
biokoda

biokoda®

X3DH in Double Ratchet

Vpogled v drobovje modernih šifrirnih algoritmov

DENIS JUSTINEK

CTO, BIOKODA

O predavanju

1. **DEL**

   UVOD

   LASTNOSTI ŠIFRIRNIH PROTOKOLOV

   X3DH (Trikratni Diffie-Hellman)

   DOUBLE RATCHET (Dvojna Raglja)

2. **DEL**

   IZVEDBA X3DH in DR nad živim šifrirnim jedrom

   DEBATA

biokoda®

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

Cryptography Engineering
Ferguson, Schneier, Kohno

biokoda®

"The system must not require secrecy and can be stolen by the enemy without causing trouble."

Auguste Kerckhoffs

biokoda®

Vir: http://thebestbikelock.com/how-to-lock-your-bike/

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

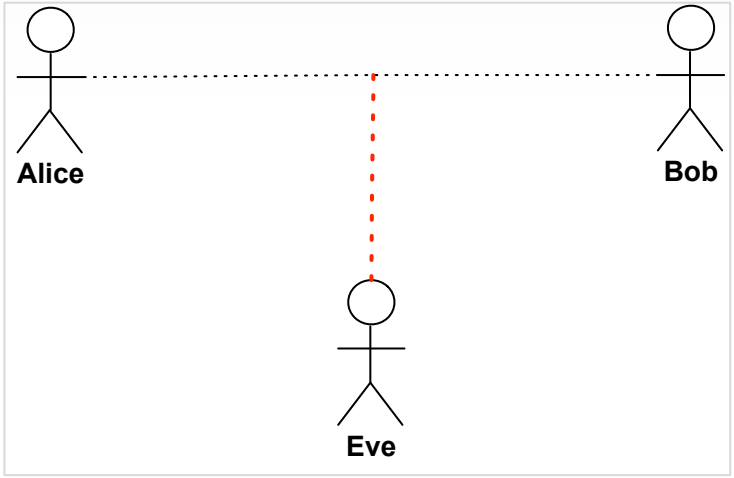
Vir: https://www.vosizneias.com/108021/2012/06/15/washington-obama-administration-will-offer-immunity-to-certain-illegal-immigrants/

- Kriptologija

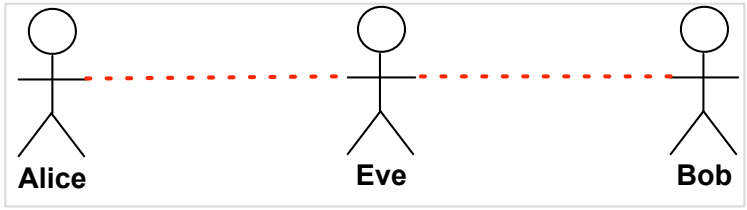
  - **Kriptografija** – tajnost, šifriranje, zakrivanje sporočil

  - **Kriptoanaliza** – razkrivanje, razbijanje tajnih podatkov

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



Eve v vlogi pasivnega napadalca



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

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
  - SHA-3
  - BLAKE2
- Simetrično šifriranje (bločne funkcije, pretočne funkcije)
  - S pomočjo zasebnega ključa (skrivnosti) transformiramo vhodni niz v šifriran niz.
  - Temelji na deljeni skrivnosti.
  - AES256 (različni algoritmi/implementacije), XSalsa20, XChaCha20, ...
- 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.
  - secp256k1, secp384r1,... Curve25519, Curve448,...
- Overjanje podatkov (digitalno podpisovanje)

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.

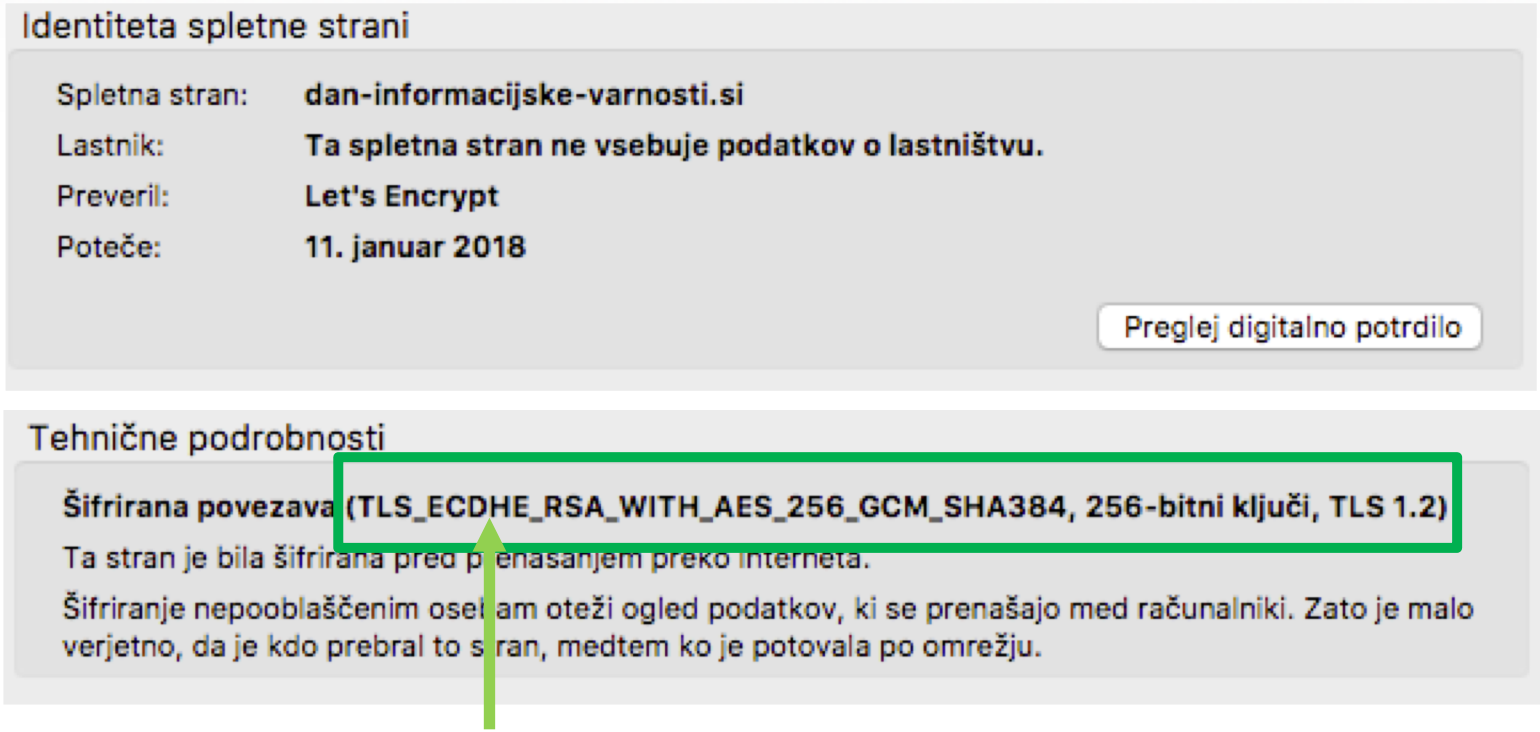
Poudarjena zaupnost (PFS)

