



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

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

Cryptography Engineering
Ferguson, Schneier, Kohno

”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/>



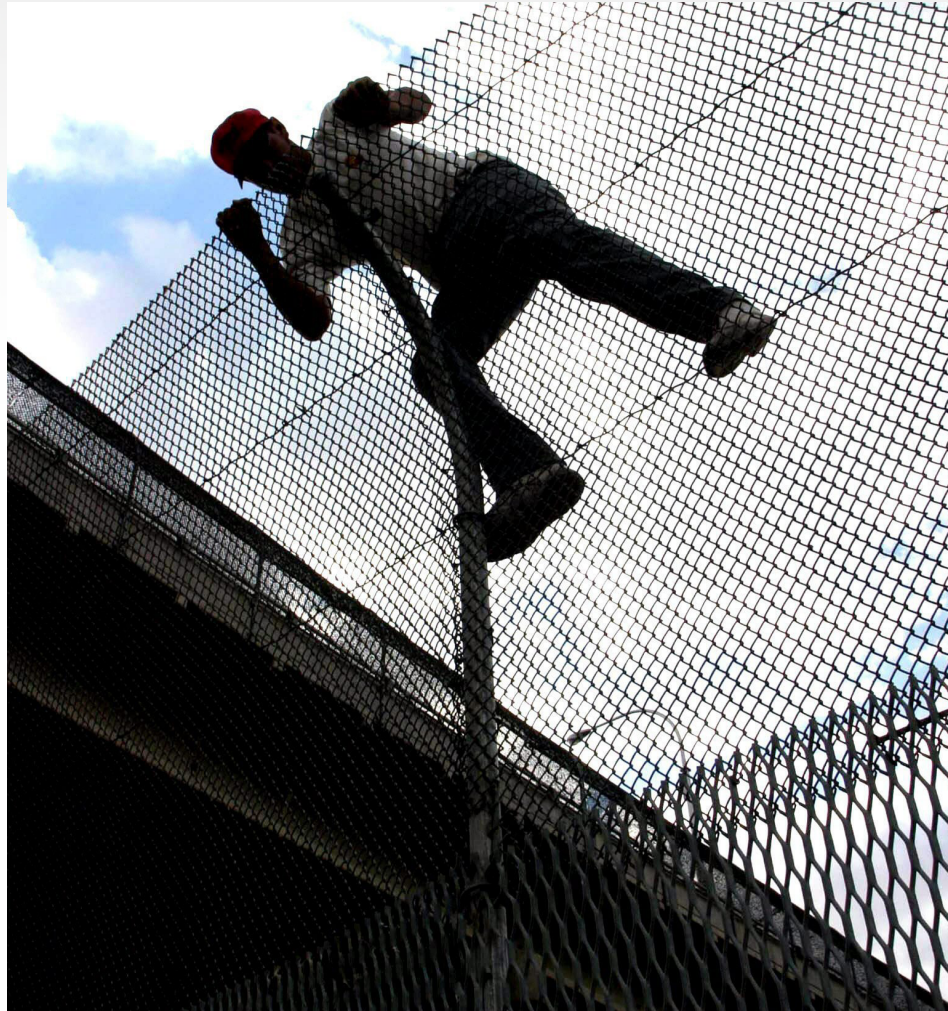
biokoda®



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



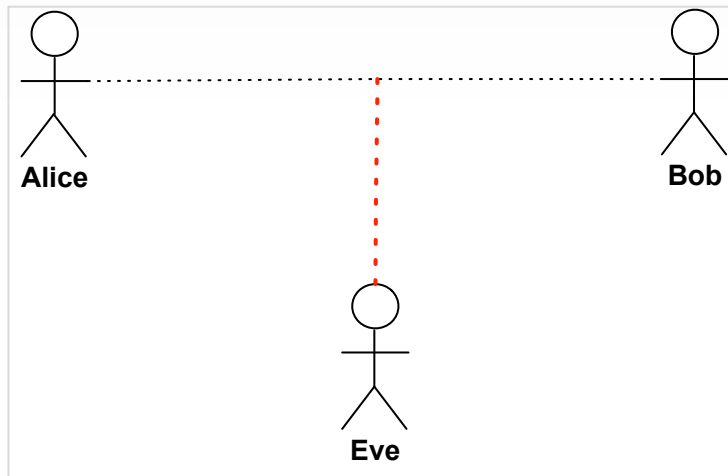
biokoda®



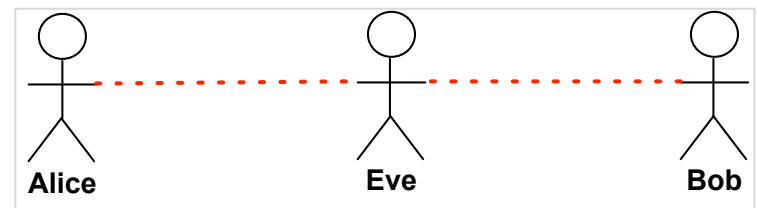
Vir: <https://www.vosizneias.com/108021/2012/06/15/washington-obama-administration-will-offer-immunity-to-certain-illegal-immigrants/>

- 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*)



- 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



- 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 šifirnih 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)



- 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 **pritrđen**.



- 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 determinističnih izračunov

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

Identiteta spletne strani

Spletna stran: **dan-informacijske-varnosti.si**
Lastnik: **Ta spletna stran ne vsebuje podatkov o lastništvu.**
Preveril: **Let's Encrypt**
Poteče: **11. januar 2018**

[Poglej digitalno potrdilo](#)

Tehnične podrobnosti

Šifrirana povezava (**TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-bitni ključi, TLS 1.2**)

Ta stran je bila šifrirana pred prenosom preko interneta.

Šifriranje nepooblaščenim osebam oteži ogled podatkov, ki se prenašajo med računalniki. Zato je malo verjetno, da je kdo prebral to stran, medtem ko je potovala po omrežju.

