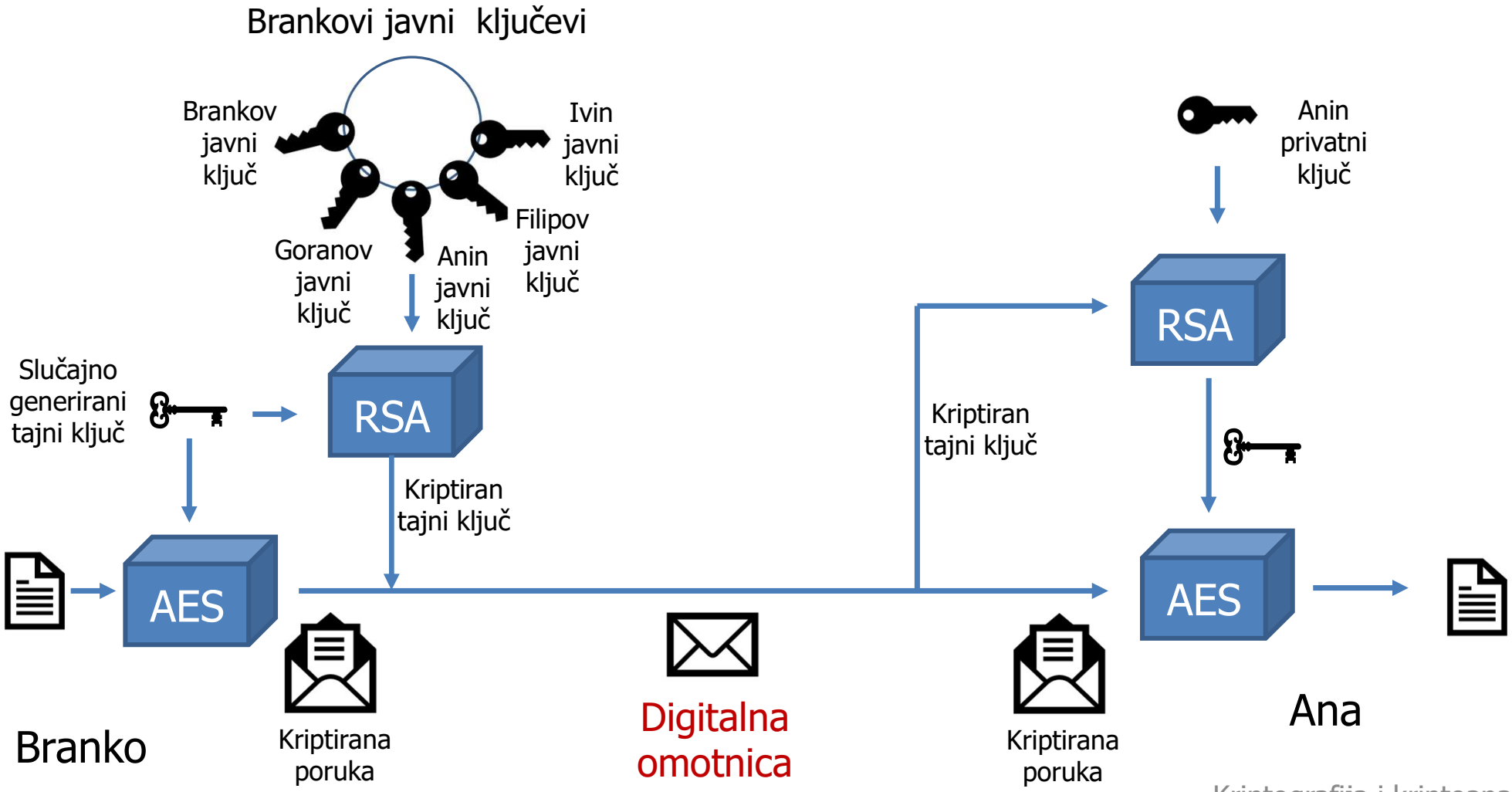
Digitalna omotnica

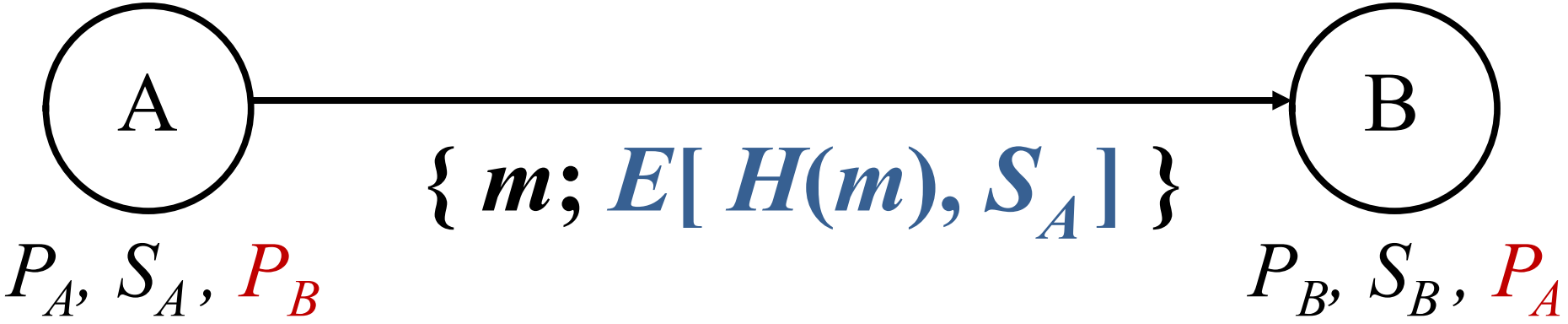
- osigurava tajnost
- pošiljatelj kriptira poruku proizvoljnim ključem K simetričnim algoritmom kriptiranja
- simetrični (sjednički) ključ K se kriptira javnim ključem primatelja P_B
- kriptirana poruka i kriptirani ključ čine digitalnu omotnicu

Kako osigurati tajnost?