- 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

X3DH + Double Ratchet

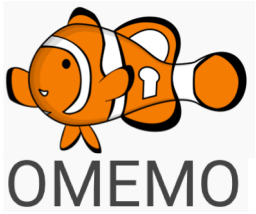
- Sodobni mehanizem v praksi – X3DH + Double Ratchet
- Implementacije za namene varovanja medčloveške in druge komunikacije
- Cilj: zagotovitev PFS, future secrecy, preprečevanje napada s posrednikom, enostavnost vzpostavitve varovanega kanala za komuniciranje, možnost preverjanja varnega kanala (seje)

- Implementacije 3DH + DoubleRatchet z variacijami

BIOCODED

Signal

wire



X3DH in Double Ratchet

- X3DH
  - Asinhrona izmenjava šifrirnega materiala za vzpostavitev šifrirane seje, pri katerem je ciljna naprava lahko nedosegljiva v času vzpostavitev
  - Akterji: Alice, strežnik, Bob
- Zahteve
  - Alice in Bob imata s strežnikom vzpostavljeno razmerje.
  - Alice želi poslati vzpostaviti šifriran kanal z osebo Bob
  - Bob želi omogočiti Alice vzpostavitev šifriranega kanala. Bob je v času vzpsotavitve lahko brez omrežne povezave.
  - Strežnik mora omogočiti Bobu, da objavi minimalni nabor podatkov s pomočjo katerih Alice lahko vzpostavi šifrirano sejo
- Tipična implementacija s Curve25519 in Curve448
  - X25519 in X448

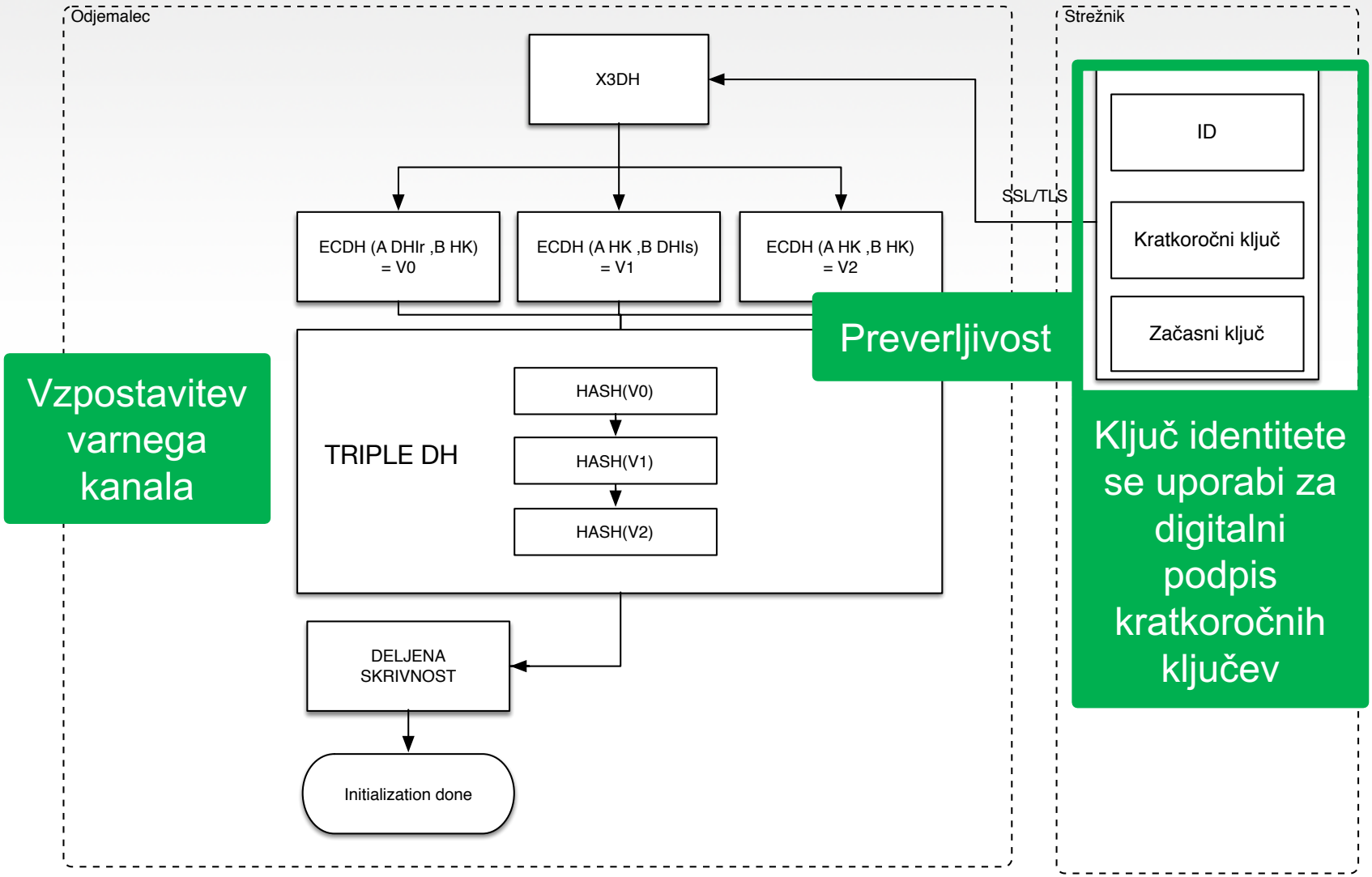
X3DH in Double Ratchet

- Šifrirni ključi za vzpostavitev šifrirnega kanala
  - Šifrirni ključ identitete (asim.)
  - Šifrirni ključ vzpostavitve seje (handshake, ephemeral,... - asim.)
  - Šifrirni ključ za enkratno uporabo (one-time prekey, ratchet prekey,... – asim.)