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

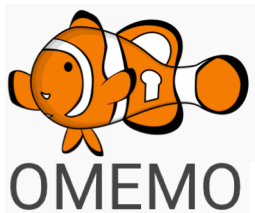


- Sodobni mehanizem v praksi – X3DH + Double Ratchet
- Implementacije za namene varovanja medčloveške in druge komunikacije
- Cilj: zagotovitev PFS, future secrecy, preprečevanje napada s posrednikom, enostavnost vzpostavitve varovanega kanala za komuniciranje, možnost preverjanja varnega kanala (seje)

- Implementacije 3DH + DoubleRatchet z variacijami



wire™





- X3DH
 - Asinhrona izmenjava šifrirnega materiala za vzpostavitev šifrirane seje, pri katerem je ciljna naprava lahko nedosegljiva v času vzpostavitve
 - 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 vzpostavitve 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

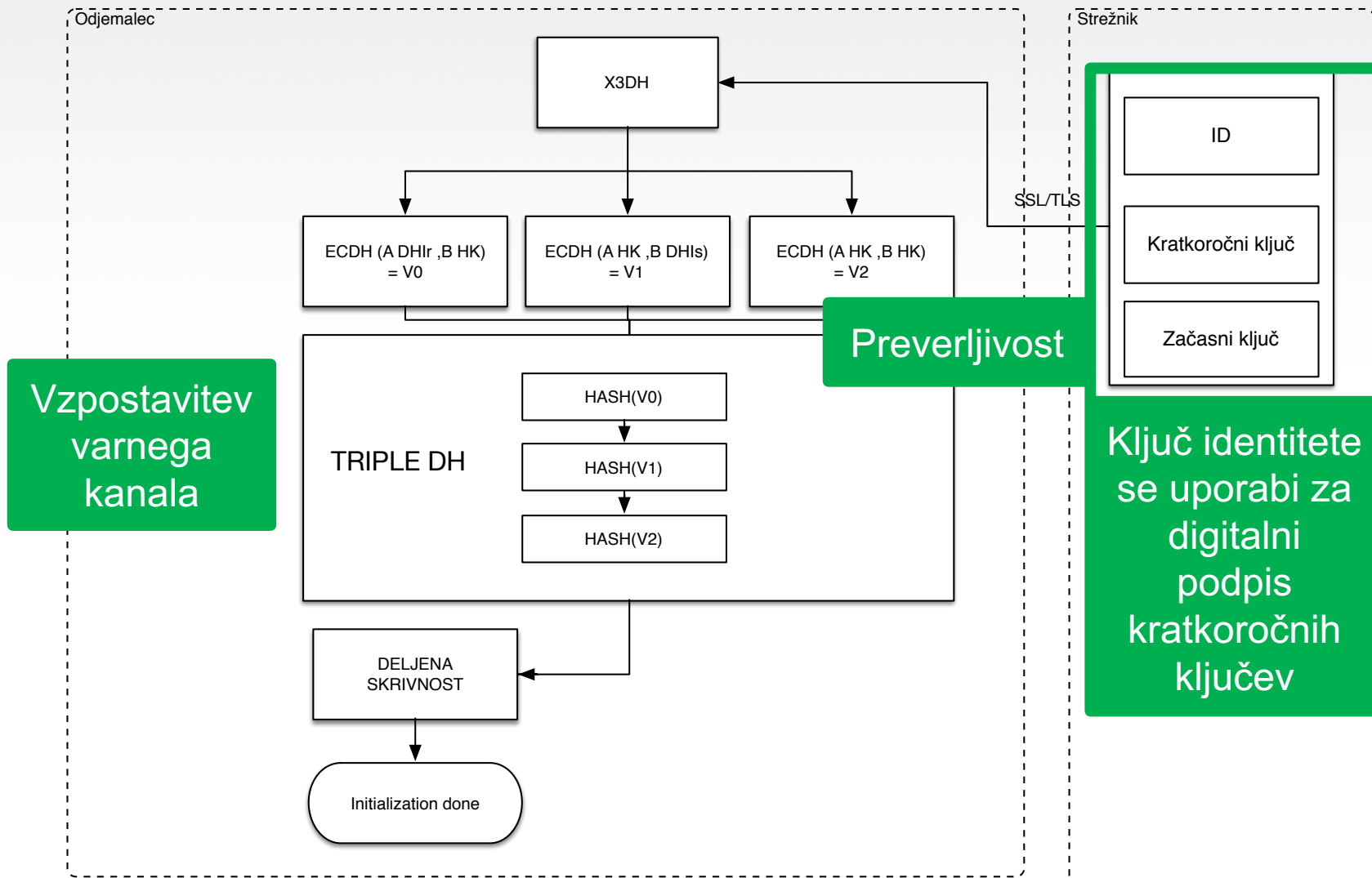


- Šifrirni ključi za vzpostavitev šifrirnega kanala
 - Šifrirni ključ identitete (asim.)
 - Šifrirni ključ vzpostavitve seje (handshake, ephemeral,... - asim.)
 - Šifrirni ključ za enkratno uporabo (one-time prekey, ratchet prekey,... – asim.)



