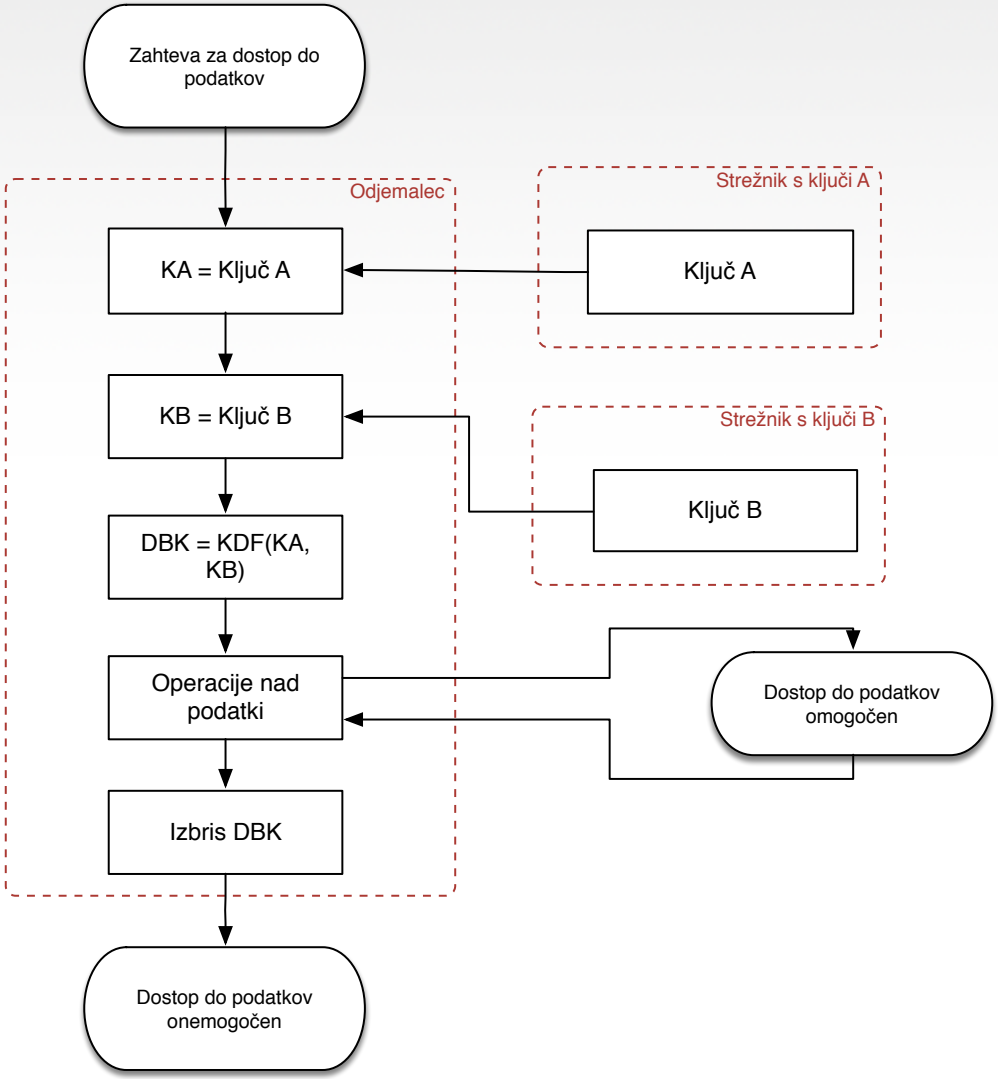
Vir: http://www.cs.unc.edu/~fabian/papers/tissec2010.pdf

- Šifriranje zvoka

Za zaščito zvočnega pogovora je zahtevano kodirane zvoka s konstantno bitno hitrostjo oz. konstantnimi velikosti paketov.

Tako preprečimo možno analizo bitnih hitrosti ter sklepanja besed v pogovoru iz statističnih informacij.

- Varovanje podatkov hranjenih na trajnih medijih
- Kje se nahaja šifrirni ključ?
- Je samo eden?
- Več ključev (distribucija)?
- Kje se nahajajo ključi za odšifriranje podatkov?


Zahteva za dostop do podatkov
Odjemalec
KA = Ključ A
KB = Ključ B
DBK = KDF(KA, KB)
Operacije nad podatki
Izbris DBK
Dostop do podatkov onemogočen
Strežnik s ključi A
Ključ A
Strežnik s ključi B
Ključ B
Dostop do podatkov omogočen

Hvala.