X3DH in Double Ratchet

- X3DH se izvede skozi 3 korake
  - Bob predhodno objavi šifrirni material za vzpostavitev šifrirane seje
  - Alice prejme šifrirni material za vzpostavitev seje iz strežnika
  - Bob prejme šifrirano sporočilo iz strežnika, vzpostavi sejo, odšifrira sporočilo

X3DH in Double Ratchet



3DH: vzpostavitev varnega kanala

POENOSTAVLJEN OPIS

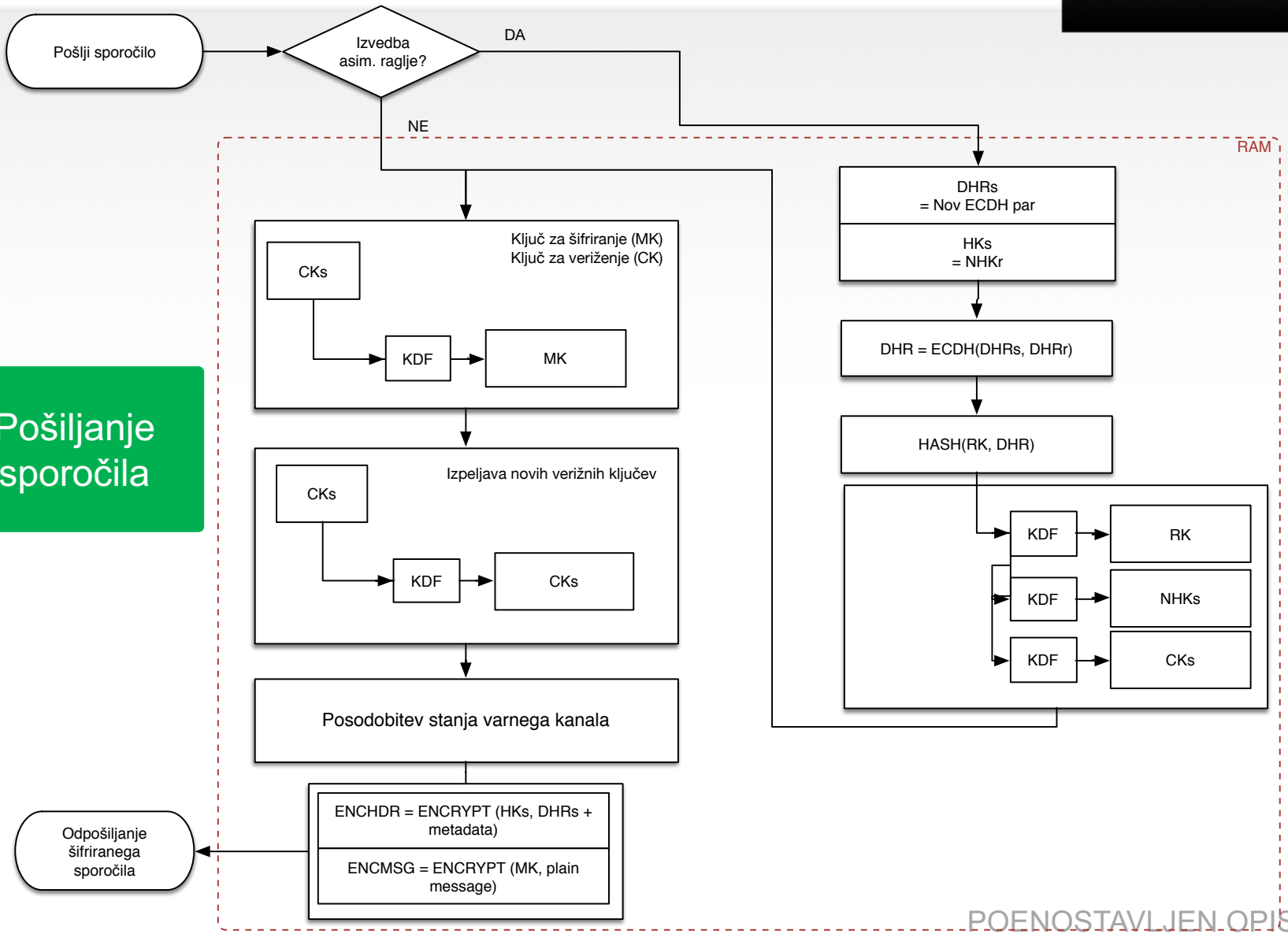
X3DH in Double Ratchet

- 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.