- X3DH 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



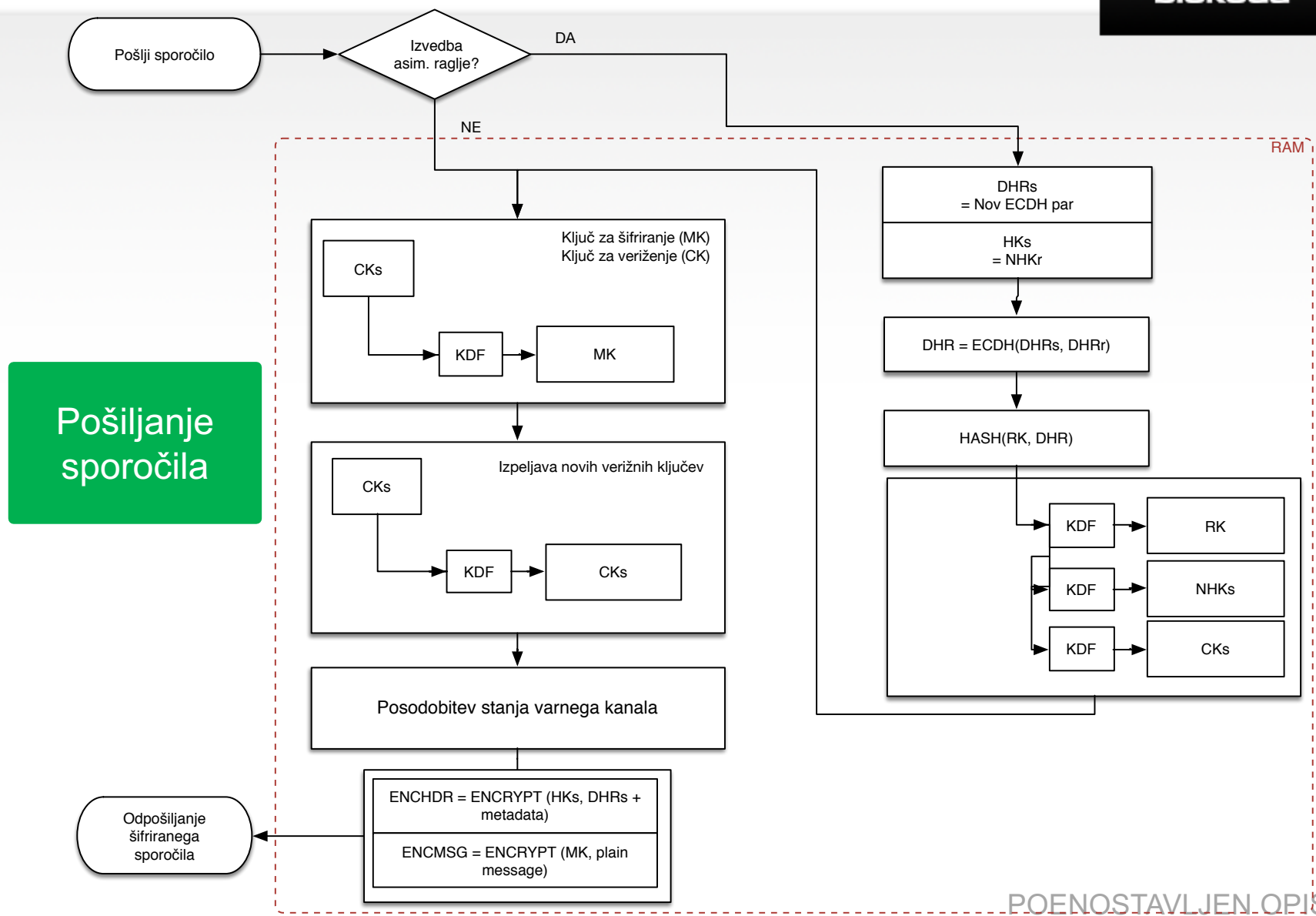
3DH: vzpostavitev varnega kanala

POENOSTAVLJEN OPIS

- Od kod poimenovanje “Double Ratchet” oz. dvosmerna raglja?
- #1 Raglja: Simetrična raglja s pomočjo zgoščevanja izpeljuje nove zasebne ključke 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 ključki #1 raglji.