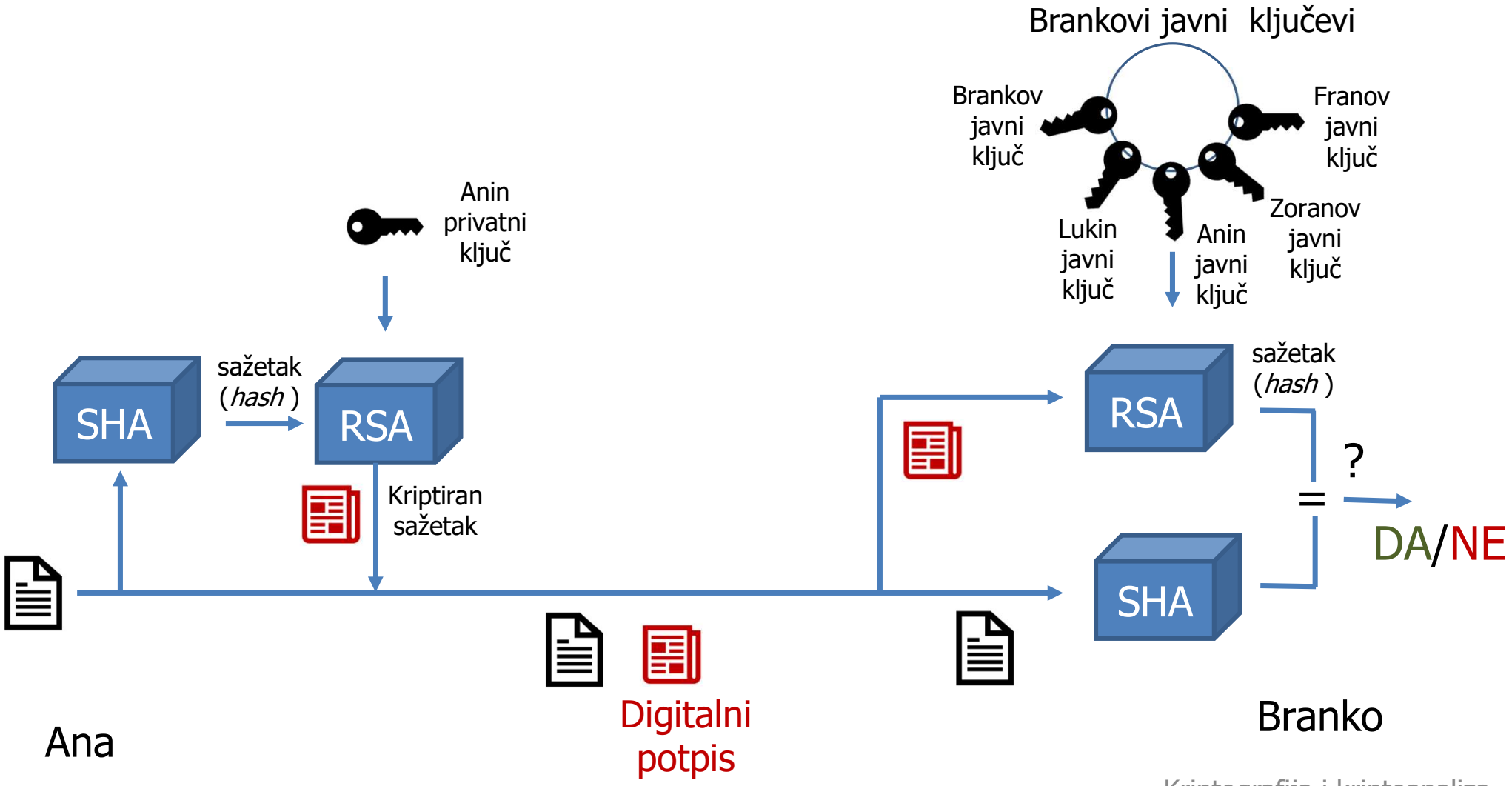


Digitalni potpis

- dodatak poruci koji služi za
  - utvrđivanje besprijekornosti informacije (integritet i neporecivost) i za
  - identifikaciju pošiljatelja (autentičnost)
- ne osigurava tajnost!



Kako osigurati integritet, autentičnost i neporecivost?



Digitalni pečat (1/2)

- digitalni pečat osigurava sva četiri sigurnosna zahtijeva:
  - tajnost
  - autentičnost
  - integritet i
  - neporecivost
- digitalni pečat je digitalno potpisana digitalna omotnica

$$\{ E(m,K); E(K,P_B) \}; E\{ H [E(m,K); E(K,P_B)], S_A \}$$

Digitalni pečat (2/2)

- češće se koristi obrnuti postupak:
  1. digitalno se potpiše poruka
  2. poruka s potpisom se kriptira slučajno generiranim tajnim ključem *K*
  3. na kraju se dodaje kriptirani ključ javnim ključem primatelja
- digitalna omotnica s digitalno potpisanom porukom:

$$E\{\,[\,m;\ \underbrace{E(H(m), S_A)}_{\text{digitalni potpis}}\,],\ K\,\};\ \ E(K, P_B)$$