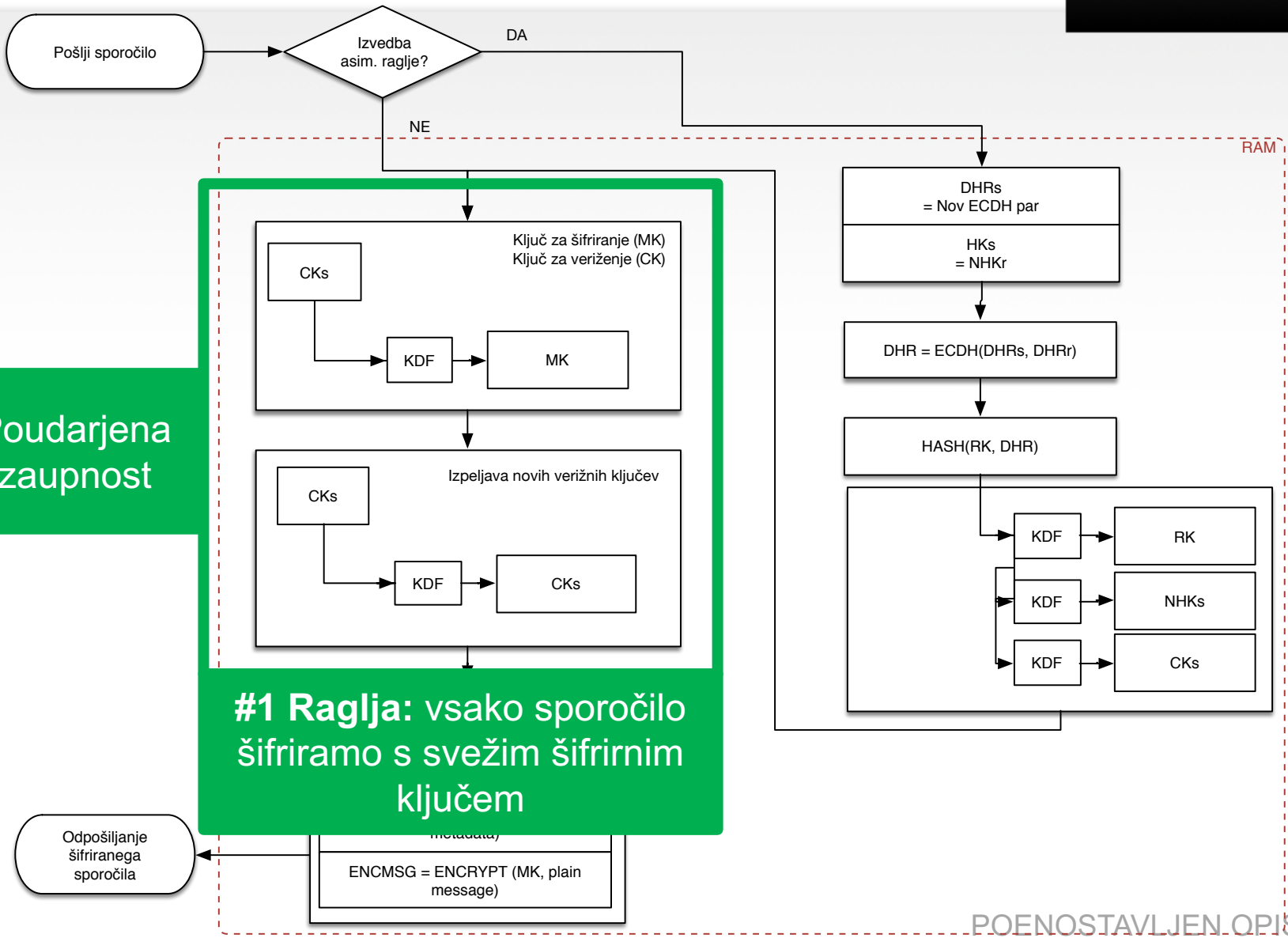
X3DH in Double Ratchet



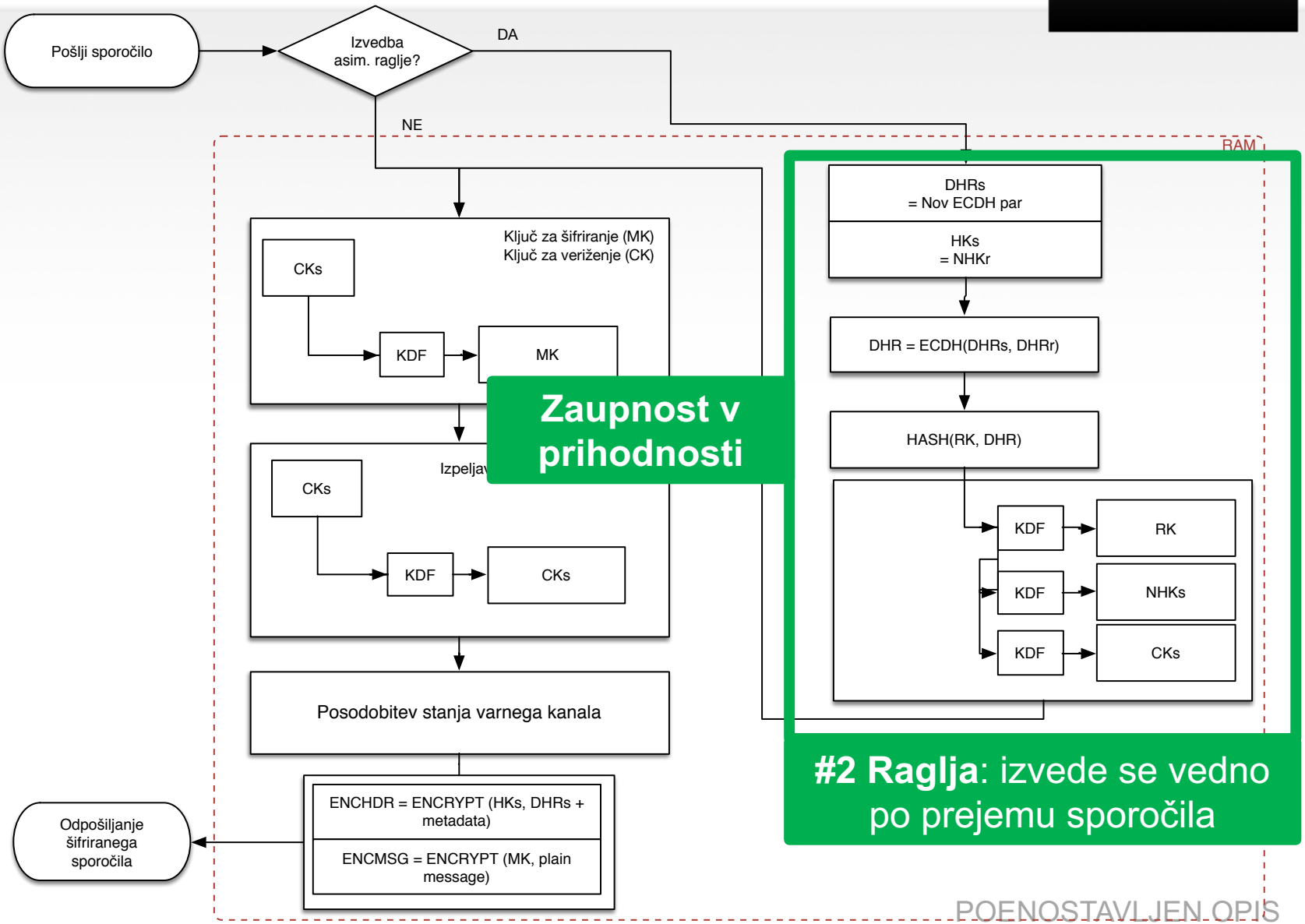
Pošiljanje sporočila

POENOSTAVLJEN OPIS

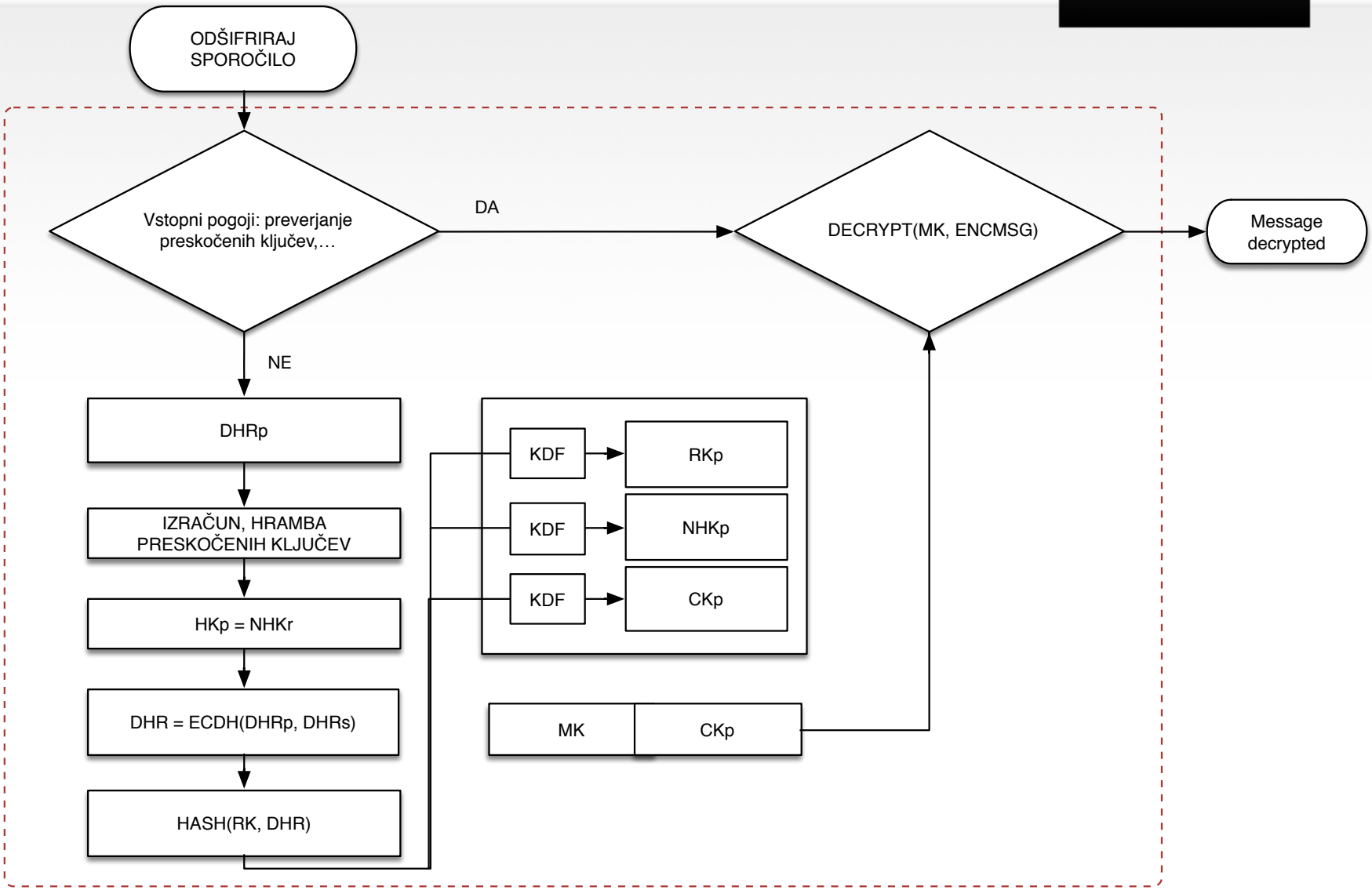