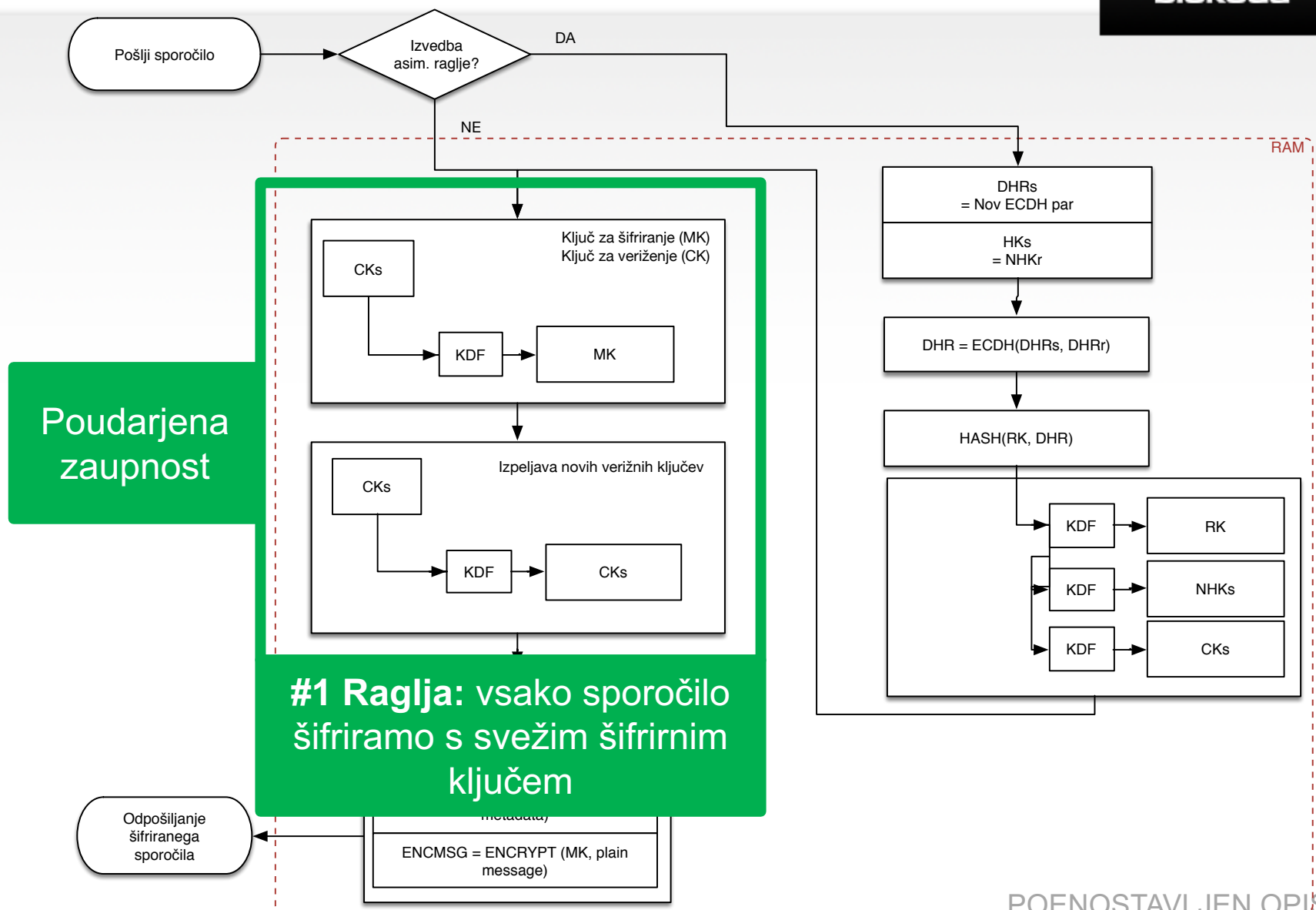


X3DH in Double Ratchet



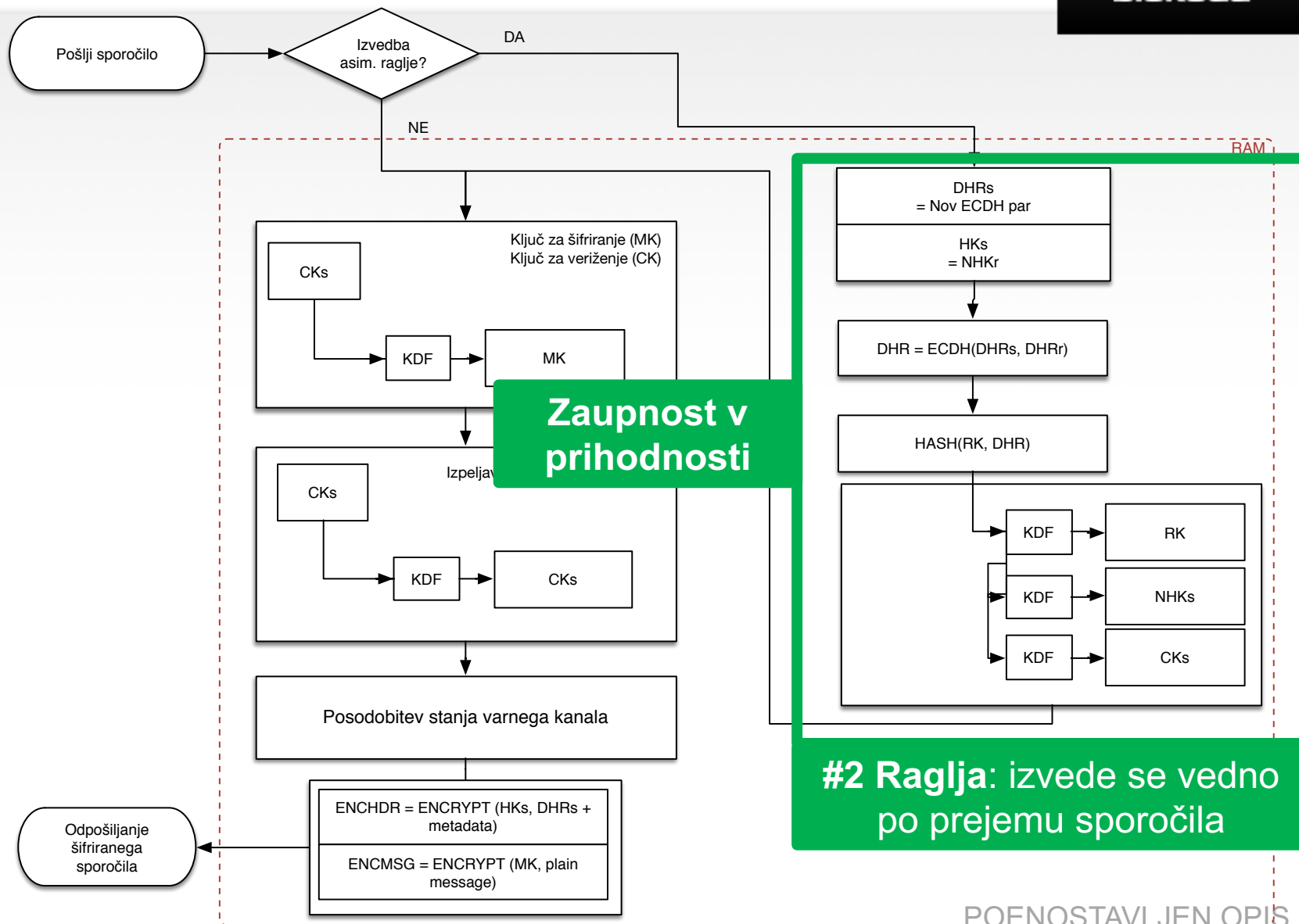
POENOSTAVLJEN OPIS

X3DH in Double Ratchet

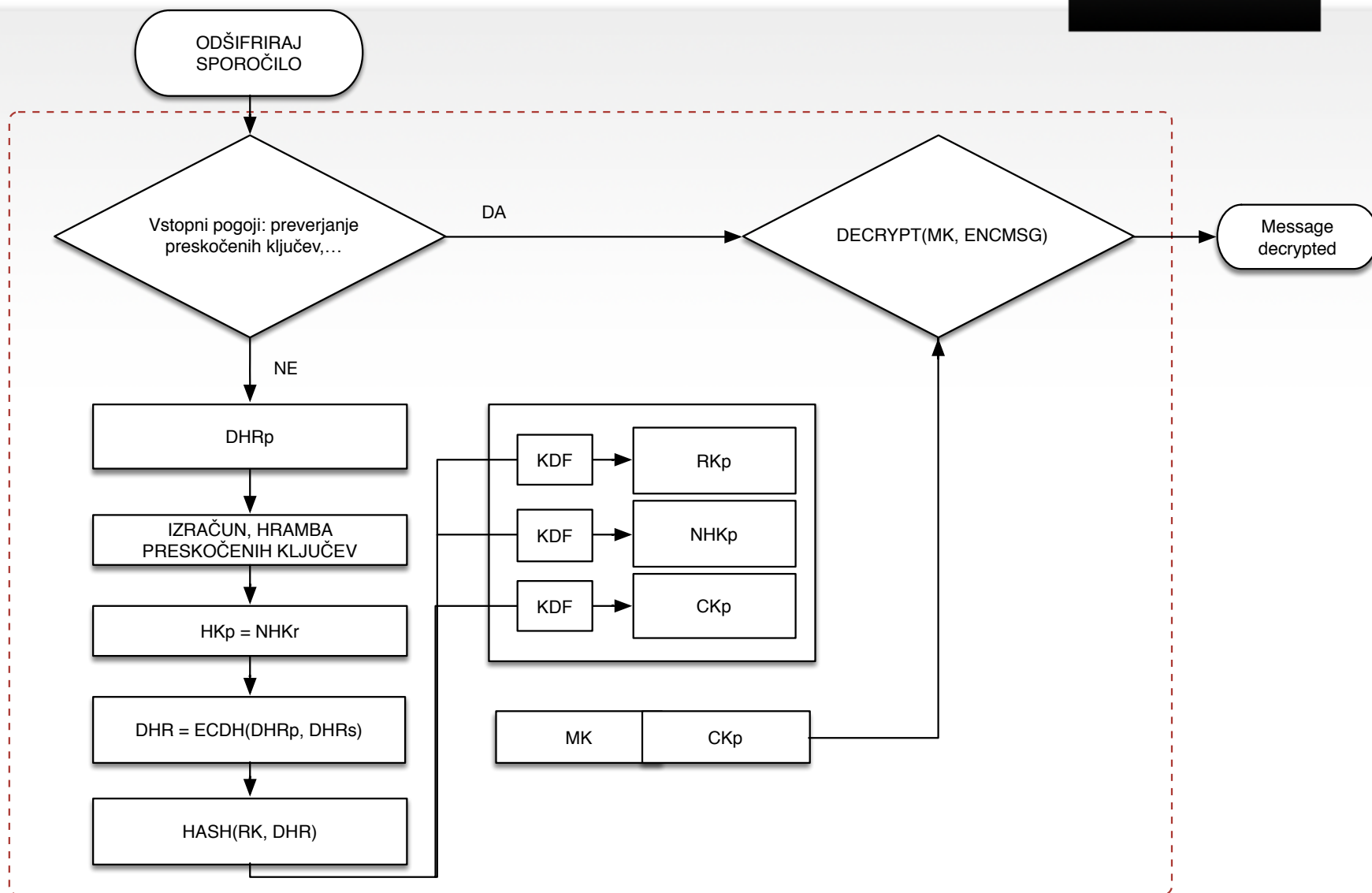


POENOSTAVLJEN OPIS

X3DH in Double Ratchet



X3DH in Double Ratchet



POENOSTAVLJEN OPIS

DEMO

Biocoded sandbox

X3DH + DR simulacija
na realnem šifrirnem jedru

```
[initialization] Creating Key Set "a" ...
output: "Done."
State] "a" state is:
v => 2
(peer_identity_pk) peer identity public key => empty
(peer_ephemeral_pk) peer handshake public key => empty
(peer_dhrs_pk) peer ratchet public key => empty
(sk) identity secret key => be 83 2d a3 26 1a b6 3a b1 87 47 47 2a c1 33 ed b5 cf b9 bb 49 33 af d3 68 88 52 84 f2 f6 9b 2f
(pk) identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(handshake_pk) handshake public key (local) => 9f 65 be e6 11 99 72 c5 07 91 d2 e6 63 02 e9 41 2c e0 f1 5d a8 ce d7 d6 ea 8c bb b4 bd fb 1f 42
(handshake_sk) handshake secret key (local) => ac 1c a9 c0 b6 d9 d0 fc a5 2a f7 39 b7 41 11 de 34 6c d2 5c 87 9c 06 d5 92 c4 41 bd 2b d4 82 1d
(dhrr) private ratchet key => 32 c6 2b 84 10 f3 3d 50 a0 82 9d 10 58 54 5d 3f ac d3 6b 35 d0 2e 13 27 f8 30 ac 7e 6d 03 84 d5
(dhrr) public ratchet key => 4c fe 65 85 a7 18 0e 75 b1 3b a3 00 26 36 c0 b9 43 ba 65 e5 86 d6 60 35 df 3e 70 4c c1 82 da 78
(rk) root key => empty
(hks) header public key (local) => empty
(hks) header public key (peer) => empty
(nhks) next header public key (local) => empty
(nhkr) next header public key (peer) => empty
(cks) chain key (local) => empty
(ckr) chain key => empty
(dhis) identity private key in use => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(dhir) identity public key => empty
(nr) num read under current ratchet => 0
(ns) num sent under current ratchet => 0
(pns) predicted number of sent => 0
(is_alice) am I Alice (initiator)? => NO
(ratchet_flag) will I ratchet? => NO
(nstaged) number of staged keys => 0
