Kako se skupina podpiše?

Tim Kalan

Mentor: doc. dr. Tilen Marc

27. maj 2024

Zakaj potrebujemo podpise?

- Mislim, da si lahko predstavljate ...
- Avtentikacija, integriteta
- Bančništvo, e-pošta, `ssh`, ...

Kaj je podpis?

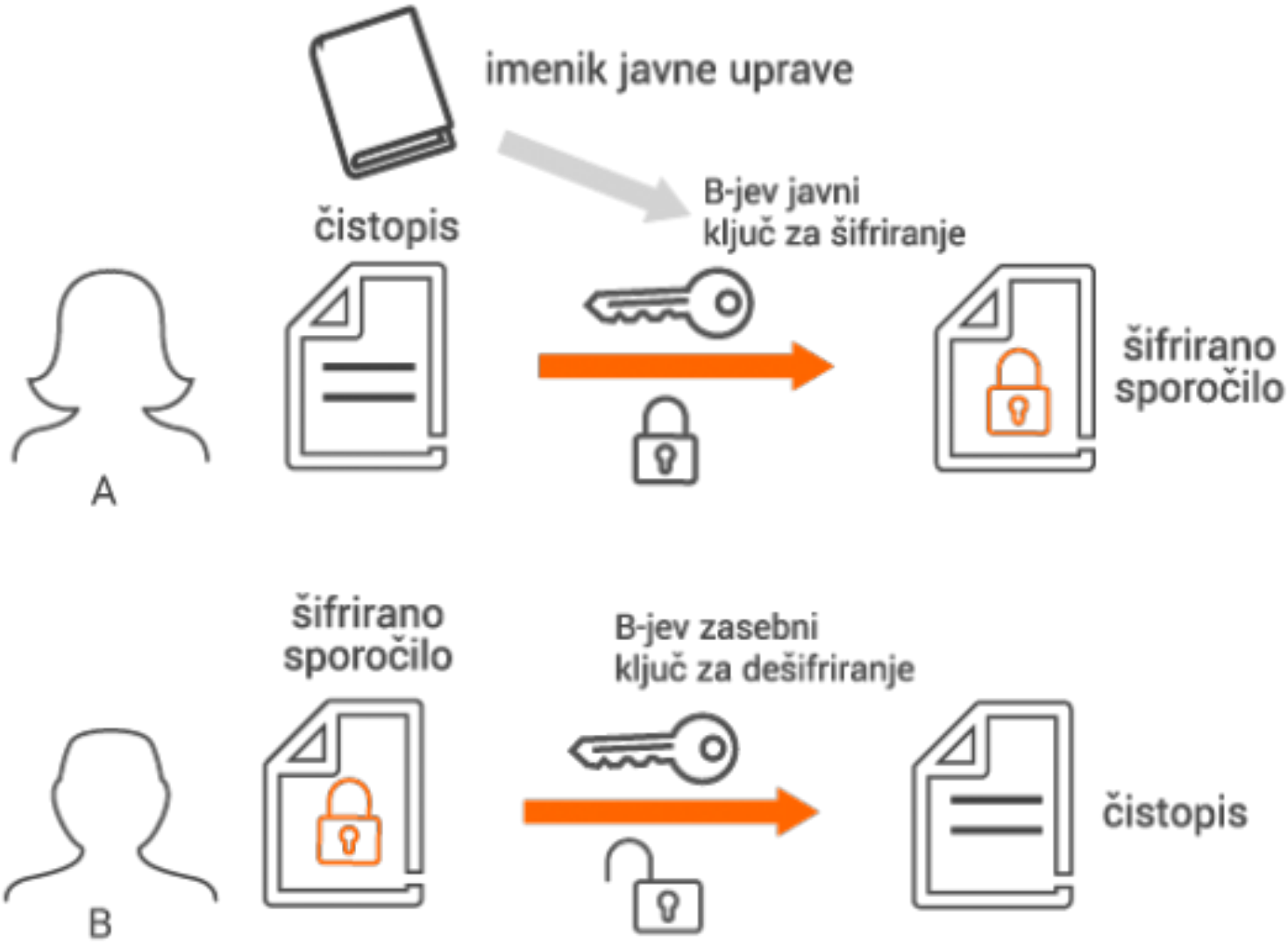
Ročni podpis

- Vsakič (približno) enak
- Enostavno ponarediti
- Težko (zares) preveriti

Digitalni podpis

- Vsakič unikaten
- Težko ponarediti
- Enostavno preveriti

Kriptografija javnega ključa 1



Kriptografija javnega ključa 2

Zgostitvene funkcije

Primer digitalnega podpisa: RSA

Odličen primer za spoznavanje osnovnih konceptov:

- Generiranje ključev
- Podpisovanje
- Preverjanje

RSA: Generiranje ključev

- Izberemo dve veliki praštevili p in q (kako?)
- Izračunamo $n = pq$ in $\phi(n) = (p-1)(q-1)$
- Izberemo e tako, da je $1 < e < \phi(n)$ in $\gcd(e, \phi(n)) = 1$
- Izračunamo d tako, da je $ed \equiv 1 \pmod{\phi(n)}$

Javni ključ: (n, e) **Zasebni ključ**: d

RSA: Podpisovanje in preverjanje

- Sporočilo m podpišemo tako, da izračunamo $s = m^d \bmod n$
- Podpis je par (m, s)

- Preverimo tako, da izračunamo $m' = s^e \bmod n$
- Podpis je pravilen, če je $m' = m$

RSA: Primer

Kako se skupina podpiše?

- **Prilagodljivost** (angl. *flexibility*)
- **Odgovornost** (angl. *accountability*)

Skupina:

$$G = P_1, P_2, \ldots, P_L$$
$$S \subseteq G$$

Skupinski podpisi (angl. *group signatures*)

- Anonimen podpis v imenu skupine
- Ni prilagodljivosti
- Delna odgovornost (vodja skupine)
- Primer:

Mejni podpisi (angl. *threshold signatures*)

- t-od-n shema
- Zmerna prilagodljivost
- Ni odgovornosti
- Primer:

Naivna ideja

- Želimo si prilagodljivost in odgovornost
- Vsak član S podpiše $(M, S) \to \sigma_i$
- Kot na papirju
- Primer:

Naivna ideja

- Želimo si prilagodljivost in odgovornost
- Vsak član S podpiše $(M, S) \to \sigma_i$
- Kot na papirju
- Primer:

Težava?

$\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8, \sigma_9, \sigma_{10}, \sigma_{11}, \sigma_{12}, \sigma_{13}, \sigma_{14}, \sigma_{15}, \ldots$

Skupni podpisi (angl. *multisignatures*)

- Skupina vrne samo en podpis
- Prilagodljivost in odgovornost
- Naivna ideja + učinkovitost
- Primer:

Schnorrov podpis

Generiranje ključa

-

Podpisovanje

-

Verifikacija

-

Varnost