X3DH in Double Ratchet



X3DH in Double Ratchet



X3DH in Double Ratchet

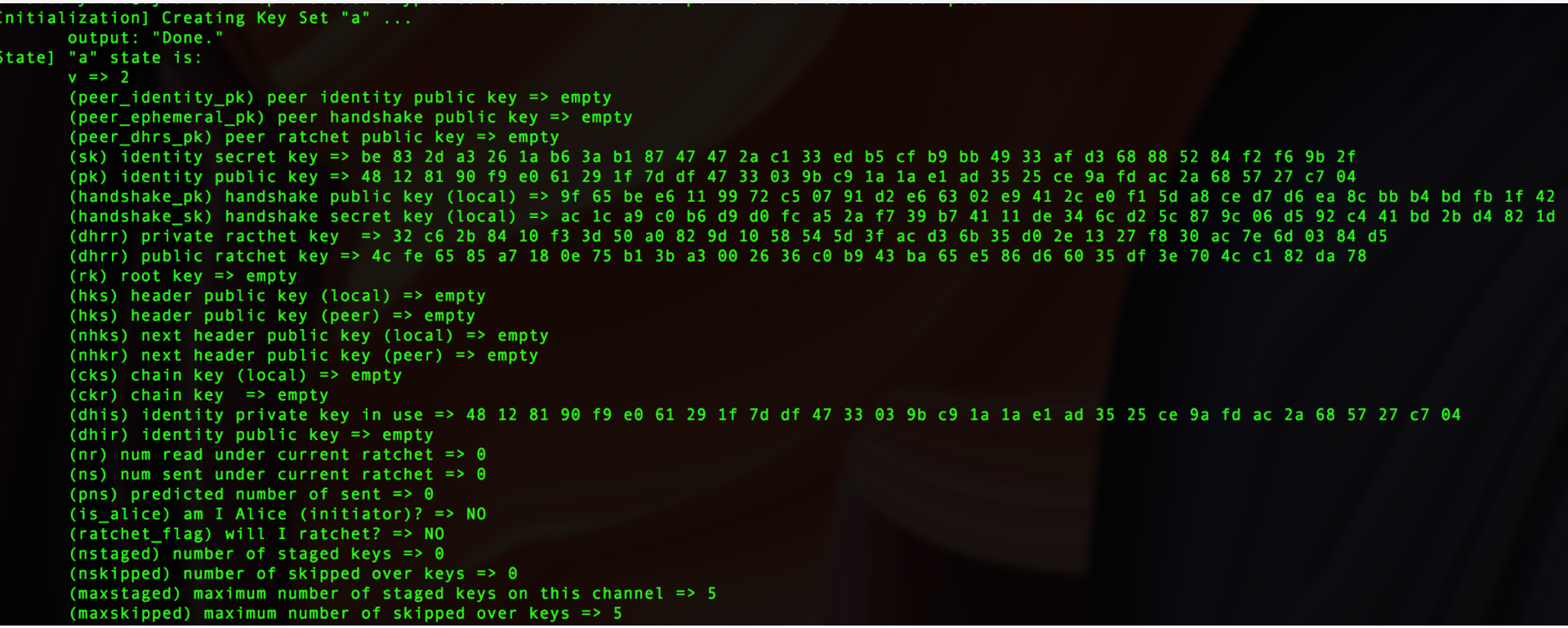


POENOSTAVLJEN OPIS

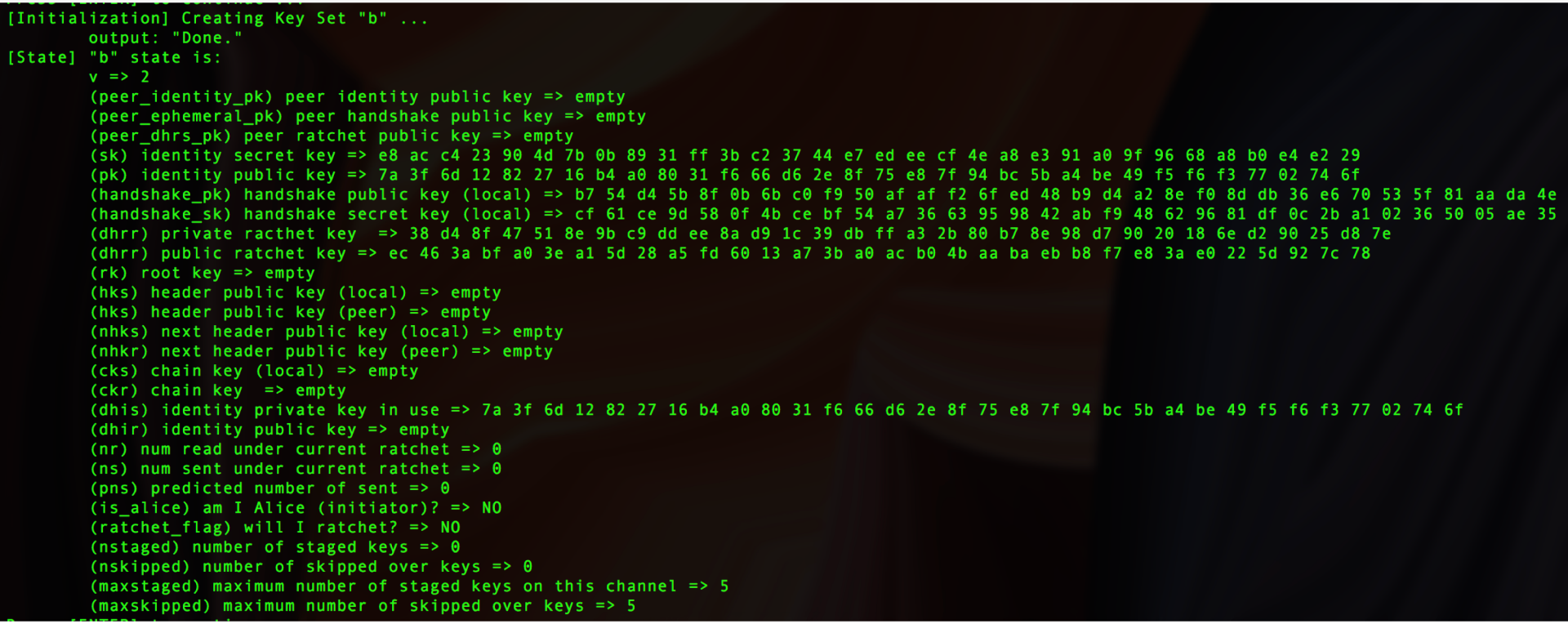