(nskipped) number of skipped over keys => 0
(maxstaged) maximum number of staged keys on this channel => 5
(maxskipped) maximum number of skipped over keys => 5
```

Ustvarimo skupke ključev (A).

```
[Initialization] Creating Key Set "b" ...
output: "Done."
[State] "b" state is:
v => 2
(peer_identity_pk) peer identity public key => empty
(peer_ephemeral_pk) peer handshake public key => empty
(peer_dhrs_pk) peer ratchet public key => empty
(sk) identity secret key => e8 ac c4 23 90 4d 7b 0b 89 31 ff 3b c2 37 44 e7 ed ee cf 4e a8 e3 91 a0 9f 96 68 a8 b0 e4 e2 29
(pk) identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(handshake_pk) handshake public key (local) => b7 54 d4 5b 8f 0b 6b c0 f9 50 af af f2 6f ed 48 b9 d4 a2 8e f0 8d db 36 e6 70 53 5f 81 aa da 4e
(handshake_sk) handshake secret key (local) => cf 61 ce 9d 58 0f 4b ce bf 54 a7 36 63 95 98 42 ab f9 48 62 96 81 df 0c 2b a1 02 36 50 05 ae 35
(dhrr) private ratchet key => 38 d4 8f 47 51 8e 9b c9 dd ee 8a d9 1c 39 db ff a3 2b 80 b7 8e 98 d7 90 20 18 6e d2 90 25 d8 7e
(dhrr) public ratchet key => ec 46 3a bf a0 3e a1 5d 28 a5 fd 60 13 a7 3b a0 ac b0 4b aa ba eb b8 f7 e8 3a e0 22 5d 92 7c 78
(rk) root key => empty
(hks) header public key (local) => empty
(hks) header public key (peer) => empty
(nhks) next header public key (local) => empty
(nhkr) next header public key (peer) => empty
(cks) chain key (local) => empty
(cckr) chain key => empty
(dhis) identity private key in use => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(dhir) identity public key => empty
(nr) num read under current ratchet => 0
(ns) num sent under current ratchet => 0
(pns) predicted number of sent => 0
(is_alice) am I Alice (initiator)? => NO
(ratchet_flag) will I ratchet? => NO
(nstaged) number of staged keys => 0
(nskipped) number of skipped over keys => 0
(maxstaged) maximum number of staged keys on this channel => 5
(maxskipped) maximum number of skipped over keys => 5
```