DEMO

Biocoded sandbox

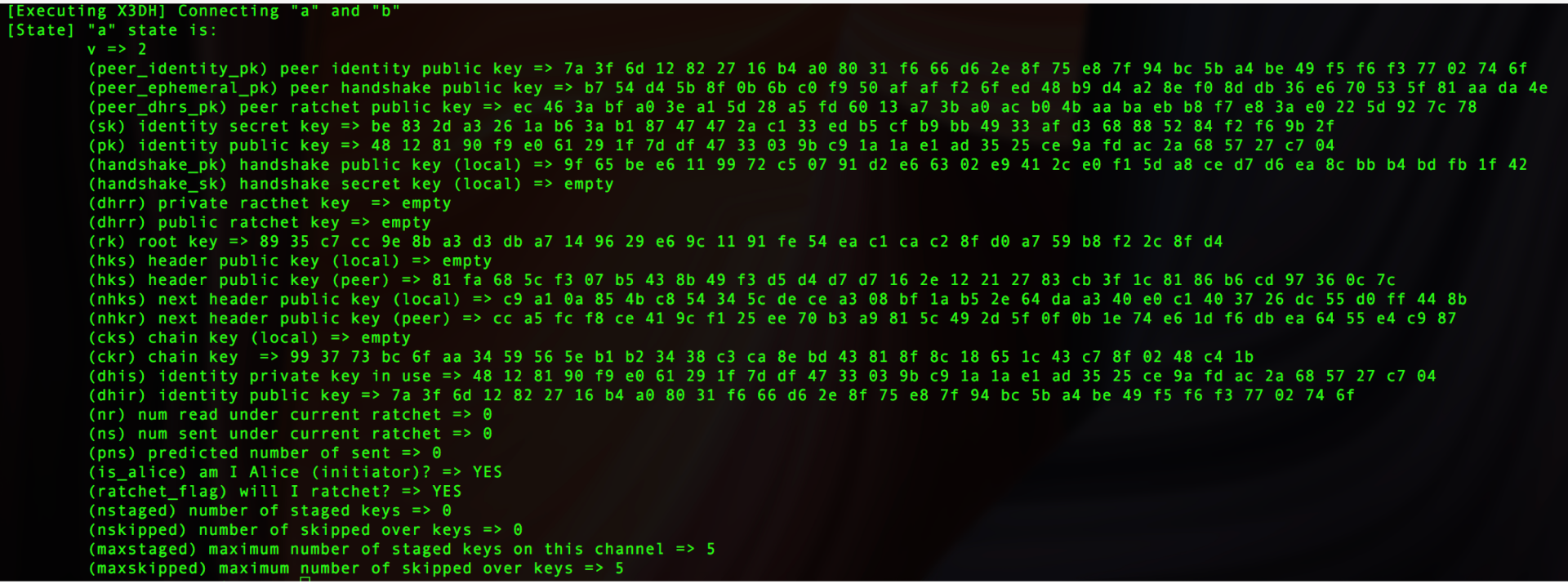
X3DH + DR simluacija
na realnem šifrirnem jedru



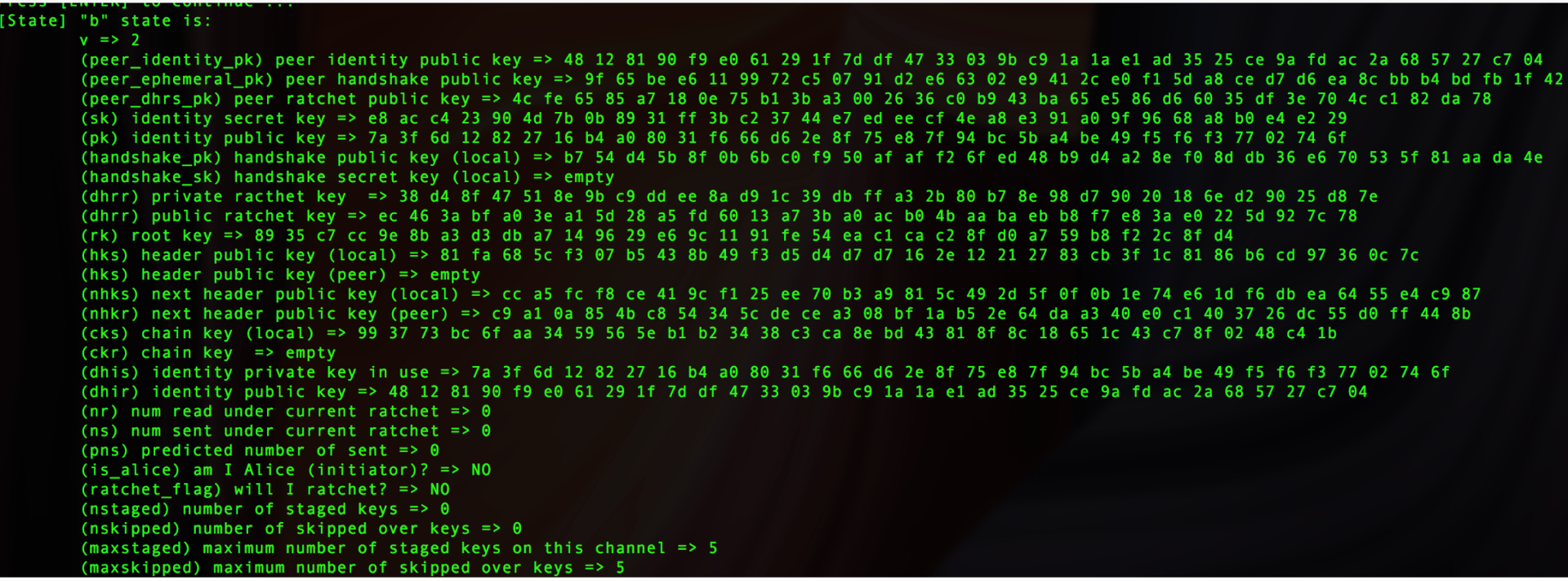
Ustvarimo skupke ključev (A).