Ustvarimo skupke ključev (B).

```
[Executing X3DH] Connecting "a" and "b"
[State] "a" state is:
v => 2
(peer_identity_pk) peer identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(peer_ephemeral_pk) peer handshake public key => b7 54 d4 5b 8f 0b 6b c0 f9 50 af af f2 6f ed 48 b9 d4 a2 8e f0 8d db 36 e6 70 53 5f 81 aa da 4e
(peer_dhrs_pk) peer ratchet public key => ec 46 3a bf a0 3e a1 5d 28 a5 fd 60 13 a7 3b a0 ac b0 4b aa ba eb b8 f7 e8 3a e0 22 5d 92 7c 78
(sk) identity secret key => be 83 2d a3 26 1a b6 3a b1 87 47 47 2a c1 33 ed b5 cf b9 bb 49 33 af d3 68 88 52 84 f2 f6 9b 2f
(pk) identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(handshake_pk) handshake public key (local) => 9f 65 be e6 11 99 72 c5 07 91 d2 e6 63 02 e9 41 2c e0 f1 5d a8 ce d7 d6 ea 8c bb b4 bd fb 1f 42
(handshake_sk) handshake secret key (local) => empty
(dhrr) private ratchet key => empty
(dhrr) public ratchet key => empty
(rk) root key => 89 35 c7 cc 9e 8b a3 d3 db a7 14 96 29 e6 9c 11 91 fe 54 ea c1 ca c2 8f d0 a7 59 b8 f2 2c 8f d4
(hks) header public key (local) => empty
(hks) header public key (peer) => 81 fa 68 5c f3 07 b5 43 8b 49 f3 d5 d4 d7 d7 16 2e 12 21 27 83 cb 3f 1c 81 86 b6 cd 97 36 0c 7c
(nhks) next header public key (local) => c9 a1 0a 85 4b c8 54 34 5c de ce a3 08 bf 1a b5 2e 64 da a3 40 e0 c1 40 37 26 dc 55 d0 ff 44 8b
(nhkr) next header public key (peer) => cc a5 fc f8 ce 41 9c f1 25 ee 70 b3 a9 81 5c 49 2d 5f 0f 0b 1e 74 e6 1d f6 db ea 64 55 e4 c9 87
(cks) chain key (local) => empty
(ckr) chain key => 99 37 73 bc 6f aa 34 59 56 5e b1 b2 34 38 c3 ca 8e bd 43 81 8f 8c 18 65 1c 43 c7 8f 02 48 c4 1b
(dhis) identity private key in use => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(dhir) identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(nr) num read under current ratchet => 0
(ns) num sent under current ratchet => 0
(pns) predicted number of sent => 0
(is_alice) am I Alice (initiator)? => YES
(ratchet_flag) will I ratchet? => YES
(nstaged) number of staged keys => 0
(nskipped) number of skipped over keys => 0
(maxstaged) maximum number of staged keys on this channel => 5
(maxskipped) maximum number of skipped over keys => 5
```

X3DH postopek. Stanje A.

Press [ENTER] to continue ...

[State] "b" state is:

```
v => 2
(peer_identity_pk) peer identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(peer_ephemeral_pk) peer handshake public key => 9f 65 be e6 11 99 72 c5 07 91 d2 e6 63 02 e9 41 2c e0 f1 5d a8 ce d7 d6 ea 8c bb b4 bd fb 1f 42
(peer_dhrs_pk) peer ratchet public key => 4c fe 65 85 a7 18 0e 75 b1 3b a3 00 26 36 c0 b9 43 ba 65 e5 86 d6 60 35 df 3e 70 4c c1 82 da 78
(sk) identity secret key => e8 ac c4 23 90 4d 7b 0b 89 31 ff 3b c2 37 44 e7 ed ee cf 4e a8 e3 91 a0 9f 96 68 a8 b0 e4 e2 29
(pk) identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(handshake_pk) handshake public key (local) => b7 54 d4 5b 8f 0b 6b c0 f9 50 af af f2 6f ed 48 b9 d4 a2 8e f0 8d db 36 e6 70 53 5f 81 aa da 4e
(handshake_sk) handshake secret key (local) => empty
(dhrr) private ratchet key => 38 d4 8f 47 51 8e 9b c9 dd ee 8a d9 1c 39 db ff a3 2b 80 b7 8e 98 d7 90 20 18 6e d2 90 25 d8 7e
(dhrr) public ratchet key => ec 46 3a bf a0 3e a1 5d 28 a5 fd 60 13 a7 3b a0 ac b0 4b aa ba eb b8 f7 e8 3a e0 22 5d 92 7c 78
(rk) root key => 89 35 c7 cc 9e 8b a3 d3 db a7 14 96 29 e6 9c 11 91 fe 54 ea c1 ca c2 8f d0 a7 59 b8 f2 2c 8f d4
(hks) header public key (local) => 81 fa 68 5c f3 07 b5 43 8b 49 f3 d5 d4 d7 d7 16 2e 12 21 27 83 cb 3f 1c 81 86 b6 cd 97 36 0c 7c
(hks) header public key (peer) => empty
(nhks) next header public key (local) => cc a5 fc f8 ce 41 9c f1 25 ee 70 b3 a9 81 5c 49 2d 5f 0f 0b 1e 74 e6 1d f6 db ea 64 55 e4 c9 87
(nhkr) next header public key (peer) => c9 a1 0a 85 4b c8 54 34 5c de ce a3 08 bf 1a b5 2e 64 da a3 40 e0 c1 40 37 26 dc 55 d0 ff 44 8b
(cks) chain key (local) => 99 37 73 bc 6f aa 34 59 56 5e b1 b2 34 38 c3 ca 8e bd 43 81 8f 8c 18 65 1c 43 c7 8f 02 48 c4 1b
(ckr) chain key => empty
(dhis) identity private key in use => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(dhir) identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(nr) num read under current ratchet => 0
(ns) num sent under current ratchet => 0
(pns) predicted number of sent => 0
(is_alice) am I Alice (initiator)? => NO
(ratchet_flag) will I ratchet? => NO
(nstaged) number of staged keys => 0
(nskipped) number of skipped over keys => 0
(maxstaged) maximum number of staged keys on this channel => 5
(maxskipped) maximum number of skipped over keys => 5
```

X3DH postopek. Stanje B.

```
[Communication "a" -> Server ] "a" is sending: "Hello Bob!"
[State] "a" state is:
v => 2
(peer_identity_pk) peer identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(peer_ephemeral_pk) peer handshake public key => b7 54 d4 5b 8f 0b 6b c0 f9 50 af af f2 6f ed 48 b9 d4 a2 8e f0 8d db 36 e6 70 53 5f 81 aa da 4e
(peer_dhrrs_pk) peer ratchet public key => ec 46 3a bf a0 3e a1 5d 28 a5 fd 60 13 a7 3b a0 ac b0 4b aa ba eb b8 f7 e8 3a e0 22 5d 92 7c 78
(sk) identity secret key => be 83 2d a3 26 1a b6 3a b1 87 47 47 2a c1 33 ed b5 cf b9 bb 49 33 af d3 68 88 52 84 f2 f6 9b 2f
(pk) identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(handshake_pk) handshake public key (local) => 9f 65 be e6 11 99 72 c5 07 91 d2 e6 63 02 e9 41 2c e0 f1 5d a8 ce d7 d6 ea 8c bb b4 bd fb 1f 42
(handshake_sk) handshake secret key (local) => empty
(dhrr) private ratchet key => 12 03 2b 56 f9 10 04 35 70 af b8 d2 de 4f 5a 1e 7b 64 3a 05 7d 5a d2 bc 3c 06 a4 b6 aa 88 1c 43
(dhrr) public ratchet key => 1e 77 00 bb 37 4d c3 c2 05 e2 1f 9c 59 2e b9 f1 28 a8 33 1b 66 16 47 79 ba 65 47 e4 df 1f d4 31
(rk) root key => e8 ec 0c 9b fe 55 36 28 d5 3e da d6 cf 7a 87 62 b6 0f b7 2b 63 1d a2 02 0d 72 b0 95 ab 05 f7 50
(hks) header public key (local) => c9 a1 0a 85 4b c8 54 34 5c de ce a3 08 bf 1a b5 2e 64 da a3 40 e0 c1 40 37 26 dc 55 d0 ff 44 8b
(hks) header public key (peer) => 81 fa 68 5c f3 07 b5 43 8b 49 f3 d5 d4 d7 d7 16 2e 12 21 27 83 cb 3f 1c 81 86 b6 cd 97 36 0c 7c
(nhks) next header public key (local) => 6c 94 9e 43 f9 23 90 af eb 0b 5e c1 fc c1 33 43 a2 6a 24 a1 79 9c 4a 9d 12 40 ae 97 b9 cd d1 35
(nhkr) next header public key (peer) => cc a5 fc f8 ce 41 9c f1 25 ee 70 b3 a9 81 5c 49 2d 5f 0f 0b 1e 74 e6 1d f6 db ea 64 55 e4 c9 87
(cks) chain key (local) => 34 9d 91 2f d5 09 93 1b c8 90 75 86 c6 50 ea 23 d8 94 91 33 8d b8 3d 49 a6 d8 85 54 2a 0c 89 60
(ckr) chain key => 99 37 73 bc 6f aa 34 59 56 5e b1 b2 34 38 c3 ca 8e bd 43 81 8f 8c 18 65 1c 43 c7 8f 02 48 c4 1b
(dhis) identity private key in use => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(dhir) identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(nr) num read under current ratchet => 0
(ns) num sent under current ratchet => 1
(pns) predicted number of sent => 0
(is_alice) am I Alice (initiator)? => YES
(ratchet_flag) will I ratchet? => NO
(nstaged) number of staged keys => 0
(nskipped) number of skipped over keys => 0
(maxstaged) maximum number of staged keys on this channel => 5
(maxskipped) maximum number of skipped over keys => 5
```

A šifrira in pošlje sporočilo. Stanje A.

```
Press [ENTER] to continue ...
[Communication "a" -> Server ] "a" is sending: "How are you?"
[State] "a" state is:
v => 2
(peer_identity_pk) peer identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(peer_ephemeral_pk) peer handshake public key => b7 54 d4 5b 8f 0b 6b c0 f9 50 af af f2 6f ed 48 b9 d4 a2 8e f0 8d db 36 e6 70 53 5f 81 aa da 4e
(peer_dhrs_pk) peer ratchet public key => ec 46 3a bf a0 3e a1 5d 28 a5 fd 60 13 a7 3b a0 ac b0 4b aa ba eb b8 f7 e8 3a e0 22 5d 92 7c 78
(sk) identity secret key => be 83 2d a3 26 1a b6 3a b1 87 47 47 2a c1 33 ed b5 cf b9 bb 49 33 af d3 68 88 52 84 f2 f6 9b 2f
(pk) identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(handshake_pk) handshake public key (local) => 9f 65 be e6 11 99 72 c5 07 91 d2 e6 63 02 e9 41 2c e0 f1 5d a8 ce d7 d6 ea 8c bb b4 bd fb 1f 42
(handshake_sk) handshake secret key (local) => empty
(dhrr) private ratchet key => 12 03 2b 56 f9 10 04 35 70 af b8 d2 de 4f 5a 1e 7b 64 3a 05 7d 5a d2 bc 3c 06 a4 b6 aa 88 1c 43
(dhrr) public ratchet key => 1e 77 00 bb 37 4d c3 c2 05 e2 1f 9c 59 2e b9 f1 28 a8 33 1b 66 16 47 79 ba 65 47 e4 df 1f d4 31
(rk) root key => e8 ec 0c 9b fe 55 36 28 d5 3e da d6 cf 7a 87 62 b6 0f b7 2b 63 1d a2 02 0d 72 b0 95 ab 05 f7 50
(hks) header public key (local) => c9 a1 0a 85 4b c8 54 34 5c de ce a3 08 bf 1a b5 2e 64 da a3 40 e0 c1 40 37 26 dc 55 d0 ff 44 8b
(hks) header public key (peer) => 81 fa 68 5c f3 07 b5 43 8b 49 f3 d5 d4 d7 d7 16 2e 12 21 27 83 cb 3f 1c 81 86 b6 cd 97 36 0c 7c
(nhks) next header public key (local) => 6c 94 9e 43 f9 23 90 af eb 0b 5e c1 fc c1 33 43 a2 6a 24 a1 79 9c 4a 9d 12 40 ae 97 b9 cd d1 35
(nhkr) next header public key (peer) => cc a5 fc f8 ce 41 9c f1 25 ee 70 b3 a9 81 5c 49 2d 5f 0f 0b 1e 74 e6 1d f6 db ea 64 55 e4 c9 87
(cks) chain key (local) => d3 03 a2 97 99 0c 36 a2 77 f7 60 bd 8b 32 80 0c c9 74 59 3e 0c 34 c1 b7 7b 14 07 97 f5 16 1b 4d
(ckr) chain key => 99 37 73 bc 6f aa 34 59 56 5e b1 b2 34 38 c3 ca 8e bd 43 81 8f 8c 18 65 1c 43 c7 8f 02 48 c4 1b
(dhis) identity private key in use => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(dhir) identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(nr) num read under current ratchet => 0
(ns) num sent under current ratchet => 2
(pns) predicted number of sent => 0
(is_alice) am I Alice (initiator)? => YES
(ratchet_flag) will I ratchet? => NO
(nstaged) number of staged keys => 0
(nskipped) number of skipped over keys => 0
(maxstaged) maximum number of staged keys on this channel => 5
(maxskipped) maximum number of skipped over keys => 5
```