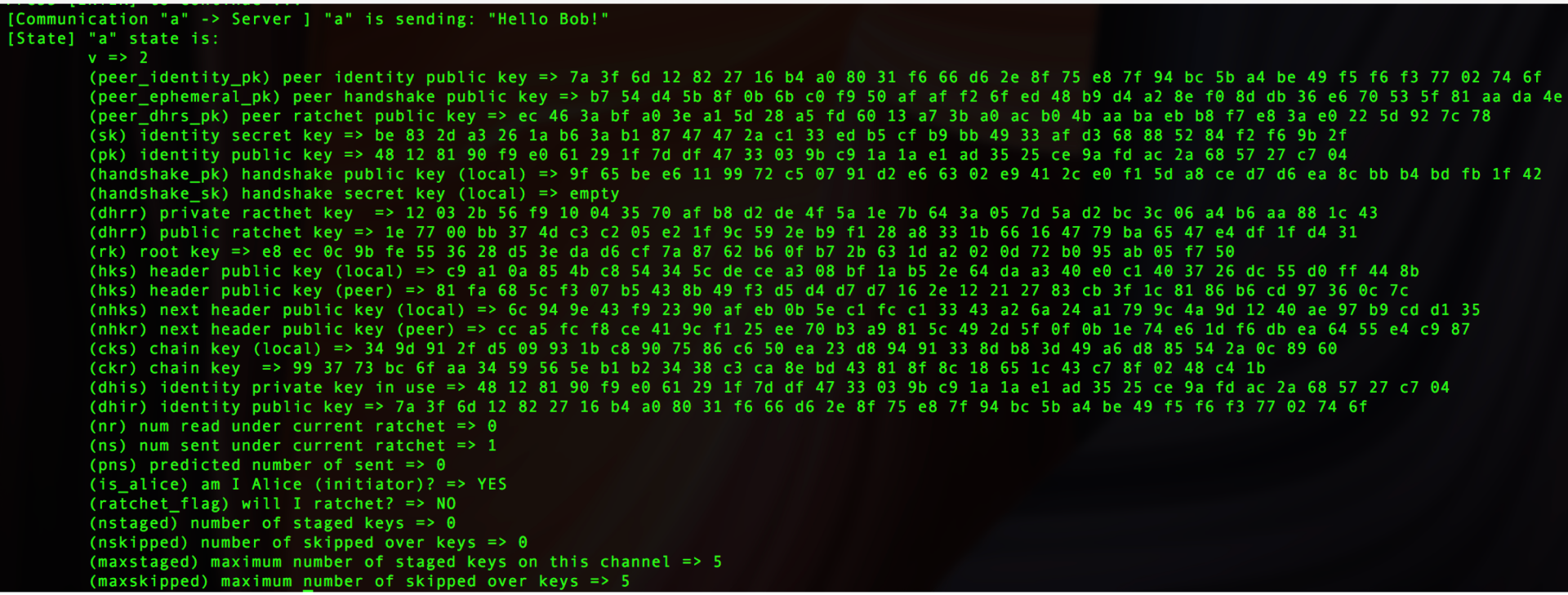
Ustvarimo skupke ključev (B).



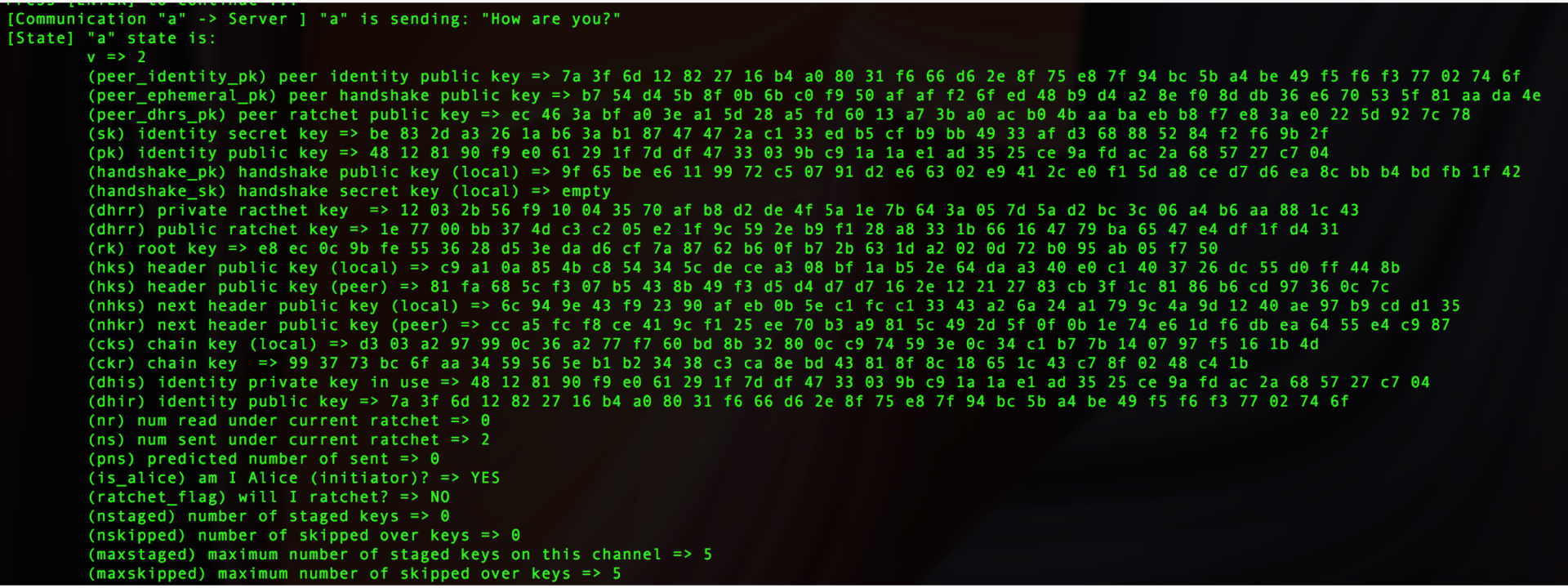
X3DH postopek. Stanje A.