A šifrira in pošlje sporočilo. Stanje A.

```
[Decryption] "b" decrypted: ["Hello Bob!"]
[State] "b" state is:
v => 2
(peer_identity_pk) peer identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(peer_ephemeral_pk) peer handshake public key => 9f 65 be e6 11 99 72 c5 07 91 d2 e6 63 02 e9 41 2c e0 f1 5d a8 ce d7 d6 ea 8c bb b4 bd fb 1f 42
(peer_dhrs_pk) peer ratchet public key => 4c fe 65 85 a7 18 0e 75 b1 3b a3 00 26 36 c0 b9 43 ba 65 e5 86 d6 60 35 df 3e 70 4c c1 82 da 78
(sk) identity secret key => e8 ac c4 23 90 4d 7b 0b 89 31 ff 3b c2 37 44 e7 ed ee cf 4e a8 e3 91 a0 9f 96 68 a8 b0 e4 e2 29
(pk) identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(handshake_pk) handshake public key (local) => b7 54 d4 5b 8f 0b 6b c0 f9 50 af af f2 6f ed 48 b9 d4 a2 8e f0 8d db 36 e6 70 53 5f 81 aa da 4e
(handshake_sk) handshake secret key (local) => empty
(dhrr) private ratchet key => empty
(dhrr) public ratchet key => empty
(rk) root key => e8 ec 0c 9b fe 55 36 28 d5 3e da d6 cf 7a 87 62 b6 0f b7 2b 63 1d a2 02 0d 72 b0 95 ab 05 f7 50
(hks) header public key (local) => 81 fa 68 5c f3 07 b5 43 8b 49 f3 d5 d4 d7 d7 16 2e 12 21 27 83 cb 3f 1c 81 86 b6 cd 97 36 0c 7c
(hks) header public key (peer) => c9 a1 0a 85 4b c8 54 34 5c de ce a3 08 bf 1a b5 2e 64 da a3 40 e0 c1 40 37 26 dc 55 d0 ff 44 8b
(nhks) next header public key (local) => cc a5 fc f8 ce 41 9c f1 25 ee 70 b3 a9 81 5c 49 2d 5f 0f 0b 1e 74 e6 1d f6 db ea 64 55 e4 c9 87
(nhkr) next header public key (peer) => 6c 94 9e 43 f9 23 90 af eb 0b 5e c1 fc c1 33 43 a2 6a 24 a1 79 9c 4a 9d 12 40 ae 97 b9 cd d1 35
(cks) chain key (local) => 99 37 73 bc 6f aa 34 59 56 5e b1 b2 34 38 c3 ca 8e bd 43 81 8f 8c 18 65 1c 43 c7 8f 02 48 c4 1b
(ckr) chain key => 34 9d 91 2f d5 09 93 1b c8 90 75 86 c6 50 ea 23 d8 94 91 33 8d b8 3d 49 a6 d8 85 54 2a 0c 89 60
(dhis) identity private key in use => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(dhir) identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(nr) num read under current ratchet => 1
(ns) num sent under current ratchet => 0
(pns) predicted number of sent => 0
(is_alice) am I Alice (initiator)? => NO
(ratchet_flag) will I ratchet? => YES
(nstaged) number of staged keys => 0
(nskipped) number of skipped over keys => 0
(maxstaged) maximum number of staged keys on this channel => 5
(maxskipped) maximum number of skipped over keys => 5
```

B prejme sporočilo in odšifrira. Stanje B.

```
[Decryption] "b" decrypted: ["How are you?"]
[State] "b" state is:
v => 2
(peer_identity_pk) peer identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(peer_ephemeral_pk) peer handshake public key => 9f 65 be e6 11 99 72 c5 07 91 d2 e6 63 02 e9 41 2c e0 f1 5d a8 ce d7 d6 ea 8c bb b4 bd fb 1f 42
(peer_dhrs_pk) peer ratchet public key => 4c fe 65 85 a7 18 0e 75 b1 3b a3 00 26 36 c0 b9 43 ba 65 e5 86 d6 60 35 df 3e 70 4c c1 82 da 78
(sk) identity secret key => e8 ac c4 23 90 4d 7b 0b 89 31 ff 3b c2 37 44 e7 ed ee cf 4e a8 e3 91 a0 9f 96 68 a8 b0 e4 e2 29
(pk) identity public key => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(handshake_pk) handshake public key (local) => b7 54 d4 5b 8f 0b 6b c0 f9 50 af af f2 6f ed 48 b9 d4 a2 8e f0 8d db 36 e6 70 53 5f 81 aa da 4e
(handshake_sk) handshake secret key (local) => empty
(dhrr) private ratchet key => empty
(dhrr) public ratchet key => empty
(rk) root key => e8 ec 0c 9b fe 55 36 28 d5 3e da d6 cf 7a 87 62 b6 0f b7 2b 63 1d a2 02 0d 72 b0 95 ab 05 f7 50
(hks) header public key (local) => 81 fa 68 5c f3 07 b5 43 8b 49 f3 d5 d4 d7 d7 16 2e 12 21 27 83 cb 3f 1c 81 86 b6 cd 97 36 0c 7c
(hks) header public key (peer) => c9 a1 0a 85 4b c8 54 34 5c de ce a3 08 bf 1a b5 2e 64 da a3 40 e0 c1 40 37 26 dc 55 d0 ff 44 8b
(nhks) next header public key (local) => cc a5 fc f8 ce 41 9c f1 25 ee 70 b3 a9 81 5c 49 2d 5f 0f 0b 1e 74 e6 1d f6 db ea 64 55 e4 c9 87
(nhkr) next header public key (peer) => cc 94 9e 43 f9 23 90 af eb 0b 5e c1 fc c1 33 43 a2 6a 24 a1 79 9c 4a 9d 12 40 ae 97 b9 cd d1 35
(cks) chain key (local) => 99 37 73 bc 6f aa 34 59 56 5e b1 b2 34 38 c3 ca 8e bd 43 81 8f 8c 18 65 1c 43 c7 8f 02 48 c4 1b
(ckr) chain key => d3 03 a2 97 99 0c 36 a2 77 f7 60 bd 8b 32 80 0c c9 74 59 3e 0c 34 c1 b7 7b 14 07 97 f5 16 1b 4d
(dhis) identity private key in use => 7a 3f 6d 12 82 27 16 b4 a0 80 31 f6 66 d6 2e 8f 75 e8 7f 94 bc 5b a4 be 49 f5 f6 f3 77 02 74 6f
(dhir) identity public key => 48 12 81 90 f9 e0 61 29 1f 7d df 47 33 03 9b c9 1a 1a e1 ad 35 25 ce 9a fd ac 2a 68 57 27 c7 04
(nr) num read under current ratchet => 2
(ns) num sent under current ratchet => 0
(pns) predicted number of sent => 0
(is_alice) am I Alice (initiator)? => NO
(ratchet_flag) will I ratchet? => YES
(nstaged) number of staged keys => 0
(nskipped) number of skipped over keys => 0
(maxstaged) maximum number of staged keys on this channel => 5
(maxskipped) maximum number of skipped over keys => 5
```

B prejme sporočilo in odšifrira. Stanje B.

Simulacija delovanja šifrirnega jedra.

Q & A

Hvala.