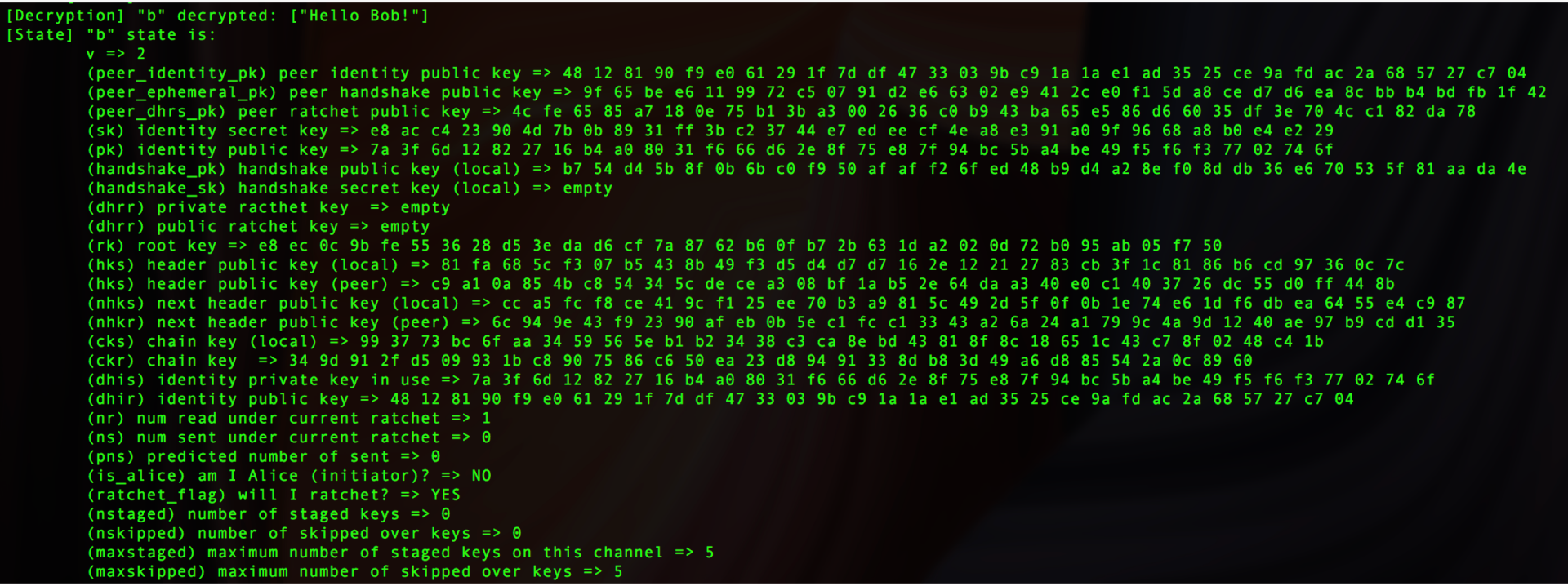
X3DH postopek. Stanje B.



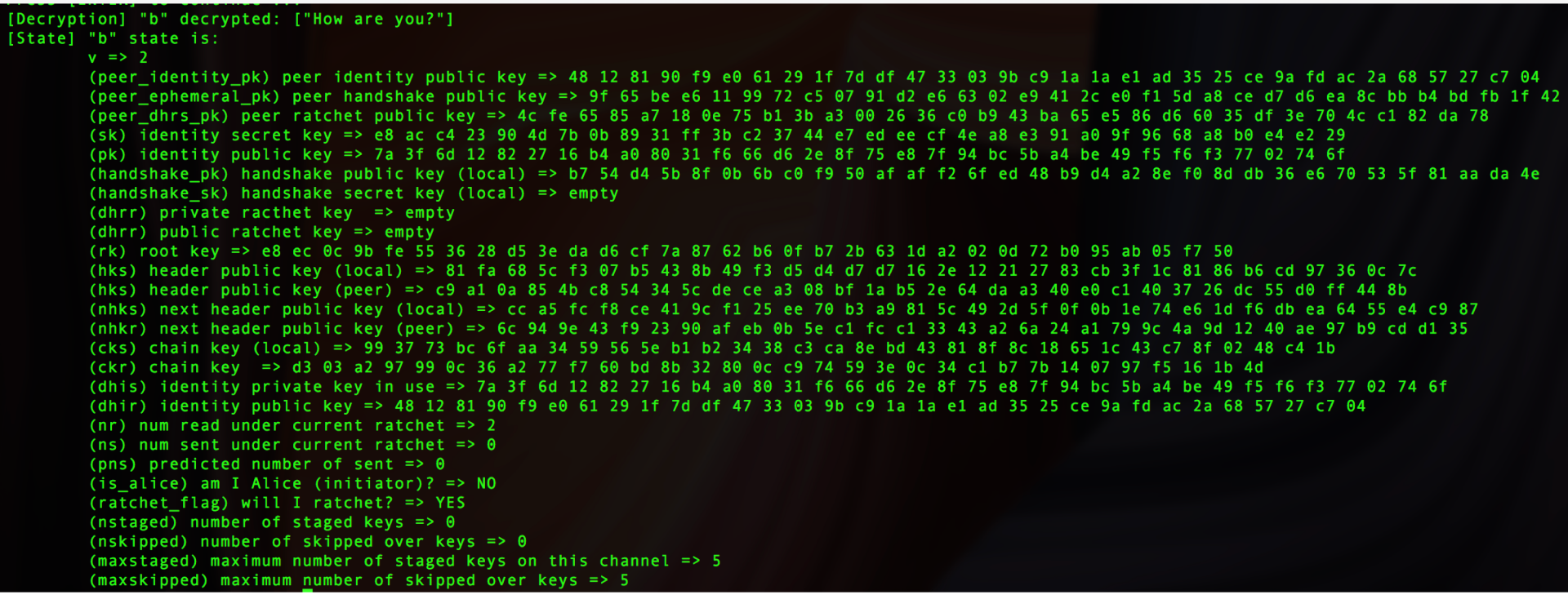
A šifrira in pošlje sporočilo. Stanje A.



A šifrira in pošlje sporočilo. Stanje A.



B prejme sporočilo in odšifrira. Stanje B.



B prejme sporočilo in odšifrira. Stanje B.

biokoda®

Simulacija delovanja šifrirnega jedra.

biokoda®

Q & A

Hvala.